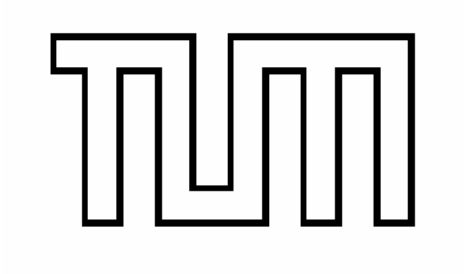


Technische Universität München
Fakultät für Informatik
Diplomarbeit

Klassifikation von Informationsquellen der Computerforensik bei Windows

Daniel Schaller

Aufgabensteller:	**Prof. Dr. H.-G. Hegering**
Betreuer:	**Dr. Helmut Reiser**
	Andreas Völkl
Abgabedatum:	**16.02.2004**

Ich versichere, dass ich diese Diplomarbeit selbständig verfasst und nur die angegebenen Quellen und Hilfsmittel verwendet habe.

_____

Datum Unterschrift

Zusammenfassung

Aufgrund der Durchdringung vieler Lebensbereiche durch die Informationstechnik sind die Anforderungen an die Administration aber auch die Aufklärung missbräuchlicher Verwendung von EDV-Systemen stark angestiegen. Ein Teil der hier zu lösenden Aufgaben sind der Computerforensik übertragen, die festzustellen versucht, wer was, wie und wann auf einem Computersystem durchgeführt hat.

Um derartige Aufgaben zukünftig systematischer durchführen zu können, wird im Rahmen dieser Diplomarbeit eine Klassifikation von Informationsquellen der Computerforensik für das Betriebssystem Windows erstellt. Dazu werden relevante Vorgänge des Betriebssystems für die Analyse bestimmt, von ihnen erzeugte Quellen aufgespürt und diese nach Kriterien bewertet. Für die Bewertung werden geeignete Kriterien festgelegt und für die Darstellung der Untersuchungsergebnisse Entscheidungen für ein benutzerfreundliches Format getroffen. Um für die Lösung aller Teilschritte eigene Folgerungen und Ergebnisse zu erreichen, werden auch Versuche an einem konkreten System durchgeführt.

Aufgezeigt werden auch erweiterte Anwendungen, die sich aus der Klassifikation und den Erkenntnissen ihrer Erstellung ableiten lassen. Darüber hinaus wird auch auf die sichtbar gewordenen Grenzen bei der Bearbeitung des Themas eingegangen und ein Ausblick auf die Überwindung dieser Grenzen und die absehbare Entstehung neuer Herausforderungen gegeben.

A Inhaltsverzeichnis

B Abbildungsverzeichnis

1 Einführung

Die fortlaufende Computerisierung unserer Gesellschaft hat leider nicht nur gute Entwicklungen mit sich gebracht. So entstanden durch die zunehmende Verbreitung von Computern und des Internets leider auch ganz neue Arten für Straftaten und herkömmliche Straftaten werden nun oft Mithilfe des Computers oder des Internets begangen. Die mit den neuen Kommunikationstechniken verbundenen Vorteile, wie der schnelle und kostengünstige Datenaustausch, eröffnen auch Straftätern ganz neue Wege. So hat sich z.B. die Kinderpornographie durch die Möglichkeiten des Internets rasant entwickelt. Die Anzahl dieser Delikte ist z.B. in Großbritannien von 1988 bis 2001 um mehr als 1500% gestiegen [Carr04]. Weiterhin spielen auch bei der Aufklärung von vielen Straftaten, die an sich selbst gar nichts mit dem Computer zu tun haben, im Computer befindliche Informationen, wie z.B. Emails oder sonstige Arbeitsdokumente, als Indizien eine entscheidende Rolle. So sind bei den jüngsten großen Gerichtsverfahren z.B. zur Bilanzfälschung der Firmen ENRON, Worldcom, Global Crossing, Tyco u.a. elektronische Dokumente von entscheidender Bedeutung [Iwat02], [Varc03].

Wie man in Abbildung 1 [Bund02] erkennen kann, hat sich die Anzahl der der Computerkriminalität zuzurechnenden Straftaten seit mehreren Jahren gesteigert.

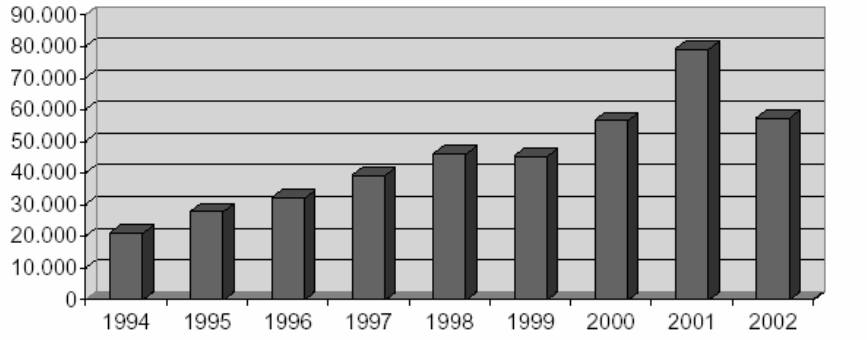


Abbildung 1: Entwicklung der Computerkriminalität in Deutschland

Die abrupte Abnahme im Jahr 2002 im Vergleich zu den Vorjahren entsteht durch eine Veränderung des zugrunde gelegten Statistikmerkmales. Somit „ist ein Vergleich des Summenschlüssels ‚Computerkriminalität' (…) mit dem Vorjahr nur sehr eingeschränkt möglich" [Bund02]. Würde man wie bisher vorgehen, „so kommt man auf einen Anstieg um 23 Prozent." [Heis03].

Die 2002 registrierten 57000 Fälle von Computerkriminalität in Deutschlang haben etwa 85 Millionen Euro Schaden verursacht [Bund02]. Dies sollte jedoch nur die Spitze des Eisberges sein, da hier naturgemäß all die Fälle, die nicht zur Anzeige gebracht werden bzw. unbemerkt geblieben sind, gar nicht berücksichtigt sind. So geht das FBI in Amerika von bis zu 10 Milliarden Dollar pro Jahr aus („$10 billion a year") [Sage00].

Man sieht also, dass es sehr wichtig ist, Taten im Computer nachweisen und aufklären zu können. Denn selbst wenn von den Straftäter oft nicht die hohen Summen als Schadensersatz zurückgefordert werden können, trägt eine hohe Aufklärungsrate bedeutend zur Abschreckung bei. Aufgrund der steigenden Zahl der Fälle sind Hilfsmittel erwünscht, die den Ermittlern ein schnelles und möglichst erfolgreiches Vorgehen ermöglichen.

1.1 Computerforensik

Um das Thema richtig einordnen zu können, soll zunächst auf die Begriffe Forensik und Computerforensik eingegangen werden.

Viele Leute kennen den Begriff der Forensik wahrscheinlich aus irgendeinem Krimi. Von vielen wird darunter die Gerichtsmedizin verstanden, die zur Aufklärung von Vorgängen wie Straftaten und Unfällen nach biologischen oder physikalischen Spuren, z.B. Beweismitteln wie Fingerabdrücken oder Erbsubstanzen, sucht, um Informationen über Personen, Tatzeiten oder den Tathergang zu erhalten.

Das Wort Forensik ist von dem ehemals lateinischen Wort „forensisch“ abgeleitet. In der Brockhaus Enzyklopädie findet sich dazu folgende Information:

> „**forensisch** [lat., eigtl. >zum Forum gehörend<]
> gerichtlich, die Gerichtsverhandlung betreffend,
> im Dienst der Rechtspflege stehend.“ [Broc88]

In der Forensik haben sich bereits frühzeitig Spezialbereiche etabliert, z.B. die forensische Chemie und die forensische Psychologie. Der Aufgabenbereich der Forensik geht weit über die allgemein bekannte Obduktion von Leichen hinaus und liefert in verschiedensten Bereichen gerichtsverwertbare Untersuchungsergebnisse. Diese können z.B. bei der Analyse eines von der Person geschriebenen Textes bis zum Erkennen des Geschlechts und der Muttersprache des Autors gehen [VCAM02]. Aber auch das Nachstellen eines Vorgangs, z.B. zur Rekonstruktion eines Unfallhergangs gehört in den weiten Bereich der Forensik.

Wie in fast allen Lebens- und Arbeitsbereichen werden in vielen Bereichen der Forensik mittlerweile auch Computer verwendet. So werden z.B. Fingerabdrücke schon lange nicht mehr nur von Menschen verglichen und Unfallhergänge nicht mehr ausschließlich in der Realität nachgestellt. Stattdessen existieren hierfür spezielle Computerprogramme, die bei dieser Arbeit unterstützen oder sie gänzlich übernehmen.

Aus diesen Gründen könnte man den Einsatz von Computern bei diesen Aufgaben mit dem Begriff Computerforensik bezeichnen. Die Verwendung von Computern als Hilfsmittel für die Lösung der Aufgaben der Forensik wird jedoch allgemein nicht mit dem Begriff Computerforensik gekennzeichnet. Vielmehr leitet sich der Name des Begriffs Computerforensik daraus ab, dass Vorgänge im Computer aufgeklärt werden müssen. Damit gilt:

Computerforensik ist die Aufklärung von Vorgängen in Computersystemen.

Damit sind die Aufgaben in der Computerforensik mit denen der Gerichtsmedizin insofern vergleichbar, als in beiden Bereichen nach Informationsquellen gesucht wird, die Aufschluss über Handlungen geben. Im Gegensatz zu anderen Bereichen der Forensik wie der Gerichtsmedizin oder Gerichtspsychologie wird in der Computerforensik jedoch nicht nach biologischen Spuren oder Persönlichkeitsmerkmalen, sondern nach Informationen im Computer gesucht. Die folgenden grundlegenden Fragen stellen sich jedoch auch im Bereich der Computerforensik:

- Wer hat etwas getan?
- Wann wurde etwas getan?
- Was wurde wie getan?
- Warum wurde etwas getan?

Auf die zuletzt genannte Frage nach dem Motiv kann die Computerforensik allerdings keine Antwort liefern. Die Beantwortung von Fragen nach den Beweggründen menschlichen Verhaltens bleibt dagegen der forensischen Psychologie vorbehalten.

Wie in den anderen Bereichen der Forensik, insbesondere in der Gerichtsmedizin, gibt es in der Computerforensik das Ziel, Beweise für die Verwendung vor Gericht zu gewinnen. Jedoch gibt es in der Computerforensik häufiger Aufgaben, die nicht gleich mit einem Gerichtsverfahren zu tun haben. In vielen Fällen will man nur Informationen über Vorgänge im verwendeten EDV-System gewinnen. Da ein absolut sicheres Computersystem leider eine Wunschvorstellung ist, spielt es in der Praxis eine wichtige Rolle, die Ausnutzung eines vorliegenden Sicherheitsproblems möglichst schnell zu erkennen, bevor immer größerer Schaden entsteht. Außerdem gehen einem erfolgreichen Angriff zunächst meist nicht erfolgreiche Versuche voraus. Erkennt man diese rechtzeitig, lässt sich möglicherweise der ansonsten irgendwann eintretende Erfolg des Hackers durch gezielte Gegenmaßnahmen vermeiden. Auch ohne die Gefahr einer missbräuchlichen Verwendung erfordern das Erreichen und der Erhalt einer funktionsfähigen komplexeren EDV-Anlage systematische Beobachtungen und Maßnahmen.

In all diesen Fällen sind auch nicht die strengen Maßstäbe für die Sicherung von gerichtsverwertbaren Beweisen anzulegen. Unabhängig davon bleibt aber zu berücksichtigen, dass die jeweiligen datenschutzrechtlichen Bestimmungen und sonstige Regelungen, z.B. Betriebsvereinbarungen, einzuhalten sind.

Zu beachten ist, dass es für die Aufklärung einer missbräuchlichen Verwendung von Computern meist nicht reicht, nur das Computersystem zu untersuchen, da damit meist nur ein Benutzerkonto oder ein Rechner identifizierbar sind. Für die vollständige Aufklärung ist meist noch der Rückschluss auf die reale Person des Verursachers nötig. In solchen Fällen muss die Computerforensik mit anderen Bereichen der Forensik oder den Ermittlungsbehörden zusammenarbeiten, um diese insgesamt zu lösen.

Nach dem allgemeinen Überblick wird die Aufgabenstellung umrissen und gezeigt, in welchem Teilbereich der Computerforensik diese Arbeit anzusiedeln ist.

1.2 Aufgabenstellung

Wie im vorausgegangenen Kapitel dargestellt ist, versucht die Computerforensik festzustellen, welche Benutzer zu welcher Zeit und auf welche Art Handlungen an einem Computersystem durchgeführt haben.

Um für Aufgabenstellungen dieser Art ein systematisches Hilfsmittel zur Verfügung stellen zu können, wird für das Betriebssystem Windows eine Klassifikation entsprechender Informationsquellen erstellt. Informationsquellen in diesem Sinne, die im Folgenden nur kurz Quellen genannt werden, sind alle Daten, die in einem Computersystem Rückschlüsse auf Handlungen von Benutzern zulassen.

Im Rahmen der Diplomarbeit wird dazu festgestellt, welche Vorgänge auf dem System Quellen hinterlassen. Für diese Quellen wird eine Klassifikation erstellt, also eine Bewertung nach Kriterien durchgeführt. Die dafür relevanten Kriterien müssen im Laufe der Diplomarbeit für die Bewertung der Quellen festgelegt werden.

Die Arbeit kann von Computerforensikern oder Administratoren eingesetzt werden, um ihnen bei forensischen Untersuchungen zu helfen. Sie ermöglicht ihnen eine einfachere, systematischere und ergiebigere bzw. überhaupt erfolgreiche Suche nach Quellen. Deren Bewertung nach wichtigen Kriterien kann helfen, die im konkreten Fall relevanten Quellen herauszufiltern, deren Interpretation zu erleichtern und damit Zeit und Aufwand zu sparen. Um die Verwendung der Klassifikation zu erleichtern, wird diese in der Darstellung möglichst übersichtlich gestaltet.

Darüber hinaus wird überprüft, ob die bei der Erstellung der Klassifikation gewonnenen Ergebnisse auch für erweiterte Anwendungen, wie z.B. das Erkennen von Fälschungsversuchen, genutzt werden können. Sofern entsprechende Möglichkeiten bestehen, wird die Methodik dafür aufgezeigt, damit die Klassifikation auch in diesem Sinne eingesetzt werden kann.

Zur Präzisierung der Aufgabenstellung sind Einschränkungen und Abgrenzungen erforderlich, weil deren Umfang sehr stark von diversen Rahmenbedingungen abhängig ist.

Verschiedenste Anwendungsprogramme erhöhen den Umfang und die Art der Vorgänge und hinterlassenen Quellen erheblich und benötigen unter Umständen eine andere Herangehensweise. Außerdem existieren u. a. Sicherheits- oder Spionageprogramme (z.B. keylogger), die auch für die Standardvorgänge des Betriebssystems zusätzliche Quellen aufzeichnen. Diese Arten von Zusatzprogrammen bleiben von den Untersuchungen ausgenommen. Untersucht und beschrieben werden also nur Vorgänge und Quellen von Programmen, die zum Lieferumfang von Windows gehören. Um jedoch die vom Grundsystem erzeugten Quellen zu finden, werden jedoch einige zusätzliche Programme genutzt. Diese werden im Kapitel 3 genauer beschrieben. Ihre Anwendung ist beim Einsatz der erstellten Klassifikation nicht mehr notwendig.

Diese Arbeit setzt sich auch nicht mit den rechtlichen Belangen auseinander, da diese so vielfältig sind, dass dafür ein juristischer Experte nötig wäre. Insbesondere bleibt ausgeklammert, ob die ermittelten Quellen vor Gericht verwendbar sind oder die Aufzeichnung von solchen Information möglicherweise gegen Gesetze oder gängige Betriebsvorschriften verstößt. Sie beschränkt sich dagegen auf die rein technische Seite.

1.3 Gliederung

Nachdem in diesem Kapitel bereits in die Thematik eingeführt und die Aufgabenstellung dargestellt ist, folgt abschließend noch eine Begriffserklärung.

Im Kapitel 2 wird beschrieben, welche Anleitungen, Computerprogramme und Dienstleistungen zu computerforensischen Fragestellungen bereits existieren bzw. gegebenenfalls vermisst werden.

Im Kapitel 3 wird das Vorgehen beim Erstellen der Klassifikation dargestellt. Es wird auf die durchgeführten Teilschritte eingegangen und für jeden dieser Schritte das spezifische Vorgehen erläutert. Zu diesen Teilschritten zählen außer dem Festlegen der Vorgänge das Auffinden der zugehörigen Quellen und deren Bewertung nach zuvor festgelegten Kriterien sowie die Wahl des Aufbaus der Klassifikation.

Im Kapitel 4 folgt die eigentliche Klassifikation. Hier finden sich u.a. Quellenblätter, die zu jeder dokumentierten Quelle eine standardisierte Beschreibung enthält, und zugehörige Suchhilfen in Listenform.

Kapitel 5 gibt Hinweise für erweiterte Anwendungen der Klassifikation die über das einfache Nachschlagen hinausgehen.

Das abschließende Kapitel 6 fasst die wichtigsten Ergebnisse zusammen und gibt einen Ausblick auf mögliche Entwicklungen.

Im Anhang werden wichtige Quellen und deren Auswertung beschrieben, wenn die Informationen für die Quellenblätter selbst zu umfangreich sind oder für eine größere Anzahl von ihnen identisch sind.

1.4 Begriffserklärungen

Folgende oft verwendete Begriffe werden im nachfolgend angegebenen Sinne verwendet:

Vorgang: Eine Handlung, die am Computersystem vom Benutzer durchgeführt wird und dabei möglicherweise eine oder mehrere Quellen hinterlässt.

Quelle: Hinterlassene Informationen über Handlungen des Computerbenutzers. Werden von Vorgängen erzeugt. Im Kontext mit der Erzeugung durch das Ausführen von Vorgängen wäre das Wort „Spur“ statt „Quelle“ für die hinterlassene Information in manchen Fällen treffender. Da diese Arbeit jedoch im Kontext der Auswertung steht, ist immer das Wort „Quelle“ verwendet, um Missverständnissen vorzubeugen. Dieselbe Quelle kann möglicherweise von verschiedenen Vorgängen angelegt werden.

Onlineauswertung: Eine forensische Untersuchung, die im laufenden Betrieb des zu untersuchenden Betriebssystems direkt auf diesem stattfindet.

Offlineauswertung: Eine forensische Untersuchung, bei der über ein anderes Betriebssystem eine früher verwendete Festplatte auf Quellen überprüft wird. Somit stehen die Funktionen des Orginalbetriebssystems nicht mehr zur Auswertung zur Verfügung.

Weiterhin werden naturgemäß viele Bezeichnungen für Windowskomponenten im Sinne der Definition von Microsoft verwendet, die dem Leser bekannt sein sollten. Da eine umfassende Darstellung den Rahmen sprengen würde, können diese hier nicht dargestellt werden. Damit nicht vertraute Personen können sich mit den leicht zugänglichen Beschreibungen des Betriebssystems vertraut machen. Dennoch wird auf die wichtigsten Funktionen im Anhang eingegangen. Dabei werden jedoch nicht nur die jeweiligen Begriffe erklärt, sondern auch erweiterte Informationen zur Durchführung einer forensischen Analyse und zur zweckmäßigen Konfiguration des Systems gegeben.

2 State of the Art

Wie in der Einführung bereits dargelegt ist, nimmt der Bedarf an Hilfsmitteln für die schnelle und möglichst erfolgreiche Lösung computerforensischer Aufgaben spürbar zu. Einen Ansatz den Bedarf an möglichst systematisch geordneten Informationen zu decken, stellt die Klassifikation entsprechender Informationsquellen dar.

Die Untersuchung von vorliegenden Veröffentlichungen zu dieser Thematik lässt rasch große Defizite erkennen. Insbesondere werden einfache und systematisch aufgebaute Darstellungen vermisst, die Computerforensikern und Administratoren bei ihren forensischen Untersuchungen eine umfassende Möglichkeit geben, zu Benutzervorgängen am Computer die hinterlassenen Quellen und zu vorgefundenen Quellen deren verursachende Vorgänge mit geringen Aufwand zu finden und auszuwerten.

In den nachfolgenden Kapiteln wird der Stand der zugänglichen Dokumente zur Computerforensik eingehender erörtert. Dabei kann und will die Darstellung nicht das Gesamtgebiet der Computerforensik abdecken, sondern nur die Teilbereiche, die für diese Arbeit von Bedeutung sind. Außerdem bleiben hier Aspekte zur Dokumentation des Betriebssystems Windows ausgeklammert.

2.1 Computerforensische Literatur

Allgemein lässt sich sagen, dass zurzeit sehr viele Entwicklungen auf dem Gebiet der Computerforensik vorangetrieben werden. Dies ist auch daran zu erkennen, dass immer neue nicht technische Artikel veröffentlicht werden, die dieses Thema der breiten Öffentlichkeit näher bringen. So liegt die Zahl der Internetseiten mit den Stichwörtern Computer und Forensik, die über Suchmaschinen zugänglich sind, am Ende deutlich höher als bei Beginn der Arbeit. Beim Aufarbeiten dieser Suchergebnisse muss aber festgestellt werden, dass diese Seiten oft nur kurze allgemeine Informationen zur Computerforensik oder sogar lediglich Werbung für computerforensische Dienstleistungen oder Hilfsprogramme enthalten. Wie zu erwarten ist, sucht man dort aussagekräftige Informationen zur Erstellung einer Klassifikation von Quellen der Computerforensik vergeblich. So finden sich in diesen Artikeln selbst Informationen über einzelne Vorgänge und die von ihnen hinterlassenen Quellen äußerst selten. Sofern ausnahmsweise einzelne Quellen beschrieben sind, gibt es dabei keine oder sehr unterschiedliche Angaben zu diversen Kriterien und keine einheitliche Bewertung.

Nach Ankündigung auf der dafür angelegten Internetseite [Gesc03] erscheint in Kürze der Titel „Computer Forensik - Systemeinbrüche erkennen, ermitteln, aufklären" des Autors Alexander Geschonneck; dies ist das erste deutschsprachige Buch zu dieser Thematik. Die wenigen dazu in englischer Sprache in den letzten Jahren erschienenen Bücher behandeln vielfältige weitere Fragestellungen, die allerdings nach den verfügbaren Rezessionen, Beschreibungen und Inhaltsverzeichnissen weder die geforderte Klassifikation enthalten noch die Erstellung einer solchen behandeln.

2.2 Computerforensische Spezialprogramme

Außer den im Betriebssystem standardmäßig enthaltenen Programmen gibt es zwei Gruppen von Spezialsoftware, die für die forensische Analyse von Belang sind.

Zum einen existieren Programme, die den Forensiker bei seinen im Nachhinein durchgeführten Analyseaufgaben unterstützen. So existieren z.B. das weit verbreitete Produkt Encase [Guid04] vom Hersteller Guidance Software sowie eine Fülle von Programmen [NewT03] vom Forensikunternehmen New Technologies Inc. (NTI). Solche Eigenentwicklungen von Forensikfirmen werden aber nicht immer weitergegeben. Oft benutzen diese die Software nur selbst, um eine Aufklärung von Quellen möglich oder einfacher zu machen und aus den angebotenen Dienstleistungen Gewinn zu erzielen.

Zum anderen gibt es Programme, die im Voraus installiert, die Möglichkeiten der Nachverfolgung durch Aufzeichnung zusätzlicher Quellen erweitern. Man denke hier z.B. an Keylogger, die alle Tastatureingaben am Computer aufzeichnen.

Nähere Untersuchungen zum Stand dieser Entwicklungen sind auch im Hinblick auf die Aufgabenstellung nicht angezeigt.

Darüber hinaus gibt es Programme, die sich zwar nicht direkt für die forensische Analyse eignen, jedoch verwendet werden können, um Einblick in das System und die ablaufenden Vorgänge zu erhalten und so Informationen für die forensische Analyse zu erhalten. Dazu zählen auch Programme, die Änderungen im Dateisystem, z.B. durch das Erstellen von Checksummen, anzeigen und Programme, die es ermöglichen bestimmte Quellen übersichtlich auszulesen.

2.3 Computerforensische Dienstleistungen

Es gibt mehrere Firmen, die sich darauf spezialisiert haben, verschiedenste Dienstleistungen im Bereich der Computerforensik anzubieten. Diese Firmen besitzen durch ihr langjähriges Engagement viel Know-how in ihren Geschäftsbereichen und können im konkreten Fall beauftragt werden, entsprechende Aufträge durchzuführen. Jedoch sind von deren Seite verständlicherweise keine genauen Informationen in Erfahrung zu bringen, da dieses Wissen ja die Grundlage ihres Geschäfts ist. So liefern diese Firmen nur vereinzelte Information auf oberflächlichem Niveau. Meist finden sich auf den Herstellerseiten also einige Artikel, die mit dem vorrangigen Ziel der Werbung Informationen über ihr Tätigkeitsfeld anbieten, jedoch keine konkreten Anleitungen oder Hinweise für eigene forensische Analysen liefern.

Es ist also davon ausgehen, dass Forensikfirmen intern entsprechendes Know-how angesammelt und dokumentiert haben, dieses aber verständlicherweise kommerziell in Form entsprechender Dienstleistungen zum Einsatz bringen und daher nicht veröffentlichen.

3 Vorgehen beim Erstellen der Klassifikation

Das Erstellen der Klassifikation wird in mehreren Teilschritten ausgeführt, die in den folgenden Kapiteln ausführlich beschrieben sind. Dies heißt jedoch nicht, dass die einzelnen Schritte strikt nacheinander abgearbeitet werden; vielmehr werden diese Schritte teilweise parallel und wiederholt bearbeitet, weil nach den ermittelten Ergebnissen vereinzelt eine Anpassung der vorherigen Festlegungen sinnvoll ist.

Zunächst wird überlegt, welche Vorgänge in einem allgemeinen Betriebssystem und speziell bei den aktuellen Windowsversionen existieren, die für eine Rückverfolgung von Interesse sind. Anschließend wird jeder dieser Vorgänge auf hinterlassene Quellen untersucht. Dabei kommt für die praktischen Untersuchungen eine neu installierte Betriebsysteminstallation mit überwiegend Standardeinstellungen zum Einsatz. Für die Bewertung dieser Quellen müssen passende sinnvolle Kriterien festgelegt werden und die gefunden Quellen so untersucht werden, dass auch genug Informationen für eine den Kriterien entsprechende Beurteilung vorliegt. Schließlich müssen die gefundenen Informationen in ein passendes übersichtliches Format gebracht werden.

3.1 Vorbemerkungen

In den nachfolgenden Vorbemerkungen sind Aspekte dargestellt, die in mehr als einem der oben genannten Teilschritte relevant sind.

3.1.1 Informationsbeschaffung

Bei der Informationsbeschaffung spielt die Literaturrecherche eine wesentliche Rolle. So ist eine Untersuchung zu der Frage sinnvoll, welche Informationen zum Thema schon existieren und welche selbst aufzuklären sind. Grundsätzliche Ergebnisse dazu sind im Kapitel „State of the Art“ bereits dargestellt. Zu Letzterem bieten sich dann durch gezielte Experimente mit den zur Verfügung stehenden Betriebsystemen weit reichende Möglichkeiten zur Informationsbeschaffung.

Es existiert eine kaum überschaubare Menge an Literatur zu den neueren Versionen des Betriebsystems Windows, die in Form von Büchern, Internetseiten und in das Betriebsystem integrierten Hilfetexten (Onlinehilfe) vorliegen und die Betriebssystemfunktionen und deren Bedienung erläutern.

Obwohl es damit für die Betriebssystemfunktionen sehr viele Beschreibungen gibt, sind diese für die computerforensische Analyse meist wenig zielführend. So fehlen sowohl zusammenhängende Darstellungen als auch wichtige Teilaspekte für computerforensische Belange. Zum Beispiel werden Informationen vermisst, aus denen direkt hervorgeht, welche Quellen von einem ausgeführten Benutzervorgang hinterlassen werden. Nichtsdestotrotz findet man zu Einzelaspekten durchaus sehr genaue Detailinformationen sowie allgemeine und besondere Hinweise zur Sicherheit und zu den Sicherheitseinstellungen des Systems, die aber zur Lö-

sung computerforensischer Fragestellungen erst noch ergänzt und in den richtigen Zusammenhang gebracht werden müssen. Außerdem sind viele wichtige Teile des Systems nur unvollständig dokumentiert. Dies gilt u. a. für viele intern verwendeten Einstellungen und Dateiformate. (z.B. die Bedeutung aller Standardschlüssel und Werte der Registry). Die Schwachstellen sind damit zu erklären, dass die Betriebssystembeschreibungen hauptsächlich mit der Absicht verfasst sind, den Anwender bei der Bedienung und den Administrator bei der Einrichtung des Systems zu unterstützen, ohne die spezifischen Belange in Sondersituationen zu berücksichtigen. Insbesondere werden forensische Gesichtspunkte vernachlässigt.

Das Betriebssystem Windows ist standardmäßig mit einem großen Umfang von Hilfsprogrammen ausgestattet, von denen sich eine Reihe von Funktionen für die forensische Analyse gebrauchen lassen. Wenn sich keine außergewöhnlichen Aufgaben stellen und eine Lösungsstrategie bekannt ist, bieten die dazu jeweils geeigneten Hilfsprogramme gute Ergebnisse. Allerdings erkennt der weniger geübte Anwender wohl nicht auf Anhieb, dass viele Programme auch für diesen Zweck einsetzbar sind. Dies ist auch dadurch verursacht, dass eine Suche in der Onlinehilfe nach Computerforensik kein einziges Ergebnis liefert und in den Hilfetexten auch sonst keine offensichtlichen Hinweise darauf enthalten sind. Da die erforderlichen Programme also vorhanden aber praktisch nutzlos sind, wenn kein Wissen über ihre Einsatzmöglichkeiten verfügbar ist, besteht das Defizit also auch hier hauptsächlich im Fehlen aussagekräftiger Anleitungen für die Nutzung der Hilfsprogramme für die Lösung computerforensischer Aufgaben.

Da viele Funktionen des untersuchten Betriebssystems aufgrund der häufigen Verwendung des Betriebssystems bzw. dessen Vorgängerversionen dem Autor schon seit langem bekannt sind, können hierfür keine genauen Quellenangaben mehr angegeben werden. Darüber hinaus erfolgt im Rahmen der Arbeit über die relevanten Themen eine systematische Information mit den beiden Büchern zum Windowsbetriebssystem [Bosw01] und [MiPr00]. Als erste Anlaufstelle für Fragen zu der Funktionalität bzw. den Einstellungen des Betriebssystems kann zuerst einmal die Onlinehilfen Verwendung finden. Weiterführende Fragestellungen werden eventuell auf den Internetseiten Technet [Tech04] und MSDN (Microsoft Developer Network) [MSDN04] von Microsoft erklärt. Hier ist die Suche aber gerade aufgrund der Fülle der angebotenen Informationen zu den verschiedensten Fragestellungen erschwert. So werden hier viele Treffer angezeigt, die oft nur entfernt mit den Suchbegriffen zu tun haben.

Die Informationsbeschaffung durch Literaturrecherche und Experimente ist bei den im Folgenden beschriebenen Teilschritten von sehr unterschiedlicher Bedeutung. Auf die Details wird deshalb dort eingegangen.

3.1.2 Detailliertheit und Benennung

Bei der Ausformulierung der Klassifikation stellt sich an vielen Stellen die Frage, wie detailliert die jeweils betroffenen Aspekte der Funktionalität und Bedienung des Betriebssystems zu beschreiben sind. Dabei geht es nicht darum eine generelle Antwort zu finden, sondern in jedem Einzelfall für das Verstehen die notwendige Ausführlichkeit in der Darstellung zu finden ohne die Lesbarkeit durch übermäßigen Umfang zu erschweren.

Das Fällen der hierbei notwendigen Entscheidungen stellt eine schwierige Gratwanderung dar, da zum einen die in der Klassifikation enthaltenen forensischen Informationen nur zusammen mit den jeweiligen Kenntnissen über die betreffenden Windowsfunktionen verwertbar sind und zum anderen der Umfang der grundlegenden Beschreibung des Betriebssystems keinen zu großen Umfang bekommen soll, damit das eigentliche Thema nicht in den Hintergrund gedrängt wird. Damit die Klassifikation für die Zielgruppe möglichst gut nachvollziehbar ist, sind die jeweils tangierten Funktionalitäten des Betriebssystems teilweise beschrieben. Dabei enthält die Klassifikation vorwiegend solche Informationen zum System, die bei dem in der Computerforensik tätigen Personal nicht vorausgesetzt oder von ihm selbst nur schwer nachgeschlagen werden können. Bei der als Teil der Klassifikation erstellten standardisierten Dokumentation der Quellen wird eine Überfrachtung mit Systeminformationen dadurch vermieden, dass umfangreichere Sachverhalte zusammenhängend in den Anhang ausgelagert sind.

Die Benennung von Systemobjekten und -einstellungen orientiert sich stark an den in der untersuchten Windowsversion jeweils verwendeten Namen. Auch wenn dies manchmal wie ein Fehler aussieht, wenn in manchen Fällen die Regeln der Groß- und Kleinschreibung nicht eingehalten sind, sind z.B. Datei- und Verzeichnisnamen immer unverändert übernommen. Soweit es möglich ist, wird auf das langwierige Beschreiben des Starts von Programmen über das Startmenü zugunsten der Angabe des Aufrufnamens mit dem gegebenenfalls erforderlichen Verzeichnispfad verzichtet. Dadurch wird dem Forensiker ein sehr einfacher Aufruf von Programmen direkt über die Eingabeaufforderung oder das Fenster Ausführen ermöglicht.

In der Regel sind Pfadbestandteile, deren Namen nicht vom Systemhersteller festgelegt, sondern für das System oder den jeweiligen Benutzer frei wählbar sind, mit möglichst selbsterklärenden Namen benannt. Wie an dem Beispiel #BENUTZERNAME# ersichtlich, ist dabei das Format so gewählt, dass die Bezeichnung ein- und ausleitend durch „#“ abgetrennt und groß geschrieben ist. Da andernfalls eine zusätzliche Angabe des Standardpfades erforderlich wäre, ist davon abweichend allerdings vereinzelt zugunsten der besseren Lesbarkeit statt einer nahe liegenden aber schwerfälligen Bezeichnung der Standardpfad selbst verwendet, das heißt statt #WINDOWSINSTALLATIONSVERZEICHNIS# steht C:\Windows\ oder statt #VERZEICHNIS DES LOKALEN PROFILES EINES BENUTZER# steht C:\Dokumtente und Einstellungen \#BENUTZERNAME#. Die Gefahr einer Missinterpretation kann hier als ausgesprochen gering angenommen werden, da die Standardpfade in der Praxis sehr häufig zur Anwendung kommen und zumindest dem forensischen Personal geläufig sind.

Leider finden sich für identische Elemente, die in unterschiedlichem Kontext angezeigt werden, mehr oder weniger drastisch abweichende Benennungen, die wohl zum Teil auf Inkonsequenz bei der Übersetzung zurückzuführen sind. Bei nur geringfügig voneinander abweichenden Bezeichnungen wird nur die aussagekräftigste in der Klassifikation verwendet. Sofern für die Benutzer sonst Verwechselungen möglich wären, sind Angaben über die Zuordnung der Bezeichnungen gegeben. So werden z.B. im Menü für die Aktivierung und für die Anzeige der Protokollierung unterschiedlichste Bezeichnungen für die verschiedenen Kategorien verwendet. Eine Tabelle für die Zuordnungen der Bezeichnungen ist im Anhang in Kapitel 7.1.2.6 eingefügt.

3.1.3 Informationsmanagement

Um die Notizen zu den folgenden Untersuchungsergebnissen nicht nur auf Papier führen zu müssen, bietet es sich bereits von Beginn ab an, ein EDV-System einzusetzen, da sonst bei den vielen Einzelaspekten schnell die Übersicht verloren geht und ein hoher Zeitaufwand für das andernfalls am Ende anfallende Eintippen bleibt, den man gerne unterschätzt. Im vorliegenden Fall ist es geschickt, für das Speichern der Daten der zu erstellenden Klassifikation, als Zwischenformat eine Datenbank zu wählen. Damit bleibt außerdem bis zuletzt die Möglichkeit eine andere Formatierung der Quellenblätter zu wählen, neue Kriterien hinzuzufügen oder deren Reihenfolge zu ändern. Wenn die Daten gleich in ein Textverarbeitungsprogramm eingetragen würden, wären spätere Änderungen nur mit wesentlich größerem Aufwand durchzuführen. Erst nach dem vollständigen Erarbeiten der Kriterien und ihrer Bewertungen werden diese mit der Serienbrieffunktion des Textverarbeitungssystems mit der nötigen Formatierung versehen und in das Enddokument eingefügt.

3.2 Vorgänge festlegen

Ziel für die Erstellung der Klassifikation ist es zuerst einmal, alle wichtigen Vorgänge aufzuspüren, die es in den zu untersuchenden Windowssystemen gibt. Denn bevor einträgliche Untersuchungen stattfinden können, muss erst einmal klar sein, was zu untersuchen ist. Um systematischer vorgehen zu können und mehr als nur die bekannten, nahe liegenden Vorgänge aufzulisten und eventuell wichtige andere zu übersehen, werden zusätzliche Überlegungen angestellt.

So wird zuerst einmal ein abstraktes Betriebssystem betrachtet. Hierfür wird das Modell aus der Vorlesung Betriebssysteme [Baum02] von Prof. Dr. U. Baumgarten an der TU München verwendet (siehe Abbildung 2 aus [Baum02a], Seite 16) und betrachtet, aus welchen Komponenten dieses aufgebaut ist.

Dann wird überprüft, ob diese auch im Fall der untersuchten Windowsversionen vorhanden sind. Dafür kommen für einen Überblick die beiden Internetartikel [Gtls02] und [Hart01] zum Einsatz. Allerdings spielen für die forensische Auswertung Scheduler und Dispatcher, Interrupt-System und die Speicherverwaltung keine oder nur eine sehr untergeordnete Rolle. Bei diesen Komponenten ist ein Rückschluss auf Benutzervorgänge nur bedingt möglich und es ist sehr fraglich, ob damit relevante Beiträge zu Aufklärung gemacht werden könnten.

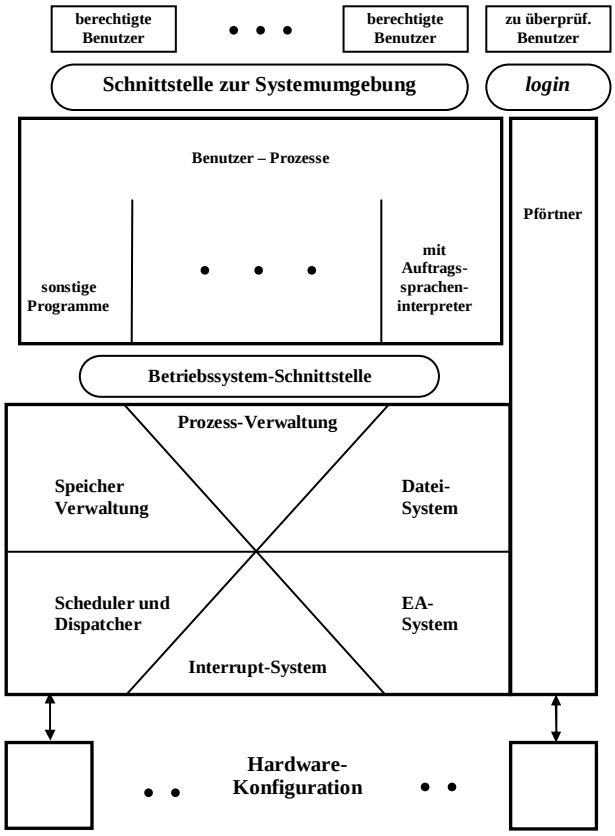


Abbildung 2: Abstraktes Betriebssystemmodel

Insofern werden als relevante Kategorien folgende isoliert:

- Benutzerverwaltung lokal
- Benutzerverwaltung Active Directory
- Dateisystem
- Netzwerk
- Prozessverwaltung
- Systemdienste

Dabei wird die Ein-/Ausgabe zu Netzwerk umbenannt, da diese Bezeichnung die relevanten Aspekte besser repräsentiert. Während unter Systemdienste verschiedene grundlegende Vorgänge zusammengefasst sind, die zu keiner anderen Kategorie passen, ist es aufgrund des speziellen Aufbaus von Windows sinnvoll, zusätzlich zur lokalen Benutzerverwaltung noch das Active Directory als eigenständige Kategorie aufzunehmen. Dieses bietet im Gegensatz zur lokalen Benutzerverwaltung u. a. netzwerkweite Benutzerkonten.

Für die so gefundenen Teilbereiche kann dann in Dokumentationen nachgelesen und direkt am Betriebssystem untersucht werden, welche dazugehörigen Vorgänge von einem Benutzer ausgeführt werden können. Dabei sind allerdings nur die Vorgänge dokumentiert, die von allgemeinem forensischem Interesse sind.

Bei der Festlegung und Benennung der Vorgänge ist außerdem sinnvollerweise die Anzahl und Eigenschaft der hinterlassenen Quellen zu berücksichtigen. So ist es nicht selbstverständlich, die in den Windowsmenüs angebotenen Funktionen als Vorgänge zu übernehmen, sondern diejenigen mit übereinstimmenden Quellen zu einem Vorgang zusammenzufassen. So sind z.B. die Funktionen „Registry Wert anlegen“, „Registry Schlüssel anlegen“, „Registry Wert ändern“, „Registry Schlüssel ändern“ und weitere Registryänderungen zum Vorgang „Registryänderungen durchführen“ zusammengefasst.

Gerade bei der Ereignisprotokollierung von Windows wird die Ausführung von Funktionen protokolliert, die viel feingranularerer als die verwendeten Vorgänge sind und dort als Ereignisse bezeichnet werden. Nun stellt sich dem Leser vielleicht die berechtigte Frage, warum nicht gleich diese Ereignisse als Vorgänge übernommen werden.

Die Antwort ist, dass dies nicht sehr viel Sinn machen würde, da den Forensiker ja Benutzerhandlungen interessieren. Die Ereignisse der Protokollierung sind jedoch zumeist Funktionen im System, die vom Benutzer nur indirekt durch Anweisen eines Betriebssystembefehls, das heißt durch Auslösen eines Vorgangs, ausgeführt werden. Dabei erzeugen die verwendeten Vorgänge dort oft gleich mehrere Ereignisse sowie verschiedene Vorgänge teilweise unter anderem dieselben Ereignisse.

Die Übernahme der Ereignisse als Vorgänge würde die entstehende Problematik der Zuordnung von Quellen zu Vorgängen zwar wesentlich erleichtern. Ein Vorgang würde dann genau einen Ereigniseintrag als Quelle erzeugen und den einfachen Schluss von jedem Eintrag auf den zugehörigen Vorgang ermöglichen.

So könnte man dann zwar abstrakt nachvollziehen, was im System passiert ist; die eigentliche Benutzerhandlung bliebe aber unbekannt.

Besonders unangenehm fällt dieser Umstand bei den Vorgängen im Dateisystem aus. Hier werden die Operationen nicht auf der Ebene von kopieren, verschieben usw. protokolliert, sondern es werden die dazu nötigen einzelnen kleinen Dateisystem-Operationen protokolliert. Siehe dazu auch im Anhang das Kapitel 7.1.2.8 Kategorie Objektzugriff.

So erstellt z.B. das Kopieren einer Datei in jeweils vom Sicherheitsprotokoll überwachten Verzeichnissen zirka 20 Einträge. Diese Einzeloperationen als Vorgänge zu betrachten, wäre also nicht sinnvoll.

Eine Liste aller dokumentierten untersuchten Vorgänge findet sich im Kapitel 4.2 „Verzeichnis der Vorgänge“ und wird hier nicht zusätzlich abgedruckt.

Bereits die Festlegung von einzelnen Benutzervorgängen ermöglicht deren Untersuchung, wie sie im nächsten Kapitel dargestellt ist.

3.3 Quellen für Vorgänge finden

Für das Finden der Quellen müssen Überlegungen für ein passendes Vorgehen angestellt werden, damit keine wichtigen Quellen übersehen werden. Diese werden im nachfolgenden schrittweise vorgestellt.

3.3.1 Literaturrecherche

Um die Quellen zu finden, die eine Aufklärung von Vorgängen ermöglichen, kommt zuerst einmal die Literaturrecherche in Betracht. Während weder komplette Sammlungen von Quellen noch Informationen über alle Quellen verfügbar sind, existieren für einzelne Vorgänge insbesondere im Internet vereinzelte Seiten mit entsprechenden Informationen.

Allerdings muss man hierbei etwas über den Bereich der Forensik hinausblicken, um diese Artikel zu finden und deren Relevanz zu erkennen. So finden sich Hinweise z.B. in Abhandlungen zum Datenschutz. In diesen wird des Öfteren kritisiert, dass bestimmte Funktionen des Betriebsystems Informationen nicht sofort wieder löschen oder sonstige Aufzeichnungen hinterlassen. Was allerdings aus der Sicht des Datenschützers ein großer Makel ist, ist für den Forensiker dagegen meist eine willkommene Quelle.

Weitere Informationen finden sich in Beschreibungen des Betriebsystems. Aber diese sind wiederum natürlich nicht direkt als Anleitung zur forensischen Analyse gedacht, sondern müssen durch entsprechende Interpretationen als Hilfsmittel zum Aufspüren von Quellen genutzt werden.

Wenn z.B. in einem Hilfetext steht, dass die zuletzt verwendeten Internetseiten als Gedächtnisstütze für die bedienende Person gespeichert werden, ist das eine nützliche Information, auch wenn der Begriff Forensik oder ähnliche Stichworte auf diesen Seiten nirgendwo vorkommen. Insofern gestaltet sich aber eine automatische Suche z.B. über Internetsuchmaschi-

nen nach solchen Informationen als schwierig, da man nicht einfach die Suchbegriffe Forensik, Quelle, Spur, entsprechende Abwandlungen dieser Worte oder ihre entsprechenden englische Äquivalente verwenden kann.

Vielmehr muss bei der Suche mit Begriffen gearbeitet werden, die im Kontext mit der üblichen Anwendung und Administration des Systems verwendet werden oder in sonstigen spezifischen Zusammenhang mit der Anwendung von EDV-Systemen (Datensicherheit, Datenschutz, etc) stehen. Dadurch erhält man wesentlich mehr Suchergebnisse, die aber dann manuell gefiltert werden müssen, was meist zumindest das kurze Überfliegen des Artikels auf entsprechende Relevanz zur forensischen Fragestellung erfordert.

3.3.2 Potentielle Quellen

Um aber nicht nur die offensichtlichen bzw. schon beschriebenen Quellen zu klassifizieren, sondern insbesondere auch auf bisher unbekannte Quellen zu stoßen, ist zusätzliche eine andere Vorgehensweise erforderlich. Alle potentiellen Quellen müssen schließlich irgendwo aufgezeichnet werden, damit sie später vorhanden sind und ausgewertet werden können. Bei einer Untersuchung der Vorgänge lassen sich durch einen Vergleich der Zustände vor und nach der Durchführung alle Änderungen feststellen. Somit lassen sich prinzipiell wirklich alle Veränderungen finden, die überhaupt Hinweise auf Quellen zur Aufklärung von Vorgängen geben können.

Im Falle eines Standardcomputersystems beschränkt sich der Aufzeichnungsort auf den Arbeitsspeicher und die Festplatte. Während der Arbeitsspeicher seinen Inhalt spätestens beim Herunterfahren des Systems vollständig verliert, können Informationen auf der Festplatte theoretisch beliebig lange vorhanden bleiben. Hierbei ist es aus mehreren Gründen angebracht, den Arbeitsspeicher von der Untersuchung ausnehmen. Der Arbeitsspeicher kommt aufgrund der Flüchtigkeit der Daten nur für die Onlineauswertung in Betracht. Da für die Onlineauswertung genügend Werkzeuge zur Verfügung stehen, ist die Ermittlung zusätzlicher Quellen nicht von großer Bedeutung. Außerdem würde die Einbeziehung des Speichers sich als sehr schwierig gestalten, da aufgrund des Speicherschutzes normalerweise gar nicht auf die betriebsysteminternen Speicherbereiche zugegriffen werden kann. Kritisch wäre auch die Erkennung der relevanten Speicherbereiche, da ein eingesetztes Überwachungsprogramm zeitgleich unweigerlich ebenfalls den Inhalt des Arbeitsspeichers verändern würde.

Das heißt aber nicht, dass in den Quellenbeschreibungen keine Quellen enthalten sind, die im Arbeitsspeicher abgelegt sind, sondern nur, dass er bei den Versuchen nicht überwacht wird. Sofern spezielle Programme, die Teile des Arbeitsspeichers auslesen und darstellen, existieren, sind die entsprechenden Quellen natürlich beschrieben.

3.3.3 Versuchsabläufe

Für eine Untersuchung der auf der Festplatte festgehaltenen Quellen ist jegliche schreibende Festplattenaktivität auf der betroffenen Betriebssystempartition aufzuzeichnen. Zu den schreibenden Festplattenaktivitäten gehören nicht nur das Anlegen neuer oder das Verändern schon bestehender Dateien, sondern auch die durch Lesen von Dateien ausgelöste Veränderung der Metadaten des Dateisystems wie der Dateizugriffszeiten.

Für die Überwachung der Veränderungen auf der Festplatte wäre eine komplette Sicherung der Festplattenpartition mit anschließendem bitweisem Vergleich aller Dateien, wie im nebenstehenden Versuchsablauf 1 dargestellt, eine theoretische Möglichkeit. Allerdings würde hierfür insgesamt der doppelte Speicherplatz benötigt. Vor allem aber erfordert eine vollständige Sicherung der Daten und ein anschließender kompletter bitweiser Vergleich nach jedem Vorgang sehr viel Zeit.

Versuchsablauf 1
(angedacht, nicht verwendet)

1. Komplette verwendete Festplattenpartition sichern
2. Vorgang durchführen
3. Aktuelle Daten mit der Sicherung bitweise vergleichen und Änderungen protokollieren
4. Protokoll auswerten
5. Wenn das Protokoll noch nicht aussagekräftig ist, Versuchsablauf mit variiertem Vorgang ab Punkt 1 wiederholen

Das bedeutet nicht nur einen hohen Zeitaufwand für die untersuchende Person, sondern auch eine lange Zeitspanne für die Sicherung. Damit fallen in den Zeitraum der Sicherung noch ganz andere periodische Prozesse, die teilweise auch Schreibvorgänge auslösen. Dementsprechend ist nicht mehr einfach rekonstruierbar, ob die Daten vom untersuchten Vorgang oder von sonstigen Systemabläufen stammen. Dies ist nicht nur ein theoretisches Problem, sondern stellt wegen der hohen Anzahl von anderen laufenden Systemvorgängen ein praktisches Hindernis dar. Dies stellt auch in den anderen Versuchsabläufen ein Problem dar, das sich aber durch eine Verkürzung der erforderlichen protokollieren Zeitspanne minimieren lässt. Über das Beenden derartiger Prozesse lässt sich das Problem nicht geeignet lösen, da zum einen um unverzichtbare Systemprozesse betroffen sind und zum anderen die zu untersuchende Systemkonfiguration geändert würde. Es könnten sonst wichtige Quellen übersehen werden, wenn Systembestandteile, die direkt oder indirekt an der Erstellung von Quellen beteiligt sind, beendet würden.

Also bleibt als Ausweg nur das Verkürzen der Zeit, die für die Aufzeichnung des Zustandes des Dateisystems nötig ist. Schon nach den ersten Überlegungen ergibt sich der Gedanke, einen Vergleich der entsprechenden Zustände vor und nach dem Durchführen des untersuchten Vorgangs über Checksummen wie CRC32 oder ähnlichem zu realisieren.

Für das Erstellen und Vergleichen der Checksummen eignen sich z.B. die beiden Programmen afick (Another File Integrity Checker) [Gerb03] und Beyond Compare [Scoo03], da diese frei (GNU) bzw. als Shareware verfügbar sind, während der prominente Vertreter Tripwire für Windows im Gegensatz zur Linuxversion nur kommerziell vertrieben wird.

Für die Dateien mit unterschiedlichen Checksummen bedarf es nun einer genaueren Untersuchung, die über ein Sichern der Dateien, anschließender nochmaliger Versuchsdurchführung und bitweisem Vergleich der beiden Dateiversionen, durchgeführt wird. Der große Unterschied liegt nun aber darin, dass nur noch die betroffenen Dateien in die Sicherung und den Vergleich einbezogen werden müssen, was die anfallende Speichergrößen und damit die Untersuchungszeit erheblich reduziert. Für den hier erforderlichen bitweisen Vergleich eignet sich das Programm Beyond Compare ebenso. Falls es sich um eine Registrydatei handelt, ist das Programm ART (Advanced Registry Tracer) [Elco03] geeigneter, das ebenso eine Sicherung der Registry mit der aktuellen Version durchführen kann, jedoch die Änderungen der Registry übersichtlicher darstellt.

Versuchsablauf 2
(angetestet, letztendlich nicht verwendet)

1. Für komplette Festplattenpartition Checksummen berechnen
2. Vorgang durchführen
3. Checksummen neu berechnen und mit alten vergleichen; damit betroffene Dateien identifizieren

Nachdem die Dateien identifiziert sind:

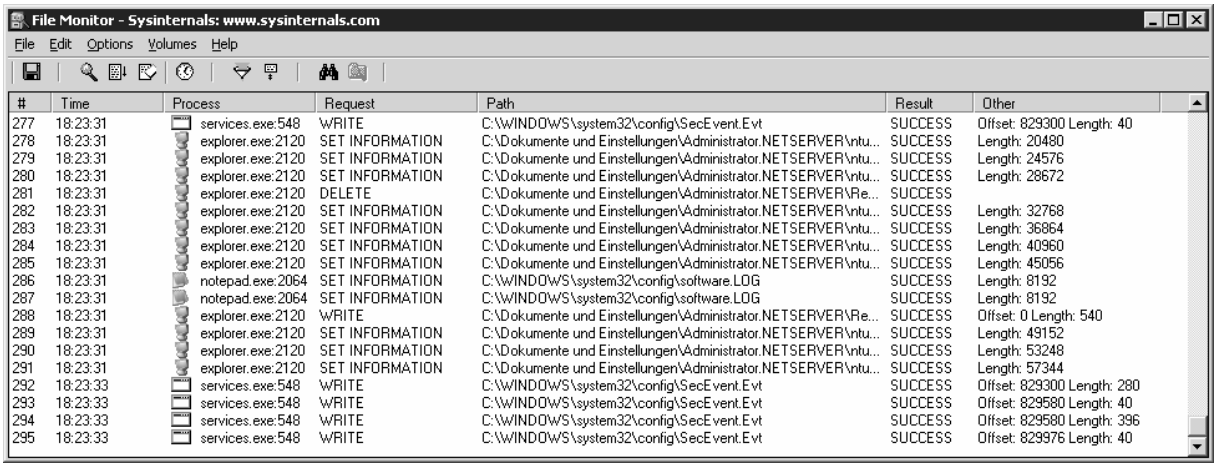
4. Dateien sichern
5. Vorgang durchführen
6. Bit- oder Zeichenweisen Vergleich durchführen (BeyondCompare für Dateien / ART für Registrydateien) und Ergebnis protokollieren
7. Protokoll auswerten
8. Wenn das Protokoll noch nicht aussagekräftig ist Versuchsablauf mit variiertem Vorgang bei Punkt 4 fortsetzen

Nach den anfänglichen Versuchen mit den Checksummen stellte sich heraus, dass auch der Versuchsablauf 2 zu lange dauert, um diesen auf alle relevanten Vorgänge anzuwenden. Immerhin benötigt das Berechnen solcher Codes auf dem verwendeten System für alle Dateien der Betriebssystempartition zirka 7 Minuten. Diese Zeit müsste man jetzt noch doppelt nehmen, um zusätzlich auch die Vergleichswerte zu erhalten. Zwar könnte man diese Zeiten mit schnelleren CPU bzw. Festplatten senken. Da diese Versuche je Vorgang mindestens einmal, mitunter aber auch öfter wiederholt werden müssen, um die Dateien, die nur von zufällig in diesen Zeitabschnitt gefallenen periodischen Prozessen erzeugt werden, erkennen zu können, wäre auch eine Verbesserung der Leistung der Komponenten um den Faktor 10 noch ein sehr mühsames Arbeiten.

Außerdem gibt es Probleme bei Dateien die gerade vom Betriebsystem in Verwendung sind. Deren Inhalt kann zumindest mit den verwendeten Tools nicht gelesen werden, und somit kann für diese Dateien auch keine Checksumme erzeugt werden. Hier besteht die Gefahr, dass Dateien mit Veränderungen nicht erkannt werden, weil die Checksummenprogramme hierauf nicht hinweisen. Auch an den für diese Dateien vergebenen Checksummen lässt sich dies mitunter nicht direkt erkennen. So vergibt z.B. afick für Dateien, bei denen die Checksumme nicht berechnet werden kann, nicht etwa die nahe liegende 0, sondern eine auf den ersten Blick vom verwendeten Format her gültige Checksumme (1B2M2Y8AsgTpgAmY7PhCfg) die offensichtlich dem Initialisierungswert entspricht. Aber gerade die dauerhaft vom System verwendeten Dateien wie die Registrydateien oder den Ereignisprotokolldateien enthalten wichtige Quellen.

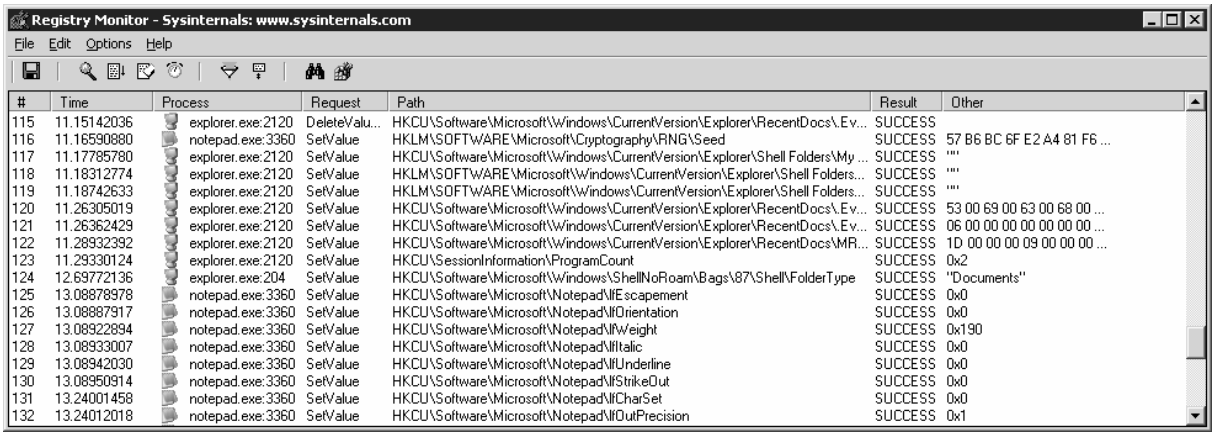
Eine weitere Verkürzung der benötigten Aufzeichnungszeit ließe sich durch Einschränkung der Aufzeichnung auf die Änderungen der Zeitstempel der Dateien erreichen. Diese wäre aber zuverlässig nur möglich, wenn die Aufzeichnung der Zeitstempel vom Betriebssystem sichergestellt wäre, was für Systemdateien nicht immer gilt. Teilweise werden hier wichtige Dateien, wie z.B. die Dateien der Ereignisprotokollierung, ständig für Lese- oder Schreibvorgänge offen gehalten. Somit werden diese Vorgänge nicht abgeschlossenen und es erfolgt keine Anpassung der Zeitstempel während des normalen Betriebs. Eine genauere Untersuchung eines derartigen Versuchsablaufs wird nicht durchgeführt, da eine wesentlich effektivere Art zur Verfügung steht, die im Folgenden dargestellt wird.

Zur Durchführung des Versuchsablaufes 3 stehen zwei sehr gut geeignete Programme, File Monitor (Filemon.exe) [RuCo03] und Registry Monitor (Regmon.exe) [RuCo03a] von Sysinternals zur Verfügung. Mit diesen ist es möglich, oben beschriebene Problematiken elegant zu umgehen, da keine Zeit für die Sicherung oder Berechnung gebraucht wird. Sie zeigen direkt im laufenden Betrieb die Dateien bzw. Registryäste an, auf die zugegriffen bzw. geschrieben wird. Abbildung 3 und Abbildung 4 zeigen die Benutzeroberfläche der beiden Programme mit Ausschnitten der protokollierten Daten.



#	Time	Process	Request	Path	Result	Other
277	18:23:31	services.exe:548	WRITE	C:\WINDOWS\system32\config\SecEvent.Evt	SUCCESS	Offset: 829300 Length: 40
278	18:23:31	explorer.exe:2120	SET INFORMATION	C:\Dokumente und Einstellungen\Administrator.NETSERVER\ntu...	SUCCESS	Length: 20480
279	18:23:31	explorer.exe:2120	SET INFORMATION	C:\Dokumente und Einstellungen\Administrator.NETSERVER\ntu...	SUCCESS	Length: 24576
280	18:23:31	explorer.exe:2120	SET INFORMATION	C:\Dokumente und Einstellungen\Administrator.NETSERVER\ntu...	SUCCESS	Length: 28672
281	18:23:31	explorer.exe:2120	DELETE	C:\Dokumente und Einstellungen\Administrator.NETSERVER\Re...	SUCCESS	
282	18:23:31	explorer.exe:2120	SET INFORMATION	C:\Dokumente und Einstellungen\Administrator.NETSERVER\ntu...	SUCCESS	Length: 32768
283	18:23:31	explorer.exe:2120	SET INFORMATION	C:\Dokumente und Einstellungen\Administrator.NETSERVER\ntu...	SUCCESS	Length: 36864
284	18:23:31	explorer.exe:2120	SET INFORMATION	C:\Dokumente und Einstellungen\Administrator.NETSERVER\ntu...	SUCCESS	Length: 40960
285	18:23:31	explorer.exe:2120	SET INFORMATION	C:\Dokumente und Einstellungen\Administrator.NETSERVER\ntu...	SUCCESS	Length: 45056
286	18:23:31	notepad.exe:2064	SET INFORMATION	C:\WINDOWS\system32\config\software.LOG	SUCCESS	Length: 8192
287	18:23:31	notepad.exe:2064	SET INFORMATION	C:\WINDOWS\system32\config\software.LOG	SUCCESS	Length: 8192
288	18:23:31	explorer.exe:2120	WRITE	C:\Dokumente und Einstellungen\Administrator.NETSERVER\Re...	SUCCESS	Offset: 0 Length: 540
289	18:23:31	explorer.exe:2120	SET INFORMATION	C:\Dokumente und Einstellungen\Administrator.NETSERVER\ntu...	SUCCESS	Length: 49152
290	18:23:31	explorer.exe:2120	SET INFORMATION	C:\Dokumente und Einstellungen\Administrator.NETSERVER\ntu...	SUCCESS	Length: 53248
291	18:23:31	explorer.exe:2120	SET INFORMATION	C:\Dokumente und Einstellungen\Administrator.NETSERVER\ntu...	SUCCESS	Length: 57344
292	18:23:33	services.exe:548	WRITE	C:\WINDOWS\system32\config\SecEvent.Evt	SUCCESS	Offset: 829300 Length: 280
293	18:23:33	services.exe:548	WRITE	C:\WINDOWS\system32\config\SecEvent.Evt	SUCCESS	Offset: 829580 Length: 40
294	18:23:33	services.exe:548	WRITE	C:\WINDOWS\system32\config\SecEvent.Evt	SUCCESS	Offset: 829580 Length: 396
295	18:23:33	services.exe:548	WRITE	C:\WINDOWS\system32\config\SecEvent.Evt	SUCCESS	Offset: 829976 Length: 40

Abbildung 3: File Monitor



#	Time	Process	Request	Path	Result	Other
115	11.15142036	explorer.exe:2120	DeleteValu...	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.Ev...	SUCCESS	
116	11.16590880	notepad.exe:3360	SetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS	57 B6 BC 6F E2 A4 81 F6 ...
117	11.17785780	explorer.exe:2120	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\My ...	SUCCESS	""
118	11.18312774	explorer.exe:2120	SetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders...	SUCCESS	""
119	11.18742633	explorer.exe:2120	SetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders...	SUCCESS	""
120	11.26305019	explorer.exe:2120	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.Ev...	SUCCESS	53 00 69 00 63 00 68 00 ...
121	11.26362429	explorer.exe:2120	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.Ev...	SUCCESS	06 00 00 00 00 00 00 00 ...
122	11.28932392	explorer.exe:2120	SetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\MR...	SUCCESS	1D 00 00 00 09 00 00 00 ...
123	11.29330124	explorer.exe:2120	SetValue	HKCU\SessionInformation\ProgramCount	SUCCESS	0x2
124	12.69772136	explorer.exe:204	SetValue	HKCU\Software\Microsoft\Windows\ShellNoRoam\Bags\87\Shell\FolderType	SUCCESS	"Documents"
125	13.08878978	notepad.exe:3360	SetValue	HKCU\Software\Microsoft\Notepad\lfEscapement	SUCCESS	0x0
126	13.08887917	notepad.exe:3360	SetValue	HKCU\Software\Microsoft\Notepad\lfOrientation	SUCCESS	0x0
127	13.08922894	notepad.exe:3360	SetValue	HKCU\Software\Microsoft\Notepad\lfWeight	SUCCESS	0x190
128	13.08933007	notepad.exe:3360	SetValue	HKCU\Software\Microsoft\Notepad\lfItalic	SUCCESS	0x0
129	13.08942030	notepad.exe:3360	SetValue	HKCU\Software\Microsoft\Notepad\lfUnderline	SUCCESS	0x0
130	13.08950914	notepad.exe:3360	SetValue	HKCU\Software\Microsoft\Notepad\lfStrikeOut	SUCCESS	0x0
131	13.24001458	notepad.exe:3360	SetValue	HKCU\Software\Microsoft\Notepad\lfCharSet	SUCCESS	0x0
132	13.24012018	notepad.exe:3360	SetValue	HKCU\Software\Microsoft\Notepad\lfOutPrecision	SUCCESS	0x1

Abbildung 4: Registry Monitor

Neben den Ausgaben von Zeilennummer und Zeit wird auch der auslösende Prozess aufgeführt. Unter Request findet sich die Art des Zugriffs, unter Path der Verzeichnis- bzw. Registrypfad. Result zeigt jeweils das Resultat der Aktion an und sollte eigentlich immer auf „SUCCESS“ stehen, wenn kein Fehler wie ein fehlendes Zugriffrecht auftritt. Im Feld Other wird im Falle von Filemon die Länge der Bytes und/oder der verwendete Offset angezeigt. Bei Regmon findet sich eine Anzeige des Beginns des Wertes.

Eine besondere Betrachtung der Registrydateien mit dem Programm Regmon ist sinnvoll, da gerade hier sehr viele Informationen aufgezeichnet werden. Mit der Information, dass in den Registrydateien Änderungen stattfinden, würde man noch keinen wesentlichen Ergebnisse erzielen.

Bei dem zuerst angedachten Versuchsablauf 2 mit den Checksummen, kommt für das Finden der betreffenden Werte das oben schon angegebene Programm ART in Betracht. Durch das neue Programm Regmon ist die Verwendung von ART aber überflüssig.

Bei einer normalen (Nicht-Registry-) Datei können die Änderungen entweder mit der Offset- und Längenangabe von Filemon oder wie schon im Versuchsablauf 2 beschrieben, mit Beyond Compare festgestellt werden.

Im Regmon sieht man hier gleich den Anfang der im jeweiligen Ast geschriebenen Werte. Zu beachten ist, dass die Anzeige nicht immer den vollständigen Wert umfasst. So wird von Regmon nur die erste Zeile eines Inhaltes unter „Other“ angezeigt. Während zu lange Zeileneintrage, die gekürzt werden, durch drei Punkte am Ende gekennzeichnet sind, werden von mehrzeiligen Einträgen ohne Kenntlichmachung nur die jeweils ersten Zeilen angezeigt. Man kann deshalb hier nicht erkennen, ob noch weitere Zeilen folgen. Zwar öffnet ein Doppelklick auf die jeweilige Zeile zusätzlich das Programm Regedit genau an diesem Ast, womit sich dann der komplette Wert ablesen lässt. Aber hier handelt es sich gegebenenfalls um einen bereits wieder aktualisierten Wert und nicht mehr zwingend um den Wert zum Zeitpunkt der Erstellung des Listeneintrages.

Versuchsablauf 3
(letztendlich verwendete Version)

1. Filemon & Regmon starten
2. Vorgang durchführen
3. Über die Ausgabe von Filemon oder Regmon Datei oder Registrypfad identifizieren
4. Relevanten Dateiinhalt bzw. Registrywerte protokollieren
5. Protokoll auswerten
6. Wenn das Protokoll noch nicht aussagekräftig ist, Versuchsablauf mit variiertem Vorgang ab Punkt 2 wiederholen

Bei allen Versuchen, die Eingaben enthalten, bietet es sich an, möglichst aussagekräftige, sonst eher selten verwendete Namen für Benutzer, Dateien oder sonstige frei wählbare Bezeichnungen zu verwenden. Dies erleichtert das Erkennen der relevanten Stellen der Einträge und verhindert Fehlinterpretationen.

Da bei komplexeren Vorgängen wie Benutzeranmeldungen sehr viele einzelne Zugriffe stattfinden, bietet es sich an, die Filterfunktionen der Programme zu nutzen, und nur noch Schreibzugriffe anzeigen zu lassen.

Aufgrund des Zeitstempels „Letzter Zugriff“ können auch Lesezugriffe von Belang sein. Die Information, dass bei einem gewissen Vorgang eine bestimmte Datei gelesen wird, ist in der Praxis aber nur dann bedeutend, wenn diese Datei nur exklusiv oder von wenigen Vorgängen beeinflusst wird. Dies trifft jedoch gerade auf die Registrydateien nicht zu, da in ihnen tausende Äste und Werte gespeichert sind und sehr viele Vorgänge eine Beeinflussung vornehmen.

Selbst Dateien mit Schreibzugriffen werden teilweise nicht in die Klassifikation aufgenommen, wenn in der Untersuchung keine relevanten Informationen zu ermitteln sind. Gleiches gilt auch für Vorgänge, bei denen aufgrund ihrer Komplexität eine Unmenge von Zugriffen stattfindet. Anderes würde allein vom Umfang den Rahmen einer handhabbaren Klassifikation sprengen, ohne einen vertretbaren Erkenntnisgewinn zu bringen, wenn bereits genügend aussagekräftige Quellen vorliegen.

So führen komplexere Vorgänge wie eine Benutzeranmeldung hunderte von Zugriffen verschiedenster Art auf das Dateisystem und die Registry durch und erstellen dadurch abhängig von den eingestellten Protokollierungsfunktionen auch eine Menge an Einträgen im Protokoll. Der Umfang der Zugriffe ist von den Systemeinstellungen und installierten Programmen abhängig. Ein Testlauf zeigt, dass bei einer Benutzeranmeldung über eine Terminalsitzung allein 1024 Schreibzugriffe auf die Registry und 640 auf das Dateisystem durchgeführt werden. In solchen Fällen ist der Verzicht auf eine komplette Liste aller Datei- und Registryzugriffe sinnvoll, da sie nicht mehr Aufschluss geben würde als die Dokumentation der wirklich informativen Quellen.

Um die Ergebnisse zu verifizieren, ist zu einem festgelegten Vorgang nicht nur eine Variante des Versuchs durchzuführen. So sind gerade die Ergebnisse bei der Untersuchung der Vor-

gänge im Dateisystem nicht allgemein gültig. Die Dateioperationen führen für die beiden Dateisysteme NTFS (New Technology File System) und FAT32 (File Allocation Table 32) und verschiedene Programme (jeweilige Shellbefehle oder Explorer) nicht immer auf das gleiche Ergebnis. Zusätzlich kann es aufgrund von Cacheverhalten auch noch eine Rolle spielen, ob der Vorgang zum ersten Mal oder wiederholt ausgeführt wird. Da es bei bestimmten Vorgängen wie „Datei/Verzeichnis verschieben“ auch noch eine Rolle spielen kann, ob der Vorgang innerhalb derselben Festplattenpartition stattfindet oder sich zwischen verschiedenen abspielt, führt das in diesem Fall nun schon zu 16 (2x2x2x2) verschiedenen Versuchen für nur einen Vorgang. Für den Leser mag diese Schilderung vielleicht nach übertriebener Vorsicht klingen, aber in den Versuchen haben sich je nach Vorgang in allen oben aufgeführten Aspekten entscheidende Unterschiede ergeben. Bei der Ergebnisdokumentation wird sich die Zahl der Fälle wieder reduzieren, weil die Varianten mit gleichem Ergebnis jeweils zusammengefasst und Abweichungen mit Bemerkungen berücksichtigt werden können.

Da das Finden der Quellen zu einer Vielzahl von Vorgängen mit den notwendigen Varianten trotz des mehrfach verbesserten Versuchsablaufs einen hohen Aufwand erfordert, muss sich eine vorausgehende Untersuchung auf die wichtigen Vorgänge beschränken. Nicht in der Klassifikation enthaltene Vorgänge müssen in einem konkreten Anwendungsfall wie im Kapitel 5.3 gegebenenfalls noch untersucht werden.

3.3.4 Untersuchtes System

Aus oben beschriebenen Gründen werden auch nicht alle dieser Tests für jede der aktuellen Windowsversionen durchgeführt. Im Sinne der Zukunftssicherheit stand bei den Tests die neueste Windowsversion, Windows 2003 Servers, im Mittelpunkt. Dabei wird stichprobenhaft überprüft, ob sich die anderen aktuellen Versionen, Windows 2000 Professional und Windows XP, genauso verhalten. Hier werden im Hinblick auf die bei allen Versionen vorhandenen Komponenten keine Abweichungen festgestellt. Die durchgeführte Untersuchung gibt natürlich keine Garantie, dass sich wirklich alle Vorgänge in diesen Betriebssystemen gleich verhalten. Eine Abweichung könnte sich hierbei nicht nur zwischen den oben genannten Hauptversionen ergeben, sondern prinzipiell bereits durch einen aufgespielten Patch oder ein ServicePack bzw. sogar nur bei ganz bestimmten Kombinationen dieser auftreten.

Insofern kann eine allgemeingültige Aussage hier immer nur für das konkret untersuchte System gemacht werden. Ebenso könnte die Erzeugung von bestimmten Quellen von Systemeinstellungen abhängen, die nicht dokumentiert oder nur durch direkte Einträge in der Registry änderbar sind. Auch in diesem Fall ist die Wirkung der Kombination bestimmter Einstellungen nicht durch Versuche abschließend erfassbar. Im Regelfall wird bei den Untersuchungen von den Standardeinstellungen ausgegangen, es sei denn, die Versuchsdurchführung oder Literaturrecherche führte zu entsprechenden Informationen. So werden z.B. verschiedenste Arten der angebotenen Protokollierung aktiviert und getestet, auch wenn die jeweilige Protokollierung nicht der Standardeinstellung entspricht. In solchen Fällen sind die nötigen Einstellungen bei der späteren detaillierten Beschreibung der jeweiligen Quelle genannt.

Zur Verifikation unerwarteter oder nicht plausibler Ergebnisse wird die Untersuchung über das Standardsystem hinaus auf Systeme mit anderen Konfigurationen, Patches und installierten Programmen ausgeweitet.

Um die Nachvollziehbarkeit der Ergebnisse zu gewährleisten, ist die genaue Konfiguration des primär verwendeten Testsystems im Anhang im Kapitel 7.3 aufgelistet.

Zusammenfassend lässt sich aus den Untersuchungen ableiten, dass die kombinierte Vorgehensweise (Literaturrecherche und Experimente) sehr ergiebig ist. Finden sich in der Literatur Hinweise auf Quellen, lassen sich diese durch die Versuche überprüfen. Versuchsergebnisse liefern wiederum Anhaltspunkte für eine erfolgsversprechendere Suche in der Literatur.

3.4 Quellen nach Kriterien bewerten

Für die Erstellung der Klassifikation sind passende Kriterien zur Bewertung der gefundenen Quellen festzulegen und diese Bewertung ist dann auch bei jeder gefundenen Quelle vorzunehmen. Diese beiden Aufgaben können nicht völlig isoliert voneinander gelöst werden, da zwischen ihnen Zusammenhänge und Abhängigkeiten bestehen. So liefert eine Untersuchung der Quellen auch wichtige Ergebnisse im Hinblick auf sinnvolle Kriterien. Schließlich bringt es nichts, ein interessantes Kriterium zu finden, bei dem aber zu fast keiner Quelle eine Aussage möglich ist, oder ein Kriterium zu haben, das für 99% der Quellen denselben Wert annimmt und nur in Sonderfällen abweicht. Ebenso ist dann eventuell eine feinere Unterteilung angebracht, so dass über die vielen zuvor gleich beurteilten Quellen nun genauere Aussagen getroffen werden können.

Insofern haben die Ergebnisse der Quellenanalyse Rückwirkungen auf die verwendeten Kriterien. Deshalb sind beide Arbeitsschritte insbesondere in der Anfangsphase teilweise parallel durchzuführen.

3.4.1 Kriterien festlegen

Auch für die Festlegung von Kriterien wird auf Literatur zurückgegriffen. Hier finden sich jedoch keine greifbaren Aussagen sachkundiger Personen über konkrete Kriterien, die für eine Bewertung von Informationsquellen wichtig sind. Allerdings bieten sich vielfältige Möglichkeiten allgemeine Probleme und Lösungen im Bereich der Sicherheit zu betrachten. Zusätzlich unterstützt die möglichst genaue Kenntnis der Vorgehensweise des Forensiker in konkreten zurückliegenden Fällen das Hineinversetzen in dessen Arbeit. Was will der Forensiker von den Quellen jeweils alles wissen, um sie einträglich verwenden zu können?

Im Einzelnen stehen für die Durchsicht u. a. folgende allgemeinen Informationen zur Sicherheit zur Verfügung. Das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebene IT-Grundschutzhandbuch [Bund02a] und der Leitfaden IT-Sicherheit [Bund02b]. Die amerikanischen National Security Acency (NSA) [Nati03] liefert mit den „Security Recommendation Guides“ u. a. speziell für Windowssysteme Sicherheitsinformationen. Wichtig sind auch das Vorgehen und die daraus gewonnen Erkenntnisse des Honeynet-Projektes. Hier bieten die Whitepapers [Hone03] einen guten Einblick.

Am wichtigsten sind aber die Seiten, die sich speziell mit den forensischen Problemen auseinandersetzten. Dazu finden sich auf den Seiten von manchen Forensik-Dienstleistungsfirmen auch nähere Informationen, die einen guten Einblick in ihre Arbeit geben. So hat der englische Zweig der Firma Vogon eine Firmenzeitschrift mit Namen „Smoking Gun“ [Vogo03] in der aus verschiedensten Artikeln Anhaltspunkte für wichtige Kriterien entnommen werden können. Ebenso liefert die amerikanische Forensikfirma New Technologies Inc. (NTI) [NewT03a] zu Werbezwecken neben der Beschreibung ihrer Dienste ausführliche Aus-

züge aus rechtlichen Publikationen [NewT03b], die computerforensische Fälle betreffen, oder zeigt an ausgewählten behandelten typischen Fällen ihr Vorgehen [NewT03c]. In diesem Sinne sind auch Artikel aus dem International Journal of Digital Evidence [Inte03] die Präsentationen aus dem Archiv des Digital Forensic Research Workshop [Digi03] und die gesammelten Kolumnen aus dem Doctor Dobb's Journal von D. Farmer und W. Venema [FaVe02] hilfreich.

Zusätzlich sind Informationen aus dem vom Leibniz Rechenzentrum angebotene Vortrag „Computer-Forensik: Grundlagen und praktische Anwendungen" vom 11.12.2003 eines Referenten der Forensikfirma Vogon International, im dem dieser kurze Einblicke in reale Fälle und die Arbeit seiner Firma gab, eingearbeitet.

Aus den genannten Erfahrungen von Forensikern und entsprechenden relevanten Fällen lassen sich gewisse Anforderungen ableiten. So ist es bei einer Analyse wichtig, wie lang die betreffende Quelle nach dem Vorgang noch auswertbar ist („Lebensdauer") und welche Informationen diese Quelle überhaupt liefern kann („Informationsgehalt"). Um eine unnötige Suche zu vermeiden und verlässliche Ergebnisse zu erzielen, ist es auch bedeutsam zu wissen, ob es bestimmter „Entstehungsbedingungen" für die Quelle bedarf, um überhaupt erzeugt zu werden. Ebenso ist auch besonders wichtig, ob die Quelle eventuell nur im laufenden Betrieb zur Verfügung steht („Verfügbarkeit") und somit für die Offlineanalyse gar nicht in Frage kommt. Wenn mehrere Quellen zur Verfügung stehen, können die gewählt werden, die den geringsten „Aufwand" in der Auswertung erfordern oder nicht anfällig für eine „Fehlinterpretation" sind. Hier kann auch von Belang sein, ob eine leicht durchführbare „Fälschung" möglich und somit auf die Aussagen der Quelle kein großer Verlass ist.

So kann durch obige Kriterien entschieden werden, ob sich die Quelle überhaupt eignet, in die jeweilige forensische Untersuchung einbezogen zu werden. Letztendlich sollte auch eine kurze Anleitung für die Durchführung der „Auswertung" nicht fehlen, bei der für Rückschlüsse die Liste eine entscheidende Rolle spielt, die „Verursachende Vorgänge" enthält.

Die Bedeutung der festgelegten Kriterien ist in der nachfolgenden Tabelle zusammenfassend dargestellt.

Kriterium	**Kurzbeschreibung**
Verursachende Vorgänge	Vorgänge, die Auswirkungen auf die Quelle haben.
Entstehungsbedingungen	Notwendige Systemeinstellungen für die Erzeugung der Quelle.
Lebensdauer	Angaben zur Lebensdauer der Quelle.
Informationsgehalt	Informationen, die die Quelle über den Vorgang liefert.
Verfügbarkeit	Angabe in welchem Modus die Auswertung stattfinden kann.
Auswertung	Vorgehen, um an die Informationen der Quelle zu gelangen.
Aufwand	Aufwand, um an die Informationen der Quelle zu gelangen.
Fehlinterpretation	Angaben zur Gefahr die Quelle falsch zu interpretieren.
Fälschung	Bedingungen zum Verändern oder Löschen der Quelle.

Im Hinblick auf die Verwendung der anzulegenden Quellenblätter ist es zweckmäßig, die genannten Kriterien um den Titel und eine kurze „Beschreibung der Quelle" zu ergänzen.

Weiterhin ist es sinnvoll, die Bewertungen für jede Quelle nicht nur durch unterschiedlichste Texte auszudrücken, sondern zu den Kriterien Standardwerte festzulegen, die den Bewer-

tungstext ergänzen oder ersetzen. Damit können die Beschreibungen der Quellen wesentlich besser verglichen werden, da eine Übereinstimmung oder Abweichung in der Bewertung sofort auffällt. Die Standardwerte müssen auch in deren Quantität sinnvoll gewählt werden. So würde eine vielteilige Skala, z.B. von 1-10, zwar eine hohe Differenzierung der Quellen ermöglichen. Wenn aber keine so differenzierten Aussagen getroffen werden können, entsteht damit kein Aussagewert. So wäre bei der oben genannten 10-teiligen Skala bei der Bewertung der festgelegten Kriterien nicht wirklich wissenschaftlich entscheidbar, was eine 8 oder nur eine 7 ist. Und selbst wenn nach einem komplizierten System eine solch feingliedrige Bewertung möglich wäre, würde dies dem Leser nur bedingt nutzen, da er die Bedeutung des jeweiligen Prädikats auch nicht genauer interpretieren könnte.

Durch die zusätzliche Bewertung mit den grobgliedrigen Standardwerten geht keine Information verloren, weil die genau auf die Quelle abgestimmte textliche Bewertung hinter den Standardwerten erfolgt.

Aus den genannten Gründen werden für die Bewertung der Kriterien jeweils nur wenige Standardwerte festgelegt, die in der nachfolgenden Tabelle dargestellt sind.

Kriterium	**Standardwerte**
Verursachende Vorgänge	*Nicht vergeben*
Entstehungsbedingungen	• Keine • Spezielle
Lebensdauer	• Solange der Zustand besteht • Bis zum nächsten Vorgang • Bedingt abhängig von anderen Vorgängen • Speziell
Informationsgehalt	• Zeit • Benutzer • Sonstiges
Verfügbarkeit	• Nur online verfügbar • Nur offline verfügbar • Online und offline verfügbar
Auswertung	*Nicht vergeben*
Aufwand	• Gering • Hoch • Nicht abschätzbar
Fehlinterpretation	• Gering • Hoch
Fälschung	• Leicht • Administratorrechte • Programmmanipulation

Im Kapitel 4.1 findet sich sowohl eine ausführliche Beschreibungen der festgelegten Kriterien als auch eine Erklärung der verwendeten Standardwerte.

3.4.2 Quellen bewerten

Um die Quellen nach den festgelegten Kriterien bewerten zu können, ist es keinesfalls ausreichend, ausschließlich die Angaben in der Quelle selbst zu verwerten. Vielmehr müssen auch vielfältige weitere Aspekte aus dem Umfeld der Quelle richtig einbezogen werden. Dies ist aber nur möglich, wenn die Funktionalität der jeweils relevanten Teile des Betriebssystems Berücksichtigung findet. Soweit entsprechende Informationen nicht direkt der Literatur des Betriebssystems zu entnehmen sind, liefern Versuche die zusätzlich erforderlichen Erkenntnisse.

So ist z.B. für das Kriterium „Lebensdauer“ zu untersuchen, ob und wie sich die Quelle durch wiederholte bzw. andere Vorgänge ändert. Die Beobachtungen, Untersuchungen und Überlegungen ergeben, dass eine Quelle entweder den Zustand eines Aspektes des Systems anzeigt oder eine Art von Protokoll über den auslösenden Vorgang ist. Im ersten Fall wird die Quelle somit durch das Rücksetzen des Zustandes gelöscht, im zweiten Fall wird die Quelle von folgenden gleichen oder anderen Vorgängen gelöscht oder deren Inhalt ersetzt. Die hier gezogenen Schlüsse über die Möglichkeit der Bewertung der Lebensdauer finden sich im Kapitel 4.1. Dort ist es daher nicht möglich, als Standardwerte für die Bewertung der „Lebensdauer“ feste Zeitwerte, wie „maximal 1 Tag“, „mindestens 1 Stunde“ oder „genau 30 Minuten“ anzugeben. Dies hat leider zur Folge, dass die Anwendung der Klassifikation damit komplexes Denken erfordert, weil die Abschätzung der Existenz der Quellen schwierig und unsicher ist.

Für die Bewertung des Kriteriums „Fälschung“ ist die Veränderung und Löschung von Quellen aus der Perspektive eines Hackers zu betrachten. Hier steht die Frage im Mittelpunkt wie dieser im konkreten Fall herangehen könnte. Hilfreichen Einblick gibt das oben schon erwähnte Honeynet Project [Hone03] und vor allem verschiedenste Artikel aus dem Hackermagazin Phrack [Phra03]. Auf den Quellenblättern werden jedoch meist nur die einfachsten und nahe liegenden Möglichkeiten der Fälschung beschrieben. Das kann hier allerdings nur im Ansatz erfolgen, da alles darüber hinausgehende den Umfang sprengen würde.

Gerade für die Offlineauswertung sind die Formate der aufgezeichneten Quellen wichtig. Bei einer Onlineanalyse können die Informationen der Quellen meist noch mit den mitgelieferten Programmen im Klartext angezeigt und ohne Kenntnisse des eigentlichen Formats ausgewertet werden. Stehen diese Programme aber für eine Offlineanalyse nicht zur Verfügung, weil sie die Verbindung zu den Quellen nur im laufenden Betrieb des Systems aufnehmen können, ist die Auswertung wesentlich schwieriger. Die Kodierung kann nicht für alle Quellen beschrieben werden; dies gilt insbesondere, wenn sich weder Informationen des Systemherstellers oder von Anwendern finden lassen noch Informationen durch eigene Untersuchungen gewinnen lassen. Soweit eine Beschreibung der Kodierung der jeweiligen Quelle bekannt ist, findet sich diese unter dem Kriterium „Auswertung“ auf dem jeweiligen Quellenblatt.

Es scheint als ist die forensische Analyse bzw. zumindest die Offlineanalyse von Microsoft gar nicht bedacht, da sich z.B. keine detaillierten Beschreibungen zu den Dateiformaten der Registry und des Ereignisprotokolls finden lassen. Hier ist wohl nur an eine Verwendung der mitgelieferten Programme gedacht. Diese funktionieren jedoch nur auf dem laufenden eigenen System und eignen sich nicht zur Analyse von Sicherungen fremder Systeme, da sie über betriebssysteminterne Funktionen direkt auf die systemeigenen Quellen zugreifen. Wegen der großen Bedeutung ist sowohl die Registry als auch die Ereignisprotokollierung mit einem eigenen Kapitel im Anhang genauer erklärt, wo auch auf diese Problematik genauer eingegangen wird.

Entgegen der beabsichtigten Planung, hier keine über den Lieferumfang von Windows hinausgehenden Programme zu untersuchen, werden für die Offlineanalyse und Bewertung einiger wichtiger Quellen, bei der die mitgelieferten Programme nicht ausreichend sind, Zusatzprogramme eruiert und untersucht. Hierzu gehören z.B. das Programm RegView [Leep03] für die Offlineanalyse der Registry und das Programm WinTrace [Xway03] für die Auswertung des Papierkorbs und der hinterlassenen Daten des Internet Explorers. Für das Betrachten von Binärdateien ist es sinnvoll einen Hexeditor, wie WinHex [Xway03a] zu verwenden, da in einem normalen Texteditor die Sonder- und Steuerungszeichen nicht angezeigt werden. Die Ergebnisse zeigen, dass bisher nicht für alle Quellen entsprechende Tools zugänglich sind.

Die gefundenen Programme sind zumindest ein teilweiser Ersatz für das Fehlen von genauen Beschreibungen zum Kodierungsformat mancher Quellen. Außerdem darf angenommen werden, dass diese Programme für den mit Windows arbeitenden Forensiker sogar wesentlich hilfreicher sind, als die ausschließliche Beschreibung des Kodes.

3.5 Wahl des Aufbaus der Klassifikation

Ein wesentliche Entscheidung bei der Erstellung der Klassifikation besteht darin, eine geeignete Form der Darstellung festzulegen, die den Zusammenhang zwischen den Quellen und den jeweiligen verursachenden Vorgängen sowie die Bewertungskriterien der Quellen enthält.

3.5.1 Struktur der Klassifikation

Wichtig für den Einsatz der Klassifikation sind sicher die Möglichkeiten zum schnellen Auffinden der relevanten Information. Dabei ist in der praktischen Anwendung der Klassifikation bei der Lösung forensischer Probleme sowohl eine Suche über die Vorgänge als auch über die Quellen von Bedeutung. Schließlich kann die Arbeit in den folgenden Situationen Verwendung finden:

Sollte zum einen schon eine konkrete Vermutung über den ausgeführten Vorgang vorliegen, ist es wichtig, dass sich alle von diesem Vorgang erzeugten Quellen finden lassen. Diese erhärten dann möglicherweise die Vermutung und liefern möglicherweise genauere Informationen zu den Umständen des Vorgangs. Dies soll folgendes Beispiel illustrieren: Ist nur bekannt, dass eine wichtige Datei verschwunden ist, finden sich über eine Suche nach den Quellen des Vorgangs „Datei löschen“ mehrere Ergebnisse. Eine Untersuchung dieser Quellen am konkreten System bestätigt möglicherweise das Löschen der Datei und liefert darüber weitere Informationen. In diesem Fall könnten dazu u. a. die Systemzeit zum Zeitpunkt der Ausführung des Vorgangs oder der verursachende Benutzer gehören.

Diese Suchmöglichkeit ist über Seitenverweise von den Vorgängen zu den jeweiligen Quellen im Kapitel 4.2 „Verzeichnis der Vorgänge“ realisiert.

Zum anderen ist aber auch eine Suche ausgehend von den Quellen in der Praxis erforderlich. Stößt man zuerst auf eine Quelle, will man daraufhin auch wissen, welche Vorgänge für die Erzeugung dieser Quelle in Frage kommen. So können gerade im Ereignisprotokoll verschiedenste Quellen aufgefunden werden. Jedoch sind aus dem Protokolleintrag für den ungeschulten Betrachter teilweise die erzeugenden Vorgänge nicht unmittelbare erkennbar.

Die für die Suche der erzeugenden Vorgänge nötigen Verweise befinden sich jeweils auf dem betreffenden Quellenblatt in Kapitel 4.4 „Quellenbeschreibungen“.

Die mögliche Alternative, die Klassifikation so aufzubauen, dass jedem Vorgang unmittelbar alle zugehörigen Quellen folgen, ist nur mit hohem Aufwand zu realisieren, da sehr viele Vorgänge dieselben Quellen erzeugen. Diese Quellen müssten dann jeweils unter mehreren verursachenden Vorgängen wiederholt dargestellt werden. Da außerdem alle Quellen nicht mehr systematisch geordnet werden könnten, wäre die Suche von Vorgängen ausgehend von den Quellen erheblich erschwert.

3.5.2 Aufbau der Quellenblätter

Der strukturelle Aufbau der Quellenblätter sollte prinzipiell immer gleich sein. So kann sich der damit vertraute Leser bei einer neuen Quelle sofort rasch zurechtfinden. Es wäre nahe liegend, dies nicht nur durch die gleiche Reihenfolge der Kriterien, sondern auch über eine feste Einteilung des Platzes zu erreichen. So würde sich Kriterium Y immer nach Kriterium X vor Kriterium Z an derselben Stelle des Blattes, z.B. in der 7.ten Zeile, befinden. Während nichts gegen die gleiche Reihenfolge spricht, ist eine starre Platzeinteilung ungeeignet, weil sich der Platzbedarf eines Kriteriums für verschiedene Quellen oft zu sehr unterscheidet. Wo bei der einen Quelle nur ein kurzer Satz zur Beschreibung ausreichend ist, kann bei einer anderen Quelle eine komplexe Erklärung von Nöten sein, um dem Leser alle nötige Information zu vermitteln. Um dennoch denselben optischen Aufbau pro Quelle zu erreichen, müsste man also für jedes Kriterium immer soviel Platz lassen, wie von der ausführlichsten Beschreibung für dieses Kriterium in allen Quellen benötigt wird. Dies würde aber sehr viel unbeschriebenen Platz und damit ein unangemessene Aufblähung der Arbeit bewirken.

Leider ist es auch bei variabler Platzeinteilung nicht sinnvoll möglich, alle Kriterien bei komplexeren Quellenbeschreibungen auf einer Seite unterzubringen. Dieses Ziel wäre nur zu erreichen, indem z.B. die verwendeten Schriftgrößen und Zeilenabstände wesentlich verkleinert würden. Dies würde aber wesentlich stärkere Abstriche bei der Lesbarkeit bedeuten. Auch das Auslagern und der Verweis auf entsprechende Kapitel im Anhang, um die Texte bei komplexeren Quellenblätter kurz zu halten, würde durch das dann ständig erforderliche Blättern nicht der Übersichtlichkeit dienen. Deshalb wird dies nur in extremen Fällen und bei sonst wiederholt auftretenden Beschreibungen, wie z.B. der Registry und der Ereignisanzeige, verwirklicht.

Auch wenn damit eine flexible Platzeinteilung verbunden ist, wird aufgrund der Trennung der Kriterien durch Querstriche und der Abhebung des Kriteriumsnamens vom Text dennoch eine übersichtliche Gestaltung gewahrt.

Der Umfang der Quellenbeschreibungen kann sich damit deutlich unterscheiden und eine oder mehrere Seiten betragen. Zur leichteren Handhabung wird für jede Quellenbeschreibung eine neue Seite begonnen.

4 Klassifikation

Im Kapitel 4.4 „Quellenbeschreibungen“, das den Kern der Diplomarbeit darstellt, sind alle Quellen detailliert nach demselben Schema beschrieben und bewertet. Das verwendete Schema wird im folgenden Kapitel erklärt.

Im darauf folgenden Kapitel 4.2 befindet sich eine nach Kategorien geordnete Auflistung aller untersuchten Vorgänge, denen die jeweils von ihnen erzeugten Quellen zugeordnet sind. Sollte die Aufgabe darin bestehen, die Quellen eines Vorgangs aufzuspüren, lassen sich diese über die Auflistung schnell auffinden. Über den Kurztitel der Quellen und die jeweils angegebene Seitennummer gelangt man im Bedarfsfall zur entsprechenden Quellenbeschreibung.

Das anschließende Kapitel 4.3 enthält eine Auflistung der Kurztitel der Quellen. Sowohl diese Liste als auch die eigentlichen Quellenbeschreibungen im nachfolgenden Kapitel sind alphabetisch geordnet.

4.1 Kriterienkatalog

Die Darstellung des Kriterienkataloges wird aufgrund der Aufgabe im Format der späteren Quellenbeschreibungen vorgenommen. Um dem Leser beim Betrachten und Vergleichen der Eigenschaften der Quellen einen schnellen Überblick bieten zu können, sind alle Quellenblätter nach demselben Muster aufgebaut. Für die räumliche Anordnung sind die Überlegungen im Abschnitt 3.5.2 maßgeblich.

Eine Quellenbeschreibung enthält neben dem Kurztitel und der Beschreibung folgende Kriterien:

Kriterium	**Kurzbeschreibung**	**Standardwerte**
Verursachende Vorgänge	Vorgänge, die Auswirkungen auf die Quelle haben.	*Nicht vergeben*
Entstehungsbedingungen	Notwendige Systemeinstellungen für die Erzeugung der Quelle.	• Keine • Spezielle
Lebensdauer	Angaben zur Lebensdauer der Quelle.	• Solange der Zustand besteht • Bis zum nächsten Vorgang • Bedingt abhängig von anderen Vorgängen • Speziell
Informationsgehalt	Informationen, die die Quelle über den Vorgang liefert.	• Zeit • Benutzer • Sonstiges
Verfügbarkeit	Angabe in welchem Modus die Auswertung stattfinden kann.	• Nur online verfügbar • Nur offline verfügbar • Online und offline verfügbar
Auswertung	Vorgehen, um an die Informationen der Quelle zu gelangen.	*Nicht vergeben*
Aufwand	Aufwand, um an die Informationen der Quelle zu gelangen.	• Gering • Hoch • Nicht abschätzbar
Fehlinterpretation	Angaben zur Gefahr die Quelle falsch zu interpretieren.	• Gering • Hoch
Fälschung	Bedingungen zum Verändern oder Löschen der Quelle.	• Leicht • Administratorrechte • Programmmanipulation

Der dadurch festgelegte grundlegende Aufbau der Quellenbeschreibungen wird zur besseren Orientierung auch bei der direkt folgenden Detailerläuterung der Kriterien und Standardwerten verwendet.

Quelle:

Die Quelle wird mit einem Kurztitel aus Beschreibung und den wichtigsten Auswertungswerkzeugen benannt.

Die Angabe der Auswertungswerkzeuge beschränkt sich in der Regel auf die in Windows standardmäßig enthaltenen Programme. Da sich diese insbesondere für die Offline-Auswertung nur bedingt eignen, sind dafür ohne Anspruch auf Vollständigkeit gegebenenfalls nicht zum Lieferumfang von Windows gehörende Programme in Klammern angegeben. Obwohl für die Offline-Untersuchung auch andere Betriebssysteme in Frage kommen, bleiben Nicht-Windows Programme sowie kommerzielle Spezialprogramme für die forensischen Untersuchung ungenannt.

Beschreibung der Quelle:

An dieser Stelle wird die Quelle ausführlicher als im Kurztitel beschrieben, da dieser als Bezeichnung für die jeweilige Quelle zu verstehen ist und sie in der Regel naturgemäß nicht eindeutig beschreiben kann.

Verursachende Vorgänge:

In diesem Unterpunkt befindet sich eine Auflistung von Vorgängen, die Auswirkungen auf die hier beschriebene Quelle haben.

Im Falle einer Quelle mit dem unten noch näher beschriebenen Lebensdauertyp „Solange der Zustand besteht“, werden an dieser Stelle die Vorgangspaare genannt, zwischen deren Ausführung die Quelle existiert.

Bei den beiden anderen Lebensdauertypen werden die Vorgänge genannt, die diese Quelle hinterlassen.

Falls der Zusammenhang zwischen Vorgang und Quelle komplizierter ist, wird die Beziehung beim jeweiligen Vorgang erwähnt und erforderlichenfalls erläutert.

Entstehungsbedingungen:

Hier werden die notwendigen Systemeinstellungen erklärt, damit die Quelle erzeugt wird.

Gegebenenfalls wird hier auch auf Spezialfälle eingegangen, bei denen sich z.B. der Systemzustand oder die Art der Auslösung eines Vorgangs auf die Entstehung der Quelle auswirken.

Standardwerte sind:

- „**Keine**“: Es sind keine besonderen Einstellungen nötig oder bekannt.
- „**Spezielle**“: Konkrete Nennung der Bedingungen, eventuell unterschieden nach dem erzeugenden Vorgang.

Lebensdauer:

Unter diesem Kriterium finden sich Angaben zur Lebensdauer der Quelle.

Da die Lebensdauer der erzeugten Quellen in der Regel keine absolut bestimmbare Zeit (wie z.B. 1 Stunde oder 2 Tage) beträgt, sondern von Systemeinstellungen oder der Ausführung von Vorgängen abhängt, werden die Quellen in folgende Standardwerte eingeteilt:

- „**Solange der Zustand besteht**“: Die Quelle beschreibt einen aktuellen Systemzustand. Dieser wird durch komplementäre Vorgänge bestimmt, die das System in einen bestimmten Zustand hineinversetzen bzw. zurückversetzten. Durch diese Vorgangspaare, die unter dem anschließenden Kriterium „Verursachende Vorgänge“ genannt sind, werden entsprechende Quellen, die den Systemzustand beschreiben, erstellt bzw. zerstört.

Im Gegensatz dazu gibt es Quellen, die Informationen über die obengenannten Vorgänge speichern, wobei zwei Typen unterschieden werden müssen:

- „**Bis zum nächsten Vorgang**“: Die Quelle beschreibt immer nur den letzten betreffenden Vorgang, weil die Information zu dem jeweils direkt vorausgehenden Vorgang überschrieben wird.
- „**Bedingt abhängig von anderen Vorgängen**“: Ein neuer Vorgang legt eine neue Instanz der Quelle gleichen Typs an. Dadurch bleiben die Informationen zu allen vorherigen Vorgängen als eigenständige Quellen erhalten. Die Lebensdauer ist somit nicht direkt von anderen Vorgängen abhängig. Trotzdem können selbst Vorgänge anderen Typs, z.B. über die zu speichernde Informationsmenge, indirekt zur Löschung von Quellen führen. Derartige Details sowie Abhängigkeiten von den Systemeinstellungen werden gegebenenfalls an dieser Stelle genannt und erforderlichenfalls auch erklärt.

Darüber hinaus wird für Fälle, die nicht den oben beschriebenen Typen zugeordnet werden können, ein weiterer Standardwert mit folgender Bezeichnung festgelegt:

- „**Speziell**“.

Informationsgehalt:

Unter diesem Begriff werden zum raschen Auffinden kurz und prägnant Informationen dargestellt, die diese Quelle über den Vorgang liefert. Gegebenenfalls sind die Angaben den Bereichen „Zeit“, “Benutzer“ und „Sonstiges“ zugeordnet.

- „**Zeit**“: Informationen über den Zeitpunkt des Vorgangs. Zu beachten ist, dass die genannte Information nicht der realen Zeit entsprechen muss, sondern nur Systemdatum und Systemzeit für die Ausführung des entsprechenden Vorgangs angibt.
- „**Benutzer**“: Informationen zur Identität des Verursachers des Vorgangs. Meist handelt es sich hierbei um den Benutzernamen, wenn der Zugriff über ein Netzwerk geschieht oder geschehen ist, ist auch eine Information über den zugreifenden Computer von Belang. Zu beachten ist, dass der aufgezeichnete Benutzername nur auf die verwendete Benutzerkennung verweist. Die reale Bedienungsperson eines Rechners kann bei einer Anmeldung mit einer Kennung/Passwortkombination, die z.B. durch Ausspionieren, Durchprobieren oder bewusste Weitergabe anderen Personen bekannt ist oder bei einem Wechsel der Bedienungsperson ohne Abmeldung, vom angemeldeten Benutzer abweichen.
- „**Sonstiges**“: Alle anderen Informationen, die Aussagen über einen Vorgang machen, aber zu unterschiedlich sind, um sie besonders zu gruppieren.

Verfügbarkeit:

Es wird angegeben, in welchem Modus die Auswertung stattfinden kann.

Standardwerte sind folgende:

- „**Nur online verfügbar**“: Die Quelle ist nur bei laufendem Betriebssystem verfügbar.
- „**Nur offline verfügbar**“: Die Quelle ist nicht bei laufenden Betriebssystem verfügbar.
- „**Online und offline verfügbar**“: Die Quelle ist sowohl bei laufendem als auch bei nicht laufendem Betriebssystem verfügbar.

Auswertung:

Unter diesem Kriterium wird das Vorgehen beschrieben, um an die Informationen dieser Quelle zu gelangen.

Dabei wird eventuell nach den im Kurztitel genannten Programme unterschieden und erforderlichenfalls eine kurze Anleitung zur Bedienung und Ausgabe gegeben. Sofern dies wegen des Umfangs oder der zusammenfassenden Darstellung für mehrere Quellen in den Anhang ausgelagert ist, findet sich hier ein entsprechender Verweis darauf.

Wenn ein Auswertungswerkzeug zum Einsatz kommt, das die Verbindung zum Speicherort der Quelle nicht automatisiert herstellt (z.B. ein Texteditor), ist für diese manuell durchzuführende Aufgabe der Speicherort (Verzeichnispfad, Registrierungsschlüssel, etc) in jedem Fall genannt. Liest dagegen das genannte Werkzeug die relevanten Daten nicht aus einer Quelldatei, sondern aus einer anderen Quelle, wie z.B. dem Arbeitsspeicher, kann der exakte Speicherort nicht ermittelt werden und dadurch hier nicht angegeben werden.

Wenn kein Auswertungswerkzeug, das die Verbindung zum Speicherort automatisch herstellt, zur Verfügung steht, ist die Auswertung der Quelle davon abhängig, dass der entsprechende Speicherort bekannt und hier beschrieben ist.

Abschließend wird erforderlichenfalls erklärt, wie mit einem gewöhnlichen Texteditor und Informationen zum Format, zum Kode bzw. zum Speicherort des Kodes die Quelle auswertbar ist. Sofern dies wiederum in den Anhang ausgelagert ist, befindet sich hier ein entsprechender Verweis darauf.

Aufwand:

Unter diesem Kriterium wird der Aufwand beschrieben um an die Informationen dieser Quelle zu gelangen.

Diese werden, gegebenenfalls differenziert nach verschiedenen Wegen beim Vorgehen, nach den folgenden Standardwerten bewertet:

- „**Gering**“: Der Standardwert „Gering“ wird vergeben, wenn der Aufwand in allen für diese Quelle relevanten Aspekten gering ist.
- „**Hoch**“: Der Standardwert „Hoch“ wird vergeben, wenn der Aufwand in mindestens einem für diese Quelle relevanten Aspekt hoch ist.

Die relevanten Aspekte sind jeweils hinter dem Standardwert angeführt. Als Aspekte kommen z.B. die Art der Kodierung der Information in der Quelle bzw. der Ausgabe des verwendeten Tools oder der Aufwand für die Filterung bei einer Vielzahl vorhandener Instanzen der Quelle in Frage.

Sofern das Vorgehen für die Gewinnung der Information einer Quelle nicht endgültig aufgeklärt werden konnte, und damit der Aufwand nicht abzuschätzen ist, wird der Standardwert

- „**Nicht abschätzbar**“

vergeben.

Fehlinterpretation:

Hier wird auf die Möglichkeit eingegangen, die Informationen falsch zu interpretieren.

Dabei wird davon ausgegangen, dass weder Quelle noch Werkzeug manipuliert sind. Dieses Kriterium fasst gegebenenfalls auch zum Teil schon genannte Dinge aus den obigen Kriterien zur Verdeutlichung zusammen.

Für die Interpretation ist es wichtig, zu beachten, ob die Quelle ausschließlich von einem Vorgang oder von mehreren Vorgängen erzeugt wird. Sofern letzteres der Fall ist, besteht nämlich die Gefahr, dass die Quelle dem falschen Vorgang zugeordnet wird, was zu weitrei-

chenden Fehlinterpretationen bis zur Annahme einer Verschleierung von Quellen führen kann.

Weiterhin spielt es eine Rolle, ob Möglichkeiten existieren, so dass durch eine bestimmte Art der Durchführung des Vorgangs die Quelle nicht erzeugt wird. Falls Sonderfälle zu dieser Quelle existieren, bei denen unter bestimmten Voraussetzungen sonst noch nicht beschriebene Veränderungen an der Quelle durchgeführt werden, sind diese hier genannt.

Fehlinterpretationen, die offensichtlich auf Fehler des Forensikers zurückgehen, werden hierbei nicht beachtet. Beispiele für solche Fehlinterpretationen sind: ein Benutzername wird automatisch mit der real existierenden Person assoziiert oder die angezeigte Zeit wird als Realzeit interpretiert.

Bewertet wird nach folgenden Standardwerten:

- „**Gering**“: Die Quelle wird verlässlich erstellt und verweist eindeutig auf einen Vorgang und es sind keine Ausnahmen bekannt.
- „**Hoch**“: Die Erzeugung der Quelle ist durch den Benutzer umgehbar, die Quelle verweist auf mehrere Vorgänge oder es sind bestimmte Sonderfälle bekannt, die eine Auswertung erschweren.

Zum Standardwert „Hoch“ werden die Gründe zu seiner Vergabe jeweils genannt.

Fälschung:

Unter diesem Kriterium wird auf die Bedingungen zum Verändern oder Löschen dieser Quelle gegebenenfalls einschließlich einer Abschätzung zum Arbeitsaufwand bzw. Ausführungszeitbedarf eingegangen.

Fälschung bezieht sich dabei auf Veränderungen am System mit dem Ziel der Vorspiegelung falscher Tatsachen. Dazu zählt beispielsweise eine Änderung einer Zeitangabe in der Aufzeichnung über einen Vorgang oder das Entfernen der gesamten Aufzeichnung. Die Veränderung einer Systemeinstellung, wie z.B. das Löschen eines Benutzers, gilt nicht als Fälschung, da in diesem Fall der Benutzer zwar nicht mehr angezeigt wird, im System aber auch nicht mehr vorhanden ist.

Eingeteilt wird in folgende Standardwerte:

- „**Leicht**“: Es reichen normale Benutzerrechte, um mit wenig Arbeitsaufwand eine Fälschung durchzuführen.
- „**Administratorrechte**“: Für die Fälschung ist die Erlangung von Administratorrechten notwendig.
- „**Programmmanipulation**“: Fälschung ist nur möglich, wenn das verwendete Anzeigeprogramm manipuliert ist. Der Forensiker kann den Versuch einer derartigen Manipulation einer Quelle vereiteln, indem er zur Auswertung seine unverfälschten Werkzeuge verwendet. Dieses wird bei der Offlineanalyse ohnehin die Regel sein.

Anschließend werden gegebenenfalls auf die Quelle abgestimmte Hinweise zur Durchführung der Fälschung gegeben. Zu beachten ist hierbei, dass die Bewertung wegen der Abhängigkeit von den Benutzerrechten sehr relativ ist. Die Bewertung „Administratorrechte“ ist dem Standardwert „Leicht“ gleichzusetzen, wenn der Täter mit diesen Rechten ausgestattet ist. Dies gilt in der Regel u. a. für alle Heimanwender auf ihren Privatrechnern.

4.2 Verzeichnis der Vorgänge

Es folgt eine Liste von Vorgängen, die nach Kategorien geordnet sind. Bei jedem Vorgang sind die von ihm erzeugten Quellen einschließlich der Seitenzahl des dazugehörigen Quellenblattes angegeben. Die Kategorien, Vorgänge und Quellen sind jeweils alphabetisch aufsteigend sortiert.

Benutzerverwaltung lokal

Benutzer ändert sein Passwort

Benutzer anlegen

Benutzer löschen

Benutzer umbenennen

Benutzer von lokaler Gruppe entfernen

Benutzer zu lokalen Gruppe hinzufügen

Benutzerabmeldung lokal

Benutzeranmeldung lokal

Benutzereigenschaften ändern

Benutzerpasswort festlegen

Lokale Gruppe anlegen

Lokale Gruppe löschen

Lokale Gruppe umbenennen

Unberechtigter Anmeldeversuch

Dateisystem

Datei anlegen

Datei kopieren

Datei lesen

Datei löschen

Datei umbenennen

Datei verschieben

Dateiattribute ändern

Dateiberechtigungen NTFS ändern

Dateiinhalt ändern

Verzeichnis anlegen

Verzeichnis kopieren

Verzeichnis lesen

Verzeichnis löschen

Verzeichnis umbenennen

Verzeichnis verschieben

Verzeichnisattribute ändern

Verzeichnisberechtigungen NTFS ändern

Netzwerk

Benutzerabmeldung Netzwerk

Benutzeranmeldung Netzwerk

Entfernter Datei-/Verzeichniszugriff

IIS Webseite von diesem Computer abrufen

in Terminalsitzung arbeiten

Internet Explorer: Internetseite aufrufen

Netzwerkverkehr verursachen

TCP Verbindung aufbauen oder Port öffnen

Terminalsitzung beenden

Terminalsitzung erstellen

Terminalsitzung unterbrechen

Terminalsitzung wiederaufnehmen

Prozessverwaltung

Programm (mit "Ausführen als" gestartet) beenden

Programm (mit "Ausführen als") starten

Programm (mit aktuellem Benutzer gestartet) beenden

Programm (mit aktuellem Benutzer) starten

Systemdienste

Drucken

Lokale Überwachungsrichtlinie ändern

Lokales Zuweisen von Benutzerrechten

Softwareinstallation

Systemprotokoll löschen

Treiberinstallation

Uhrzeit ändern

Verzeichnis Netzwerkfreigabe beenden

4.3 Verzeichnis der Quellen

Über die folgende alphabetische Liste der Quellen lässt sich die Seite der Quellenbeschreibung finden.

4.4 Quellenbeschreibungen

Es folgen die einzelnen Quellenbeschreibungen.

Quelle:
Aktuell bestehende Benutzersitzungen - Anzeige.....taskmgr.exe; tsadmin.exe

Beschreibung der Quelle:

Eine Liste aller aktuell bestehenden interaktive Benutzersitzungen (also alle zurzeit entweder lokal oder über Terminalclient eingeloggte Benutzer, aber keine Benutzer die nur auf freigegebene Verzeichnisse zugreifen) mit entsprechenden zusätzlichen Informationen. Die Anzeige erfolgt über die Programme Task-Manager (taskmgr.exe) oder Terminaldiensteverwaltung (tsadmin.exe).

Verursachende Vorgänge:

- AD Benutzeranmeldung an Active Directory / AD Benutzerabmeldung vom Active Directory
  (Die Programme zeigen auch an einem Domänencontroller nur die lokal oder über Terminalclient eingeloggten Benutzer, jedoch nicht die lokalen Benutzer an Clients an, die sich über den Domänencontroller nur authentifiziert haben.)
- Benutzeranmeldung lokal / Benutzerabmeldung lokal
- Terminalsitzung erstellen / Terminalsitzung beenden
- Terminalsitzung unterbrechen / Terminalsitzung wiederaufnehmen
  (Diese beiden Vorgänge ändern die Anzeige im Feld Status der jeweiligen Benutzersitzung)

Entstehungsbedingungen:

Keine.

Lebensdauer:

Solange der Zustand besteht.

Informationsgehalt:

Zeit:	Sofern die Anzeige über die Terminaldiensteverwaltung geschieht, sieht man bei aktiven Sitzungen die "Anmeldezeit", also Systemdatum und Systemzeit zu der diese Sitzung erstellt wurde.
Benutzer:	"Benutzername" und bei einer Terminalsitzung der Computername, von dem die Anmeldung ausgeführt wurde ("Clientname").
Sonstiges:	Feld "Sitzung" zeigt, ob es sich um eine lokale Anmeldung (Console) oder um eine Terminalsitzung (RDP-Tcp#xx) handelt; die eigene Sitzung wird statt durch ein weißes durch ein farbiges Icon (grün in der Terminaldiensteverwaltung, blau im Taskmanager) dargestellt. Im Falle einer Terminalverbindung lässt sich im Feld Status ablesen, ob die Verbindung "Aktiv" ist, oder gerade keine Verbindung besteht "Getrennt" bzw. "Verbindung getrennt".

Verfügbarkeit:

Nur online verfügbar.

Auswertung:

Nach Aufruf des Taskmanagers taskmgr.exe muss in die Registerkarte "Benutzer" gewechselt werden.
Bei Verwendung der Terminaldiensteverwaltung tsadmin.exe muss zwischen den Registerkarten Benutzer und Sitzungen gewechselt werden, um an alle oben beschriebenen Informationen zu gelangen (Feld "Sitzung" nur in der Registerkarte Benutzer, „Clientname“ dagegen nur in der Registerkarte Sitzungen)

Aufwand:

Gering.

Fehlinterpretation:

Gering.
Anhand der Informationen kann entschieden werden, um welchen Anmeldetyp es sich handelt.

Fälschung:

Programmmanipulation.
Die Programme müssten jeweils durch manipulierte Versionen ersetzt werden, die z.B. bestimmte Benutzer nicht mehr anzeigen.

Quelle:
Aktuell bestehende Benutzersitzungen - Registryeinträge.....regedit.exe; (regview.exe)

Beschreibung der Quelle:

Eine Liste aller Benutzer die zurzeit aktiv am Systemgeschehen teilnehmen: Im Gegensatz zu den aktuellen Benutzersitzungen, die von dem Task-Manager bzw. tsadmin.exe angezeigt werden, sind hier nicht nur die lokal und per Terminalserver eingeloggten Benutzer aufgelistet, sondern auch alle Benutzer unter deren Kennung mindestens ein (über „Ausführen als“ gestarteter) Prozess läuft.

Verursachende Vorgänge:

- AD Benutzeranmeldung an Active Directory / AD Benutzerabmeldung vom Active Directory
  (Die Einträge zeigen auch an einem Domänencontroller nur die lokal oder über Terminalclient eingeloggten Benutzer und von diesen am betrachteten Rechner gestarteten Prozesse, jedoch nicht die lokalen Benutzer an Clients an, die sich über den Domänencontroller nur authentifiziert haben.)
- Benutzeranmeldung / Benutzerabmeldung
- Programm starten (Ausführen als) / Programm beenden (Ausführen als)
- Terminalsitzung erstellen / Terminalsitzung beenden

Entstehungsbedingungen:

Keine.

Lebensdauer:

Solange der Zustand besteht.

Informationsgehalt:

Benutzer: Benutzer-SID und Benutzername.
Sonstiges: Jeder angezeigte Benutzer führt mindestens einen Prozess auf dem Rechner aus.
In Verbindung mit anderen Quellen kann festgestellt werden, ob er lokal oder über Terminalserver angemeldet ist oder seine Benutzerrechte nur für die Ausführung eines Prozesses nutzt.

Verfügbarkeit:

Nur online verfügbar.
Diese Bereiche der Registry stellen die aktuell angemeldeten Benutzer dar. Beim Herunterfahren des Systems erlischt die Anmeldung. Auch im Sonderfall, dass der Computer nicht normal heruntergefahren wurde, sondern im laufenden Betrieb ausgeschaltet wurde, kann nicht offline ausgewertet werden, wer zu diesem Zeitpunkt angemeldet war. Diese Teile der Registry verweisen auf das Benutzerprofil ntuser.dat des jeweiligen Benutzers, das auch offline bestehen bleibt, aber die Verknüpfung welcher Benutzer angemeldet ist, also welche ntuser.dat im Registrybaum gemountet werden soll, existiert nur im Arbeitsspeicher und geht somit verloren.

Auswertung:

Unter HKEY_USERS finden sich alle aktiven Benutzer aufgelistet. Einträge der Form S-1-5-xx oder S-1-5-xx_Classes sind systemspezifische Benutzer. Interessant sind die Einträge der Form S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxx-xxx(x) und ein jeweils gleichlautender Eintrag der Form S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxx-xxx(x)_Classes.
Diese Zahlenkombination entspricht dem Security Identifier (SID - siehe Anhang Kapitel 7.2.1). Diese sind normalerweise nicht für die weitere Verwendung geeignet, aber auch der reguläre Benutzername lässt sich in den Unterpfaden des erstgenannten Schlüssels finden. Im Unterschlüssel ..\Software\Microsoft\Windows\CurrentVersion\Explorer\ steht der Benutzername im Wert „Logon User Name“ und im Unterschlüssel ..\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\ steht er in den verschiedenen Werten, die auf das Benutzerverzeichnis verweisen, das den Benutzernamen enthält.

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Programmmanipulation.
Um den eigentlichen SID Eintrag zu fälschen, ist außer der Manipulation der Anzeigeprogramme nichts bekannt. Selbst mit Zugriff auf die Registrybäume kann man sie nicht komplett löschen, da sie gerade in Verwendung sind. Außerdem würden durch die Löschung die Einstellungen des Benutzers entfernt, so dass nicht nur die Informationen nicht mehr angezeigt würden, sondern das Benutzerprofil auch unbrauchbar wäre.

Quelle:
Aktuell bestehende Freigaben - Anzeige .....filesvr.msc/fsmgmt.msc; net.exe share; explorer.exe

Beschreibung der Quelle:

Eine Liste aller freigegebenen Verzeichnisse und Drucker des Computers.

Verursachende Vorgänge:

- Verzeichnisfreigabe erstellen / Verzeichnisfreigabe beenden

Entstehungsbedingungen:

Keine.

Lebensdauer:

Solange der Zustand besteht.

Informationsgehalt:

Sonstiges: Freigabenamen und dahinter stehende Verzeichnisse (nicht beim Explorer).
Bei filesvr.msc/fsmgmt.msc ist außerdem ersichtlich, wie viele Clients aktuell auf diese Freigabe zugreifen.

Verfügbarkeit:

Nur online verfügbar.

Auswertung:

Nach Aufruf von „Freigegebene Ordner“ (filesvr.msc bei Windows 2003 Server / fsmgmt.msc bei Windows XP und Windows 2000) ist in die Ansicht "Freigaben (lokal)" zu wechseln, um die tabellarische Übersicht zu erhalten. Oder man lässt sich die Übersicht über den Aufruf von net.exe share ausgeben.
Versteckte Freigaben, die nicht im Explorer angezeigt werden, sind an einem Dollarzeichen $ nach dem Namen der Freigabe zu erkennen.

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Programmmanipulation.
Die Programme müssten jeweils durch manipulierte Versionen ersetzt werden, die z.B. bestimmte Freigaben nicht mehr anzeigen.

Quelle:
Aktuell bestehende Freigaben - Registryeinträge .....regedit.exe; (regview.exe)

Beschreibung der Quelle:

In der Registry befindet sich für die freigegebenen Verzeichnisse des Computers jeweils ein Eintrag im Pfad HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Sevices\lanmanserver\Shares\.
Hier fehlen jedoch die Administratorfreigaben wie C$.

Verursachende Vorgänge:

- Verzeichnisfreigabe erstellen / Verzeichnisfreigabe beenden

Entstehungsbedingungen:

Keine.

Lebensdauer:

Solange der Zustand besteht.
Mit Beendigung der Freigabe z.B. über den Explorer verschwinden auch die Einträge sofort. Jedoch werden manuelle Änderungen in der Registry selbst (z.B. mit regedit) erst nach einem Neustart aktiv.

Informationsgehalt:

Sonstiges: Freigabenamen und dahinter stehende Verzeichnisse

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Die Registry ist im Schlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Sevices\lanmanserver-\Shares\ zu öffnen. Für jede Freigabe existiert ein Wert vom Typ REG_MULTI_SZ, in dem sich als Textinhalt u. a. der Pfad des Verzeichnisses im lokalen Dateisystem in der dritten Zeile unter Path= findet.
Für die Offlineanalyse ist die Datei C:\Windows\System32\config\system mit einem geeigneten Programm wie regview.exe, das die Registrystruktur beherrscht zu untersuchen. Als Einstiegspunkt befindet man sich in der Datei sofort im Unterschlüssel HKEY_LOCAL_MACHINE\SYSTEM\.
Mehr zur Registry im Kapitel 7.1.1 im Anhang.

Aufwand:

Gering.

Fehlinterpretation:

Hoch.
Es werden nur die von Benutzern angelegten, nicht die vom System standardmäßig erzeugten Freigaben angezeigt. Außerdem werden diese Einstellungen, falls sie einfach über die Registry geändert werden, erst nach einem Neustart aktiv, siehe Fälschung.

Fälschung:

Administratorrechte.
Die Einträge in der Registry selbst sind mit entsprechenden Rechten änderbar. Da die Registryeinträge nur beim Systemstart ausgelesen werden, können diese geändert werden, ohne bis zum nächsten Neustart aktiv zu werden. Deshalb sollte zusätzlich die Quelle „Aktuell bestehende Freigaben – Anzeige“ ausgewertet werden, die den realen Systemzustand liefert.

Quelle:
Aktuell existierende Benutzer und Gruppen im Active Directory..... ..... dsa.msc; net.exe user; net.exe localgroup; net.exe group, dsquery.exe user; dsquery.exe group

Beschreibung der Quelle:

Über dsa.msc und die Befehle net.exe bzw. dsquery.exe mit den angegebenen Parametern finden sich Informationen zu allen Benutzern und den globalen und lokalen Gruppen, wenn das Active Directory auf dem betreffenden Computer installiert ist.

Verursachende Vorgänge:

- AD Benutzer anlegen
- AD Benutzer löschen
- AD Benutzer umbenennen
- AD Benutzer von globaler Gruppe entfernen
- AD Benutzer von lokaler Gruppe entfernen
- AD Benutzer zu globalen Gruppe hinzufügen
- AD Benutzer zu lokaler Gruppe hinzufügen
- AD Benutzereigenschaften ändern
- AD Globale Gruppe anlegen
- AD Globale Gruppe löschen
- AD Globale Gruppe umbenennen
- AD Lokale Gruppe anlegen
- AD Lokale Gruppe löschen
- AD Lokale Gruppe umbenennen

Entstehungsbedingungen:

Spezielle.
Nur zutreffend, wenn Active Directory auf diesem Computer installiert ist.

Lebensdauer:

Solange der Zustand besteht.

Informationsgehalt:

Benutzer: Anzeige der existierenden Benutzer und der globalen und lokalen Gruppen mit ihren jeweiligen Eigenschaften.

Verfügbarkeit:

Nur online verfügbar.
Zwar existieren die Datenbankdateien selbst auch offline. Da deren Formate nicht öffentlich dokumentiert sind, können die in diesen Dateien enthaltenen Informationen bei einer Offlineauswertung allenfalls bruchstückhaft interpretiert werden.

Auswertung:

Zur Anzeige von Benutzern oder Gruppen
- Aufruf des Fensters „Active Directory-Benutzer und –Computer“ (dsa.msc) und Wechsel in die entsprechenden Organisationseinheiten, die die zu untersuchenden Elemente enthalten

oder Ausführung eines der Befehle
- net.exe mit den Parametern user, group oder localgroup und
- dsquery.exe mit den Parametern user, group.

Die Ausgabe über den net-Befehl liefert nur Benutzer oder Gruppen aus der Organisationseinheit „Users“.

Über die Eigenschaften der Objekte in dsa.msc bzw. den Aufruf net user|localgroup|group ergänzt um den Benutzernamen/Gruppennamen, deren Informationen angezeigt werden sollen, erhält man auch die jeweiligen Gruppenmitgliedschaften. Über dsa.msc stehen insgesamt mehr Informationen zur Verfügung als beim net Befehl. Auch der dsquery-Befehl kann sehr vielfältige Informationen liefern. Eine Beschreibung über die diesbezüglichen Abfragemöglichkeiten finden sich unter Aufruf von dsquery.exe /?.

Auswertung Fortsetzung:

Die Datenbankdateien in denen die Daten gespeichert sind, finden sich im Verzeichnis Windows\NTDS\. Außer dem eigentlichen Datenfile ntds.dit existieren die Transaktionslogs und Checkpunktdateien edb.chk, edb.log, res1.log, res2.log und temp.edb. Eine genauere Beschreibung des Zwecks dieser Dateien, deren Format bisher nicht öffentlich dokumentiert ist, findet sich unter [Bosw03].

Aufwand:

Gering.

Fehlinterpretation:

Gering.
Dabei ist allerdings zu berücksichtigen, dass sich die Benutzer und Gruppen in einer großen Organisation in einer vielfältig gegliederten Struktur von Organisationseinheiten befinden können und deshalb im Fenster dsa.msc der gesamte Baum durchsucht werden muss. Bei der Ausgabe über den net-Befehl ist dagegen zu beachten, dass nur Benutzer oder Gruppen aus der Organisationseinheit „Users“ angezeigt werden.

Fälschung:

Programmmanipulation.

Die Programme müssten jeweils durch manipulierte Versionen ersetzt werden, die z.B. bestimmte Benutzer nicht mehr anzeigen.

Quelle:

Aktuell existierende lokale Benutzer und Gruppen – Anzeige ....lusrmgr.msc; net.exe user; net.exe localgroup

Beschreibung der Quelle:

Über lusrmgr.msc bzw. mit dem net.exe Befehl mit den angegebenen Parametern finden sich Informationen zu allen Benutzern und den lokalen Gruppen des Computers.

Verursachende Vorgänge:

- Benutzer anlegen
- Benutzer löschen
- Benutzer umbenennen
- Benutzer von lokaler Gruppe entfernen
- Benutzer zu lokalen Gruppe hinzufügen
- Benutzereigenschaften ändern
- Lokale Gruppe anlegen
- Lokale Gruppe löschen
- Lokale Gruppe umbenennen

Entstehungsbedingungen:

Spezielle.
Nicht zutreffend, wenn Active Directory auf diesem Computer installiert ist.

Lebensdauer:

Solange der Zustand besteht.

Informationsgehalt:

Benutzer: Anzeige der existierenden Benutzer und der lokalen Gruppen mit ihren jeweiligen Eigenschaften.

Verfügbarkeit:

Nur online verfügbar.

Auswertung:

Zur Anzeige von Benutzern oder Gruppen

- Aufruf des Fensters „Lokale Benutzer und Gruppen“ (lusrmgr.msc) und Wechsel in den Unterast Benutzer bzw. Gruppen
- oder Ausführung des Befehls net.exe mit den Parametern user oder localgroup.

Über die Eigenschaften der Objekte in lusrmgr.msc bzw. den Aufruf net user|localgroup ergänzt um den Benutzernamen/Gruppennamen, deren Informationen angezeigt werden sollen, erhält man auch die jeweiligen Gruppenmitgliedschaften. Über lusrmgr.msc stehen insgesamt mehr Informationen zur Verfügung als beim net Befehl.

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Programmmanipulation.
Die Programme müssten jeweils durch manipulierte Versionen ersetzt werden, die z.B. bestimmte Benutzer nicht mehr anzeigen.

Quelle:
Aktuell existierende lokale Benutzer und Gruppen - Registryeinträge.....regedit.exe; (regview.exe)

Beschreibung der Quelle:

Die Informationen aller lokal verwalteter Benutzer und lokalen Gruppe werden in der Registry im Schlüssel HKEY_LOCAL_MACHINE\SAM\SAM\Domains gespeichert.

Verursachende Vorgänge:

- Benutzer anlegen
- Benutzer ändert sein Passwort
- Benutzer löschen
- Benutzer umbenennen
- Benutzer von lokaler Gruppe entfernen
- Benutzer zu lokalen Gruppe hinzufügen
- Benutzereigenschaften ändern
- Benutzerpasswort festlegen
- Lokale Gruppe anlegen
- Lokale Gruppe löschen
- Lokale Gruppe umbenennen

Entstehungsbedingungen:

Spezielle.
Nicht zutreffend, wenn Active Directory auf diesem Computer installiert ist. In diesem Fall finden sich hier nur die Standardbenutzer lokaler Administrator und Gast. Alle anderen Einträge werden in der Active Directory-Datenbank verwaltet.

Lebensdauer:

Solange der Zustand besteht.

Informationsgehalt:

Benutzer: Anzeige der existierenden Benutzer und der lokalen Gruppen mit ihren jeweiligen Eigenschaften. Allerdings liegen nicht alle Informationen im Klartext vor und die Kodierung der Einträge ist bisher nicht vollständig öffentlich dokumentiert.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

In dem Abschnitt der Registry, die die lokale Benutzerdatenbank enthält, besteht standardmäßig auch für Administratoren weder Schreib noch Leserecht. Da der Benutzer „SYSTEM“ die erforderlichen Rechte besitzt, lässt sich mit einem kleinen Trick jedoch auch darauf Zugriff verschaffen:
Durch einen zeitversetzten Start von regedit im interaktiven Modus mit Hilfe des Kommandos „at“ (z.B. Eingabe des Befehls „at 13:06 /interactive regdit.exe“ um 13:05 Uhr), das nur von Administratoren ausgeführt werden kann, erhält man einen regedit Prozess der unter dem Konto SYSTEM läuft und auf die sonst unzugänglichen Einträge zugreifen kann.

Der Schlüssel HKEY_LOCAL_MACHINE\SAM\SAM\Domains (Datei C:\Windows\System32\config\SAM) ist zunächst in die Unterschlüssel

- „Account“ für selbst angelegte Objekten und
- „BuiltIn“ für standardmäßig existierende Objekte geteilt.

Diese beiden Schlüssel sind nach folgendem Schema aufgebaut:

- Unterschlüssel „Users“ mit einer Struktur, die die Benutzer enthält,
- Unterschlüssel „Aliases“ mit einer Struktur, die die lokalen Gruppen enthält,
- Unterschlüssel „Groups“ mit einer Struktur, die ausschließlich im Pfad Accounts\Groups die intern verwendeten Gruppe „Kein“ enthält.

Zu beachten ist, dass sich die lokalen Gruppen nicht im Unterschlüssel „Groups“ befinden. Diese Struktur ist ein Überbleibsel aus älteren Windowsversionen und bleibt aus Gründen der Kompatibilität erhalten.

In Users bzw. Aliases existieren für die Benutzer bzw. Gruppen

- Schlüssel mit achtstelligen Hexcode Namen wie 000001F4 und
- ein Schlüssel „Names“, in dem sich Schlüssel mit den Namen aller Benutzer bzw. Gruppen im Klartext finden.

In dem Schlüssel „Names“ finden sich jedoch nicht die eigentlichen Benutzerdaten, sondern nur Verweise auf die genannten Hexcodenamen.
In den Hexcodeschlüssel befinden sich für den jeweiligen Benutzer zwei Werte vom Typ REG_BINARY mit den Namen V und F bzw. für die jeweilige Gruppe ein Wert dieses Typs mit dem Namen C.
Die Kodierung des Binärformates dieser Werte ist allerdings bisher nicht öffentlich dokumentiert.
Einige Texte wie der „Vollständige Name“ und die „Beschreibung“ des Benutzerkontos können hier jedoch abgelesen werden, da diese als reiner Text im Wert stehen. Die weiteren Einstellungen sind aber nicht ersichtlich.

Aufwand:

Gering.
Die Namen der Benutzer und Gruppen sind leicht ersichtlich.
Bei der Bewertung des Aufwandes bleibt außer Betracht, dass die Entschlüsselung der weiteren Eigenschaften solange nur mit sehr hohem Aufwand möglich ist, bis eine Veröffentlichung des entsprechenden Codes erfolgt.

Fehlinterpretation:

Gering.

Fälschung:

Administratorrechte.
Sofern Administrationsrechte vorliegen und damit über das beschriebene at-Kommando Systemrechte erlangt werden, können die Einträge in der Benutzerdatenbank geändert und damit Anzeigen über die Quelle erzeugt werden, die nicht die entsprechende Funktionalität besitzen.

Quelle:
Aktuell geöffnete Netzwerkports.....netstat.exe -ao

Beschreibung der Quelle:

Der Shell-Befehl netstat -a zeigt alle bestehenden TCP-Verbindungen an und alle geöffneten Ports (TCP und UDP) an.

Verursachende Vorgänge:

- TCP Verbindung aufbauen oder Port öffnen

Entstehungsbedingungen:

Keine.

Lebensdauer:

Solange der Zustand besteht.

Informationsgehalt:

Benutzer: Unter Zuhilfenahme zusätzlicher Quellen (siehe Auswertung) kann der Benutzer ermittelt werden, der das kommunizierende Programm gestartet hat.

Sonstiges:
- Lokale Portnummer,
- Remoteadresse, Remoteportnummer und Status der Verbindung (nur bei TCP-Verbindungen),
- Prozessnummer des Programms, das die jeweilige Netzwerkverbindung verwendet.

Verfügbarkeit:

Nur online verfügbar.

Auswertung:

Die Ausgabe des „netstat.exe -ao“ Befehls liefert eine Liste mit den bestehenden TCP Verbindungen inklusive deren Status, alle geöffneten TCP und UDP Ports und (wegen des Parameters o) die jeweils zugehörige Prozesskennung des verantwortlichen Prozesses.
Über die Verwendung der Quelle "Aktuell laufende Prozesse" kann - wie auf Seite 53 beschrieben - sowohl auf den Prozessnamen als auch auf den Benutzer des Prozesses geschlossen werden.

Aufwand:

Hoch.
Bei bestehender Internetverbindung nehmen viele Anwendungsprogramme und Betriebssystemfunktionen automatisch Verbindung zu bestimmten Servern auf. Ebenso bestehen viele geöffnete Ports wegen Funktionen die auf Kontaktaufnahme warten. Um die Ausgabe interpretieren zu können, sind also mehr Informationen zu den Prozessen als auch zu den IP-Adressen zu ermitteln.

Fehlinterpretation:

Hoch.
Siehe Beschreibung beim Aufwand. Gefahr hoch zwischen den "normalen" Verbindungen etwas Gefährliches, wie die Verbindung eines Trojaners zu übersehen. Dies steht auch in Verbindung damit, dass die zugeordneten Prozessnamen nur begrenzt aufschlussreich sind (Siehe auch die Quellenbewertung für "Aktuell laufende Prozesse").

Fälschung:

Programmmanipulation.
Es ist denkbar Netstat.exe durch eine manipulierte Version austauschen, die z.B. einen Teil der Verbindungen nicht mehr anzeigt.

Quelle:
Aktuell laufende Prozesse.....taskmgr.exe; tsadmin.exe; tasklist.exe; (procexp.exe)

Beschreibung der Quelle:

Die Programme taskmgr.exe, tsadmin.exe und tasklist.exe liefern eine Liste aller aktuell laufenden Prozesse. Für einen einzelnen laufenden Prozess kann das Programm procexp.exe [RuCo04] genauere Auskunft geben.

Verursachende Vorgänge:

- Programm (mit "Ausführen als") starten / Programm (mit "Ausführen als" gestartet) beenden
- Programm (mit aktuellem Benutzer) starten / Programm (mit aktuellem Benutzer gestartet) beenden

Entstehungsbedingungen:

Keine.

Lebensdauer:

Solange der Zustand besteht.

Informationsgehalt:

Benutzer: "Benutzername" mit dessen Rechten der Prozess läuft.
Sonstiges: Der Dateiname des Prozesses ("Name", "Image" oder "Abbildname", je nach verwendetem Anzeigeprogramm) und zusätzliche Informationen, z.B. der Arbeitsspeicherbedarf des Prozesses und die Prozessnummer;
Falls es sich um einen Prozess handelt, der ein grafisches Windowsfenster erzeugt, lässt sich der Name des zum Prozess gehörenden Fensters bzw. der Prozessname für ein bestimmte Fenster ermitteln.

Verfügbarkeit:

Nur online verfügbar.

Auswertung:

- Beim Taskmanager (taskmgr.exe) ist in die Registerkarte "Prozesse" zu wechseln, um alle Prozesse mit ihren jeweiligen Benutzernamen anzuzeigen. Die Registerkarte "Anwendungen" zeigt dagegen nur die Prozesse mit ihrem Fenstertitel an, die ein eigenes Fenster auf dem Bildschirm öffnen. Um für ein bestimmtes angezeigtes Fenster den Prozessnamen zu finden, kann in der Ansicht "Anwendungen" mit einem Klick auf den jeweiligen Fenstertitel aus dem Kontextmenü "zu Prozess wechseln" ausgewählt werden. Es wird zur Registerkarte "Prozesse" gewechselt und der betreffende Prozess ist markiert.
- Bei der Terminaldiensteverwaltung (tsadmin.exe) zeigt die Registerkarte "Prozesse" wie im Taskmanager alle laufenden Prozesse an.
- Die Ausgabe des in der Eingabeaufforderung gestarteten Shell-Befehls tasklist.exe zeigt eine Liste aller laufenden Prozesse. Unter Verwendung der Option /v wird zusätzlich der Benutzername für jeden Prozess und bei Prozessen die Fenster erzeugen der jeweiligen Fenstertitel angezeigt.

Hier lässt sich jeweils auch die Prozessnummer des jeweiligen Prozesses ablesen, was z.B. für die Zuordnung der Prozessnummer aus anderen Quellen von Belang ist. Ein Beispiel dafür ist die Quelle "Aktuell geöffnete Netzwerkports", die nur eine zuordnungsbedürftige Prozessnummer liefert.

Allerdings wird hier bei den Prozessen jeweils nur der Dateiname der gestarteten Prozesse angezeigt. Um auch an den Pfad der zugehörigen Programmdatei zu kommen, kann eine Suche nach der Datei durchgeführt werden, was aber nicht immer eindeutig ist, wenn mehrere Dateien mit selben Namen gefunden werden. In einigen Fällen kann hier auch der Vergleich mit den automatisch gestarteten Prozessen beim Systemstart bzw. der Benutzeranmeldung (siehe dortige Quellen) Erkenntnisse bringen. Mit dem Zusatzprogramm Process Explorer [RuCo04] kann bei Anzeige der DLLs neben dem Dateinamen auch der Pfad der verwendeten Datei abgelesen werden.

Auswertung Fortsetzung:

Um an Informationen über die Funktionalität weitverbreiteter Prozesse zu gelangen, können die Sammlung der „Namen von wichtigen Prozessen" im Kapitel 7.2.3 des Anhangs und die dort angegebenen Verweise eingesetzt werden. Aussagekraft besitzen diese Informationen jedoch nur für solche Dateien, deren Dateinamen unverändert sind. Falls daran Zweifel bestehen, bleibt außer dem aufwendigen Studieren des Maschinencodes gegebenenfalls nur eine überwachte Ausführung des jeweiligen Programms auf einem isolierten System.

Aus den genannten Gründen empfiehlt sich die Dokumentation der im Normalzustand laufenden Prozesse, um bei später auftretenden Problemen eine Vergleichsbasis zu besitzen.

Aufwand:

Gering.
Allerdings erhält man nur die Namen der Programmdateien der Prozesse. Eine Analyse der Funktionalität des Programms wäre weit komplizierter, da dies letztendlich ein Studium des Programmcode erfordern würde.

Fehlinterpretation:

Hoch.
Da die Quelle nur die Namen der Programmdateien liefert und permanent neue Programme in Umlauf kommen, besteht die Gefahr, nicht das richtige Programm unter dem Namen zu vermuten.

Fälschung:

Leicht.
Wenn man verhindern wollte, dass ein gestartetes Programm in den genannten Werkzeugen überhaupt nicht angezeigt wird, müsste man die Programme durch eine manipulierte Version ersetzen. Dies ist allerdings nicht erforderlich, da die Werkzeuge nur den Dateinamen der Programme anzeigen. Zur Vertuschung ist es deshalb ausreichend, das zu startende Programm auf einen generischen Namen umzubenennen, um keinen Verdacht zu erregen.

Quelle:
Aktuell verwendete Dateien und Verzeichnisse von Netzwerkbenutzern..... ..... net.exe file; net.exe session; filesvr.msc/fsmgmt.msc;

Beschreibung der Quelle:

Der Befehl net.exe mit Parameter file zeigt alle mit dem Windows Standardprotokoll von anderen Computern über ein Netzwerk verwendeten Verzeichnisse und Dateien an. Net.exe session zeigt dabei den zugreifenden Rechner (IP-Adresse oder Hostname) an. Selbiges ist in der graphischen Oberfläche mit „Freigegebene Ordner“ (filesvr.msc bei Windows 2003 Server / fsmgmt.msc bei Windows XP und Windows 2000) unter „Geöffnete Dateien“ bzw. „Sitzungen“ möglich.

Verursachende Vorgänge:

- Entfernter Datei-/Verzeichniszugriff

Entstehungsbedingungen:

Spezielle.
Zugriff unter Verwendung des Windows Standardprotokolls.

Lebensdauer:

Solange der Zustand besteht.

Informationsgehalt:

Zeit:	Durch die Anzeige der "Verbindungszeit" (filesvr.msc/fsmgmt.msc) kann in Verbindung mit der aktuellen Systemzeit des Dateiservers die Zeit ermittelt werden, wann der Zugriff begonnen hat
Benutzer:	Der Benutzername mit dem sich die Person an dem Dateiserver angemeldet hat (muss nicht gleich dem Benutzernamen auf dem Computer sein, auf dem er lokal angemeldet ist). IP-Adresse oder Hostname ("Computer") von der der Benutzer kommt.
Sonstiges:	Auf welche Dateien/Verzeichnisse zugegriffen wird ("Pfad" bzw. "Geöffnete Datei").

Verfügbarkeit:

Nur online verfügbar.

Auswertung:

Aufruf von filesvr/fsmgmt.msc und Wechsel in den Unterast „Geöffnete Dateien“ bzw. „Sitzungen“ oder Betrachten der Ausgabe von net.exe file bzw. net.exe session.

Aufwand:

Gering.

Fehlinterpretation:

Hoch.
Zu beachten ist aber, dass hier nur der über das Standardprotokoll von Windows ausgetauschte Dateiverkehr angezeigt wird. Zugriffe die über eigene installierte Programme mit anderem Protokollformat, wie z.B. ftp erfolgen, werden hier nicht angezeigt.

Fälschung:

Programmmanipulation.
Die Programme müssten jeweils durch manipulierte Versionen ersetzt werden, die z.B. Zugriffe auf bestimmte Freigaben nicht mehr anzeigen.
Sofern der Zugang zum System und die Berechtigung zum Starten von Programmen gegeben ist, lassen sich Programme starten, die Netzwerkzugriffe mittels sonstiger Protokolle ermöglichen. Solche Zugriffe bleiben bei einer Untersuchung dieser Quelle selbst dann verborgen, wenn keinerlei Veränderungen an den Werkzeugen vorgenommen worden.

Quelle:
Aktueller Netzwerkverkehr - Anzeige ..... taskmgr.exe

Beschreibung der Quelle:

Im Task-Manager (taskmgr.exe) wird in der Registerkarte Netzwerk die aktuelle Auslastung der Netzwerkverbindung angezeigt und für kurze Zeit protokolliert. Diese Registerkarte existiert nur bei Windows XP und Windows 2003 Server, nicht jedoch bei Windows 2000.

Verursachende Vorgänge:

- Netzwerkverkehr verursachen

Entstehungsbedingungen:

Keine.

Lebensdauer:

Speziell.
Die Größe des Netzwerkverkehrs wird für die Dauer des Programmlaufes protokolliert und bleibt jeweils für zirka eine Minute und längstens bis zur Beendigung des Programms gespeichert.

Informationsgehalt:

Sonstiges: Bestehender Netzwerkverkehr in Prozent der maximalen Übertragungsrate, wobei die laufend wechselnde Netzwerkauslastung als jeweils aktuell gültiger Zahlenwert und der Verlauf der letzten Minute in einer kurzen Historie graphisch dargestellt wird.

Verfügbarkeit:

Nur online verfügbar.

Auswertung:

Betrachten der grafischen Anzeige unter taskmgr.exe, Registerkarte Netzwerk (nur bei Windows XP und Windows 2003 Server, nicht bei Windows 2000).

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Programmmanipulation.
Das Programm müsste durch eine manipulierte Version ersetzt werden, die z.B. falsche Anzeigen erzeugt.

Quelle:
Auslagerungsdatei ..... (Hexeditor)

Beschreibung der Quelle:

Für den Fall, dass der physische Arbeitsspeicher nicht ausreicht, werden Seiten des Arbeitsspeichers in diese Datei ausgelagert.

Verursachende Vorgänge:

Zum einen ist festzustellen, dass im Arbeitsspeicher sowohl Informationen zu Benutzervorgängen als auch zu verarbeiteten Daten aufgefunden werden können, sofern eine Auslagerung der entsprechenden Seiten des Arbeitsspeichers stattgefunden hat. Zum anderen beeinflussen alle arbeitsspeicherrelevanten Vorgänge gegebenenfalls das Auslagern von Seiten des Arbeitsspeichers und können damit das Beschreiben und das Überschreiben der Auslagerungsdatei verursacht.

Entstehungsbedingungen:

Spezielle.
Die Auslagerungsdatei ist aktiviert und der Umfang der Rechneraktivität erfordert die Auslagerung von Seiten des Arbeitsspeichers.

Lebensdauer:

Speziell.
Je nach den laufenden Vorgängen können ausgelagerte Seiten wiedereingelagert und dann auch überschrieben werden. Sollten sie jedoch bis zum Untersuchungszeitpunkt noch nicht überschrieben sein, stehen sie für eine Auswertung zur Verfügung.

Informationsgehalt:

Sonstiges: Theoretisch alles was aus dem Arbeitsspeicher ausgelagert wurde. Praktisch lassen sich hier jedoch nur die Inhalte interpretieren, denen ihr Darstellungscode zugeordnet werden kann. Dies gelingt wohl am häufigsten bei Texten, die mit den gebräuchlichen Codes dargestellt sind.

Verfügbarkeit:

Online und offline verfügbar.
Im Onlinemodus ist jedoch höchste Vorsicht vor unbeabsichtigter Überschreibung geboten.

Auswertung:

Die Datei c:\pagefile.sys ist auf die gesuchten Textfragmente oder sonstige vermutete Inhalte z.B. mit einem Hexeditor zu untersuchen.

Aufwand:

Hoch.
Die typische Größe der Auslagerungsdatei beträgt mehrere hundert Megabyte. Ohne eine zielgerichtete automatisierte Suche ist dafür enormer Zeitaufwand erforderlich. Die automatisierte Suche setzt zunächst voraus, dass die Untersuchungsperson durch Versuche einen Überblick über die gespeicherten Informationen erlangt und damit geeignete Suchwörter generiert.

Fehlinterpretation:

Hoch.
Da das Auslagern und damit das Überschreiben von sehr vielen Größen abhängig sind, ist das Zurückbleiben und damit das Auffinden ehemals im Arbeitsspeicher gehaltener Daten sehr vom Zufall abhängig.

Fälschung:

Administratorrechte.
Mit Administrationsrechten kann die Auslagerungsdatei deaktiviert werden. Damit wird allerdings eine neue Quelle erzeugt und die Daten der Auslagerungsdatei gehen in die Quelle „Fragmente von Daten (Unallocated File Space, File Slack und Shadow Data)“ über. Weitere Information zu dieser auf dem entsprechenden Quellenblatt.
Auch ist eine Änderung der einzelnen Inhalte z.B. mit einem Hexeditor möglich.

Quelle:

Dateiattribut "Archiv" ..... explorer.exe; attrib.exe

Beschreibung der Quelle:

Das Dateiattribut "Archiv" einer Datei ist dazu bestimmt, Änderungen am Inhalt und am Speicherort der Datei anzuzeigen. Es wird von vielen Sicherungsprogrammen zur Feststellung benutzt, ob die Datei bei einer inkrementellen Sicherung mitzusichern ist.

Verursachende Vorgänge:

Dateiattribut wird gesetzt:
- Datei anlegen
- Datei kopieren (nur für neue Datei)
- Datei umbenennen
- Datei verschieben
- Dateiinhalt ändern

Dateiattribut kann je nach Benutzerwahl gesetzt oder rückgesetzt werden:
- Dateiattribute ändern

Bei einem Sicherungslaufs mit den meisten Sicherungsprogrammen wird das Attribut für alle gesicherten Dateien zurückgesetzt.

Entstehungsbedingungen:

Keine.

Lebensdauer:

Bis zum nächsten Vorgang.
Der Wert bleibt solange gesetzt bis das Dateiattribut manuell entfernt wird oder der nächste Backupdurchlauf das Dateiattribut zurücksetzt.

Informationsgehalt:

Zeit:	Indirekt, wenn Zeit des letzten Sicherungslaufes bekannt.
Sonstiges:	Nur der Fakt das einer der obigen Vorgänge durchgeführt wurde.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

In Kombination mit dem Wissen über den wahren Zeitpunkt des letzten Backupdurchlaufes mit einem Programm, das die Dateiattribute "Archiv" zurücksetzt (wie zum Beispiel das mitgelieferte Programm Start/Programme/Zubehör/Systemprogramme/Sicherung), kann vermutet werden, dass mindestens einer der genannten Vorgänge danach noch auf die Datei zugegriffen hat, wenn das Attribut gesetzt ist.

Aufwand:

Hoch.
Die Untersuchung ist nur sinnvoll, wenn ein passendes Sicherungsprogramm eingesetzt wurde. Dann muss die Zeit des letzten Sicherungslaufes ermittelt werden, in den diese Datei einbezogen war.

Fehlinterpretation:

Hoch.
Wenn das Attribut nicht gesetzt ist, heißt das allerdings nicht zwingend, dass die Datei seit der letzten Sicherung nicht verändert wurde, da die bei Änderungen an der Datei entstehende Setzung des Attributs wieder durch eine manuelle Löschung entfernt werden kann.

Fälschung:

Leicht.
Wenn die benötigten Rechte vorliegen, kann das Dateiattribut einfach entfernt werden.
Dies ist normal aber der Fall, wenn die oben angegebenen Vorgänge ausführbar sind.

Quelle:
Daten des Indexdienstes..... ciadv.msc

Beschreibung der Quelle:

Bei der Installation des Indexdienstes und Aktivierung der Indizierung für bestimmte Verzeichnisse werden die enthaltenen Dateien nach Stichwörtern indiziert um später eine schnellere Suche zu ermöglichen.
Da die Aktualisierung dieses Indexes nicht sofort nach der Änderung bzw. Löschung der Dateien stattfindet, lassen sich hier noch Informationen zum ehemaligen Inhalt und Namen geänderter bzw. nicht mehr vorhandener Dateien finden. Die Verwaltung und Durchsuchung kann über ciadv.msc oder über die Computerverwaltung compmgmt.msc Teilast „Dienste und Anwendungen“ Unterpunkt „Indexdienst“ erfolgen.

Verursachende Vorgänge:

Die Quelle selbst wird nicht direkt von den untersuchten Vorgängen erzeugt. Vielmehr werden die Indexdaten periodisch je nach Einstellungen angelegt.
Jedoch können dadurch Informationen zu Vorgängen verfügbar sein, die den Inhalt von Dateien ändern, wenn der Index noch nicht aktualisiert ist.

- Datei löschen
- Dateiinhalt ändern

Allerdings gilt dies nur für die Dateien, die vom Indexdienst indiziert werden (siehe Entstehungsbedingungen).

Entstehungsbedingungen:

Spezielle.
Das Verzeichnis muss für die Indizierung eingestellt sein, ein korrekter Durchlauf der Indizierung muss vor der Änderung oder Löschung der jeweiligen Datei abgeschlossen sein, danach darf die Indexdatei nicht mehr aktualisiert werden.
Standardmäßig werden nicht alle Dateitypen indiziert. Die einbezogenen Dateitypen hängen von den installierten Filtern ab; standardmäßig werden die gebräuchlichen Dateitypen wie txt, html, xml und die Microsoft Office Dateiformate einbezogen. Durch Aktivierung "Dateien mit unbekannter Erweiterung indizieren" kann die Indizierung auf alle Dateitypen erweitert werden, wobei nur Textbestandteile der Dateien indiziert werden.

Lebensdauer:

Speziell.
Jeder Durchlauf des Indexdienstes überschreibt die jeweiligen alten Indexdaten. Die Wiederholung der Indizierung einer Datei hängt von den Systemeinstellungen, vom Umfang der insgesamt zu indizierenden Dateien, der Systemleistung und der Systemauslastung ab. Je länger eine Indizierung zurückliegt, desto wahrscheinlicher ist die nächste Aktualisierung.

Informationsgehalt:

Sonstiges: Textinhalte und den Namen von Dateien die zum Zeitpunkt der Indizierung existierten.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Online kann eine Untersuchung dadurch erfolgen, dass einfach nach vermuteten Texten gesucht wird. Dies kann durch das Programm ciadv.msc jeweils mit dem Befehl "Katalog durchsuchen" eingeleitet werden.
Eine Suche nach einem Text bringt eine Liste mit allen Dateien und deren Pfaden, die im Katalog indiziert sind und diesen Text enthalten.

Die Indexdaten selbst werden in einem Verzeichnis mit Namen catalog.wci gespeichert. Hierin befinden sich mehrere Dateien, die z.B. unter [Micr96] einführend beschrieben sind.

Das für die Offlineanalyse erforderliche Dateiformat ist nicht bekannt. Jedoch können die Indexdateien auf ein lauffähiges System mit installiertem Indexdienst übertragen werden. Dort wird mit dem Verwaltungsprogramm ciadv.msc ein neuer Katalog erstellt, dieser auf das kopierte Verzeichnis verwiesen und damit die Suche durchgeführt werden. Dabei darf die Aktualisierung dieses Kataloges nicht gestartet werden und am besten sind diese Dateien mit einem Schreibschutz zu versehen, damit keine Änderungen vorgenommen werden können.

Aufwand:

Hoch.
Für manche Anwendungsfälle mag eine Suche nach Texten sehr erfolgsversprechend sein. In anderen Fällen wo genau der Inhalt einer bestimmten Datei nachvollzogen werden soll, ist dies mit beschriebener Methode nur eingeschränkt möglich, da alle relevanten Wörter durchprobiert werden müssten.
Hierfür benötigt man noch ein Programm, das die Indexstruktur so auslesen kann, dass für eine Datei alle enthaltenen Textstellen ausgegeben werden.

Fehlinterpretation:

Hoch.
Die in einer Datei gefundenen Wörter müssen vom Forensiker in der richtigen Reihenfolge kombiniert werden. Deshalb besteht die Gefahr, dass aus den Wörtern auf Inhalte geschlossen wird, die nicht dem ursprünglichen Inhalt entsprechen.

Fälschung:

Administratorrechte.
Nur mit Administratorrechten direkte Änderung dieser Dateien möglich.

Quelle:
Eintrag im Sicherheitsprotokoll der Kategorie "An-/Abmeldung".....eventvwr.msc

Beschreibung der Quelle:

Es handelt sich um einen Eintrag einer bestimmten Ereigniskennung der Kategorie "An-/Abmeldung" im Sicherheitsprotokoll. Die verschiedenen Ereigniskennungen wurden aufgrund ähnlicher Eigenschaften nicht als eigenständige Quellen auf separaten Blättern beschrieben.

Im Anhang der Arbeit findet sich ein extra Kapitel 7.1.2.7 zu den Einträgen dieser Kategorie.

Die Kriterien Lebensdauer, Verfügbarkeit und Fälschung sowie das allgemeine Vorgehen sind bei den Einträgen im Sicherheitsprotokoll aller Ereigniskennungen gleich und deshalb nur einmal bei der Quellenbeschreibung "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen" erwähnt.

Verursachende Vorgänge:

Die Vorgänge sind differenziert nach den jeweiligen erzeugten Ereigniskennungen dargestellt. Zu berücksichtigen ist, dass ein Teil der Vorgänge mehrere Einträge erzeugt.

Ereigniskennung 528 "Ein Benutzer hat sich erfolgreich an einem Computer angemeldet":
- AD Benutzeranmeldung an Active Directory (wird auf dem Client erzeugt)
- Benutzeranmeldung lokal
- Programm (mit "Ausführen als") starten
- Terminalsitzung erstellen
- Terminalsitzung wiederaufnehmen

Ereigniskennung 529 "Anmeldefehler: Ein Anmeldeversuch erfolgte mit einem unbekannten Benutzernamen oder einem bekannten Benutzernamen mit einem falschem Kennwort":
- AD Unberechtigter Anmeldeversuch Active Directory (wird auf dem Client erzeugt)
- Unberechtigter Anmeldeversuch

Ereigniskennung 530 "Anmeldefehler: Ein Anmeldeversuch erfolgte, wobei sich das Benutzerkonto außerhalb der zulässigen Zeit anzumelden versuchte":
- AD Unberechtigter Anmeldeversuch Active Directory (wird auf dem Client erzeugt)
- Unberechtigter Anmeldeversuch

Ereigniskennung 531 "Anmeldefehler: Ein Anmeldeversuch erfolgte mit einem deaktivierten Konto ":
- AD Unberechtigter Anmeldeversuch Active Directory (wird auf dem Client erzeugt)
- Unberechtigter Anmeldeversuch

Ereigniskennung 532 "Anmeldefehler: Ein Anmeldeversuch erfolgte mit einem abgelaufenen Konto":
- AD Unberechtigter Anmeldeversuch Active Directory (wird auf dem Client erzeugt)
- Unberechtigter Anmeldeversuch

Ereigniskennung 533 "Anmeldefehler: Ein Anmeldeversuch erfolgte durch einen Benutzer, der sich nicht an diesem Computer anmelden darf":
- AD Unberechtigter Anmeldeversuch Active Directory (wird auf dem Client erzeugt)
- Unberechtigter Anmeldeversuch

Ereigniskennung 534 "Anmeldefehler: Der Benutzer hat beim Anmelden einen unzulässigen Anmeldetyp verwendet":
- AD Unberechtigter Anmeldeversuch Active Directory (wird auf dem Client erzeugt)
- Unberechtigter Anmeldeversuch

Ereigniskennung 535 "Anmeldefehler: Das Kennwort für das angegebene Konto ist abgelaufen":
- AD Unberechtigter Anmeldeversuch Active Directory (wird auf dem Client erzeugt)
- Unberechtigter Anmeldeversuch

Ereigniskennung 536 "Anmeldefehler: Der Anmeldedienst ist nicht aktiv":
- AD Unberechtigter Anmeldeversuch Active Directory (wird auf dem Client erzeugt)
- Unberechtigter Anmeldeversuch

Ereigniskennung 537 "Anmeldefehler: Der Anmeldeversuch ist aus anderen Gründen fehlgeschlagen":
- AD Unberechtigter Anmeldeversuch Active Directory (wird auf dem Client erzeugt)
- Unberechtigter Anmeldeversuch

Ereigniskennung 538 "Der Abmeldevorgang wurde für einen Benutzer durchgeführt":
- AD Benutzerabmeldung vom Active Directory (wird auf dem Client und dem Server erzeugt)
- Benutzerabmeldung Netzwerk
- Programm (mit "Ausführen als" gestartet) beenden
- Terminalsitzung beenden
- Terminalsitzung wiederaufnehmen

Ereigniskennung 540 "Ein Benutzer hat sich erfolgreich an einem Netzwerk angemeldet":
- AD Benutzeranmeldung an Active Directory (Wird auf Server erzeugt)
- Benutzeranmeldung Netzwerk

Ereigniskennung 551 "Ein Benutzer hat den Abmeldevorgang gestartet":
- Benutzerabmeldung lokal
- Terminalsitzung beenden

Ereigniskennung 552 "Ein Benutzer hat sich mit expliziten Anmeldeinformationen erfolgreich an einem Computer angemeldet, wobei er bereits als ein anderer Benutzer angemeldet ist":
- Benutzeranmeldung lokal
- Programm (mit "Ausführen als") starten
- Terminalsitzung erstellen
- Terminalsitzung wiederaufnehmen

Ereigniskennung 682 "Ein Benutzer hat erneut eine Verbindung zu einer getrennten Terminalserversitzung hergestellt":
- Terminalsitzung wiederaufnehmen

Ereigniskennung 683 "Ein Benutzer hat eine Terminalserversitzung getrennt, ohne sich abzumelden":
- Terminalsitzung unterbrechen

Entstehungsbedingungen:

Spezielle.
In den Systemrichtlinien des Computers muss die Überwachungsrichtlinie "Anmeldeereignisse überwachen" folgendermaßen aktiviert sein:
Option "Erfolgreich" für folgende Ereigniskennungen:
528, 538, 540, 551, 552, 682, 683
Option "Fehlgeschlagen" für folgende Ereigniskennungen:
529-537
Standardmäßig aktiviert ist erfolgreiche Anmeldeereignisse überwachen.

Lebensdauer:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Informationsgehalt:

Zeit:
Systemdatum und Systemzeit des Vorgangs in den Feldern "Datum" und "Uhrzeit"

Benutzer:
Folgende Tabelle gibt Auskunft über die bei den verschiedenen Ereigniskennungen vorhandenen Informationen und die Felder, aus denen diese Einträge abzulesen sind.

	Benutzerkonto, das für die An-/Abmeldung verwendet wird	Angemeldeter Benutzer, der zusätzliche Anmeldung durchführte	IP-Adresse des Rechners, von dem die An-/Abmeldung ausging	Computername des Rechners, von dem die An-/Abmeldung ausging
528	„Benutzername“	-	- „Quellnetzwerkadresse“ beim Vorgang „Terminalsitzung erstellen“ oder „Terminalsitzung wiederaufnehmen“; - Wert 127.0.0.1 beim Vorgang „Benutzeranmeldung lokal“; - leeres Feld bei „Programm (mit "Ausführen als") starten“	-
529 - 537	„Benutzername“	-	„Quellnetzwerkadresse“	-
538	„Benutzername“	-	-	-
540	„Benutzername“	-	„Quellnetzwerkadresse“	„Arbeitsstationsname“ bei Eintrag für „AD Benutzeranmeldung an Active Directory“ auf dem Server
551	„Benutzername“	-	-	-
552	„Zielbenutzername“	„Benutzername“ - Beim Vorgang „Programm (mit "Ausführen als") starten“; - Beim Vorgang „Terminalsitzung erstellen“ oder „Terminalsitzung wiederaufnehmen“ steht hier nur der Computername gefolgt von einem $-Zeichen	„Quellnetzwerkadresse“ - Beim Vorgang „Terminalsitzung erstellen“ oder „Terminalsitzung „wiederaufnehmen“; - Feld leer beim erzeugenden Vorgang „Programm (mit "Ausführen als") starten “	-
682	„Benutzername“	-	„Clientadresse“	„Clientname“
683	„Benutzername“	-	„Clientadresse“	„Clientname“

Zu berücksichtigen ist, dass das scheinbar offensichtliche Feld "Benutzer" z.B. bei den Ereigniskennungen 529, 682 und 683 statt des Benutzernamens den Eintrag NT-AUTORITÄT\SYSTEM enthält.

Sonstiges:

(529-537): das Feld "Ereigniskennung" des Eintrages gibt Hinweise auf den Grund des Fehlschlages der Anmeldung.
(528, 529-537, 538, 540): Der "Anmeldetyp" im Textfenster gibt Hinweise auf die Art der Anmeldung (z.B. 2 für lokal, 3 für Active Directory, 8 für Netzwerk, 10 für Terminalsitzung; komplette Liste im Anhang)

Verfügbarkeit:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Auswertung:

Beim Auffinden eines bestimmten Eintrages sind alle unten genannten Fälle durchzugehen, in denen die vorliegende Ereigniskennung genannt ist, und es ist zu überprüfen, ob auch die sonstigen Bedingungen zutreffen. Die Reihenfolge der Ereigniskennungen ist so gewählt wie sie im Protokoll angelegt werden.

- Ereigniskennung 528:
  mit Anmeldetyp 2; kein zusätzlicher Eintrag 552; es handelt sich um einen Client der Teil einer Active Directory Struktur ist => AD Benutzeranmeldung an Active Directory
- Ereigniskennung 529 bzw. 530-537:
  => Unberechtigter Anmeldeversuch (über den Anmeldetyp lässt sich auf die Art der versuchten Anmeldung schließen);
- Ereigniskennung 538:
  mit Anmeldetyp 2 => Programm (mit "Ausführen als" gestartet) beenden oder AD Benutzerabmeldung vom Active Directory (auf Client erzeugt)
- Ereigniskennung 538:
  mit Anmeldetyp 3 => AD Benutzerabmeldung vom Active Directory (auf Server erzeugt)
- Ereigniskennung 538:
  mit Anmeldetyp 8 => Benutzerabmeldung Netzwerk
- Ereigniskennung 540:
  mit Anmeldetyp 8 => Benutzeranmeldung Netzwerk
- Ereigniskennung 540:
  mit Anmeldetyp 3; es handelt sich um einen Server mit Active Directory Funktionalität => AD Benutzeranmeldung an Active Directory (auf dem Server erzeugt)
- Ereigniskennung 551+538:
  beide Einträge mit dem selbem Benutzer und der Eintrag 538 mit Anmeldetyp 10 => Terminalsitzung beenden
- Ereigniskennung 551:
  kein zusätzlicher Eintrag 538 mit demselben Benutze r => Benutzerabmeldung lokal
- Ereigniskennung 552+528:
  beide Einträge mit IP-Adresse 127.0.0.1 und Eintrag 528 mit Anmeldetyp 2 => Benutzeranmeldung lokal
- Ereigniskennung 552+528:
  beide Einträge ohne IP-Adresse und Eintrag 528 mit Anmeldetyp 2 => Programm (mit "Ausführen als") starten;
- Ereigniskennung 552+528:
  beide Einträge mit selber IP-Adresse und Eintrag 528 mit Anmeldetyp 10, keine Einträge 538 und 682 => Terminalsitzung erstellen;
- Ereigniskennung 552+528+538+682:
  alle vier Einträge mit selber IP-Adresse, Einträge 528 und 538 mit Anmeldetyp 10 => Terminalsitzung wiederaufnehmen
- Ereigniskennung 683:
  => Terminalsitzung unterbrechen

Es wurden zur besseren Übersicht nur die wichtigsten Entscheidungspunkte angeführt, auf den Vergleich zusätzlicher Informationen z.B. anderer Quellen, die Kontrollmöglichkeiten bieten würden, wird nicht direkt eingegangen.

Aufwand:

Gering.

Fehlinterpretation:

Gering.
Obwohl verschiedene Vorgänge teilweise Einträge der gleichen Ereigniskennung erzeugen, ist über den Inhalt der Einträge (z.B. Anmeldetyp, Quellnetzwerkadresse) und deren Kombination eine eindeutig Zuordnung von den Quellen auf die Vorgänge möglich. Dies wird beim Vorgehen genauer erklärt.

Fälschung:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Quelle:

Eintrag im Sicherheitsprotokoll der Kategorie "Detaillierte Überwachung" .....eventvwr.msc

Beschreibung der Quelle:

Es handelt sich um einen Eintrag einer bestimmten Ereigniskennung der Kategorie "Detaillierte Überwachung" im Sicherheitsprotokoll. Die verschiedenen Ereigniskennungen wurden aufgrund ähnlicher Eigenschaften nicht als eigenständige Quellen auf separaten Blättern beschrieben.

Die Kriterien Lebensdauer, Verfügbarkeit und Fälschung sowie das allgemeine Vorgehen sind bei den Einträgen im Sicherheitsprotokoll aller Ereigniskennungen gleich und deshalb nur einmal bei der Quellenbeschreibung "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen" erwähnt.

Verursachende Vorgänge:

Die Vorgänge sind differenziert nach den jeweiligen erzeugten Ereigniskennungen dargestellt:

Ereigniskennung 592 "Ein neuer Prozess wurde erstellt":
- Programm (mit "Ausführen als") starten
- Programm (mit aktuellem Benutzer) starten

Ereigniskennung 593: "Ein Prozess wurde beendet":
- Programm (mit "Ausführen als" gestartet) beenden
- Programm (mit aktuellem Benutzer gestartet) beenden

Entstehungsbedingungen:

Spezielle.
In den Systemrichtlinien des Computers muss die Überwachungsrichtlinie "Prozessverfolgung überwachen" aktiviert sein (diese ist standardmäßig nicht aktiviert)

Lebensdauer:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Informationsgehalt:

Zeit:	Systemdatum und Systemzeit des Vorgangs in den Feldern "Datum" und "Uhrzeit"
Benutzer:	Benutzername ("Benutzer"/"Benutzername")
Sonstiges:	unter "Bilddateiname" findet sich der Pfad und Dateiname des gestarteten oder beendeten Programms.

Verfügbarkeit:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Auswertung:

Ob das Programm unter der gleichen Benutzerkennung oder unter einer anderen mit "Ausführen als" erstellt wurde, kann mit den bei Einträgen der Kategorie An-/Abmelden einbezogen werden.

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Quelle:

Eintrag im Sicherheitsprotokoll der Kategorie "Kontenverwaltung" .....eventvwr.msc

Beschreibung der Quelle:

Es handelt sich um einen Eintrag einer bestimmten Ereigniskennung der Kategorie "Kontenverwaltung" im Sicherheitsprotokoll. Die verschiedenen Ereigniskennungen wurden aufgrund ähnlicher Eigenschaften nicht als eigenständige Quellen auf separaten Blättern beschrieben.

Die Kriterien Lebensdauer, Verfügbarkeit und Fälschung sowie das allgemeine Vorgehen sind bei den Einträgen im Sicherheitsprotokoll aller Ereigniskennungen gleich und deshalb nur einmal bei der Quellenbeschreibung "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen" erwähnt.

Verursachende Vorgänge:

Die Vorgänge sind differenziert nach den jeweiligen erzeugten Ereigniskennungen dargestellt. Zu beachten ist, dass ein Teil der Vorgänge mehrere Einträge erzeugt.

Ereigniskennung 624 "Ein Benutzerkonto wurde erstellt":
- AD Benutzer anlegen
- Benutzer anlegen

Ereigniskennung 626 "Aktiviertes Benutzerkonto":
- AD Benutzer anlegen
- AD Computerkonto anlegen
- Benutzer anlegen

Ereigniskennung 627 "Ein Benutzerkennwort wurde geändert":
- AD Benutzer ändert sein Passwort
- Benutzer ändert sein Passwort

Ereigniskennung 628 "Ein Benutzerkennwort wurde festgelegt":
- AD Benutzer anlegen (hier auch bei leerem Passwort erzeugt)
- AD Benutzerpasswort festlegen/zurücksetzen
- AD Computerkonto anlegen
- Benutzer anlegen (wenn gleichzeitig ein Passwort vergeben wird)
- Benutzerpasswort festlegen

Ereigniskennung 630 "Ein Benutzerkonto wurde gelöscht":
- AD Benutzer löschen
- Benutzer löschen

Ereigniskennung 631 "Eine globale Gruppe wurde erstellt":
- AD Globale Gruppe anlegen

Ereigniskennung 632 "Ein Mitglied wurde zu einer globalen Gruppe hinzugefügt":
- AD Benutzer zu globaler Gruppe hinzufügen
- Benutzer anlegen (wird automatisch zur globalen Gruppe kein hinzugefügt)

Ereigniskennung 633 "Ein Mitglied wurde aus einer globalen Gruppe entfernt":
- AD Benutzer von globaler Gruppe entfernen
- Benutzer löschen (wird von globaler Gruppe kein entfernt)

Ereigniskennung 634 "Eine globale Gruppe wurde gelöscht":
- AD Globale Gruppe löschen

Ereigniskennung 635 "Eine neue lokale Gruppe wurde erstellt":
- AD Lokale Gruppe anlegen
- Lokale Gruppe anlegen

Ereigniskennung 636 "Ein Mitglied wurde zu einer lokalen Gruppe hinzugefügt":
- AD Benutzer zu lokaler Gruppe hinzufügen
- Benutzer anlegen (automatisch zu Gruppe Benutzer hinzugefügt)
- Benutzer zu lokalen Gruppe hinzufügen

Ereigniskennung 637 "Ein Mitglied wurde aus einer lokalen Gruppe entfernt":
- AD Benutzer von lokaler Gruppe entfernen
- Benutzer löschen (für jede Gruppe in der er Mitglied war ein Eintrag)
- Benutzer von lokaler Gruppe entfernen

Ereigniskennung 638 "Eine lokale Gruppe wurde gelöscht":
- AD Lokale Gruppe löschen
- Lokale Gruppe löschen

Ereigniskennung 639 "Das Konto einer lokalen Gruppe wurde geändert":
- AD Benutzer zu lokaler Gruppe hinzufügen
- AD Benutzer von lokaler Gruppe entfernen
- Lokale Gruppe anlegen
- Lokale Gruppe umbenennen

Ereigniskennung 641 "Das Konto einer globalen Gruppe wurde geändert":
- AD Benutzer zu globaler Gruppe hinzufügen
- AD Benutzer von globaler Gruppe entfernen

Ereigniskennung 642 "Ein Benutzerkonto wurde geändert":
- AD Benutzer anlegen
- AD Benutzer ändert sein Passwort
- AD Benutzer umbenennen (wenn der wirkliche Benutzeranmeldename geändert wird, und nicht nur Vor-, Nach- oder der Vollständige Name)
- AD Benutzereigenschaften ändern (nicht für alle Eigenschaften, z.B. für Textfelder wie Anschrift, Telefonnummer nicht)
- AD Benutzerpasswort festlegen/zurücksetzen
- Benutzer anlegen
- Benutzer umbenennen
- Benutzereigenschaften ändern
- Benutzerpasswort festlegen

Ereigniskennung 645: "Ein Computerkonto wurde erstellt":
- AD Computerkonto anlegen

Ereigniskennung 646: "Ein Computerkonto wurde geändert":
- AD Computerkonto anlegen
- AD Computerkontoeigenschaften ändern

Ereigniskennung 647: "Ein Computerkonto wurde gelöscht":
- AD Computerkonto löschen

Ereigniskennung 685 "Der Name einer Kontos wurde geändert":
- AD Globale Gruppe umbenennen
- AD Lokale Gruppe umbenennen
- Lokale Gruppe umbenennen

Entstehungsbedingungen:

Spezielle.
In den Systemrichtlinien des Computers muss die Überwachungsrichtlinie "Kontenverwaltung überwachen" für Erfolg aktiviert sein (diese ist standardmäßig nur auf Domänencontrollern für Erfolg aktiviert).

Lebensdauer:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Informationsgehalt:

Zeit: Systemdatum und Systemzeit des Vorgangs in den Feldern "Datum" und "Uhrzeit"

Benutzer: Benutzername ("Benutzer"/"Aufruferbenutzername") der Aktion durchführte

Sonstiges:

	Name des Benutzerkontos, das verändert wird	Name der Gruppe, die verändert wird	Wichtiges Sonstiges
624	„Neuer Kontenname“	Nicht zutreffend	Bestimmte kontospezifische Einstellungen wie „Anzeigename“, „Stammverzeichnis“, „Skriptpfad“, „Profilpfad“, etc
626	„Zielkontenname“	Nicht zutreffend	-
627	„Zielkontenname“	Nicht zutreffend	-
628	„Zielkontenname“	Nicht zutreffend	-
630	„Zielkontenname“	Nicht zutreffend	-
631	Nicht zutreffend	Neuer erstellter Gruppenname unter „Neuer Kontoname“	-
632	„Mitgliedkennung“	Nicht zutreffend	-
633	Nur noch die SID des ehemals bestehenden Kontos unter „Mitgliedkennung“	Nicht zutreffend	-
634	Nicht zutreffend	Gelöschter Gruppenname unter „Zielkontoname	-
635	Nicht zutreffend	Neuer erstellter Gruppenname unter „Zielkontoname“	-
636	Unter „Mitgliedkennung“ das Konto das einer Gruppe hinzugefügt wird	Unter „Zielkontoname“ die Gruppe zu der ein Benutzer hinzugefügt wird	-
637	Unter „Mitgliedkennung“ das Konto das von einer Gruppe entfernt wird	Unter „Zielkontoname“ die Gruppe von der ein Benutzer entfernt wird	-
638	Nicht zutreffend	Gelöschter Gruppenname unter „Zielkontoname“	-
639	Nicht zutreffend	Geänderte Gruppe unter „Zielkontoname“	-
641	Nicht zutreffend	Geänderte Gruppe unter „Zielkontoname“	-
642	Neuer vergebener Name unter „Neuer Kontoname“	Nicht zutreffend	Bestimmte kontospezifische Einstellungen wie „Anzeigename“, „Stammverzeichnis“, „Skriptpfad“, „Profilpfad“, etc
645	-	-	Neues des neuen Computerkontos unter „Neuer Kontenname“
646	-	-	Name des geänderten Computerkontos unter „Neuer Kontenname“
647	-	-	Gelöschtes Computerkonto unter „Zielkontenname“
685	Nicht zutreffend	Alter Gruppenname unter „Alter Kontoname“; neuer Name unter „Neuer Kontoname“	-

Verfügbarkeit:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Auswertung:

Zwar werden dieselben Ereigniskennungen hier zum Teil von verschiedenen Vorgängen angelegt. Trotzdem lassen sich die ausgeführten Vorgänge relativ leicht nachvollziehen.
Ob es sich jeweils um den Vorgang in der lokalen Benutzerdatenbank oder im Active Directory handelt, ist schon dadurch gegeben, ob auf dem Rechner von dem das Protokoll stammt, das Active Directory überhaupt installiert ist.
Weiterhin werden manche Einträge bei Handlungen im Active Directory sowohl mit Benutzer- als auch Computerkonten erstellt. Eine Unterscheidung ist an der Darstellung des Namens erkennbar, der bei Computern hier mit Dollarzeichen $ endend angezeigt wird.
Bei den restlichen Uneindeutigkeiten erkennt man an den unmittelbar darauf oder davor folgenden Einträgen, ob alle Einträge für einen in Frage kommenden Vorgang vorhanden sind.

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Quelle:

Eintrag im Sicherheitsprotokoll der Kategorie "Kontoanmeldung".....eventvwr.msc

Beschreibung der Quelle:

Es handelt sich um einen Eintrag einer bestimmten Ereigniskennung der Kategorie "Kontenanmeldung" im Sicherheitsprotokoll. Die verschiedenen Ereigniskennungen wurden aufgrund ähnlicher Eigenschaften nicht als eigenständige Quellen auf separaten Blättern beschrieben.

Die Kriterien Lebensdauer, Verfügbarkeit und Fälschung sowie das allgemeine Vorgehen sind bei den Einträgen im Sicherheitsprotokoll aller Ereigniskennungen gleich und deshalb nur einmal bei der Quellenbeschreibung "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen" erwähnt.

Verursachende Vorgänge:

Die Vorgänge sind differenziert nach den jeweiligen erzeugten Ereigniskennungen dargestellt:

Ereigniskennung 672 "Ein AS-Ticket (Authentication Service, Authentifizierungsdienst) wurde erfolgreich ausgestellt und überprüft":
- AD Benutzeranmeldung an Active Directory

Ereigniskennung 673 "Ein TGS-Ticket (Ticket Granting Service, Ticket-genehmigender Dienst) wurde erteilt":
mit Typ Erfolgsüberwachung:
- AD Benutzeranmeldung an Active Directory

mit Typ Fehlerüberwachung:
- AD Unberechtigter Anmeldeversuch Active Directory (bei ungültigem Benutzernamen)

Ereigniskennung 675 "Die Präauthentifizierung ist fehlgeschlagen. Dieses Ereignis wird auf einem Schlüsselverteilungscenter (KDC) generiert, wenn ein Benutzer ein falsches Kennwort eingibt":
- AD Unberechtigter Anmeldeversuch Active Directory (bei falschem Kennwort)

Entstehungsbedingungen:

Spezielle.
Alle Ereignisse dieser Kategorie werden nur auf dem Server, auf dem das Active Directory verwaltet wird, generiert und nicht auf den Clients.

In den Systemrichtlinien des Computers mit dem Active Directory muss die Überwachungsrichtlinie "Anmeldeversuche überwachen" folgendermaßen aktiviert sein:
Option "Erfolgreich" für folgende Ereigniskennungen:
672, 673 (im Erfolgsfall)
Option "Fehlgeschlagen" für folgende Ereigniskennungen:
673 (im Fehlerfall), 675
Standardmäßig aktiviert ist erfolgreiche Anmeldeversuche überwachen.

Lebensdauer:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Informationsgehalt:

Zeit:	Systemdatum und Systemzeit des Vorgangs in den Feldern "Datum" und "Uhrzeit"
Benutzer:	"Benutzername" und IP-Adresse ("Clientadresse")
Sonstiges:	An dem Wert des Feldes "Typ" ist erkennbar, ob der Vorgang erfolgreich oder fehlerhaft verlief.

Verfügbarkeit:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Auswertung:

Die Zuordnung der Ereigniskennungen zu den Vorgängen ist trivial.

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Quelle:

Eintrag im Sicherheitsprotokoll der Kategorie "Objektzugriff" .....eventvwr.msc

Beschreibung der Quelle:

Es handelt sich um einen Eintrag einer bestimmten Ereigniskennung der Kategorie "Objektzugriff" im Sicherheitsprotokoll. Die verschiedenen Ereigniskennungen wurden aufgrund ähnlicher Eigenschaften nicht als eigenständige Quellen auf separaten Blättern beschrieben.

Im Anhang der Arbeit findet sich ein extra Kapitel 7.1.2.8 zu den Einträgen dieser Kategorie.

Die Kriterien Lebensdauer, Verfügbarkeit und Fälschung sowie das allgemeine Vorgehen sind bei den Einträgen im Sicherheitsprotokoll aller Ereigniskennungen gleich und deshalb nur einmal bei der Quellenbeschreibung "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen" erwähnt.

Verursachende Vorgänge:

Von den unten dargestellten Vorgängen werden bei gegebenen Entstehungsbedingungen die Ereigniskennungen 560, 562 und 567 erstellt. Aufgrund der im Anhang erklärten Komplexität wird hier nicht auf die Quantität oder Reihenfolge der Einträge oder ihrer genauen Rückverfolgung eingegangen. Mit 560 wird ein Handle zu einen bestimmten Objekt mit bestimmten Berechtigungen erstellt, 567 bezeichnet die Ausführung dieser Rechte und 562 zeigt an, dass das Handle geschlossen wurde. Dabei kann 567 mehrmals für dasselbe Handle vorkommen.

Ereigniskennung 560 "Der Zugriff wurde auf ein bereits vorhandenes Objekt gewährt":
- Rechteverletzung Dateisystem (mit Typ „Fehlerüberw.“ für eine fehlgeschlagene Anforderung)
- Alle unten im Block dargestellten Vorgänge

Ereigniskennung 562 "Ein Handle zu einem Objekt wurde geschlossen".
- Alle unten im Block dargestellten Vorgänge

Ereigniskennung 567 "Eine Berechtigung, die mit einem Handle verknüpft ist, wurde verwendet".
- Alle unten im Block dargestellten Vorgänge

Die nachfolgenden Vorgänge können aufgrund vollständiger Übereinstimmung im Bezug auf die hinterlassenen Ereigniskennungen undifferenziert für alle drei Ereigniskennungen 560, 562 und 567 zusammenfassend dargestellt werden.
- Datei anlegen
- Datei kopieren
- Datei lesen
- Datei löschen
- Datei umbenennen
- Datei verschieben
- Dateiattribute ändern
- Dateiberechtigung NTFS ändern
- Dateiinhalt ändern
- Drucken
- Programm (mit "Ausführen als") starten
- Programm (mit aktuellem Benutzer) starten
- Registryänderung durchführen (Schlüssel/Wert anlegen/ändern/löschen)
- Registryberechtigungen ändern
- Verzeichnis anlegen
- Verzeichnis kopieren
- Verzeichnis löschen
- Verzeichnis umbenennen
- Verzeichnis verschieben
- Verzeichnisattribute ändern
- Verzeichnisberechtigungen NTFS ändern

Entstehungsbedingungen:

Spezielle.
In den Systemrichtlinien des Computers muss die Überwachungsrichtlinie "Anmeldeereignisse überwachen" für „Erfolg“ und/oder „Fehlgeschlagen“ aktiviert sein. Dies ist davon abhängig, ob nur ausgeführte Zugriffe oder auch Zugriffsversuche, die mangels ausreichender Rechte nicht durchgeführt werden, aufgezeichnet werden. (Standardmäßig ist keine von beiden Optionen aktiviert).
Weiterhin muss für das betreffende Objekt die Überwachung für den ausführenden Benutzer aktiviert sein, was im Falle der Überwachung des Dateisystems nur für NTFS aber nicht für FAT32 möglich ist. Diese kann wahlweise für bestimmte Aspekte aktiviert werden, so das z.B. im Dateisystem Zugriffe der Art "Löschen", aber nicht solche der Art "Attribute lesen" protokolliert werden. Siehe auch Kapitel 7.1.2.8 im Anhang.

Lebensdauer:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Informationsgehalt:

Zeit:	Systemdatum und Systemzeit des Vorgangs in den Feldern "Datum" und "Uhrzeit"
Benutzer:	Benutzername im Feld "Primärer Benutzername"
Sonstiges:	Das Objekt des Zugriffs ("Objektname", "Objekttyp")
	Das Programm, mit dem zugegriffen wurde ("Abbilddateiname")
	Die Art des Zugriffs ("Zugriffe")
	An der "Handlekennung" kann abgelesen werden, welche Einträgstupel 560, 562 und 567 zusammengehören, da die Ereigniskennungen jedes Handles einen identischen Wert haben.
	Aus der "Prozesskennung" kann die Nummer des zugreifenden Prozesses identifiziert werden.
	Am Eintrag im Feld "Typ" kann abgelesen werden, ob der Vorgang erfolgreich oder fehlerhaft war.

Verfügbarkeit:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Auswertung:

Systemdatum und Systemzeit, Benutzername, Objektname und Programm brauchen nur abgelesen zu werden.

Für Registryvorgänge kann über das Feld "Zugriffe" die Art der Handlung abgelesen werden.
Aber bei Vorgängen im Dateisystem ist es wesentlich schwerer über die Einträge genaue Informationen zum ausgeführten Vorgang zu finden.
Siehe dazu und allgemein zur Auswertung dieser Quellen die zusammenfassenden Beschreibungen im Kapitel 7.1.2.8 im Anhang.

Allgemein ist zu beachten, dass hier extrem viele Einträge anfallen können, wenn eine umfangreiche Protokollierung eingestellt wird.

Aufwand:

Hoch.
Beim Dateisystem sind zur vollständigen Aufklärung des erzeugenden Vorgangs komplexe Überlegungen anzustellen.

Fehlinterpretation:

Hoch.
Vorgänge im Dateisystem: Leider wird nicht sehr deutlich welcher Vorgang genau ausgeführt wurde. Aber immerhin weiß man die genaue Datei bzw. das genaue Verzeichnis und mit welchem Programm darauf zugegriffen wurde.

Fälschung:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Quelle:

Eintrag im Sicherheitsprotokoll der Kategorie "Richtlinienänderung" .....eventvwr.msc

Beschreibung der Quelle:

Es handelt sich um einen Eintrag einer bestimmten Ereigniskennung der Kategorie "Richtlinienänderung" im Sicherheitsprotokoll. Die verschiedenen Ereigniskennungen wurden aufgrund ähnlicher Eigenschaften nicht als eigenständige Quellen auf separaten Blättern beschrieben.

Die Kriterien Lebensdauer, Verfügbarkeit und Fälschung sowie das allgemeine Vorgehen sind bei den Einträgen im Sicherheitsprotokoll aller Ereigniskennungen gleich und deshalb nur einmal bei der Quellenbeschreibung "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen" erwähnt.

Verursachende Vorgänge:

Die Vorgänge sind differenziert nach den jeweiligen erzeugten Ereigniskennungen dargestellt:

Ereigniskennung 608 "Ein Benutzerrecht wurde zugewiesen":
- Lokales Zuweisen von Benutzerrechten

Ereigniskennung 609 "Ein Benutzerrecht wurde entfernt":
- Lokales Zuweisen von Benutzerrechten

Ereigniskennung 612 "Eine Überwachungsrichtlinie wurde geändert":
- Lokale Überwachungsrichtlinien ändern

Ereigniskennung 621 "Der Systemzugriff wurde einem Konto gewährt":
- Lokales Zuweisen von Benutzerrechten

Ereigniskennung 622 "Der Systemzugriff wurde einem Konto entzogen":
- Lokales Zuweisen von Benutzerrechten

Abhängig davon, welches Benutzerrecht geändert wird, generiert das System eine der Ereigniskennungen 608/609 oder 621/622.

Entstehungsbedingungen:

Spezielle.
In den Systemrichtlinien des Computers muss die Überwachungsrichtlinie "Richtlinienänderungen überwachen" auf Erfolg aktiviert sein (diese ist standardmäßig nur auf Domänencontrollern für Erfolg aktiviert).

Lebensdauer:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Informationsgehalt:

Zeit:	Systemdatum und Systemzeit des Vorgangs in den Feldern "Datum" und "Uhrzeit".
Benutzer:	"Benutzername" des Benutzers der Änderung durchführte.
Sonstiges:	Bei 621/622: "Geändertes Konto" welches Benutzerkonto verändert wurde; "Gewährter Zugriff"/"Gelöschter Zugriff" welches Recht hinzugefügt/entfernt wurde. Bei 608/609: "Zugeteilt zu"/"Entfernt von" welches Benutzerkonto geändert wurde; "Benutzerberechtigung" welche Berechtigung hinzugefügt oder entfernt wurde. Bei 612: Der Protokolleintrag enthält Informationen über die zum Zeitpunkt der Erstellung des Eintrages gültigen Überwachungseinstellungen aller Kategorien.

Verfügbarkeit:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Auswertung:

Die jeweilige Benutzerberechtigung wird
- im Feld "Benutzerberechtigung" bei 608/609 bzw.
- im Feld "Gewährter Zugriff"/"Gelöschter Zugriff" bei 621/622 genannt.
Allerdings wird im Protokolleintrag nicht die deutsche Übersetzung angezeigt, die für das Einstellen verwendet wird, sondern es finden sich hier die englischen Systembezeichnungen der Rechte z.B. „SeDenyRemoteInteractiveLogonRight“ für „Anmelden über Terminaldienste verweigern“.

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Quelle:

Eintrag im Sicherheitsprotokoll der Kategorie "Systemereignis".....eventvwr.msc

Beschreibung der Quelle:

Es handelt sich um einen Eintrag einer bestimmten Ereigniskennung der Kategorie "Systemereignis" im Sicherheitsprotokoll. Die verschiedenen Ereigniskennungen wurden aufgrund ähnlicher Eigenschaften nicht als eigenständige Quellen auf separaten Blättern beschrieben.

Die Kriterien Lebensdauer, Verfügbarkeit und Fälschung sowie das allgemeine Vorgehen sind bei den Einträgen im Sicherheitsprotokoll aller Ereigniskennungen gleich und deshalb nur einmal bei der Quellenbeschreibung "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen" erwähnt.

Verursachende Vorgänge:

Die Vorgänge sind differenziert nach den jeweiligen erzeugten Ereigniskennungen dargestellt:

Ereigniskennung 512 "Windows wird gestartet":
- Windows starten
- Windows Neustart

Ereigniskennung 513 "Windows wird heruntergefahren":
- Windows beenden
- Windows Neustart

Ereigniskennung 517 "Das Überwachungsprotokoll wurde gelöscht":
- Systemprotokoll löschen

Ereigniskennung 520 "Die Systemzeit wurde geändert":
- Uhrzeit ändern

Entstehungsbedingungen:

Spezielle.
In den Systemrichtlinien des Computers muss die Überwachungsrichtlinie "Systemereignisse überwachen" für Erfolg aktiviert sein (diese ist standardmäßig nur auf Domänencontrollern für Erfolg aktiviert).

Lebensdauer:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Informationsgehalt:

Zeit:	Systemdatum und Systemzeit des Vorgangs in den Feldern "Datum" und "Uhrzeit".
Benutzer:	Bei 517 und 520 wird der Benutzername ("Clientbenutzername") angegeben. Bei 512 und 513 findet sich hier keine Information.
Sonstiges:	Bei 520 finden sich Uhrzeit und Datum vor ("Alte Zeit") und nach ("Neue Zeit") der Umstellung.

Verfügbarkeit:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Auswertung:

Die Zuordnung der Ereigniskennungen zu den Vorgängen ist trivial.

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Quelle:

Eintrag im Sicherheitsprotokoll der Kategorie "Verzeichnisdienstzugriff" .....eventvwr.msc

Beschreibung der Quelle:

Es handelt sich um einen Eintrag einer bestimmten Ereigniskennung der Kategorie "Verzeichnisdienstzugriff" im Sicherheitsprotokoll. Die verschiedenen Ereigniskennungen wurden aufgrund ähnlicher Eigenschaften nicht als eigenständige Quellen auf separaten Blättern beschrieben.

Die Kriterien Lebensdauer, Verfügbarkeit und Fälschung sowie das allgemeine Vorgehen sind bei den Einträgen im Sicherheitsprotokoll aller Ereigniskennungen gleich und deshalb nur einmal bei der Quellenbeschreibung "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen" erwähnt.

Verursachende Vorgänge:

Ereigniskennung 565 "Der Zugriff wurde auf einen bereits vorhandenen Objekttyp gewährt":
(Obwohl diese Ereigniskennung in den Windowsbeschreibungen fälschlicherweise unter Objektzugriff aufgeführt ist gehört sie nach Sinn und Funktionalität in diese Kategorie.)

- AD Benutzer anlegen
- AD Benutzereigenschaften ändern (wird nicht bei allen Änderungen angelegt, z.B. für Änderungen der Textbeschreibungen nicht)
- AD Benutzerpasswort festlegen/zurücksetzen
- AD Computerkonto anlegen
- AD Computerkontoeigenschaften ändern

Ereigniskennung 566 "Ein allgemeiner Objektvorgang wurde durchgeführt":

- AD Änderungen an den Gruppenrichtlinien (z.B. Benutzerrechte und Überwachungsrichtlinien)

Entstehungsbedingungen:

Spezielle.
In den Systemrichtlinien des Computers muss die Überwachungsrichtlinie "Verzeichnisdienstzugriff überwachen" für Erfolg aktiviert sein (diese ist standardmäßig nur auf Domänencontrollern für Erfolg aktiviert).

Lebensdauer:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Informationsgehalt:

Zeit:	Systemdatum und Systemzeit des Vorgangs in den Feldern "Datum" und "Uhrzeit".
Benutzer:	Benutzername des zugreifenden Benutzers ("Clientbenutzername").
Sonstiges:	"Objekttyp" und "Objektname" des Objektes, auf das zugegriffen wurde. Unter "Zugriffe" wird die Art des Objektzugriffes angegeben.

Verfügbarkeit:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Auswertung:

Beispiele für Objekttypen sind SAM_USER für Benutzer oder GroupPolicyContainer für Benutzerrichtlinien.
Bei Objektname jeweiliger Pfad zum Objekt, auf das zugegriffen wurde. Dieser ist in der Form CN=[31B2F340-016D-11D2-945F-00C04FB984F9},CN=policies,CN=System,DC=home,DC=de für eine Richtlinie angeben.
Das angegebene Objekt lässt sich im Active Directory Baum finden, wenn der Pfad von hinten nach vorne aufgelöst wird. Der Active Directory Baum kann z.B. mit dem Programm „Active Directory-Benutzer und –Computer“ (dsa.msc) angezeigt werden. Damit dort kein Objekt ausgeblendet bleibt, ist unter Ansicht die Option "Erweiterte Funktionen" zu aktivieren.
Beim Zugriff auf Benutzerkonten steht im Feld „Objektname“ die SID des Benutzers.
Eine Zuordnung der SID zum Benutzernamen ist am betreffenden System über das Programm sid2user [Rudn98] möglich.
Unter "Zugriffe" finden sich ausgeführte Zugriffe auf das Objekt. Dies geschieht aber ähnlich wie in der Kategorie "Objektzugriff" nur auf sehr abstrakter Ebene der Einzelaktionen.

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Siehe die Beschreibung auf dem Quellenblatt "Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen".

Quelle:

Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen .....eventvwr.msc

Beschreibung der Quelle:

Im Sicherheitsprotokoll werden sicherheitsrelevante Ereignisse aufgezeichnet.
Genaueres zum Sicherheitsprotokoll siehe Kapitel 7.1.2.6 zum Sicherheitsprotokoll im Anhang.
Die Sicherheitsereignisse sind sowohl in den Überwachungsrichtlinien als auch im Ereignisprotokoll nach folgenden Kategorien gegliedert:

- An-/Abmeldung
- Kontoanmeldung
- Kontenverwaltung
- Objektzugriff
- Detaillierte Überwachung
- Berechtigungen
- Richtlinienänderung
- Systemereignis
- Verzeichnisdienstzugriff

Für alle Kategorien außer „Berechtigungen“ ist eine eigene Quellenbeschreibung angelegt.

In dieser Quellenbeschreibung sind nur die Kriterien beschrieben, in denen die Eigenschaften der Einträge im Sicherheitsprotokoll über die oben genannten Kategorien hinweg ganz oder ausschnittsweise identisch sind. Sofern hier ein Kriterium bereits vollständig beschrieben ist, findet sich bei den Quellenbeschreibungen der einzelnen Kategorien nur ein entsprechender Verweis auf diese Beschreibung.

Verursachende Vorgänge:

Siehe die unterschiedlichen Einzelbeschreibungen der jeweiligen Kategorie.

Entstehungsbedingungen:

Spezielle.
Abhängig von den Einstellungen des Sicherheitsprotokolls. Siehe dazu die speziellen Angaben im Kapitel 7.1.2.5 „Entstehungsbedingungen und Lebensdauer von Einträgen“ des Anhangs.
Siehe zusätzlich die unterschiedlichen ergänzenden Einzelbeschreibungen der jeweiligen Kategorie.

Lebensdauer:

Bedingt abhängig von anderen Vorgängen.
Genaueres siehe Kapitel 7.1.2.5 im Anhang.

Informationsgehalt:

Siehe die unterschiedlichen Einzelbeschreibungen der jeweiligen Kategorie.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Mit Hilfe der Ereignisanzeige eventvwr.msc sind die protokollierten Daten übersichtlich darstellbar. Außerdem ist in der Vielzahl der Einträge eine gezielte Filterung und Sortierung möglich.

Falls z.B. für die Offline-Auswertung nur ein Hexeditor zur Verfügung steht, ist die Entschlüsselung - wie im Anhang beschrieben - wesentlich komplizierter. Gemeine Texteditoren sind für diese Aufgabe nicht ausreichend, da sie nur die druckbaren Zeichen darstellen. Alle aufgezeichneten Einträge des Sicherheitsprotokolls finden sich standardmäßig in der Datei C:\Windows\system32\config\SecEvent.Evt.

Für ein kategoriespezifisches Vorgehen siehe auch die unterschiedlichen ergänzenden Einzelbeschreibungen der jeweiligen Kategorie.

Aufwand:

Generell lässt sich hier sagen, dass für die Gewinnung entsprechender forensischer Daten ein deutlicher Unterschied im Aufwand in Abhängigkeit von der Art der Auswertung besteht.
- Gering.
  Gilt bei einer Auswertung mit der Ereignisanzeige (eventvwr.msc). Mit diesem Programm ist eine übersichtliche Ausgabe der meist sehr umfangreichen Daten möglich, die sich mit geringem Aufwand filtern lassen.
- Hoch
  Gilt bei Einsatz eines Hexeditors. Näheres zum Dateiformat und zur Informationscodierung siehe im Kapitel 7.1.2.4 des Anhangs.

Zur Interpretation dieser Informationen, insbesondere der Zuordnung der Quellen zu den erzeugenden Vorgängen siehe die unterschiedlichen Einzelbeschreibungen der jeweiligen Kategorie.

Fehlinterpretation:

Siehe die unterschiedlichen Einzelbeschreibungen der jeweiligen Kategorie.

Fälschung:

Administratorrechte.
Nur Administratoren können das Protokoll über die Ereignisanzeige (eventvwr.msc) löschen. Auf die Datei SecEvent.Evt, in der die Informationen gespeichert sind, haben Administratoren zwar Lese- und Schreibzugriff. Da die Datei im laufenden Betrieb in Verwendung ist, lässt sich aber auch mit einem Hexeditor keine Änderung vornehmen.

Wenn "Ereignisse bei Bedarf überschreiben" (Standardeinstellung) aktiviert ist, ist es möglich, die älteren verdächtigen Einträge die man entfernen will, durch Generieren vieler anderer Einträge zu überschreiben.
Wenn dagegen "Ereignisse nie überschreiben" oder "Ereignisse überschreiben, die älter als [x] Tage sind" und gleichzeitig in den Sicherheitseinstellungen "Überwachung: System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können" deaktiviert ist, kann man vor dem Ausführen der Handlungen, die nicht aufgezeichnet werden sollen, das Protokoll mit unverdächtigen Handlungen füllen, so das kein Speicherplatz mehr für die Aufzeichnung der späteren Handlungen vorhanden ist.
Mit Aktivierung des Herunterfahrens ist dieser Nachteil zwar vermeidbar, das System wird jedoch für „Denial of Service“-Attacken anfällig.

Quelle:
Firewall Logdatei.....notepad.exe

Beschreibung der Quelle:

Die mitgelieferte Firewall (nur Windows XP und Windows 2003 Server) zeichnet bei Aktivierung für die jeweilige Netzwerkverbindung darüber laufenden Verkehr auf.

Verursachende Vorgänge:

- Netzwerkverkehr verursachen

Entstehungsbedingungen:

Spezielle.
Die Firewall muss für die jeweilige Netzwerkverbindung aktiviert werden. Für eine entsprechende Aufzeichnung müssen die Einstellungen "Verworfene Pakete protokollieren" und "Erfolgreiche Verbindungen protokollieren" ebenfalls aktiviert sein.

Lebensdauer:

Bedingt abhängig von anderen Vorgängen.
Wenn das eingestellte Größenlimit für die Protokolldatei erreicht ist, werden die ältesten Einträge überschrieben (Standardgröße 4096 KB, maximal 32767 KB möglich).

Informationsgehalt:

Zeit: Datum und Zeit
Sonstiges: QuellIP, Quellport, ZielIP, Zielport, abgelehnt oder angenommen, Größe des Paketes, etc.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Die Datei C:\Windows\pfirewall.log ist mit einem gängigen Texteditor zu betrachten. Die Einträge sind durch Leerzeichen getrennt und der Name dieser "Spalten" befindet sich am Anfang der Datei.

Aufwand:

Hoch.
Es sind sehr viele Einträge zu analysieren, wenn nicht schon Informationen zum gesuchten Netzverkehr, wie die IP-Adresse oder der Zeitraum bekannt sind.

Fehlinterpretation:

Gering.

Fälschung:

Administratorrechte.
Nur mit Administratorrechten ist ein direkter Schreibzugriff auf diese Datei möglich. Durch weiteren späteren unbedeutenden Netzwerkverkehr ist es allerdings möglich die Protokolldatei so weit zu füllen, dass die gegebenenfalls wichtigen Anfangsaufzeichnungen überschrieben werden.

Quelle:
Fragmente von Daten (Unallocated File Space, File Slack und Shadow Data)..... ..... besondere Programme nötig (nicht im Lieferumfang)

Beschreibung der Quelle:

Bei einer Löschung von Dateien im Dateisystem werden diese Daten nicht überschrieben, sondern nur der Verweis darauf gelöscht. Die eigentlichen Daten existieren als Unallocated File Space [NewT03d] weiter. Erst durch eine Benutzung dieses vermeintlich freien Platzes durch neue Daten werden diese überschrieben. Da aber wegen der Organisation des Dateisystems in Zuordnungseinheiten nicht jedes einzelne Bit unabhängig adressierbar ist, bleibt hier weiterhin der vorherige Zustand erhalten (File Slack [NewT03e]), falls diese Zuordnungseinheiten nicht komplett gefüllt werden, weil die Dateigröße kein ganzzahliges Vielfaches der Größe der Zuordnungseinheiten ist.
Außerdem trifft der Schreibkopf der Festplatte beim Beschreiben einer Spur nicht jedes Mal exakt dieselben Stellen, so dass sich hier geringe Unterschiede der Magnetisierung ergeben können, was unter dem Namen Shadow Data [BrAn01] bekannt ist. Durch eine sehr aufwändige Untersuchung können selbst nach dem Überschreiben der früheren Datenbits noch Daten rekonstruiert werden.

Verursachende Vorgänge:

- Datei löschen
- Datei verschieben (auf andere Partition)
- Verzeichnis löschen
- Verzeichnis verschieben (auf andere Partition)

Entstehungsbedingungen:

Keine.

Lebensdauer:

Bedingt abhängig von anderen Vorgängen.
Die alten Daten können durch ein Überschreiben mit neuen Daten zerstört oder schwer aufklärbar werden.

Informationsgehalt:

Sonstiges: Die ursprünglichen Daten vor der Löschung.

Verfügbarkeit:

Online und offline verfügbar.
Während die Analyse des unbenutzten Speicherplatzes und des File Slacks auch online möglich ist, kann dies im Falle der Auswertung der Shadow Data nur offline vorgenommen werden.

Auswertung:

Es sind spezielle Programme nötig, die diese Daten auslesen. Im Lieferumfang von Windows findet sich dazu nichts.
Wenn die Daten schon einmal überschrieben sind wird die Untersuchung noch wesentlich komplizierter. Hierfür ist gegebenenfalls besondere Hardware nötig, um die Festplattenscheiben ohne ihre eigene Elektronik mit wesentlich empfindlicheren Sensoren zu untersuchen.

Aufwand:

Hoch.
Hoher Zeitaufwand bei heutigen Plattengrößen. Für eine effektive Suche sind präzise Suchwörter erforderlich. Wenn diese zu generisch gewählt werden, erhält man zu viele Treffer. Ohne eine programmgestützte Suche ist ein enormer Zeitaufwand erforderlich, um eine Festplatte vollständig zu analysieren.
Im Falle der Shadow Data ist der Aufwand noch wesentlich höher.

Fehlinterpretation:

Gering.

Fälschung:

Leicht.
Die Fragmente lassen sich durch (eventuell wiederholtes) Überschreiben der kompletten Festplatte vernichten. Ein passendes Programm ist mit cipher (Aufruf cipher /W:#Laufwerksbuchstabe#), das den freien Speicher der Partition dreimal überschreibt (1x Nullen, 1x Einsen, 1x zufällig), schon im Lieferumfang von Windows enthalten. Dieses braucht jedoch sehr lange, um eine übliche Festplatte zu bearbeiten. In der Literatur finden sich verschiedenste Aussagen darüber, ob drei Durchgänge schon ausreichend sind, um die Information so zu löschen, dass auch eine Shadow Data Analyse der Festplatte erfolglos bleibt. Aber bei genügend Zeit kann der Vorgang natürlich beliebig wiederholt werden.

Quelle:
Geplante Dienste bei Systemstart.....services.msc; regedit.exe; (regview.exe)

Beschreibung der Quelle:

Dienste sind Anwendungen, die meist nur im Systemhintergrund ausgeführt werden und zentrale Betriebssystemfunktionen zur Verfügung stellen. Die beim Systemstart zu startenden Dienste sind im Registrypfad HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\ gespeichert.

Verursachende Vorgänge:

- zukünftigen oder periodischen Programmstart planen

Entstehungsbedingungen:

Spezielle.
Die Planung von Programmstarts kann auf verschiedene Arten erfolgen, die jeweils andere Quellen verursachen. Deshalb sind für diesbezügliche Untersuchungen die Quellen zu allen Startvorgängen zu berücksichtigen.

Lebensdauer:

Solange der Zustand besteht.

Informationsgehalt:

Sonstiges: Die beim Systemstart gestarteten Dienste.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Vorhandene Dienste finden sich unter HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\. Für jeden Dienst existiert hier ein extra Unterschlüssel mit abgekürztem Namen.
Unter dem darin enthaltenen Wert \ImagePath\ vom Typ REG_EXPAND_SZ findet sich die dem Dienst entsprechende Datei im Dateisystem.
Unter \Description\ findet sich bei den meisten Einträgen ein Beschreibungstext vom Typ REG_SZ.
Die Startart findet sich jeweils im DoubleWord-Wert \Start\ mit
0x2 für automatisch,
0x3 für manuell und
0x4 für deaktiviert.

Die Dienste können auch über das Programm services.msc anzeigt werden. Jedoch finden sich hier nicht alle Einträge aus der Registry wieder.

Aufwand:

Gering.

Fehlinterpretation:

Gering.
Man muss sich aber bewusst sein, dass nur die Namen und Pfade der Programmdateien im Dateisystem angezeigt werden. Hier besteht die Gefahr nicht das richtige Programm dahinter zu erkennen.

Fälschung:

Programmmanipulation.
Das Programm müsste durch eine manipulierte Version ersetzt werden, das falsche Anzeigen erzeugt.
Die Werte selbst dürfen nicht verändert werden, weil sonst nicht mehr die gewünschte Funktionalität erreicht wird.

Quelle:
Geplante Programmstarts bei Benutzeranmeldung - Autostart.....explorer.exe; dir

Beschreibung der Quelle:

Eine Möglichkeit, Programme bei einer Benutzeranmeldung zu starten, bietet sich über einen Eintrag in dem Verzeichnis Autostart des jeweiligen Benutzers.

Verursachende Vorgänge:

- zukünftigen oder periodischen Programmstart planen

Entstehungsbedingungen:

Spezielle.
Die Planung von Programmstarts kann auf verschiedene Arten erfolgen, die jeweils andere Quellen verursachen. Deshalb sind für diesbezügliche Untersuchungen die Quellen zu allen Startvorgängen zu berücksichtigen.

Lebensdauer:

Solange der Zustand besteht.

Informationsgehalt:

Sonstiges: Die bei der Benutzeranmeldung gestarteten Programme.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Die unten angegebenen Verzeichnisse für alle Benutzer (dieses beinhaltet Gemeinsame Einstellungen von allen Benutzern) und des jeweils speziell zu untersuchenden Benutzers sind jeweils auf enthaltene Verknüpfungen und Programmdateien zu prüfen. Im Falle von Verknüpfungen ist diese auf die verwiesene Programmdatei zu untersuchen.

Die entsprechenden Verzeichnispfade lauten:
Für alle Benutzer:
C:\Dokumente und Einstellungen\All Users\Startmenü\Programme\Autostart
Für den jeweiligen Benutzer:
C:\Dokumente und Einstellungen\#BENUTZERNAME#\Startmenü\Programme\Autostart

Aufwand:

Gering.

Fehlinterpretation:

Gering.
Man muss sich aber bewusst sein, dass nur die Namen und Pfade der Programmdateien im Dateisystem angezeigt werden. Hier besteht die Gefahr nicht das richtige Programm dahinter zu erkennen.
Außerdem ist zu bedenken, dass auch andere Möglichkeiten für einen automatischen Programmstart genutzt werden können.

Fälschung:

Programmmanipulation.
Das Programm müsste durch eine manipulierte Version ersetzt werden, das falsche Anzeigen erzeugt.
Die Werte selbst dürfen nicht verändert werden, weil sonst nicht mehr die gewünschte Funktionalität erreicht wird.

Quelle:
Geplante Programmstarts bei Benutzeranmeldung - Registryeinträge.....regedit.exe; (regview.exe)

Beschreibung der Quelle:

Eine Möglichkeit Programme bei einer Benutzeranmeldung zu starten, bietet sich über einen Eintrag in der Registry.

Verursachende Vorgänge:

- zukünftigen oder periodischen Programmstart planen

Entstehungsbedingungen:

Spezielle.
Die Planung von Programmstarts kann auf verschiedene Arten erfolgen, die jeweils andere Quellen verursachen. Deshalb sind für diesbezügliche Untersuchungen die Quellen zu allen Startvorgängen zu berücksichtigen.

Lebensdauer:

Solange der Zustand besteht.

Informationsgehalt:

Sonstiges: Die bei der Benutzeranmeldung gestarteten Programme.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Mit einem Registryeditor sind folgende Schlüssel auf das Vorhandensein von Einträgen zu prüfen:
In der Registrydatei c:\Windows\system32\config\software (diese gelten für jeden Benutzer):
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
In der jeweiligen ntuser.dat des Benutzers:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

Einträge sind ein vom Namen her beliebiger Typ REG_SZ mit dem Programmpfad und -namen als Wert

Einträge in RunOnce werden jeweils nur noch bei der nächsten Anmeldung gestartet und danach gelöscht.

Aufwand:

Gering.

Fehlinterpretation:

Gering.
Man muss sich aber bewusst sein, dass nur die Namen und Pfade der Programmdateien im Dateisystem angezeigt werden. Hier besteht die Gefahr nicht das richtige Programm dahinter zu erkennen.
Außerdem ist zu bedenken, dass auch andere Möglichkeiten für einen automatischen Programmstart genutzt werden können.

Fälschung:

Programmmanipulation.
Das Programm müsste durch eine manipulierte Version ersetzt werden, das falsche Anzeigen erzeugt.
Die Werte selbst dürfen nicht verändert werden, weil sonst nicht mehr die gewünschte Funktionalität erreicht wird.

Quelle:
Geplante Programmstarts bei Systemstart - Registryeinträge .....regedit.exe; (regview.exe)

Beschreibung der Quelle:

Besondere Programme können über einen Eintrag in der Registry ganz am Anfang des Windowsstarts gestartet werden. Diese sind jedoch besonders zu programmieren, da zu diesem Zeitpunkt noch nicht die normale Windowsumgebung und die von ihr angebotenen Funktionen zur Verfügung stehen.

Verursachende Vorgänge:

- zukünftigen oder periodischen Programmstart planen

Entstehungsbedingungen:

Spezielle.
Die Planung von Programmstarts kann auf verschiedene Arten erfolgen, die jeweils andere Quellen verursachen. Deshalb sind für diesbezügliche Untersuchungen die Quellen zu allen Startvorgängen zu berücksichtigen.

Lebensdauer:

Solange der Zustand besteht.

Informationsgehalt:

Sonstiges: Die zu Beginn des Systemstarts gestarteten speziell programmierten Programme.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Der Wert HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute ist auslesen. Hierüber können jedoch nur speziell programmierte Programme gestartet werden.
Der Wert sollte nur "autocheck autochk *" enthalten.

Aufwand:

Gering.

Fehlinterpretation:

Gering.
Man muss sich aber bewusst sein, dass nur die Namen und Pfade der Programmdateien im Dateisystem angezeigt werden. Hier besteht die Gefahr nicht das richtige Programm dahinter zu erkennen.
Außerdem ist zu bedenken, dass auch andere Möglichkeiten für einen automatischen Programmstart genutzt werden können.

Fälschung:

Programmmanipulation.
Das Programm müsste durch eine manipulierte Version ersetzt werden, das falsche Anzeigen erzeugt.
Die Werte selbst dürfen nicht verändert werden, weil sonst nicht mehr die gewünschte Funktionalität erreicht wird.

Quelle:
Geplante Programmstarts nach Zeitplan - Anzeige.....at.exe

Beschreibung der Quelle:

Alle mit dem Befehl at.exe angelegten zukünftig oder periodisch geplanten Programmstarts lassen sich mit dem selbem Befehl auch anzeigen. Hier finden sich jedoch nicht die Programmstarts, die über Systemsteuerung/Geplante Tasks angelegt wurden oder bei einem Systemstart oder bei Benutzeranmeldungen stattfinden. Siehe hierzu die jeweiligen anderen Quellenblätter.

Verursachende Vorgänge:

- zukünftigen oder periodischen Programmstart planen

Entstehungsbedingungen:

Spezielle.
Nur wenn die Programmstarts mit dem Programm at.exe geplant worden sind.

Lebensdauer:

Solange der Zustand besteht.
Solange ein periodischer Start vorgesehen ist, werden die zum Start bestimmten Programme angezeigt. Einmalige Programmstarts werden nur bis zu ihrer Ausführung angezeigt.

Informationsgehalt:

Zeit: Die Zeit, zu der die Vorgangsplanung festgelegt wurde, ist unter Umständen sehr grob abschätzbar.
Sonstiges: Der zu startende Befehl, die dazugehörige Startzeit sowie gegebenenfalls die Periodizität.

Verfügbarkeit:

Nur online verfügbar. Siehe Quelle "Zukünftig geplante Programmstarts C:\Windows\Tasks" für Offlineanalyse.

Auswertung:

Der Befehl at.exe ohne Parameter liefert eine Liste der geplanten Programmstarts. Der Programmname, die geplante Startzeit sowie gegebenenfalls die Periodizität lassen sich einfach ablesen.
Aus der Taskkennung kann unter Umständen auf den Zeitraum geschlossen werden, zu dem der Programmstart geplant wurde. Diese Taskkennungen werden aufsteigend vergeben. Sollten hier über bereits festgelegte Programmstarts die Zeiten der Eingabe vorliegen, kann aus höheren Nummern der Taskkennungen auf einen späteren Zeitpunkt bei den zugehörigen Planungseingaben geschlossen werden.

Aufwand:

Gering.

Fehlinterpretation:

Gering.
Es ist zu bedenken, dass auch andere Möglichkeiten für einen geplanten Programmstart genutzt werden können.

Fälschung:

Programmmanipulation.
Das Programm müsste durch eine manipulierte Version ersetzt werden, das falsche Anzeigen erzeugt.

Quelle:
Geplante Programmstarts nach Zeitplan - C:\Windows\Tasks.....notepad.exe; explorer.exe

Beschreibung der Quelle:

Im Verzeichnis C:\Windows\Tasks befindet sich für die mit den Programmen at.exe oder Systemsteuerung\Geplante Tasks geplanten Programmstarts für jeden Auftrag eine eigene .job Datei.

Verursachende Vorgänge:

- zukünftigen oder periodischen Programmstart planen

Entstehungsbedingungen:

Spezielle.
Die Programmstarts wurden mit at.exe oder mit Systemsteuerung\Geplante Tasks geplant.

Lebensdauer:

Solange der Zustand besteht.
Solange periodischer Start vorgesehen, werden diese angezeigt. Einmalige Programmstarts werden nur bis zu ihrer Ausführung angezeigt.

Informationsgehalt:

Zeit:	Zeit, zu dem der Start geplant wurde.
Benutzer:	Benutzer, der sie geplant hat.
Sonstiges:	Der zu startende Befehl, die dazugehörige Startzeit sowie gegebenenfalls die Periodizität.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Die *.job Dateien im Verzeichnis C:\Windows\Tasks sind zu untersuchen.
Die mit dem Befehl at.exe für die Programmstarts erzeugten Startdateien sind mit at1.job, at2.job u.s.w. benannt, die von der Systemsteuerung\Geplante Tasks erzeugten Startdateien haben einen vom Benutzer festgelegten Namen, der um das Kürzel job erweitert ist.

Obwohl im Inhalt der Jobdatei nicht alles im Klartext lesbar ist, kann hier jedoch mit einem Texteditor zwar nicht die geplante Zeit, jedoch zumindest der Programmname und -pfad und der Benutzer, unter dem es ausgeführt werden soll, erkannt werden. Wenn die Planung mit at.exe vorgenommen wurde, findet sich hier der Benutzer System und zusätzlich die Zeile „Erstellt von NetScheduleJobAdd“.
Im Explorer können mit einem Klick auf Eigenschaften des Jobs zusätzliche Informationen wie die geplante Zeit abgelesen werden. Hier lässt sich also selbst für eine Offlineanalyse die Datei einfach zur Auswertung auf ein anderes Windowssystem kopieren, wobei dann genauso vorgegangen werden kann.
An dem Zeitstempel "Erstellt am" der jeweiligen .job Datei sieht man, wann die Planung vorgenommen wurde.

Aufwand:

Gering.

Fehlinterpretation:

Gering.
Es ist zu bedenken, dass auch andere Möglichkeiten für einen geplanten Programmstart genutzt werden können.

Fälschung:

Programmmanipulation.
Eine Änderung der eigentlichen Inhalte würde auch die Funktionalität beeinflussen. Insofern kann nur das Anzeigeprogramm dahingehend abgeändert werden, dass die Dateien in diesem Verzeichnis nicht wahrheitsgemäß angezeigt wird.

Quelle:
Gespeicherte Benutzerprofile ..... regedit.exe; (regview.exe); Systemsteuerung/System >Erweitert > Benutzerprofile; explorer.exe; dir

Beschreibung der Quelle:

Es existiert eine Liste der auf dem Computer vorhandenen Benutzerprofile. Diese enthalten außer den lokalen Profilen gegebenenfalls auch Kopien von servergespeicherten Profilen von Active Directory Benutzern, die sich an diesem Rechner angemeldet haben.

Verursachende Vorgänge:

- AD Benutzeranmeldung an Active Directory
- Benutzeranmeldung lokal
- Terminalsitzung erstellen

Entstehungsbedingungen:

Keine.

Lebensdauer:

Bedingt abhängig von anderen Vorgängen.
Das Benutzerprofil kann unter Umständen manuell gelöscht werden. Bei servergespeicherten Benutzerprofilen ist auch eine Einstellung zum Löschen der lokalen Kopie des Profils beim Abmelden möglich.

Informationsgehalt:

Zeit: Systemdatum und Systemzeit des letzen Ausloggens an diesem Computer
Benutzer: Name der Benutzer, die sich an diesem Rechner jemals eingeloggt haben.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Eine Anzeige kann entweder über den Aufruf von System in der Systemsteuerung, Wechsel in Registerkarte „Erweitert“, Schaltfläche „Benutzerprofile“ oder direkt über die jeweiligen Registrywerte erfolgen.
Diese finden sich in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ als Schlüssel mit dem Namen ihrer SID.
Als Unterwert existiert im Falle der Verwendung des Active Directory ein Wert vom Typ REG_SZ mit der GUID des Benutzers.
Bei der grafischen Anzeige über System findet sich auch bei "Geändert" der Zeitpunkt des letzen Ausloggens an diesem Computer, da zu diesem Zeitpunkt das Profil zuletzt geschrieben wurde.
Über die Registry kommt man auch an diese Information, indem der Unterwert ProfileImagePath (Typ REG_EXPAND_SZ) weiterverfolgt wird und der Zeitstempel "Geändert am" des Benutzerverzeichnisses im Dateisystem angezeigt wird. Siehe auch Quelle "Zugriffe auf Benutzerprofil".

Aufwand:

Gering.

Fehlinterpretation:

Gering.
Wegen des Löschens ist zu beachten, dass nicht jeder jemals angemeldete Benutzer dauerhaft ein Benutzerprofil hinterlässt.

Fälschung:

Administratorrechte.
Die Benutzerprofile können im Betrieb nicht vom Benutzer selbst gelöscht werden. Außer dem Benutzer selbst haben standardmäßig nur Administratoren Zugriff, weshalb das Erlangen solcher Rechte notwendig ist.

Quelle:
Hibernate Datei..... (Hexeditor)

Beschreibung der Quelle:

Wenn der Computer in den Ruhemodus heruntergefahren wird, um z.B. Strom zu sparen, wird der Arbeitsspeicher auf eine Datei in der Festplatte geschrieben. Beim nächsten Start werden diese Daten wieder in den Arbeitsspeicher geladen.

Verursachende Vorgänge:

Praktisch alle Vorgänge die zur Zeit des Aktivieren des Ruhezustandes aktiv waren, oder über die Informationen im Arbeitsspeicher vorlagen sind hiervon betroffen.

Entstehungsbedingungen:

Spezielle.
Computer wird in den Ruhemodus heruntergefahren.

Lebensdauer:

Bedingt abhängig von anderen Vorgängen.
Die Daten der Datei bleiben so auch bestehen wenn das System aus dem Ruhezustand wieder hochgefahren wird. Neue ausgeführte Vorgänge im Arbeitsspeicher ändern diese Daten nicht. Erst ein nochmaliges Aktivieren des Ruhezustandes würde die Daten überschreiben.

Informationsgehalt:

Sonstiges: Theoretisch alles was zum Zeitpunkt vor dem Ruhezustand im Speicher war. Praktisch lassen sich hier jedoch nur die Inhalte interpretieren, denen ihr Darstellungscode zugeordnet werden kann. Dies gelingt wohl am häufigsten bei Texten, die mit den gebräuchlichen Codes dargestellt sind.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Die Datei c:\hiberfil.sys ist auf die gesuchten Textfragmente oder sonstige vermutete Inhalte z.B. mit einem Hexeditor zu untersuchen.

Aufwand:

Hoch.
Die Dateigröße entspricht der Größe des Arbeitsspeichers, wodurch die Datei typischerweise einige mehrere hundert Megabyte groß ist. Ohne eine zielgerichtete automatisierte Suche ist dafür enormer Zeitaufwand erforderlich. Die automatisierte Suche setzt zunächst voraus, dass die Untersuchungsperson durch Versuche einen Überblick über die gespeicherten Informationen erlangt und damit geeignete Suchwörter generiert.

Fehlinterpretation:

Hoch.
Nur die Textfragmente allein können leicht falsch interpretiert werden.

Fälschung:

Administratorrechte.
Mit Administrationsrechten kann die Aktivierung des Ruhezustandes deaktiviert werden. Damit wird allerdings eine neue Quelle erzeugt und die Daten der Datei gehen in die Quelle „Fragmente von Daten (Unallocated File Space, File Slack und Shadow Data)“ über. Weitere Information zu dieser auf dem entsprechenden Quellenblatt. Auch ist eine Änderung der einzelnen Inhalte z.B. mit einem Hexeditor möglich.

Quelle:

Inhalt von Dateien .....notepad.exe; (jeweiliges Anzeigeprogramm für bestimmte Formate)

Beschreibung der Quelle:

Der Dateiinhalt einer Datei, die vom Benutzer angelegt oder verändert wurde kann eine wichtige Quelle sein, die zwar nicht auf besondere Vorgänge im Computer schließen lässt, jedoch auf das, was der Benutzer wirklich bezweckt hat, wenn z.B. der Inhalt eines geschriebenen Briefs gefunden wird.

Verursachende Vorgänge:

- Datei anlegen
- Dateiinhalt ändern

Entstehungsbedingungen:

Keine.

Lebensdauer:

Bis zum nächsten Vorgang.
Eine erneute Änderung zerstört die Daten zu diesem Zustand. Jedoch finden sich dann z.B. eventuell in den unter der Quelle „Fragmente von Daten (Unallocated File Space, File Slack und Shadow Data)“ Teile dieses Zustandes.

Informationsgehalt:

Sonstiges: Dateiinhalte die der Benutzer erstellt hat.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Die Datei muss mit dem entsprechenden Betrachtungsprogramm, das dieses Format anzeigt, geöffnet werden.

Aufwand:

Gering.
Solange ein betreffendes Betrachtungsprogramm, das dieses Format anzeigt, vorhanden ist, kann mit geringem Aufwand nachvollzogen werden, woran der Benutzer gearbeitet hat.

Fehlinterpretation:

Gering.

Fälschung:

Programmmanipulation.
Ein Verbergen des Inhalts der Datei ohne ihn zu löschen, wäre nur denkbar, wenn die Anzeigeprogramme so manipuliert würden, dass diese nur noch Teile des Inhalts von bestimmten Dateien anzeigen.

Quelle:
Installierte Komponenten/Treiber..... devmgmt.msc; explorer.exe; dir; regedit.exe; (regview.exe)

Beschreibung der Quelle:

Die Treiber für die installierten Hardwarekomponenten lassen sich im Betrieb anzeigen oder finden sich in der Registry als Einträge.

Verursachende Vorgänge:

- Treiberinstallation

Entstehungsbedingungen:

Keine.

Lebensdauer:

Solange der Zustand besteht.

Informationsgehalt:

Zeit: Wann der Treiber installiert wurde.
Sonstiges: Welche Treiber installiert sind.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Mit devmgmt.msc erhält man eine Liste der installierten Hardwarekomponenten. Informationen zu dem dahinterstehenden Treiber erhält man indem für eine Komponente die Eigenschaften, Registerkarte Treiber, Treiberdetails angezeigt werden. Hier finden sich der Pfad und die genauen Dateinamen des Treibers. Diese können im Dateisystem gesucht werden und über ihre Zeitstempel (Erstellt am) erfährt man wann diese installiert wurden Die Einstellungen welche Treiber aktiv sind finden sich im Registrypfad HKEY_LOCAL_MACHINE\SYSTEM\Controlset001\Enum. Insofern ist die Registrydatei System zu untersuchen. Hier finden sich z.B. im Unterschlüssel PCI alle Komponenten die über eine PCI-Verbindung angeschlossen sind. Ebenso existiert u. a. ein Schlüssel USB und IDE. Jede dieser Komponenten besteht aus einem Unterschlüssel mit abstrakter Identifikationsnummer, aber in diesem findet sich ein Wert REG_SZ mit Namen “DeviceDesc“ der den Namen enthält der auch in der grafischen Verwaltung angezeigt wird. In den anderen Werten finden sich hier die restlichen Informationen.

Um auf den Benutzer zu schließen, der den Treiber installiert hat, sind andere Quellen hinzuzuziehen, die für die Erstellung der Treiberdateien selbst Information enthalten, wie ein eventuell vorhandenes Protokoll über Aktivitäten im Dateisystem.

Aufwand:

Hoch.
Hier muss man sich in sehr vielen Einträgen zurechtfinden, da sehr viele systeminterne Treiber wie die ACPI Funktionen hier ebenfalls eingetragen sind und nicht nur die offensichtlichen Treiber die normalerweise vom Benutzer zu installieren sind.

Fehlinterpretation:

Hoch.
Ob die installierten Treiber so wirklich funktionieren oder Fehler vorliegen lässt sich nicht oder nicht leicht erkennen.

Fälschung:

Programmmanipulation.
Das Programm müsste durch eine manipulierte Version ersetzt werden, das falsche Anzeigen erzeugt.

Quelle:
Installierte Software .....Systemsteuerung/Software; explorer.exe

Beschreibung der Quelle:

Die meisten Windowsprogramme tragen sich bei einer Installation in eine Liste ein, die vom Benutzer abgerufen werden kann und auch zum Deinstallieren dieser Programme genutzt werden kann.
Ebenso finden sich Verknüpfungen zu den Programmen meist, aber nicht notwendigerweise im Startmenü des jeweiligen Benutzers oder im für alle Benutzer gleichen Teil des Startmenüs und die Programmdaten selbst in oft in demStandardverzeichnis C:\Programme\.

Verursachende Vorgänge:

- Softwareinstallation

Entstehungsbedingungen:

Spezielle.
Nicht bei allen Programmen zutreffend; vor allem kleinere Tools erfordern mitunter gar keine Installation sondern bestehen nur aus einer einzigen ausführbaren Datei, die überall hinkopiert werden kann. Die Standardprogramme lassen sich aber auf diesem Weg überprüfen

Lebensdauer:

Solange der Zustand besteht.

Informationsgehalt:

Sonstiges: Welche Programme installiert sind.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Die Liste der installieren Programme lässt sich über die Systemsteuerung/Software aufrufen. Diese Daten liegen in der Registry im Pfad
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall.
Jeder Eintrag befindet sich in einem Unterschlüssel der oft, aber nicht zwingend, dem Programmnamen entspricht. Der angezeigte Wert in der grafischen Oberfläche entspricht dem Wert „DisplayName“ vom Typ REG_SZ. Hier finden sich auch Werte die u. a. auf das Programmverzeichnis („InstallLocation“) verweisen. Diese können dann eventuell über andere Quellen nachvollzogen werden, wann diese angelegt worden sind und vom welchem Benutzer (siehe z.B. Vorgang "Datei anlegen").

Das Verzeichnis C:\Programme kann einfach mit dem Explorer durchsucht werden.
Das Startmenü des jeweiligen Benutzers findet sich unter C:\Dokumente und Einstellungen\#BENUTZERNAME#\Startmenü\ und der Teil des Startmenüs, der für alle Benutzer gleich ist, unter C:\Dokumente und Einstellungen\All Users\Startmenü.

Aufwand:

Gering.

Fehlinterpretation:

Hoch.
Die allermeisten Programme verhalten sich wie oben beschrieben. Deshalb kann leicht vergessen werden, das dies nicht zwingend ist.

Fälschung:

Leicht.
Die Registry und Startmenüeinträge können von normalen Benutzern verändert oder ganz gelöscht werden. Dies verändert noch nichts an der Funktionalität der Programme selbst.

Quelle:
Internet Explorer: Cookies.....explorer.exe; dir

Beschreibung der Quelle:

Um die Einstellungen eines Benutzers auf besuchten Internetseiten zu speichern, existiert die Methode die Einstellungen auf dem Rechner des Benutzers zu speichern. Diese Cookie genannten Dateien werden nicht für jeden besuchten Server angelegt, sondern nur bei denen, die diese Funktion nutzen. Zu beachten ist, dass der Name oft der eines anderen Servers, der nur die Werbeanzeigen schaltet, ist.

Verursachende Vorgänge:

- Internet Explorer: Internetseite aufrufen

Entstehungsbedingungen:

Spezielle.
Server sendet Cookie für aufgerufene Seite und der Internet Explorer ist so eingestellt, dass er die Cookies annimmt.

Lebensdauer:

Bedingt abhängig von anderen Vorgängen.
Cookie bleibt bis zur manuellen Löschung erhalten.

Informationsgehalt:

Zeit:	Systemdatum und Systemzeit der Verbindung zu diesem Server der das Cookie erstellte.
Benutzer:	Benutzername für den dieses Cookie erstellt wurde.
Sonstiges:	Das eine Verbindung mit diesem Server stattgefunden hat.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

In dem Verzeichnis des jeweiligen Benutzers C:\Dokumente und Einstellungen\#Benutzername#\Cookies sind die vorhanden Cookies zu betrachten. Deren Name gibt Auskunft über den besuchten Server: "Cookie:#BENUTZERNAME#@#BESUCHTER SERVER#"
Der Zeitstempel "Erstellt am" eines Cookies gibt an, wann der erste Besuch war, Zeitstempel "Geändert am" wann ein eventueller späterer Besuch, bei dem die Einstellungen geändert wurden und der den Zeitstempel aktualisiert hat und der Zeitstempel "Letzter Zugriff" wann der letzte Besuch war, bei dem der Server nur die Einstellungen aus dem Cookie angefordert hat.
Der Inhalt des Cookies enthält eventuell noch mehr Informationen zu den Benutzeraktivitäten auf diesen Webseiten, aber je nach Server haben diese ein unterschiedliches Format für die spezifischen Informationen die dieser Server speichert.
Außerdem existiert in diesem Verzeichnis auch eine Datei namens index.dat. Deren Eigenschaften werden auf dem Quellenblatt "Internet Explorer: index.dat" genauer erläutert.

Aufwand:

Gering.

Fehlinterpretation:

Hoch.
Die Cookies kommen oft von speziellen Servern, die die Werbung auf anderen Seiten schalten. Der Benutzer muss also die angegebenen Rechner nicht wissentlich besucht haben, sondern die Erzeugung kann durch den Besuch ganz anderer Seiten ausgelöst worden sein.

Fälschung:

Leicht.
Internet Explorer, Extras, Internetoptionen, Temporäre Internetdateien - "Cookies löschen" löscht diese Dateien. Aber auch eine direkte Löschung oder Änderung dieser Dateien in diesem Verzeichnis vom Benutzer selbst, oder mit Administratorrechten auch bei anderen möglich.

Quelle:
Internet Explorer: index.dat.....notepad.exe; (trace.exe)

Beschreibung der Quelle:

Bei den beschriebenen Quellen Cookies, Temporary Internet Files und Verlauf des Internet Explorers wird jedes Mal teilweise die Datenstruktur der index.dat verwendet. Auf diese geht dieses Quellenblatt genauer ein. Im Normalfall sollten diese mit den anderen Quellen übereinstimmen und dieselben Informationen liefern. Sind jedoch die anderen Quellen gefälscht oder schon gelöscht, bietet sich hiermit noch eine Möglichkeit dennoch an die Informationen zu kommen.

Verursachende Vorgänge:

- Internet Explorer: Internetseite aufrufen

Entstehungsbedingungen:

Keine.

Lebensdauer:

Bedingt abhängig von anderen Vorgängen.
Kann manuell gelöscht werden. Je nach dem um welche index.dat sich handelt (Cookies/Temporary Internet Files/Verlauf) je nach Einstellungen dort auch Überschreibung.

Informationsgehalt:

Zeit:	Systemdatum und Systemzeit wann letzter Zugriff auf bestimmte Seite stattgefunden hat
Benutzer:	Benutzername der auf Seiten zugegriffen hat
Sonstiges:	URL der Seiten

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Diese Dateiname und das Dateiformat wird sowohl für die Cookies, die Termporären Internet Dateien und auch den Verlauf, die alle schon auf einem extra Quellenblatt erklärt wurden, verwendet.
Insofern findet sich eine solche Datei unter
C:\Dokumente und Einstellungen\#BENUTZERNAME#l\Lokale Einstellungen\Temporary Internet Files\Content.IE5,
in C:\Dokumente und Einstellungen\#BENUTZERNAME#l\Lokale Einstellungen\Verlauf\History.IE5 und den darin enthaltenen Unterverzeichnissen und in
C:\Dokumente und Einstellungen\#BENUTZERNAME#\Cookies.

Von den enthaltenen Informationen sind nur die URLs der Aufgerufenen Seiten im Klartext sichtbar. Der Benutzer ist dadurch festgelegt, dass man durch den Verzeichnispfad schon einen bestimmten Benutzer für die Untersuchung bestimmt hat. Mehr Informationen lassen sich erhalten, wenn das Programm WinTrace [Xway03] verwendet wird. Mit diesem kann diese Datei anaylsiert werden. Dazu kann es allerdings nötig sein die Datei erst mit z.B. xcopy /H info2 c:\temp\ in ein normales Verzeichnis kopieren, um dem Programm den Zugriff zu erleichtern.

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Leicht.
Über die jeweiligen Internet Explorer Funktionen „Cookies löschen“ / „Dateien löschen“ / „Verlauf leeren“ bleiben zwar teilweise Einträge zurück. Allerdings lassen sich die Dateien auch direkt selbst löschen.

Quelle:
Internet Explorer: Temporäre Dateien.....explorer.exe; dir

Beschreibung der Quelle:

Dateien die bei einem Besuch von Internetseiten zwischengespeichert wurden. Umfasst die html-Seiten, auf den Seiten enthaltene Bilder wie gif oder jpg und auch andere Dateiformate, wie z.B. im Internet Explorer betrachtete pdf-Dokumente.

Verursachende Vorgänge:

- Internet Explorer: Internetseite aufrufen

Entstehungsbedingungen:

Keine.

Lebensdauer:

Bedingt abhängig von anderen Vorgängen.
Je nach den Einstellungen des Internet Explorers wie viel Speicherplatz hierfür verwendet werden soll, und wie intensiv die Internetnutzung ist, erfolgt hier eine Überschreibung der alten mit neuen Daten früher oder später.

Informationsgehalt:

Zeit: Systemdatum und Systemzeit
Benutzer: Benutzer bei dem die Dateien durch den Besuch von Seiten angefordert wurden.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Im Ordner des Benutzers unter C:\Dokumente und Einstellungen\#BENUTZERNAME#l\Lokale Einstellungen\Temporary Internet Files\ findet sich ein verstecktes Unterverzeichnis Content.IE5. Für die Anzeige versteckter Unterverzeichnisse kann dir /Ad verwendet werden.
Zu beachten ist, dass eine aufgeschlüsselte Anzeige mit dem Explorer nur bei dem Verzeichnis des verwendeten Benutzers erfolgt.
Hierin existiert eine Datei namens index.dat (Siehe auch Quelle "Internet Explorer: index.dat") deren Inhalt zur Verwaltung der gecachten Objekte dient. Diese selbst befinden sich hier in mehreren versteckten Unterverzeichnissen mit keine Systematik erkennen lassenden Namen wie 6TE9UDWT. In diesen befinden sich die eigentlichen Dateien. Von diesen ist der Name, Typ und Inhalt interessant. Die Zeit des Abrufes erhält man über die Zeitstempel.

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Leicht.
Internet Explorer, Extras, Internetoptionen, Temporäre Internetdateien - "Dateien löschen" löscht diese Dateien. Aber auch eine direkte Löschung oder Änderung von Dateien in diesem Verzeichnis ist vom Benutzer bei sich selbst, oder mit Administratorrechten auch bei anderen möglich.

Quelle:
Internet Explorer: Verlauf ..... explorer.exe; dir.exe; notepad.exe

Beschreibung der Quelle:

Die mit dem Internet Explorer besuchten Seiten werden aufgezeichnet um über die Funktion Verlauf auf die Besuche der letzten Tage zurückschauen zu können.

Verursachende Vorgänge:

- Internet Explorer: Internetseite aufrufen

Entstehungsbedingungen:

Keine.

Lebensdauer:

Bedingt abhängig von anderen Vorgängen.
Einträge bleiben solange erhalten, wie in den Einstellungen des Internet Explorers unter "Tage, die die Seiten in 'Verlauf' aufbewahrt werden:" eingestellt ist (Standard 20 Tage).

Informationsgehalt:

Zeit: Systemdatum, aber meist nicht auf den Tag genau, sondern für weit zurückliegende Besuche nur auf die Woche oder den Monat genau.
Benutzer: Benutzer der Seiten besucht hat

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Der Verlauf befindet sich in C:\Dokumente und Einstellungen\#BENUTZERNAME#l\Lokale Einstellungen\Verlauf
Zu beachten ist, dass eine aufgeschlüsselte Anzeige mit dem Explorer nur beim Betrachten des Verzeichnisses des verwendeten Benutzers passiert.
Für eine Offlineanalyse ist in das enthaltene versteckte Unterverzeichnis History.IE5 zu wechseln. Die Anzeige versteckter Unterverzeichnisse kann mit dir /Ad erfolgen. Hier befinden sich nun mehrere versteckte Ordner vom Format MSHist01#JAHR1##MONAT##TAG1##JAHR2##MONATt2##TAG2# wobei jeweils die Einträge enthalten sind die zwischen den Angaben 1 und 2 exklusive das Datum von 2 selbst liegen.
Beispielsweise enthält MSHist012004011920040126 die Einträge für die Woche vom 19.01.2004 bis zum 26.01.2004.
Die Zeiträume dabei sind entweder ganze Monate, Wochen, oder einzelne Tage, wobei z.B. die angefangenen Monate bei einer Initialisierung des Verlaufs erst ab dem Datum der Installation anfangen. In diesen Verzeichnissen ist die jeweilige Datei index.dat mit einem Texteditor zu öffnen. Hier finden sich neben vielen Sonderzeichen im Klartext die besuchten Seiten. Zwar findet sich auch hier vor jeder URL nochmals die zugehörige Datumsangabe im Klartext. Allerdings entspricht diese auch nur dem Zeitraum der schon für Verzeichnisnamen verwendet wurde und ist bei allen in derselben index.dat gleich.
(Siehe dazu auch Quelle "Internet Explorer: index.dat")

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Leicht.
Internet Explorer, Extras, Internetoptionen, "Verlauf leeren" löscht den Verlauf. Über eine direkte Änderung an der index.dat ist neben der Löschung auch eine Änderung auf falsche Daten durch den Benutzer selbst, oder mit Administratorrechten auch bei anderen Benutzern möglich.

Quelle:
Internet Explorer: Zuletzt eingegebene URLs.....regedit.exe; (regview.exe)

Beschreibung der Quelle:

Bis zu 25 der zuletzt eingegebenen URLs die direkt in die Adressleiste des Internet Explorers eingegeben wurden und dort auch noch zur Auswahl angezeigt werden, finden sich in der Registry.

Verursachende Vorgänge:

- Internet Explorer: Internetseite aufrufen

Entstehungsbedingungen:

Spezielle.
Nur wenn Internetadresse direkt über die Adresszeile aufgerufen wurde.

Lebensdauer:

Bedingt abhängig von anderen Vorgängen.
Nach 25 Adressen werden die ältesten auf die Einträge, deren die am längsten nicht mehr benutzt wurden, wieder überschrieben.

Informationsgehalt:

Benutzer: Benutzer der Internetadresse eingegeben hat.
Sonstiges: Internetseite die eingegeben wurden.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

In der jeweiligen ntuser.dat des Benutzers finden sich unter HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs in Werten mit dem Namen url1 und fortlaufenden Nummern, die eingegebenen Adressen.

Aufwand:

Gering.

Fehlinterpretation:

Gering.
Wenn ein sich hier eine Eintrag findet, ist auf diese Adresse zugegriffen worden.
Aus nichtvorhandenen Einträgen lässt sich jedoch nicht folgern, dass auf diese nicht zugegriffen wurde (siehe Entstehungsbedingungen).

Fälschung:

Leicht.
Benutzer selbst hat auf diesen Schlüssel jeweils Zugriff und kann diese Löschen oder Verändern. Auch für Benutzer die sich nicht mit der Registry auskennen, besteht die Möglichkeit diese Liste durch einen grafischen Dialog zurückzusetzen: Internet Explorer, Extras, Internetoptionen, "Verlauf leeren" löscht neben dem Verlauf auch diese Liste.

Quelle:
Letzter angemeldeter Benutzer .....regedit.exe; (regview.exe)

Beschreibung der Quelle:

Der letzte sich erfolgreich lokal oder über das Active Directory angemeldete Benutzer bleibt an dem Computer, an dem er sich eingeloggt hat, in der Registry gespeichert.

Verursachende Vorgänge:

- AD Benutzeranmeldung an Active Directory (an Client der sich anmeldet)
- Benutzeranmeldung lokal

Entstehungsbedingungen:

Keine.

Lebensdauer:

Bis zum nächsten Vorgang.

Informationsgehalt:

Benutzer: Zuletzt angemeldeter Benutzer.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Im Schlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon im Wert DefaultUserName befindet sich der Name des Benutzers, der sich zuletzt lokal angemeldet hat

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Leicht.
Wert ist mit Benutzerrechten änder- oder löschbar.

Quelle:
Netzwerkverkehr - Aufzeichnung .....netmon.exe

Beschreibung der Quelle:

Das Programm C:\WINDOWS\system32\netmon\netmon.exe zeigt Daten zum aktuellen Netzwerkverkehr an und zeichnet während der Laufzeit des Programms hierzu Daten auf.
Der Netzwerkmonitor ist nicht standardmäßig installiert, befindet sich jedoch auf der Installations-CD und kann von dort über „Systemsteuerung/Software/Windowskomponenten hinzufügen“ installiert werden.

Verursachende Vorgänge:

- Netzwerkverkehr verursachen

Entstehungsbedingungen:

Spezielle.
Aufzeichnung muss manuell vor den Vorgängen gestartet werden.

Lebensdauer:

Speziell.
Einige Informationen wie z.B. Bytes pro Sekunde stehen nur aktuell zur Verfügung. Diese fließen zwar in Statistik „Byteanzahl insgesamt versendet“ ein. Aber die Information, dass um die Zeit genau der Verkehr war, geht verloren.
Die aufgezeichneten Daten können dagegen abgespeichert werden und bleiben dann erhalten.

Informationsgehalt:

Sonstiges: Es werden sowohl aktuell bestehende Daten wie die gesendeten und empfangenen Bytes pro Sekunde als auch eine Statistik aller seit der Aufzeichnung angefallenen Daten aufgezeichnet. Besonders interessant kann die Information sein, welche MAC-Adressen zueinander Daten schicken. (Hierbei wird aber nur zu oder vom dem lokalen Computer gehende Kommunikation aufgezeichnet und nicht die theoretisch auch abhörbare Kommunkation anderer Rechner bei einer Shared Medium Verbindung)

Verfügbarkeit:

Nur online verfügbar.

Auswertung:

Nach gegebenenfalls Installation ist der Netzwerkmonitor zu starten und die Aufzeichnung zu starten. Dabei können die aktuellen Werte zur Auslastung betrachtet werden. Die gesammelten Statistikdaten können am Ende der Aufzeichnung abgespeichert werden..

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Programmmanipulation.
Das Programm müsste durch eine manipulierte Version ersetzt werden, das falsche Anzeigen erzeugt.

Quelle:
Netzwerkverkehr - Statistik..... netstat -e -s

Beschreibung der Quelle:

Die Ausgabe des Befehls netstat -e -s zeigt die Ethernetstatistik seit der Initialisierung der Netzwerkverbindung an.

Verursachende Vorgänge:

- Netzwerkverkehr verursachen

Entstehungsbedingungen:

Keine.

Lebensdauer:

Bedingt abhängig von anderen Vorgängen.

Informationsgehalt:

Sonstiges: Verschiedenste Daten zur Netzwerkverbindung wie empfangene und gesendete Bytes oder die Anzahl der Pakete/Datagramme bei TCP/UDP.

Verfügbarkeit:

Nur online verfügbar.

Auswertung:

Ausgabe von netstat -e -s betrachten.

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Programmmanipulation.
Das Programm müsste durch eine manipulierte Version ersetzt werden, das falsche Anzeigen erzeugt.

Quelle:
Papierkorb ..... dir; notepad.exe; (trace.exe)

Beschreibung der Quelle:

Der Papierkorb ist ein spezielles Verzeichnis in das standardmäßig mit dem Explorer "gelöschte" lokale Dateien verschoben werden.

Verursachende Vorgänge:

- Datei löschen
- Verzeichnis löschen

Entstehungsbedingungen:

Spezielle.
Einstellungen des Papierkorbs "Dateien sofort löschen" muss deaktiviert sein (Standard).

Die betreffenden Dateien und Verzeichnisse werden nur in den Papierkorb verschoben, wenn sie auf lokalen Datenträgern über den Explorer gelöscht werden (ohne dabei Shift gedrückt zu halten). Bei der Verwendung des Befehls del in der Eingabeaufforderung entsteht die Quelle nicht.

Lebensdauer:

Bedingt abhängig von anderen Vorgängen.
Allerdings abhängig davon welche Dateien und Verzeichnisse später gelöscht werden und Einstellungen wie viel Platz der Papierkorb beanspruchen darf (Standard: 10% des Laufwerks). Danach werden ältere Dateien und Verzeichnisse mit neu gelöschten überschrieben.

Informationsgehalt:

Zeit:	Systemdatum und Systemzeit des Löschzeitpunktes
Benutzer:	Benutzer, der die Löschung veranlasst hat
Sonstiges:	Welche Datei oder welches Verzeichnis gelöscht wurde, und der Inhalt der Datei bzw. des Verzeichnisses.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Der Papierkorb befindet sich auf dem jeweiligen Festplattenlaufwerk im Verzeichnis RECYCLER.
In diesem existiert für jeden Benutzer ein Unterverzeichnis mit dessen gelöschten Dateien. Dieses hat allerdings nicht den Benutzernamen, sondern die SID des Benutzers als Titel. Eine Zuordnung der SID zum Benutzernamen ist am betreffenden System über das Programm sid2user [Rudn98] möglich.

Zu beachten ist, dass der Explorer den Papierkorb nur für den eigenen Benutzer anzeigt. Auch wenn hier in das Verzeichnis eines anderen Benutzers gewechselt wird zeigt er das eigene Papierkorbverzeichnis an. Hier ist gegebenenfalls mit den Shellbefehlen vorgehen.

Im Verzeichnis selbst finden sich die gelöschten Dateien oder Verzeichnisse. Allerdings wurden diese umbenannt, und sind nun im Format DCx.#BISHERIGE ENDUNG#, also z.B. DC10.txt für eine gelöschte Textdatei. Die Inhalte der gelöschten Verzeichnisse existieren unter ihren normalen Datei- oder Verzeichnisnamen weiter. Der vorherige Name der direkt gelöschten Dateien oder Verzeichnisse findet sich in der INFO2 Datei in selbem Verzeichnis. Dort findet sich eine Liste aller Dateien mit ursprünglichem Pfad und Verweis auf die DC-Nummer. Die ursprünglichen Namen stehen dabei mit Pfadangabe im Klartext in der Datei.

Hierbei kann auch das Programm Wintrace [Xway03] zum Einsatz kommen, das diese INFO2 Dateien analysieren und neben dem ursprünglicher Namen und Pfad auch das Löschdatum liefer kann. Dazu kann es allerdings nötig sein die Datei erst mit z.B. xcopy /H info2 c:\temp\ in ein normales Verzeichnis kopieren, um dem Programm den Zugriff zu erleichtern.

Aufwand:

Gering.

Fehlinterpretation:

Gering.
Wenn ein sich hier eine Datei oder ein Verzeichnis findet, ist dieses gelöscht worden.
Aus nichtvorhandenen Dateien oder Verzeichnissen lässt sich jedoch nicht folgern, dass diese nicht gelöscht worden sind.

Fälschung:

Leicht.
Den eigenen Papierkorb zu löschen ist mit normalen Benutzerrechten möglich. Auch die Entstehung kann einfach umgangen werden, wenn der del-Befehl verwendet wird oder wenn während der Auswahl des Befehls im Explorer die Shift-Taste gedrückt gehalten wird.

Quelle:
Terminaldiensteverwaltung - Remoteüberwachung .....tsadmin.exe

Beschreibung der Quelle:

Über die Terminaldiensteverwaltung (tsadmin.exe) lässt sich die komplette Bildschirmausgabe von anderen Terminalbenutzersitzungen betrachten.

Verursachende Vorgänge:

- in Terminalsitzung arbeiten

Entstehungsbedingungen:

Spezielle.
In der Terminaldienstekonfiguration (tscc.msc) muss die Remoteüberwachung aktiviert sein ((Ast Verbindung, Eigenschaften von RDP-Tcp, Registerkarte Remoteüberwachung, "Remoteüberwachung mit folgenden Einstellungen verwenden" aktivieren und "Benutzerberechtigung anfordern" deaktivieren).
Die Terminaldiensteveraltung (tsadmin.exe) muss selbst in einer Terminalsitzung aufgerufen werden, um die Überwachung zu beginnen.

Lebensdauer:

Speziell.
Es kann immer nur der gerade aktuelle Bildschirminhalt beobachtet werden.

Informationsgehalt:

Sonstiges: Man sieht alles was der Benutzer auf seinem Bildschirm sieht

Verfügbarkeit:

Nur online verfügbar.

Auswertung:

Sich selbst auf einem Terminalserver entfernt anmelden. In dieser Remotesitzung unter tsadmin.exe die jeweilige andere existierende Terminalbenutzersitzung auswählen und Remoteüberwachung im Kontextmenü auswählen. Nun kann man alles beobachten, was dieser Benutzer in seiner Benutzersitzung selbst sieht.

Aufwand:

Hoch.
Man muss die Benutzersitzung über deren gesamte Dauer beobachten.

Fehlinterpretation:

Gering.

Fälschung:

Programmmanipulation.
Hier ist es nur denkbar die betreffenden Terminalserverkomponenten auf dem Terminalserver selbst zu manipulieren, um falsche Ausgaben zu erzeugen.

Quelle:
Verknüpfungen zu Datei in 'Recent' ..... explorer.exe; dir

Beschreibung der Quelle:

Wenn Dateien von Programmen zum Lesen geöffnet werden hinterlassen sie in vielen Fällen (siehe Entstehungsbedingungen) eine Verknüpfung im Benutzerverzeichnis \Recent für die zuletzt verwendeten Dokumente.

Verursachende Vorgänge:

- Datei lesen

Entstehungsbedingungen:

Spezielle.
Hier gibt es bei der Entstehung Ausnahmefälle. So spielt es eine Rolle ob der Startvorgang über den Explorer erfolgt, über die Shell ausgeführt wird, oder ob nur der Öffnen-Dialog des entsprechenden Anwenderprogramms verwendet wird. Hierbei ist es dann von Anwenderprogramm zu Anwenderprogramm unterschiedlich.

	Über Explorer	Über Shell	Über Menüdialog „Öffnen“ im Programm
Edit.com	Ja	Nein	Nein
Notepad.exe	Ja	Nein	ja

Lebensdauer:

Bedingt abhängig von anderen Vorgängen.
Während im Eintrag des Startmenüs 'Zuletzt verwendete Dokumente' nur die letzten 10 Dokumente angezeigt werden, befinden sich im Verzeichnis selbst wesentlich mehr Verknüpfungen. Nach welchem Schema diese Verknüpfungen wieder überschrieben werden, konnte nicht abschließend ermittelt werden. Jedoch können sich hier einige hundert Verknüpfungen zu teils sehr lang zurückliegenden Zugriffen finden lassen.

Informationsgehalt:

Zeit: Systemdatum und Systemzeit
Benutzer: Benutzer der auf Datei zugegriffen hat
Sonstiges: Dateien auf die zugegriffen wurde.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Die bei erfüllten Entstehungsbedingungen erstellten Verknüpfungen finden sich im Benutzerverzeichnis (Standard C:\Dokumente und Einstellungen\#Benutzername#\) im Unterordner \Recent.
Der Benutzer kann dadurch identifiziert werden, in wessen Benutzerverzeichnis sich die Verknüpfung befindet Die Zeitstempel der Verknüpfung "Geändert am" / "Letzter Zugriff am" zeigen wann zuletzt auf die Datei zugegriffen wurde. Falls "Erstellt am" eine andere Zeit anzeigt heißt das, dass mehrmals auf die Datei zugegriffen wurde, und dieser Zeitpunkt war das erste Mal, oder das erste Mal nach dem Ablauf der Lebensdauer eines früheren Zugriffes.

Achtung:
- Verzeichnis Recent taucht im Explorer nicht bei allen Windowsversionen auf, durch Eingabe in die Pfadleiste kommt man aber immer dahin.
- Über den Eintrag im Startmenü 'Zuletzt verwendete Dokumente' werden nur die letzten 10 verwendeten Verknüpfungen angezeigt.

Aufwand:

Gering.

Fehlinterpretation:

Hoch.
Wenn ein sich hier eine Verknüpfung findet, ist auf diese Datei zugegriffen worden.
Aus nichtvorhandenen Verknüpfungen lässt sich jedoch nicht folgern, dass auf diese nicht zugegriffen wurde (siehe Entstehungsbedingungen).

Fälschung:

Leicht.
Es ist sowohl möglich die Erstellung zu umgehen, als auch diese mit normalen Benutzerrechten nachträglich zu löschen.

Quelle:
Verknüpfungen zu Ordner in 'Recent'.....explorer.exe; dir

Beschreibung der Quelle:

Wenn Dateien von Programmen zum Lesen geöffnet werden hinterlassen sie in vielen Fällen (siehe Entstehungsbedingungen) neben einer Verknüpfung auf die Datei für die zuletzt verwendeten Dokumente auch eine Verknüpfung in den Ordner der Datei im Benutzerverzeichnis \Recent.

Verursachende Vorgänge:

- Datei lesen

Entstehungsbedingungen:

Spezielle.
Hier gibt es bei der Entstehung Ausnahmefälle. So spielt es eine Rolle ob der Startvorgang über den Explorer erfolgt, über die Shell ausgeführt wird, oder ob nur der Öffnen-Dialog des entsprechenden Anwenderprogramms verwendet wird. Hierbei ist es dann von Anwenderprogramm zu Anwenderprogramm unterschiedlich.

	Über Explorer	Über Shell	Über Menüdialog „Öffnen“ im Programm
Edit.com	Ja	Nein	Nein
Notepad.exe	Ja	Nein	ja

Lebensdauer:

Bedingt abhängig von anderen Vorgängen.
Nach welchem Schema diese Verknüpfungen wieder überschrieben werden konnte nicht abschließend ermittelt werden, jedoch können sich hier einige hundert Verknüpfungen zu teils sehr lang zurückliegenden Zugriffen finden lassen.

Informationsgehalt:

Zeit: Systemdatum und Systemzeit
Benutzer: Benutzer der auf Dateien im Verzeichnis zugegriffen hat
Sonstiges: Verzeichnis in dem auf Dateien zugegriffen wurde.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Die bei erfüllten Entstehungsbedingungen erstellten Verknüpfungen zu Verzeichnissen finden sich im Benutzerverzeichnis (Standard C:\Dokumente und Einstellungen\#Benutzername#\) im Unterordner \Recent.
Der Benutzer kann identifiziert werden, in wessen Benutzerverzeichnis sich die Verknüpfung befindet.
Die Zeitstempel der Verknüpfung "Geändert am" / "Letzter Zugriff am" zeigen wann zuletzt auf eine Datei im Ordner zugegriffen wurde. Falls "Erstellt am" einen andere Zeitpunkt anzeigt, heißt das, dass mehrmals auf Dateien in diesem Ordner zugegriffen wurde, und dieser Zeitpunkt war das erste Mal, oder das erste Mal nach dem Ablauf der Lebensdauer eines vorigen Males.

Achtung:
- Verzeichnis Recent taucht im Explorer nicht bei allen Windowsversionen auf, durch Eingabe in die Pfadleiste kommt man aber immer dahin.
- Über den Eintrag im Startmenü 'Zuletzt verwendete Dokumente' werden keine Ordnerverknüpfungen sondern nur die Dateiverknüpfungen angezeigt.

Aufwand:

Gering.

Fehlinterpretation:

Hoch.
Wenn Verzeichnis hier nicht vorkommt, heißt das noch nicht, dass eine Datei dieses Verzeichnisses nicht geöffnet wurde (siehe Entstehungsbedingungen)

Fälschung:

Es ist sowohl möglich die Erstellung zu umgehen, als auch diese mit normalen Benutzerrechten nachträglich zu löschen.

Quelle:
Webserver IIS Protokollierungsdateien.....notepad.exe

Beschreibung der Quelle:

Für die einzelnen auf dem Computer zur Verfügung gestellten Webseiten lässt sich mit dem Internetinformationsdienste-Manager (C:\Windows\system32\inetsrv\iis.msc) eine Protokollierung aktivieren. Hierfür stehen verschieden Protokollformate (Microsoft IIS, NCSA allgemein, ODBC und W3C erweitert) zur Verfügung.

Verursachende Vorgänge:

- IIS Webseite von diesem Computer abrufen

Entstehungsbedingungen:

Spezielle.
Die Protokollierung muss für die jeweilige Website aktiviert sein (Standard) und es muss noch Speicherplatz

Lebensdauer:

Bedingt abhängig von anderen Vorgängen.
Einmal angelegte Einträge werden nicht mehr überschrieben. Die Einstellung „maximale Protokollgröße“ bezieht sich bei Aktivierung und Setzen eines Größenwertes nur darauf, ab welcher Größe eine neue Protokolldatei erstellt werden soll. Die alten Protokolldateien bleiben erhalten. Jedoch können die Dateien manuell gelöscht werden.

Informationsgehalt:

Zeit:	Systemdatum und Systemzeit des Zugriffs
Benutzer:	Client Adresse von dem eine Anfrage kam
Sonstiges:	Name der abgerufenen Seite

Die genauen Einstellungen was bei Benutzerdefinierten Einstellungen im W3C-Format alles protokolliert wird, kann hiervon abweichen. Obige Daten sind jedoch die Standardeinstellung.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Je nach gewählten Einstellungen des Protokollformats befinden sich die aufgezeichneten Informationen entweder in der angegebenen ODBC Datenbank oder im Protokolldateiverzeichnis (Standard C:\Windows\system32\LogFiles\W3SVC1 (für Formate Microsoft IIS, NCSA allgemein und W3C erweitert. Hier wird je nach Einstellung eine Neue Protokolldatei Stündlich/Täglich/Wöchentlich/Monatlich mit beschränkter Datengröße oder unbeschränkt angelegt.
Der Name der Datei variiert je nach Einstellung des Protokollformats und des Zeitplans. Bei zeitabhängigen Einstellungen findet sich die jeweilige Datumsangabe im Namen wieder. So ist für die Standardeinstellung W3C erweitert und Täglich das Format exjjmmtt.log also am konkreten Beispiel ex040112 für das W3C-Protokoll zum 12. Januar 2004. Für Protokolle im NCSA Format beginnt der Dateiname mit "nc", für das IIS Format mit "in". Die anderen Namensgebungen können unter [Micr03] nachgesehen werden.

Die Dateien selbst können mit einem Texteditor angezeigt werden. Das jeweilige Format dazu findet sich z.B. unter folgenden Adressen:

- Protokollformat "W3C erweitert" unter [HaBe96]
- Protokollformat "NCSA allgemein" (NCSA common) unter [Inte03]
- Protokollformat "Microsoft IIS" unter [Micr00]

Außerdem können bestehende Logdateien in den drei Textformaten mit dem mitgelieferten Tool convlog.exe in ein anderes der drei Formate umgewandelt werden.

Zu beachten ist, dass die Zeitangaben beim Format „W3C erweitert“ nicht in lokaler Zeit, sonder GMT (Greenwich Mean Time) aufgezeichnet werden. Die Benennung der entsprechenden Protokolldateien entspricht standardmäßig auch der GMT, kann aber auch auf die lokale Zeit eingestellt werden.

Aufwand:

Hoch.
In Produktivsystem fallen hier sehr viele zu analysierende Einträge an. Wenn nicht schon bestimmte Verdächtigung im Hinblick auf die gesuchten Übertragung, wie die IP-Adresse des Abrufers, die abgerufene Seite oder der Zeitraum, bestehen, ist die Auswertung höchst zeitaufwändig.

Fehlinterpretation:

Gering.
Zu beachten ist, dass die Zeit beim W3C Format in GMT (Greenwich Mean Time) und nicht der lokalen Zeit angegeben ist.

Fälschung:

Administratorrechte.
Für eine Änderung oder Löschung der Protokolldateien sind Administratorenrechte nötig, da Benutzer standardmäßig für diese nur Leseberechtigungen besitzen.

Quelle:
Zeitstempel "Erstellt am" von Dateien .....explorer.exe; dir /Tc

Beschreibung der Quelle:

Der Zeitstempel "Erstellt am" der betroffenen Datei gibt das Systemdatum und die Systemzeit für deren Erstellung durch die folgenden Vorgänge an.

Verursachende Vorgänge:

- Datei anlegen
- Datei kopieren (für die neue Datei, der Zeitstempel der alten bleibt unverändert)
- Datei verschieben

Entstehungsbedingungen:

Spezielle.
Abhängig von der Art der Ausführung ausschließlich bei folgendem Vorgang:

- Beim Vorgang "Datei verschieben":
  Innerhalb derselben Partition (FAT32 oder NTFS) gibt es keine Änderung dieses Zeitstempels.
  Von einer Partition in eine andere wird der Zeitstempel "Erstellt am" nur verändert, wenn mit dem move-Befehl der Shell verschoben wird. Mit dem Explorer wird er nicht verändert.

Lebensdauer:

Speziell.
Von der nachfolgenden Ausnahme abgesehen, existiert dieser Zeitstempel bis die Datei gelöscht wird.
Wenn die Datei jedoch mit dem move-Befehl der Shell in eine andere Partition verschoben wird, wird dieser Zeitstempel aktualisiert.

Informationsgehalt:

Zeit: Systemdatum und Systemzeit

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Mit der Eingabeaufforderung oder dem Explorer in das Verzeichnis wechseln, in dem sich die betreffende Datei befindet. In der Eingabeaufforderung dir /Tc eintippen oder im Explorer Zeitstempel „Erstellt am“ ablesen (gegebenenfalls über die Menüs „Ansicht“ und „Details auswählen...“ die Option "Erstellt am" aktivieren).

Aufwand:

Gering.

Fehlinterpretation:

Hoch.
Quelle kann von mehreren Vorgängen erzeugt werden.
Die Belegung des Zeitstempels wird vom System nicht konsequent umgesetzt (vgl. Entstehungsbedingungen).

Fälschung:

Leicht.
Abhängig von Rechten auf die Datei. Wenn Benutzer die Datei löschen oder zumindest umbenennen können, kann eine neue Datei mit selben Namen und gegebenenfalls manipulierten Systemdatum und Systemzeit erstellt werden. Normalerweise hat der Benutzer der die Dateien anlegen kann aber meist auch Rechte, um sie zu löschen.

Quelle:
Zeitstempel "Erstellt am" von Verzeichnissen .....explorer.exe; dir /Tc

Beschreibung der Quelle:

Der Zeitstempel "Erstellt am" des betroffenen Verzeichnisses gibt das Systemdatum und die Systemzeit für dessen Erstellung durch die folgenden Vorgänge an.

Verursachende Vorgänge:

- Verzeichnis anlegen
- Verzeichnis kopieren (für das neue Verzeichnis; der Zeitstempel des alten bleibt unverändert)
- Verzeichnis verschieben

Entstehungsbedingungen:

Spezielle.
Abhängig von der Art der Ausführung ausschließlich bei folgendem Vorgang:

- Beim Vorgang "Verzeichnis verschieben":
  Nur wenn das Verzeichnis in eine andere Partition verschoben wird.

Lebensdauer:

Speziell.
Von der nachfolgenden Ausnahme abgesehen, existiert dieser Zeitstempel bis das Verzeichnis gelöscht wird.
Wenn das Verzeichnis jedoch in eine andere Partition verschoben wird, wird dieser Zeitstempel aktualisiert.

Informationsgehalt:

Zeit: Systemdatum und Systemzeit

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Mit der Eingabeaufforderung oder dem Explorer in das Verzeichnis wechseln, in dem sich das betreffende Verzeichnis befindet. In der Eingabeaufforderung dir /Tc eintippen oder im Explorer Zeitstempel „Erstellt am“ ablesen (gegebenenfalls über die Menüs „Ansicht“ und „Details auswählen...“ die Option "Erstellt am" aktivieren).

Aufwand:

Gering.

Fehlinterpretation:

Hoch.
Quelle kann von mehreren Vorgängen erzeugt werden.
Die Belegung des Zeitstempels wird vom System nicht ganz konsequent umgesetzt (vgl. Entstehungsbedingungen).

Fälschung:

Leicht.
Abhängig von Rechten auf das Verzeichnis. Wenn Benutzer das Verzeichnis löschen oder zumindest umbenennen können, kann ein neues Verzeichnis mit selben Namen und gegebenenfalls manipulierten Systemdatum und Systemzeit erstellt werden. Normalerweise hat der Benutzer der die Dateien anlegen kann aber meist auch Rechte um sie zu löschen.

Quelle:
Zeitstempel "Geändert am" von Dateien.....explorer.exe; dir /Tw

Beschreibung der Quelle:

Der Zeitstempel "Geändert am" der betroffenen Datei gibt das Systemdatum und die Systemzeit für deren letzte Veränderung durch die folgenden Vorgänge an.

Verursachende Vorgänge:

- Datei anlegen
- Dateiinhalt ändern

Entstehungsbedingungen:

Keine

Lebensdauer:

Bis zum nächsten Vorgang.
Beim nächsten Ändern des Dateiinhalts wird der Zeitstempel auf den aktuellen Wert gesetzt und damit die alte Information überschrieben. Wird die Datei gelöscht verschwindet auch der Zeitstempel.

Informationsgehalt:

Zeit: Systemdatum und Systemzeit

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Mit der Eingabeaufforderung oder dem Explorer in das Verzeichnis wechseln, in dem sich die betreffende Datei befindet. In der Eingabeaufforderung dir /Tw eintippen oder im Explorer Zeitstempel „Geändert am“ ablesen (gegebenenfalls über die Menüs „Ansicht“ und „Details auswählen...“ die Option "Geändert am" aktivieren).

Aufwand:

Gering.

Fehlinterpretation:

Niedrig.

Fälschung:

Leicht.
Mit passenden Berechtigungen ist das Ändern des Dateiinhalts möglich, das den Zeitstempel neu setzt.
In Verbindung mit der Änderung der Systemzeit ist ein Vor- oder Rückdatieren möglich.

Quelle:
Zeitstempel "Geändert am" von Verzeichnissen .....explorer.exe; dir /Tw

Beschreibung der Quelle:

Der Zeitstempel "Geändert am" des betroffenen Verzeichnisses gibt das Systemdatum und die Systemzeit für dessen letzte Veränderung durch die folgenden Vorgänge an.

Verursachende Vorgänge:

Direkt das Verzeichnis betreffend:
- Verzeichnis anlegen
- Verzeichnis kopieren (für die neue Verzeichnis, Zeitstempel des alten bleibt unverändert)
- Verzeichnis verschieben

Indirekt das Verzeichnis betreffend da innerhalb diesem stattfindende Vorgänge deren Inhalt ändern:
Alles weitere nur wenn Verzeichnis in NTFS-Partition!
- Datei anlegen
- Datei kopieren (wenn dieses Verzeichnis Zielverzeichnis des Kopiervorgangs)
- Datei verschieben (für Quell- und Zielverzeichnis)
- Datei löschen
- Datei umbenennen
- Verzeichnis anlegen
- Verzeichnis kopieren (wenn dieses Verzeichnis Zielverzeichnis des Kopiervorgangs)
- Verzeichnis verschieben (für Quell- und Zielverzeichnis)
- Verzeichnis löschen
- Verzeichnis umbenennen

Entstehungsbedingungen:

Spezielle.
Abhängig von der Art der Ausführung ausschließlich bei folgenden Vorgängen:

- Beim Vorgang "Verzeichnis kopieren":
  nur wenn über Explorer, nicht wenn mit xcopy-Befehl (xcopy /E für Verzeichnisse) kopiert wird,
- Beim Vorgang "Verzeichnis verschieben":
  nur wenn in eine andere Partition verschoben wird.

Lebensdauer:

Bis zum nächsten Vorgang.
Bei einem weiteren der oben aufgeführten Vorgänge wird der den Zeitstempel gegebenenfalls auf den aktuellen Wert gesetzt und damit die alte Information überschrieben.

Informationsgehalt:

Zeit: Systemdatum und Systemzeit

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Mit der Eingabeaufforderung oder dem Explorer in das Verzeichnis wechseln, in dem sich das betreffende Verzeichnis befindet. In der Eingabeaufforderung dir /Tw eintippen oder im Explorer Zeitstempel „Geändert am“ ablesen (gegebenenfalls über die Menüs „Ansicht“ und „Details auswählen...“ die Option "Geändert am" aktivieren).

Aufwand:

Gering.

Fehlinterpretation:

Hoch.
Quelle kann von mehreren Vorgängen erzeugt werden.
Die Belegung des Zeitstempels wird vom System nicht konsequent umgesetzt (vgl. Entstehungsbedingungen).

Fälschung:

Leicht.
Ausführung eines der angeführten Vorgänge setzt den Zeitstempel neu.
In Verbindung mit Änderung der Systemzeit auch ein Vordatieren möglich.

Quelle:
Zeitstempel "Letzter Zugriff am" von Dateien.....explorer.exe; dir /Ta

Beschreibung der Quelle:

Der Zeitstempel "Letzter Zugriff am" der betroffenen Datei gibt das Systemdatum und die Systemzeit (nur bei NTFS-Dateisystem) für deren letzten Zugriff mit folgenden Vorgänge an:

Verursachende Vorgänge:

- Datei anlegen
- Datei kopieren (für die neue Datei, Zeitstempel des alten bleibt unverändert)
- Datei lesen
- Datei umbenennen
- Datei verschieben
- Dateiattribute ändern
- Dateiberechtigungen NTFS ändern
- Dateiinhalt ändern
- Programm (mit "Ausführen als") starten
- Programm (mit aktuellem Benutzer) starten

Entstehungsbedingungen:

Spezielle.
Abhängig von der Art der Ausführung ausschließlich bei folgenden Vorgängen:

- Beim Vorgang "Dateiattribute ändern":
  Die Zeit wird nur geändert, wenn die Änderung mit dem Explorer durchgeführt wird, über die Eingabeaufforderung mit Befehl attrib nicht.
- Beim Vorgang "Programm starten":
  bei NTFS wird nur beim 1.ten Zugriff innerhalb einer Zeitspanne der Wert geändert, danach befinden sich die Datei wohl in einer Art Cache und der Zeitstempel ändert sich bei wiederholtem Zugriff für die nicht bekannte Zeit des Bestehens im Cache bei weiteren Zugriffen nicht mehr.
  bei FAT32 bei jedem Zugriff
- Beim Vorgang "Datei verschieben":
  Innerhalb derselben FAT Partition gibt es keine Änderung. Bei NTFS oder wenn zwei verschiedene Partitionen beteiligt sind schon.
- Beim Vorgang "Datei lesen":

		Über Explorer geöffnet		Über „Datei öffnen“ - Dialog	
		Edit.com	Notepad.exe	Edit.com	Notepad.exe
FAT32		Ja	Nein	Ja	Ja
NTFS	1.ter Zugriff	Ja	Ja	Ja	Ja
	Wiederholt	Nein	Nein	Nein	Nein

Lebensdauer:

Bis zum nächsten Vorgang.
Bei einem weiteren der oben aufgeführten Vorgänge wird der den Zeitstempel gegebenenfalls auf den aktuellen Wert gesetzt und damit die alte Information überschrieben.

Informationsgehalt:

Zeit: Bei NTFS-Dateisystem: Systemdatum und Systemzeit
Bei FAT32-Dateisystem: nur Systemdatum (ohne Systemzeit)

Verfügbarkeit:

Online und offline verfügbar. Möglichst nur offline, da gerade der Zugriffszeitstempel sehr leicht verändert werden kann, da z.B. der Explorer bei manchen Dateitypen Informationen zum Inhalt gleich automatisch ausliest, wenn man sich nur im Verzeichnis befindet.

Auswertung:

Mit der Eingabeaufforderung oder dem Explorer in das Verzeichnis wechseln, in dem sich die betreffende Datei befindet. In der Eingabeaufforderung dir /Ta eintippen oder im Explorer Zeitstempel „Letzter Zugriff am“ ablesen (gegebenenfalls über die Menüs „Ansicht“ und „Details auswählen...“ die Option "Letzter Zugriff am" aktivieren).

Aufwand:

Gering.

Fehlinterpretation:

Hoch.
Die Quelle kann von mehreren Vorgängen erzeugt werden.
Die Belegung des Zeitstempels wird vom System nicht konsequent umgesetzt (vgl. Entstehungsbedingungen).
Insbesondere ist wegen des Cacheverhaltens des NTFS-Dateisystems kein Verlass auf die Zeitangabe.

Weiterhin gibt es noch Vorgänge, die nicht zweckmäßig in die Klassifikation eingruppiert werden können, aber auch diesen Zeitstempel verändern. So kann bereits eine Betrachtung der Dateien eines Verzeichnisses mit dem Explorer einstellungsabhängig das Setzen dieses Zeitstempels durch die automatische Erstellung der Dateivorschau für Bild oder Videodateien verursachen.
Aufgrund der genannten Ausnahmen ist nur die Aussage möglich, dass einer der obigen Vorgänge zum genannten Zeitpunkt durchgeführt wurde, jedoch weder, dass es unbedingt der letzte war, noch dass es eine direkte Folge einer Benutzerhandlung war.

Fälschung:

Leicht.
Ausführung eines der angeführten Vorgänge setzt den Zeitstempel neu.
In Verbindung mit Änderung der Systemzeit auch ein Vordatieren möglich.

Quelle:
Zeitstempel "Letzter Zugriff am" von Verzeichnissen.....explorer.exe; dir /Ta

Beschreibung der Quelle:

Der Zeitstempel "Letzter Zugriff am" des betroffenen Verzeichnisses gibt das Systemdatum und die Systemzeit (nur bei NTFS-Dateisystem) für dessen letzten Zugriff mit folgenden Vorgänge an:

Verursachende Vorgänge:

Direkt das Verzeichnis betreffend:
- Verzeichnis anlegen
- Verzeichnis kopieren (für neu erstelltes Verzeichnis und bei NTFS auch für kopiertes Verzeichnis)
- Verzeichnis verschieben
- Verzeichnisattribute ändern
- Verzeichnisberechtigungen NTFS ändern

Indirekt das Verzeichnis betreffend, da innerhalb diesem stattfindende Vorgänge deren Inhalt ändern:
Alles weitere nur wenn sich das Verzeichnis in einer NTFS-Partition befindet.
- Datei anlegen
- Datei kopieren (wenn dieses Verzeichnis Zielverzeichnis des Kopiervorgangs)
- Datei verschieben (für Quell- und Zielverzeichnis)
- Datei löschen
- Datei umbenennen
- Dateiinhalt ändern
- Verzeichnis anlegen
- Verzeichnis kopieren (wenn dieses Verzeichnis Zielverzeichnis des Kopiervorgangs)
- Verzeichnis verschieben (für Quell- und Zielverzeichnis)
- Verzeichnis löschen
- Verzeichnis umbenennen

Entstehungsbedingungen:

Spezielle.
Abhängig von der Art der Ausführung ausschließlich bei folgenden Vorgängen:

- Beim Vorgang "Verzeichnisattribute ändern":
  Die Zeit wird nur geändert wenn die Änderung mit Explorer im Dateisystem NTFS durchgeführt wird, über die Eingabeaufforderung mit Befehl attrib oder bei FAT32 nicht.
- Beim Vorgang "Verzeichnis verschieben":
  Nur wenn in andere Partition verschoben.

Lebensdauer:

Bis zum nächsten Vorgang.
Bei einem anderen der oben aufgeführten Vorgänge wird der den Zeitstempel auf den aktuellen Wert gesetzt und damit die alte Information überschrieben.

Informationsgehalt:

Zeit:	Bei NTFS-Dateisystem: Systemdatum und Systemzeit Bei FAT32-Dateisystem: nur Systemdatum (ohne Systemzeit)

Verfügbarkeit:

Online und offline verfügbar.
Möglichst nur offline, da gerade der Zugriffszeitstempel sehr leicht verändert werden kann.

Auswertung:

Mit der Eingabeaufforderung oder dem Explorer in das Verzeichnis wechseln, in dem sich das betreffende Verzeichnis befindet. In der Eingabeaufforderung dir /Ta eintippen oder im Explorer Zeitstempel „Letzter Zugriff am“ ablesen (gegebenenfalls über die Menüs „Ansicht“ und „Details auswählen...“ die Option "Letzter Zugriff am" aktivieren).

Aufwand:

Gering.

Fehlinterpretation:

Hoch.
Die Quelle kann von mehreren Vorgängen erzeugt werden.
Die Belegung des Zeitstempels wird vom System nicht konsequent umgesetzt (vgl. Entstehungsbedingungen).
Außerdem kommt es zur Veränderung von diesen Zeitstempeln durch den Explorer, weil dieser z.B. den Inhalt eines Teils der darin enthaltenen Dateien für eine Dateivorschau einliest.
Somit ist der Zeitstempel nicht unbedingt Anzeichen einer bewussten Aktion.

Fälschung:

Leicht.
Ausführung eines der angeführten Vorgänge setzt den Zeitstempel neu.
In Verbindung mit Änderung der Systemzeit auch ein Vordatieren möglich.

Quelle:
Zugriffe auf Benutzerprofile ..... explorer.exe; dir

Beschreibung der Quelle:

Während eine Benutzersitzung besteht, ändert sich durch vielfältigste Handlungen das Benutzerprofil des aktiven Benutzers. Dazu zählt insbesondere das eigentliche An- und Abmelden.

Verursachende Vorgänge:

Nicht nur die verursachenden Vorgänge hinterlassen Informationen in der Quelle, sondern auch die während der Benutzersitzung anfallenden Vorgänge hinterlassen hier Informationen, die Rückschlüsse auf die Dauer der Sitzung zulassen.

- AD Benutzeranmeldung an Active Directory / AD Benutzerabmeldung vom Acitve Directory
- Benutzeranmeldung lokal / Benutzerabmeldung lokal
- Terminalsitzung erstellen / Terminalsitzung beenden
- Terminalsitzung wiederaufnehmen / Terminalsitzung unterbrechen
- Programm (mit "Ausführen als") starten / Programm (mit "Ausführen als" gestartet) beenden

Entstehungsbedingungen:

Keine.

Lebensdauer:

Bis zum nächsten Vorgang.
Auf die Daten des Benutzerprofils in der Registry (ntuser.dat, ntuser.dat.log) wird ständig zugegriffen; dadurch ist feststellbar, wann die Benutzersitzung beendet wurde. Diese Information bleibt auch nach dem Ende der Benutzersitzung bzw. dem Herunterfahren des Rechners bis zur nächsten Benutzersitzung erhalten.

Informationsgehalt:

Zeit: Systemdatum und Systemzeit, zu der der Benutzer zuletzt mit diesem Profil eingeloggt war und das er zu bestimmten andere Zeiten Aktionen durchgeführt hat.

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Das Benutzerprofil umfasst die vielfältigsten Dateien und Verzeichnisse. An den Zeitstempeln der Dateien und Verzeichnisse des Benutzerverzeichnisses kann die Rechneraktivität eines Benutzers teilweise nachvollzogen werden. Das Benutzerverzeichnis befindet sich jeweils unter dem Pfad C:\Dokumente und Einstellungen\#BENUTZERNAME#.

Die Struktur hängt von den gewählten Einstellungen und installierten Programmen ab.

Standardunterverzeichnisse im Hauptpfad sind:

Anwendungsdaten	Cookies	Desktop	Druckumgebung
Eigene Dateien	Favoriten	Lokale Einstellungen	Netzwerkumgebung
Recent	SendTo	Startmenü	UserData
Vorlagen	WINDOWS		

Standarddateien im Hauptpfad sind:

NTUSER.DAT	ntuser.dat.log	ntuser.ini	Sti_Trace.log

In den Unterverzeichnissen existiert noch eine Vielzahl weiterer Verzeichnisse und Dateien.

Besonders interessant ist die Datei NTUSER:DAT, in der sich der Registryast des Benutzers befindet. Daneben existiert die ntuser.dat.log, die Änderungen zur Erreichung einer Fehlertoleranz sehr kurzfristig zwischenspeichert. Da laufende Prozesse einer Sitzung fast ständig auf irgendwelche Registryäste dieses Profils zugreifen, kann an den Zeitstempel dieser beiden Dateien besonders gut erkannt werden, zu welchem Zeitpunkt das Benutzerkonto zuletzt benutzt wurde.

Aber auch die anderen Dateien können von Bedeutung sein, da auf dieses Verzeichnis standardmäßig nur der Administrator und der Benutzer selbst Zugriff haben. Die Zeitstempel der unterschiedlichen enthaltenen Dateien und Verzeichnisse kann also auf den Zeitpunkt vergangener Aktivität verweisen.
So lässt sich auch für länger zurückliegende Zeiträume eine allerdings lückenhafte Historie durchgeführter Dateizugriffe und damit stattgefundener Benutzeraktivitäten ablesen.

Wenn das Active Directory und servergespeicherte Profile verwendet werden, wird das Profil beim Anmelden vom Server geladen und beim Abmelden wieder zurückgeschrieben. Damit können auch auf dem Server die Zeitstempel der Profildateien betrachtet werden.

Aufwand:

Gering.

Fehlinterpretation:

Gering.

Fälschung:

Leicht.
Wenn eine Änderung der Systemzeit möglich ist, kann mit falschen Zeiteinstellungen ein An-/Abmeldevorgang ausgeführt werden.

Quelle:
Zuletzt über Ausführen gestartete Programme .....regedit.exe; (regview.exe)

Beschreibung der Quelle:

Die Funktion "Ausführen" im Startmenü speichert die 25 zuletzt über sie aufgerufenen Programme.

Verursachende Vorgänge:

- Programm (mit aktuellem Benutzer) starten

Entstehungsbedingungen:

Spezielle.
Nur wenn über Ausführen im Startmenü gestartet.

Lebensdauer:

Bedingt abhängig von anderen Vorgängen.
Wird nicht sofort überschrieben, aber es werden nur die letzten 25 Programmaufrufen gespeichert. Ist die Liste voll werden die zuletzt verwendeten wieder überschrieben.

Informationsgehalt:

Sonstiges: Welche Programme gestartet wurden (eingeschränkt auf mit dieser Funktion gestartet).

Verfügbarkeit:

Online und offline verfügbar.

Auswertung:

Unter der jeweiligen ntuser.dat des Benutzers finden sich in HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU unter den Werten a, b, c, etc die zuletzt ausgeführten Programme. Über den Wert MRUList findet sich die Reihenfolge angefangen bei den zuletzt verwendeten. Wenn hier also hgae... steht heißt das das zuletzt der Eintrag unter h, davor der unter g, davor a und zuvor e verwendet wurde.

Aufwand:

Gering.

Fehlinterpretation:

Gering.
Wenn ein sich hier ein Eintrag findet, ist dieses Programm gestartet worden.
Aus nichtvorhandenen Einträgen lässt sich jedoch nicht folgern, dass hier nichtvorhandene Programme auch nicht gestartet wurden, da andere Möglichkeiten des Aufrufes genutzt worden sein können.

Fälschung:

Leicht.
Der jeweilige Benutzer kann diese Einträge z.B. mit regedit.exe abändern oder löschen.

5 Anwendungen

Es folgen nun Kapitel, in denen zunächst Grundsätzliches zur Durchführung einer forensischen Analyse und zum Standardeinsatz der erstellten Klassifikation beschrieben ist. Anschließend folgen als erweiterte Anwendungen der Einsatz der zum Erstellen der Klassifikation entwickelten Methodik, prophylaktische Maßnahmen bei der Administration von Systemen sowie Aspekte zur Verschleierung von Quellen.

5.1 Grundsätzliches

Allgemein soll diese Arbeit nur die Informationen zu den Quellen bieten. Auf das genaue Vorgehen, das nötig ist, um z.B. die Gerichtsverwertbarkeit der Untersuchungsergebnisse zu erreichen, kann hier nicht vollständig eingegangen werden. Allerdings werden einige kurze generelle Hinweise dazu gegeben.

Grundsätzlich wird empfohlen, das System für eine forensische Analyse herunterzufahren und offline zu untersuchen, um selbst am System keine unbeabsichtigten Verfälschungen durchzuführen. Eine Onlineuntersuchung ist nur ratsam, wenn das System gebraucht wird und durch das Abschalten Schaden durch die Nichtverfügbarkeit des Systems entstehen würde oder die für eine Aufklärung notwendigen Quellen durch das Abschalten zerstört würden. Letzteres könnte beispielsweise eintreten, wenn ein aktuell stattfindendes unbefugtes Eindringen aufgeklärt werden soll.

Für die Offlineuntersuchung fertigt man am besten zuerst mit geeigneten Programmen ein Bitstream-Image der Festplatten an. Dieses enthält im Gegensatz zu einem normalen Backup eine exakte Kopie der Festplatte, also z.B. auch die nicht mehr im Dateisystem angezeigten Fragmente von gelöschten Dateien (File Slack und unbenutzter Speicherplatz). Diese Images werden dann unter einem anderen System, das nur zur Untersuchung verwendet wird, mit Schreibschutz gemountet, um unbeabsichtigtes Verändern zu vermeiden. Andernfalls besteht die Gefahr, dass vorhandene Quellen durch das Vorgehen bei der Untersuchung geändert bzw. vernichtet werden. So kann das Lesen von Dateien offensichtlich deren Zeitstempel „Letzter Zugriff am“ verändern. Aber auch vermeintlich sichere Quellen wie die Protokolleinträge im Ereignisprotokoll werden bei Standardeinstellungen durch die beim Vorgehen neu hinzukommenden Einträge irgendwann überschrieben.

Bei einer Offlineuntersuchung können aber die beschriebenen Windowsprogramme nicht mehr genutzt werden, wenn ein ganz anderes Betriebssystem wie Linux zum Einsatz kommt. In einem solchen Fall muss der Forensiker selbst das passende Werkzeug für die zu untersuchende Quelle auswählen, das ihm aber bei einem verwendeten System seiner Wahl bekannt sein dürfte.

Allgemein sollten am besten auch bei einer Onlineuntersuchung eigene Programme eingesetzt werden, da die Gefahr besteht, dass die auf dem System vorhandenen manipuliert sind und somit nicht die wirklichen Informationen der Quelle anzeigen könnten.

Für die weitere Verwertung von Zeitangaben in den Quellen, ist es entscheidend, die aktuelle Systemzeit mit der wirklichen Zeit zu vergleichen. Sollten hier Abweichungen auftreten, sind

diese unter Umständen zu den Zeiten aus den Quellen zu addieren oder zu subtrahieren. Jedoch kann weder eindeutig davon ausgegangen werden, dass abweichende Zeiten zum Untersuchungszeitpunkt auch in der Vergangenheit genau so bestanden haben, noch dass bei übereinstimmenden Zeiten zum Untersuchungszeitpunkt auch die damaligen Vorgänge mit der korrekten Systemzeit ausgeführt worden sind. Deshalb sind Zeitangaben generell kritisch zu betrachten. Zwar wird bei geeigneter Einstellung bei einer Änderung der Systemzeit ein Protokolleintrag angelegt. Aber durch eine Änderung über das BIOS kann dies umgangen werden. Eventuell können die Zeiten aber über Vorgänge, die sowohl auf dem System als auch auf externen Geräten mit zuverlässiger Zeitprotokollierung, wie bestimmten Netzwerkkomponenten, Quellen hinterlassen haben, berichtigt werden.

Da sich die möglichen Anwendungsfälle sehr voneinander unterscheiden können und zusätzliche externe Informationen für das Vorgehen eine große Rolle spielen, kann hier keine allgemeine, immer gültige Vorgehensweise beschrieben werden, die für jede Art von Untersuchung passend ist. Dennoch kann gesagt werden, dass das Sicherheitsprotokoll dafür eine gute erste Anlaufstelle ist (siehe Quellenblätter „Eintrag im Sicherheitsprotokoll für alle Ereigniskennungen“ bzw. der jeweiligen Kategorie und Kapitel 7.1.2 im Anhang). Wenn ein von einem Eindringling kompromittiertes System vermutet wird, sollte das System auf Verdächtiges, wie vorher noch nicht existierende Benutzer und Freigaben, überprüft werden (siehe Quellenblätter zu aktuell bestehenden Freigaben und aktuell bestehenden lokalen Benutzern oder Benutzern im Active Directory). Bei einer Untersuchung im laufenden Betrieb sind die geöffneten Ports und die laufenden Prozesse auf unbekannte Prozesse, die eventuell Trojaner sein könnten, zu überprüfen (siehe Quellen „Aktuell geöffnete Netzwerkports“ und „Aktuell laufende Prozesse“). Bei der Offlineuntersuchung sollte dazu überprüft werden, welche Programme beim Systemstart geladen werden (siehe Quellenblätter zu geplanten Programmstarts bei Systemstart bzw. Benutzeranmeldung). Die im vermuteten Tatzeitraum veränderten Dateien, die sich über eine Suche nach Dateien mit passenden Zeitstempeln finden lassen, können eine große Rolle spielen. Wenn es nötig ist, Informationen aus gelöschten Dokumenten ausfindig zu machen, bietet sich eine Durchsuchung aller Datenträger inklusive des unbenutzten Speicherplatzes und des File Slacks (siehe Quellenblatt zu Fragmenten von Daten) nach vermuteten Textausschnitten mit einem entsprechenden Hilfsprogramm an. Bei der Suche nach Textfragmenten können gegebenenfalls insbesondere auch die Inhalte der Auslagerungsdatei des Arbeitsspeichers oder der Hibernate-Datei, in die der Inhalt des Arbeitsspeichers beim Versetzten des Computers in den energiesparenden Ruhemodus geschrieben wird, von Interesse sein. Nähere Informationen zu diesen Quellen finden sich auch hier auf den jeweiligen Quellenblättern.

Das weitere Vorgehen hängt aber von dem konkreten Fall ab. Hier muss die Klassifikation passend angewandt werden. Wie das geht, wird im nächsten Kapitel erläutert.

5.2 Standardeinsatz der Klassifikation

Da Zeitangaben und unter Umständen auch Benutzerangaben allein wenig Informationswert haben, bietet es sich zunächst an, von den sich in der Computerforensik zu lösenden Fragen diejenige nach dem ausgeführten Vorgang zu beantworten. Die Klassifikation ist so angelegt, dass dabei die folgenden beiden in der Praxis auftretenden Suchrichtungen unterstützt werden:

Soll die Ausführung eines vermuteten Vorgangs nachgewiesen werden, können alle von ihm erzeugten Quellen ausgehend von dem Verzeichnis der Vorgänge nachgeschlagen werden (Fall 1).

Soll der Vorgang für eine bereits vorliegende Quelle aufgeklärt werden, findet man eine Liste aller in diesem Fall in Frage kommenden Vorgänge über den Punkt „Vorgänge“ auf dem jeweiligen Quellenblatt (Fall 2).

Vor die Anwendung der Klassifikation für diese beiden Aufgaben nachfolgend eingehender beschrieben ist, muss noch angemerkt werden, dass die darin enthaltenen Zuordnungen zu den Quellen jeweils nur die primären Vorgänge berücksichtigt. Dadurch ausgelöste weitere Vorgänge sind vom Anwender selbst zu berücksichtigen. Dazu ein Beispiel:

In der Klassifikation ist für den Vorgang „Verzeichnis Netzwerkfreigabe erstellen“ die Änderung eines Registrywerts als zugehörige unmittelbare Quelle beschrieben. Wenn für die Registryänderung die Protokollierung entsprechend aktiviert ist, entsteht als weitere mittelbare Quelle ein Protokolleintrag, der beim auslösenden Vorgang nicht genannt ist, da derartige Angaben die Klassifikation total überfrachten würden. Der Aufbau der Klassifikation erfordert also in diesem Fall, dass der Anwender neben dem primären Vorgang „Verzeichnis Netzwerkfreigabe erstellen“ auch den sekundären Vorgang „Registryänderung durchführen (Schlüssel/Wert anlegen/ändern/löschen)“ im Blick hat, um alle hinterlassenen Quellen zu erfassen. Entsprechendes gilt fortgesetzt für den tertiären Vorgang „Dateiinhalt ändern“ falls für die Änderung der betreffenden Registrydatei aufgrund aktivierter Protokollierung dafür Protokolleinträge angelegt werden.

Vergleichbares gilt u. a. bei allen Vorgängen, die zunächst den Start eines bestimmten Programms erfordern und hierfür die Protokollierung aktiviert ist.

Fall 1:

Sofern die Quellen zu einem Vorgang gesucht werden, sollte die Suche nicht gleich bei der zuerst gefundenen Quelle abgebrochen werden, sondern es sollten zunächst erst einmal alle Quellen dieses Vorgangs betrachtet werden. Ein Vergleich zwischen ihrer Bewertung des Kriteriums „Aufwand“ liefert möglicherweise Hinweise, dass einige Quellen leichter auszuwerten sind als andere. Ebenso ist es möglich, dass eine Quelle allein gar nicht alle gewünschten Informationen liefert, was sich am Kriterium „Informationsgehalt“ ablesen lässt. So ist es möglich, das eine Quelle nur Angaben zum Benutzer liefert, die Zeitangaben aber in einer anderen stehen. Somit ist die Kombination mehrer oder aller Quellen nötig, um die maximale Ergiebigkeit zu erhalten. In die weitere Auswahl kann auch einfließen, ob gemäß dem Kriterium „Fehlinterpretation“ falsche Schlussfolgerungen möglich sind oder nach dem Kriterium „Fälschung“ Daten leicht zu fälschen sind. Besonders wichtig ist ferner, ob die Quelle für die gewünschte Auswertung überhaupt zur Verfügung steht. Hier liefern die Kriterien „Entstehungsbedingungen“, „Lebensdauer“ und „Verfügbarkeit“ eventuell kombiniert mit dem Wis-

sen zu den Systemeinstellungen und über die in der bereits abgelaufenen Zeit durchgeführten Systemveränderungen, wichtige Anhaltspunkte. Während über die Angaben zur „Verfügbarkeit“ eindeutig entscheidbar ist, ob die Quelle für eine Offline-Analyse geeignet ist, ist die Einschätzung, ob die Quelle wegen ihren „Entstehungsbedingungen“ überhaupt angelegt wird bzw. wegen ihrer „Lebensdauer“ noch vorhanden ist, oft wesentlich komplizierter und nicht immer zuverlässig möglich. Zum einen ist es meistens schwer, aufgrund der Lebensdauer zu entscheiden, ob die Quelle noch vorhanden ist, da meistens keine konkreten Zeitangaben wie eine Angabe von Stunden oder Minuten möglich sind, sondern das Vorhandensein von der Durchführung anderer Vorgänge abhängt. Zum anderen sind in vielen Fällen die Zeit des Vorgangs und die Systemeinstellungen, die die Entstehungsbedingungen und die Lebensdauer beeinflussen, gar nicht bekannt.

Zwar kann die weitere Untersuchung am realen System auf eine Auswahl der Quellen beschränkt werden, die sich nach den oben genannten Kriterien am besten für eine Analyse eignen. Selbst wenn dabei alle direkt erwünschten Informationen ermittelbar sind, verzichtet man in diesem Fall jedoch darauf, die Existenz aller Quellen und die Widerspruchsfreiheit der darin enthaltenen Daten zu überprüfen. Damit entfällt die Möglichkeit eine möglicherweise durchgeführte Manipulation der Quellen zu erkennen (siehe weiter unten folgendes Kapitel 5.5).

Fall 2:

Bei einem Teil der Quellen kann aus dem Inhalt der Quelle direkt auf den verursachenden Vorgang zurück geschlossen werden. Jedoch ist dies bei vielen anderen Quellen nicht möglich. Zum Beispiel findet sich bei den Zeitstempeln im Dateisystem lediglich eine Zeitangabe über die Durchführung eines Vorgangs, auf den jedoch sonst keinerlei Angaben in der Quelle verweisen. Damit ist der verursachende Vorgang für diese Quelle über einen anderen Weg aufzuklären. Bei einer derartigen Suche des verursachenden Vorgangs zu einer bereits vorliegenden Quelle ist es zweckmäßig, zunächst die Angaben im Punkt „Vorgänge“ des betreffenden Quellenblattes, das über das Verzeichnis der Quellen aufzufinden ist, zu betrachten. Bei vielen Quellen wird man dabei allerdings auf die Angabe mehrerer Vorgänge stoßen und deshalb nicht sofort zum Ziel kommen. In diesen Fällen sind alle in Frage kommenden potentiellen Vorgänge weiterzuverfolgen, bis sich klärt, welcher dieser Vorgänge hier der verursachende ist. Das heißt jeden dieser Vorgänge nach dem oben unter Fall 1 beschriebenen Vorgehen daraufhin zu untersuchen, ob die von ihm gemäß Klassifikation erzeugten mit den im System vorhandenen Quellen übereinstimmen. Die zu einer Quelle genannten erzeugenden Vorgänge hinterlassen außer dieser jeweils meist auch noch andere Quellen. Ist bei einem solchen Vorgang nicht jede Quelle existent, obwohl sie aufgrund ihrer Kriterien „Entstehungsbedingungen“ und „Lebensdauer“ vorhanden sein müsste, ist dieser Vorgang jeweils auszuschließen. So sollte am Ende der Untersuchung nur für einen der in Frage kommenden Vorgänge eine Übereinstimmung zwischen den in der Klassifikation beschriebenen und den vorhandenen Quellen vorliegen und somit dieser als tatsächlich verursachender Vorgang identifiziert sein.

Im Abbildung 5 ist ein etwas komplexeres Beispiel angegeben. Angenommen es finden sich verdächtige Zugriffe auf das Benutzerprofil zu ungewöhnlichen Zeitpunkten und es soll aufgeklärt werden, für welche Anmeldung das Benutzerkonto zuletzt benutzt wurde. Aufgrund des Zugriffes auf das Benutzerprofil kommen fünf Vorgänge in Frage, die dem entsprechenden Quellenblatt zu entnehmen sind. Da der Vorgang damit noch nicht identifizierbar ist, werden nun alle Quellen von jedem dieser Vorgänge verfolgt. Es wird die Durchführung einer Offlineanalyse dieses Rechners angenommen, weshalb nur die offline auswertbaren Quellen des Rechners abgebildet sind, an dem die Anmeldung vermutet wird.

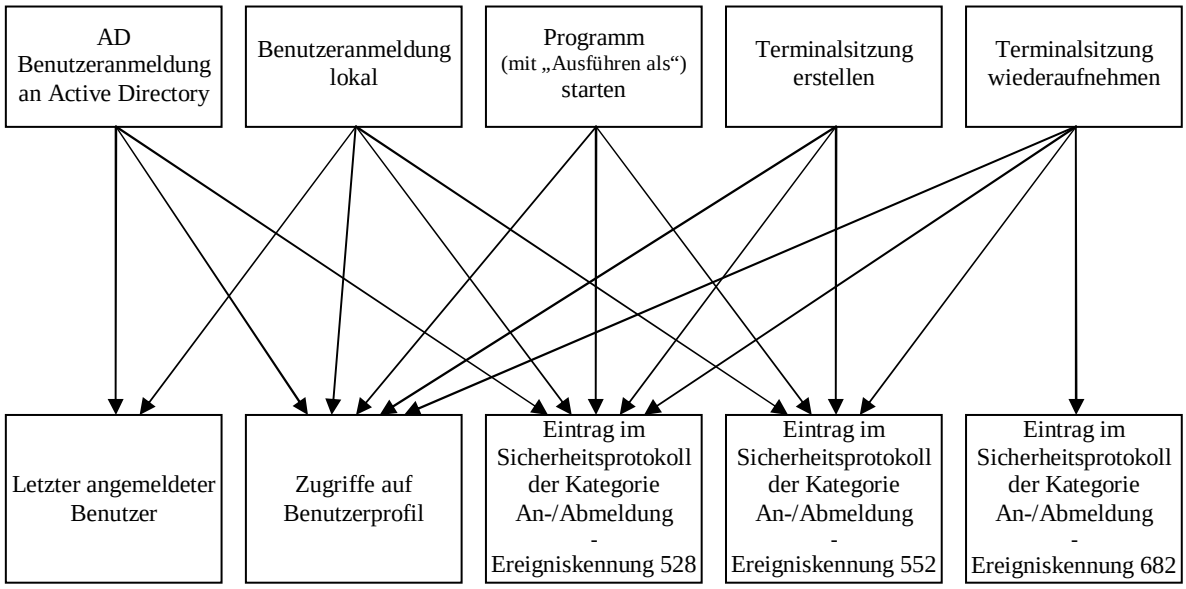


Abbildung 5: Von Quellen auf Vorgänge schließen

Beim Verfolgen der Quellen dieser Vorgänge sieht man, dass die Vorgänge auch noch andere Quellen angelegt haben müssten, wenn die Protokollierung aktiv war. Die Quelle „Letzter angemeldeter Benutzer“ ist eventuell zu ignorieren, wenn bekannt ist, dass in der Zwischenzeit schon weitere Anmeldeversuche stattgefunden haben. Die Zusammengehörigkeit der Quellen kann über einen identischen Benutzernamen und im selben Zeitraum liegende Zeitangaben erfolgen. Hierbei ist zu bedenken, dass zwar zu einem Vorgang gehörende Protokolleinträge alle zur selben Zeit erstellt sein müssen, die Zeitangaben des Benutzerprofils aber davon abweichen werden, da die Lebensdauer des betreffenden Zeitstempels längst abgelaufen ist, da dieser während der laufenden Sitzung aktualisiert wird. War die Protokollierung für die An-/Abmeldung aktiv und es findet sich neben den Einträgen mit den Ereigniskennungen 528 und 552 ein Eintrag mit der Kennung 682 zu passender Zeit vom selben Benutzer, war der auslösende Vorgang „Terminalsitzung wiederaufnehmen“. Liegt nur ein Eintrag der Ereigniskennung 528 für den Benutzer vor und ist im Netzwerk für die Anmeldung ein Server mit Active Directory installiert, kommt als Vorgang die Active Directory Anmeldung in Betracht. In diesem Fall können auch die Quellen auf dem Active Directory Server hinzugezogen werden. Verfolgt man dagegen die Möglichkeit einer lokalen Anmeldung weiter, weil nur passende Einträge der Kennungen 528 und 552 vorhanden sind, bleiben noch drei mögliche Vorgängen in der Auswahl {Benutzeranmeldung lokal, Programm (mit „Ausführen als“) starten und Terminalsitzung erstellen}. Jedoch finden sich im Inhalt des Eintrages 528 unter Anmeldetyp und Quellnetzwerkadresse in diesem Fall Informationen, die trotzdem eine eindeutig Aufklärung erlauben. So wird bei Terminalsitzungen der Anmeldetyp 10 vergeben, bei der lokalen Benutzeranmeldung und der Anmeldung zum Programmstart der Anmeldetyp 2. Findet sich hier eine 2 kann letztendlich zwischen „Benutzeranmeldung lokal“ und „Programm (mit „Ausführen als“) starten“ dadurch unterschieden werden, dass sich bei der lokalen Be-

nutzeranmeldung die Quellnetzwerkadresse 127.0.0.1 findet, während beim Programmstart dieses Feld leer bleibt.

Die Möglichkeit der Terminalsitzung könnte natürlich bei einem Rechner, bei dem diese Funktionalität nicht installiert oder deaktiviert wäre, auch aus diesem Grund ausgeschlossen werden.

Man sieht also, dass bei komplexeren Sachverhalten sehr viele Erkenntnisse und Informationen einfließen müssen. Deshalb sind zur leichteren Zuordnung der Ereigniseinträge zu den Vorgängen auf dem Quellenblatt unter dem Punkt Auswertung solche Zusammenhänge gegebenenfalls ausführlicher dargelegt. Insbesondere sind hier die Kombinationen von Ereigniskennungen und deren Inhalte angegeben, die existieren müssen, um den verursachenden Vorgang gegebenenfalls in Verbindung mit dem beschriebenen Vorgehen eindeutig zu identifizieren. Besondere Bedeutung hat diese Entscheidungshilfe bei den Quellenbeschreibungen, bei denen die Ereignisprotokoll-Quellen mehrerer Vorgänge zusammengefasst sind.

In Ausnahmefällen ist es jedoch möglich, dass immer noch mehrere potentielle erzeugende Vorgänge existieren und somit nicht vollständig aufgeklärt werden kann, um welchen Vorgang es sich handelt. Insbesondere kann dies zutreffen, wenn nicht mehr alle Quellen verfügbar sind, weil z.B. ihre Lebensdauer schon abgelaufen ist oder sie wegen bestimmter Entstehungsbedingungen nicht erzeugt wurden. So ist im oberen Beispiel bei fehlender Protokollierung für einen schon weiter zurückliegenden Vorgang aus den Zugriffen auf das Benutzerprofil keine genauere Einschränkung der verursachenden Vorgänge mehr möglich, sondern es kommen alle fünf in Frage.

Die inhaltlichen Angaben der Quellen, die bei der Untersuchung Indizien für die Zusammengehörigkeit von Quellen und Vorgängen liefern müssen, können auch direkte Hinweise auf den verursachenden Vorgang liefern und damit den Entscheidungsprozess abkürzen. Über diesen Weg kann der verursachende Vorgang eventuell selbst dann aufgeklärt werden, wenn wie im oben dargestellten Beispiel mehrere Vorgänge jeweils die gleiche Quelle oder mehrere gleiche Quellen hinterlassen.

Wie bei der Beschreibung des Kriteriums „Lebensdauer“ im Kapitel 4.1 dargestellt ist, ist bei vielen Quellen keine Angabe einer absoluten Lebensdauer möglich. Weil sich bei vielen Quellen die Existenz dadurch nur unscharf bestimmen lässt, sollte bei solchen Untersuchungen immer bedacht werden, dass fehlende Quellen auf eine fehlerhafte Einschätzung der Lebensdauer zurückzuführen sein können und die Auswertung der vorhandenen Quellen immer noch (eingeschränkte) Ergebnisse liefern kann. Aus diesen Gründen darf hierbei auch nicht vorschnell an Fälschungen der Quellen gedacht werden, obwohl diese nie völlig ausgeschlossen werden können (siehe dazu auch Kapitel 5.5).

Wenn man sich Klarheit über den durchgeführten Vorgang und die davon hinterlassenen Quellen verschafft, werden unter Umständen auch bereits die Fragen über den verursachenden Benutzer und den Ausführungszeitpunkt geklärt. Die Klassifikation bietet für verbliebene offene Fragen auf den Quellenblättern in den Kriterien „Informationsgehalt“ und „Auswertung“ Hinweise zur Existenz, zum Auffinden und zum Auslesen der entsprechenden Informationen. Sieht man davon ab, dass der für bestimmte Quellen verwendete Code nicht allgemein bekannt ist, treten hier im Vergleich zur Klärung der durchgeführten Vorgänge wesentlich einfachere Schritte auf. Nichtsdestotrotz sind für die Quellenanalyse in der Registry und im Ereignisprotokoll zusammenfassende Hilfen im Anhang zusammengestellt.

5.3 Einsatz der Methodik

In der Diplomarbeit werden nur die relevanten Funktionen des Standardbetriebsystems auf von ihnen hinterlassene Quellen untersucht. Allerdings sind oft gerade Informationen zu den Vorgängen von Anwenderprogrammen, die auf dem zu untersuchenden System verwendet werden, und den von ihnen erzeugten Quellen nötig. Auf die unterschiedlichsten Varianten diverser Hersteller konnte im Rahmen der Arbeit aufgrund des Umfangs nicht einzeln eingegangen werden. Sollten in der Praxis jedoch Vorgänge von solchen, bisher nicht untersuchten Programmen aufgeklärt werden müssen, gibt es also dazu noch keine Quellenblätter in der Arbeit. Jedoch kann das beschriebene Vorgehen, das zum Erstellen der Klassifikation genutzt wird, hier angewendet werden, um an die Quellen neuer Vorgänge zu gelangen. Insbesondere betrifft das die im Kapitel 3.3 „Quellen für Vorgänge finden“ beschriebenen Versuchsabläufe sowie die in der Arbeit verwendete Literatur, um Quellen aufzufinden und zu den gefunden Quellen an Information zu deren Eigenschaften zu gelangen.

Da am zu untersuchenden System selbst keine Daten verändert werden sollten, ist es nicht direkt als Testsystem verwendbar. Es bietet es sich an, als Testsystem eine Sicherungskopie des zu untersuchenden Systems zu verwenden. Wenn dies nicht möglich ist, z.B. weil das System im Onlinebetrieb weiterlaufen soll oder die Installation nicht mehr lauffähig ist, ist ein möglichst ähnlich konfiguriertes System für die Tests zu verwenden, auf dem natürlich mindestens das zu untersuchende Programm installiert sein muss. Dann sollten die Programme Regmon und Filemon installiert und in derselben Weise wie beschrieben benutzt werden, um die Quellen der gewünschten Vorgänge zu finden.

5.4 Prophylaktische Maßnahmen

Grundvorrausetzung für die Aufklärung eines Vorgangs ist die Erzeugung und der Erhalt einer Quelle bis zum Untersuchungstermin. Der Umfang und die Lebensdauer der angelegten Quellen sind sowohl von den Einstellungen des Betriebssystems als auch vom Auftreten weiterer Vorgänge abhängig. Die Informationen der Klassifikation können von Systemadministratoren deshalb in begrenzten Umfang auch dazu genutzt werden, Sicherheitsvorkehrungen dahingehend zu verbessern, mehr Quellen aufzuzeichnen und dadurch bestimmte Vorgänge leichter bzw. überhaupt erst aufklärbar zu machen.

So muss bei den verschiedensten Quellen deren Anlegung durch Systemeinstellungen erst einmal aktiviert werden. Ebenso kann man die Lebensdauer mancher Quellen durch geeignete Systemeinstellungen im Original verlängern. Auch indirekt bietet sich die Möglichkeit vom Administrator als wichtig eingestufte Quellen z.B. auf Bändern zu archivieren, um damit ihre Lebensdauer erheblich zu verlängern. Je nach eingeschätzter Bedeutung sind dafür sowohl die Namen der zu sichernden Dateien als auch die Zeiten der Backupläufe zu definieren.

Geeignete Einstellungen zu den oben genannten Punkten können nicht generell definiert werden, da der Umfang der Sicherheitsvorkehrungen sich am verwendeten Einsatz des Computersystems orientieren muss. So kann eine übermäßige Protokollierung sehr wohl auch schädlich sein, weil dadurch u. a. die Systemgeschwindigkeit herabgesetzt wird. Je nach Gefährdungslage, also Zugänglichkeit und Bedeutung des Systems, sollten mehr oder weniger Vorkehrungen getroffen werden.

Sofern zutreffende Systemeinstellungen existieren und bekannt sind, sind sie auf den Quellenblättern jeweils bei den Kriterien „Entstehungsbedingungen“ und „Lebensdauer“ beschrie-

ben. Um nicht alle Quellen durchsehen zu müssen, kann das folgende Vorgehen gewählt werden: Zunächst sind die Vorgänge auszuwählen, die man bei Bedarf gerne nachvollziehen will. Dann lassen sich von diesen über das Verzeichnis der Vorgänge die von ihnen erzeugten Quellen ermitteln. Falls Systemeinstellungen standardmäßig nicht oder nur mit ungünstigen Werten gesetzt sind, lässt sich dies an den beiden Kriterien ablesen und falls gewünscht verbessern. Alle für das konkrete System wichtig eingestuften Quellen sind in die Sicherungsabläufe einzubeziehen, um nicht nur eine längere Nachvollziehbarkeit dieser Quellen zu erreichen sondern sie auch gegen nachträgliche Verschleierungsversuche abzusichern.

Hier sei insbesondere noch auf den Anhang verwiesen, in dem in Kapitel 7.1.2 speziell auf die Ereignisprotokollierung eingegangen wird. Gerade hier lässt sich durch eine geeignete Aktivierung der Protokollierung für bestimmte Funktionen und passende Wahl des für das Protokoll zur Verfügung stehenden Speicherplatzes und des dafür geltenden Überschreibungsmodus die Entstehung und Lebensdauer der Quellen entscheidend beeinflussen.

5.5 Aufdecken von Verschleierungen

Interessant ist weiterhin die Untersuchung der Möglichkeit, erfolgreiche Verschleierungen von Quellen oder entsprechende Versuche aufdecken lassen. Verschleiern kann dabei sowohl das komplette Entfernen oder Ändern von hinterlassenen Quellen sein.

Allgemein deuten einige ungewöhnliche Systemeinstellungen oder Systemzustände auf ein Verschleiern hin. Als außergewöhnliche Systemeinstellung gelten in diesem Zusammenhang deutliche Abweichungen von den Standardwerten, die dazu führen, dass die Zahl der verfügbaren Quellen, durch die Beeinflussung der Entstehung oder der Lebensdauer dieser Quellen, erheblich abnimmt. Ein Beispiel hierzu ist ein sehr kleiner Wert im Internet Explorer für die Tage, die die besuchten Internetseiten im Verlauf aufbewahrt werden. Abnorme Zustände sind z.B. ein leeres „Temporary Internet Files“ Verzeichnis, in dem die den besuchten Seiten zugrunde liegenden Dateien gespeichert werden, oder dass keine Cookies vorhanden sind. Dies gilt natürlich nur als mögliches Anzeichen einer Verschleierung von Quellen, wenn bekannt ist, dass das Internet mit dem Internet Explorer sehr wohl genutzt wird. Ebenso sind leere Ereignisprotokolle als verdächtige Anzeichen zu betrachten.

Beispiele dieser Art sind natürlich nicht automatisch als versuchte oder vollendete Verschleierung zu interpretieren. Dies einzuschätzen hängt im Einzelfall auch wesentlich davon ab, ob es für die Administration der EDV-Geräte einheitliche Sicherheitsanweisungen gibt. Sind solche Regeln nicht vorhanden ist zu bedenken, dass ein Benutzer eine Löschung eventuell auch nur deshalb ausführt, weil es sich bei ihm um eine vorsichtige Natur handelt, die generell keine Aufzeichnungen über ihr Handeln hinterlassen will.

Die Klassifikation kann dabei mit ihren Kriterien „Entstehungsbedingungen“ und „Lebensdauer“ helfen, für jede der Quellen die Einstellungen zu finden, die für ihre Erzeugung und weitere Existenz maßgeblich sind.

Eine gute Chance Verschleierungsversuche zu erkennen bietet sich jedoch, wenn aus der Klassifikation hervorgeht, dass von dem Vorgang möglichst viele, schwer änderbare Quellen erzeugt werden. In diesem Fall bietet sich die Möglichkeit, dass nicht alle Quellen geändert oder gelöscht sind, da sie dem Angreifer nicht alle bekannt sind oder ihm das nötige Vorgehen zu kompliziert oder zeitaufwendig ist.

Falls wenigstens eine Quelle nicht geändert oder beseitigt ist, kann folgende Methodik zum Aufdecken der Verschleierung führen:

Für den betroffenen Vorgang sind alle von ihm erzeugten Quellen auf ihr Vorhandensein zu überprüfen.

Sollten zwei oder mehrere dieser Quellen in ihren Aussagen nicht übereinstimmen, also teilweise nicht vorhanden sein, obwohl jeweils ihre Entstehungsbedingungen erfüllt sind und auch ihre Lebensdauer noch nicht abgelaufen ist, oder widersprüchlichen Inhalt liefern, ist dafür eine Manipulation verantwortlich.

Allerdings ist die Einschätzung, ob die Lebensdauer schon abgelaufen ist, in den allermeisten Fällen schwer, weil in der Regel keine absoluten Zeitangaben darüber vorliegen, wie dies bei der Beschreibung des Kriteriums „Lebensdauer“ in Kapitel 4.1 bereits allgemein dargestellt ist.

Zusätzlich ist hierbei auch die Bewertung des Kriteriums „Fehlinterpretation“ der betroffenen Quellen von Belang. Darin wird nämlich für eine Quelle, die von mehreren Vorgängen erzeugt werden kann, unter anderem zum Ausdruck gebracht, dass die Zuordnung zu ihrem verursachenden Vorgang fehlerträchtig sein kann. Sofern dieser Fehler begangen wird, führt dies in der Regel fälschlicherweise zu der Annahme, dass die Quelle verschleiert ist.

Selbst bei gefälschten oder teilweise gelöschten Quellen, können diese nach dem beschriebenen Vorgehen ausgewertet werden, jedoch zu völlig falschen Schlussfolgerungen führen. Wenn dabei Widersprüche in den Daten verschiedener Quellen auftreten, ist es nicht klar, welche gefälscht und welche richtig sind. Zwar können bei einer diesbezüglichen Auswertung eine Einschätzung des Bekanntheitsgrades der Quelle und das Kriterium „Fälschung“, in dem beschrieben wird, wie leicht eine Quelle zu fälschen ist, einfließen. Aber eine verbindliche Folgerung, dass die weniger bekannten oder schwerer zu ändernden Quellen die Wahrheit sagen, verbietet sich ausdrücklich. So könnte ein gewiefter Fälscher so vorgehen, nur die bekannten und leicht entfernbaren Quellen zu löschen, aber alle sonstigen zu ändern. Eine nahe liegende Folgerung wäre zwar, dass von dem Hacker nur die simplen Quellen entfernt werden, die anderen aber entweder wegen Unbekanntheit oder schwerer Fälschbarkeit unverändert sind. Dies muss aber eben nicht in allen Fällen zutreffen. Sobald also ein Hinweis auf eine Verschleierung besteht, ist aus den geschilderten Gründen große Zurückhaltung bei der weiteren Verwendung der Quellen geboten.

Bei geschickten Fälschungen, bei denen alle noch vorhandenen Quellen zu einem widerspruchsfreien Ergebnis führen, sind fehlerhafte Folgerungen leider nicht auszuschließen.

Außerdem bietet sich auch die Möglichkeit, die Vorgänge, die zum Verschleiern von früher hinterlassenen Quellen unternommen werden, durch dabei neu erzeugte Quellen aufzuklären. So erfordern die Fälschung oder auch bereits der Versuch dazu das Ausüben von neuen Vorgängen, die abhängig von den Systemeinstellungen wiederum neue Quellen hinterlassen. Dies gilt z.B. bereits für die normalerweise zur Abänderung von bestehenden Quellen erforderliche Systemanmeldung und die dann ausgeführten Vorgänge.

Es dürfte aber nur in Ausnahmefällen gelingen, mit diesen Quellen Rückschlüsse auf die ursprünglichen Vorgänge zu erreichen, wenn die ursprünglichen Quellen verändert oder gelöscht sind. Da diese Quellen wie gesagt nur bedingt Rückschlüsse auf die ursprünglichen Vorgänge möglich machen, bleibt deren Aufklärung davon abhängig, dass von den ursprünglichen Quellen möglichst viele aussagekräftige erhalten bleiben. Dies dürfte außer von den Fähigkeiten des Fälschers und den Aufzeichnungseigenschaften des Betriebssystems davon

abhängig sein, wie leicht entsprechende Informationen über diese computerforensische Quellen zu erhalten sind.

5.6 Durchführen von Verschleierungen

Während sich bisher alle beschriebenen Anwendungen mit positiven Absichten das Ziel der Aufklärung von Vorgängen verfolgt haben, sind natürlich auch wenig erwünschte Anwendungen denkbar. Obwohl die Arbeit nicht unter diesem Gesichtspunkt geschrieben ist, hindert das eine Person mit negativen Absichten natürlich nicht, durch Studium der Arbeit zu erfahren, auf welchem Weg sie vorgehen muss, um möglichst wenige Quellen zu hinterlassen. Die Person kann dann möglichst nur die Einzelvorgänge zum Erreichen ihrer Ziele verwenden, bei denen sie möglichst wenige Quellen erzeugt, und die nicht vermeidbaren Quellen anschließend fälschen oder vernichten.

Entsprechend können die Erkenntnisse der Arbeit auch genutzt werden, wenn ohne verwerfliche Absichten ausschließlich das Ziel verfolgt wird, sich durch Zerstörung von Quellen davor zu schützen, dass Unbefugte an schützenswerte Informationen gelangen.

6 Zusammenfassung und Ausblick

Der Computerforensik stellen sich heute vielfältige Aufgaben, die mit entsprechenden Hilfsmitteln systematischer gelöst werden können. Im Rahmen der Diplomarbeit ist eine Klassifikation ihrer Informationsquellen für das Betriebssystem Windows entstanden. Zum einen können damit für die beschriebenen Vorgänge die wichtigsten Quellen erschlossen werden und zum anderen ist es möglich, ausgehend von diesen Quellen auf ihre verursachenden Vorgänge zurück zu schließen.

Zunächst wurden die möglichen Vorgänge des Betriebssystems recherchiert und unter ihnen die relevanten für die weitere Analyse bestimmt. Für diese Analyse wurden anschließend Hinweise aus verschiedenster Literatur zusammengetragen und Versuche an einem Testsystem durchgeführt, um möglichst alle hinterlassenen Quellen für die festgelegten Vorgänge zu erfassen. Hierzu musste ein geeigneter Versuchsablauf erarbeitet werden, der die auftretenden Hindernisse umging oder in ihrer Wirkung so abschwächte, dass die Untersuchung einer Vielzahl von Vorgängen realisiert werden konnte. Um die aufgespürten Quellen nach einheitlichen Kriterien bewerten zu können, mussten relevante Kriterien für die Erstellung eines Kriterienkatalogs bestimmt werden. Um den Erfordernissen eines praxistauglichen Einsatzes der Klassifikation Rechnung zu tragen, musste ein übersichtliches, benutzerfreundliches Darstellungsformat der Bewertungsergebnisse der Quellen entwickelt werden. Neben den Quellenbeschreibungen enthält die Klassifikation zum schnellen Auffinden von Vorgängen und Quellen sowie insbesondere zur Dokumentation des Zusammenhangs zwischen den verursachenden Vorgängen und erzeugten Quellen entsprechend gestaltete Verzeichnisse.

Das oben nur kurz beschriebene Vorgehen ist in der Arbeit ausführlich dokumentiert, um die Nachvollziehbarkeit sicherzustellen und dem Leser die Möglichkeit zu geben, dieselbe Methodik auch auf neue entsprechende Problemstellungen anwenden zu können. Aufgezeigt sind auch erweiterte Anwendungen, die sich aus der Klassifikation und den Erkenntnissen ihrer Erstellung ableiten lassen.

Einzelne Ergebnisse der Untersuchung überraschen gewaltig. So finden sich z.B. bei den Vorgängen im Dateisystem so nicht erwartete Unterschiede bei den erzeugten Quellen, die nur durch die gründliche Untersuchung der Vorgänge mit mehreren Abwandlungen, wie am Ende von Kapitel 3.3.3 beschrieben, überhaupt entdeckt werden können. Man sieht diese z.B. an den vielen Ausnahmen, die bei Quellenbeschreibungen der verschiedenen Zeitstempel angegeben sind. Während Unterschiede bei verschiedenen Dateisystemen noch nahe liegend sind, ist es erstaunlich, dass das zur Ausführung eines Vorgangs verwendete Programm (z.B. Shellbefehl oder Explorer) eine Rolle bei der Erzeugung der Quellen spielen kann. Das erhöht in diesen Fällen den Aufwand um Schlussfolgerungen durchzuführen und mindert zumindest in den Fällen nicht erzeugter Quellen den Erfolg.

Ebenso ist festzustellen, dass sich lesende Vorgänge, wozu auch Programm starten zählt, im NTFS Dateisystem nur beim „ersten“ Zugriff den Zeitstempel „Letzter Zugriff am“ ändern. Für später folgende Zugriffe bleibt der Zeitstempel einige Zeit lang unangetastet. Dies ist wohl auf den in NTFS integrierten Cache zurückzuführen. Hierfür kann aber die Zeit, in der die Datei noch im Cache vorliegt, nicht angegeben werden, weshalb über diese Quellen keine genauen Angaben zum Zeitpunkt des letzten Zugriffes auf die Datei zu ermitteln sind.

Weiterhin überraschte, dass die extra dafür vorgesehene Option, das Dateisystem zu protokollieren, nicht in allen Punkten brauchbare, leicht auswertbare Ergebnisse liefert. (siehe Kapitel 7.1.2.8 im Anhang).

Im Gegensatz zu der für die Diplomarbeit künstlich geschaffenen Testsituation sind in der Praxis nicht nur vom Betriebssystem hinterlassene Quellen zu untersuchen. So sind in der Regel gerade Informationen zu den auf dem zu untersuchenden System verwendeten Anwenderprogrammen und den von ihnen erzeugten Quellen nötig. Da aber z.B. für Textverarbeitungs-, Email- oder sonstige spezielle Programme verschiedenste Varianten unterschiedlichster Hersteller existieren, konnte auf diese im Rahmen der Arbeit auf keinen Fall einzeln eingegangen werden. Zwar können die zum Aufspüren von Quellen beschriebenen Methoden genutzt werden, um beim Auftreten einer entsprechenden Fragestellung diese Programme zu untersuchen. Eine noch umfassendere Klassifikation, die auch die Quellen dieser Programme umfassen würde, könnte jedoch die benötigten Untersuchungszeiten wesentlich verkürzen.

Um zu verhindern, dass die Analyse von Vorgängen weit verbreiteter Programme auf hinterlassene Quellen von verschiedenen Personen wiederholt neu durchgeführt wird, würde sich eine Klassifikation anbieten, die über das Internet (Datenbank/Internetfrontend) eingesehen und erweitert werden kann. Der Aufbau einer solchen eventuell frei zugänglichen Wissensdatenbank bringt jedoch die Probleme mit sich, dass falsche Informationen absichtlich oder unwissentlich eingetragen werden können. Die Qualität und Verlässlichkeit der beschriebenen Informationen ist jedoch für deren Nutzwert entscheidend. Aus diesem Grund wären hier sicher noch genauere Überlegungen über den Benutzerkreis sowie Bewertungs- bzw. Revisionsmöglichkeiten anzustellen.

Mit einer vom Papier losgelösten Darstellung bieten sich andere, übersichtlichere Darstellungen an. So können die Beziehungen zwischen den Vorgängen und Quellen graphisch dargestellt werden. Während dies auf Papier vom Platz her viel zu umfangreich und unübersichtlich wäre, kann für eine Darstellung im Computer eine Anwendung so programmiert werden, dass nur die jeweils relevanten Teilabschnitte angezeigt werden. Gerade bei der Suche, bei der mehrere verursachende Vorgänge in Frage kommen, oder der Untersuchung auf Fälschungen, würde dies das Blättern zwischen den Seiten ersparen und somit für komplizierte Sachverhalte entschieden zur Übersichtlichkeit beitragen. So könnte auch durch geeignete Farbgebung für die Quellen schon in der Übersicht erkannt werden, welche Bewertung sie für interaktiv auswählbare Kriterien erhalten haben.

Dies würde bei entsprechender Ausführung die Suche erleichtern und die Zusammenhänge besser klar machen. Die nötigen Informationen befinden sich bereits sowohl in der ausgedruckten Klassifikation als auch in der zu ihrer Erstellung verwendeten Datenbank.

Außer eine bessere Darstellungsmöglichkeit der Informationen anzustreben, könnte auch daran gedacht werden, die Informationen der Klassifikation für die Entwicklung von automatischen Analysetools zu gebrauchen, die ohne menschliche Hilfe Rückschlüsse durchführen und Schlussfolgerungen ziehen.

Für ein Programm, das verschiedenste Quellen automatisch auswertet, müssten aber erst sehr viele differenzierte Regeln definiert werden, da oft nur die Kombination mehrerer Quellen, bzw. die Quantität deren Auftreten relevante Rückschlüsse erlauben. Solche Software zu schreiben ist auch deshalb schwierig, weil die menschlichen Denkvorgänge bisher nur begrenzt im Computer abgebildet werden können. Um die forensischen Quellen richtig interpre-

tieren zu können, ist aber oft gerade die Kombinationsfähigkeit des menschlichen Gehirns gepaart mit einer entsprechend umfangreichen, allgemeinen menschlichen Erfahrung gefragt.

So kann das versuchte Einloggen mit falschem Passwort bei geringer Häufigkeit einfach auf ein Vertippen der Benutzer zurückzuführen sein. Finden jedoch zu ungewöhnlichen Uhrzeiten, an denen normalerweise niemand arbeitet, eine Vielzahl versuchter Anmeldeversuche mit derselben Benutzerkennung statt, deutet dies dagegen auf eine Brute-Force Passwortattacke hin.

Außerdem liegen bestimmte relevante Informationen gar nicht im Computer selbst vor. Man denke an DNA-Spuren auf der Tastatur, die einem Benutzer zuzuordnen sind, oder die Motivsuche, die meist nur über die Zuhilfenahme von Informationen aus der Lebenswelt der Betroffenen möglich ist.

Allerdings könnte man sich gut eine Software vorstellen, die vorläufige Einzelergebnisse liefert, die jeweils noch von einem menschlichen Forensiker geprüft, kombiniert und weiterverarbeitet werden müssen. Um Fälle komplett aufzuklären, könnten dann die schnelle Verarbeitung umfangreicher Datenmengen in Computern mit den Stärken des menschlichen Denkens und die Erkenntnisse der Computerforensik mit anderen forensischen Informationen kombiniert genutzt werden.

In der Arbeit sind nur direkt auf dem Computersystem hinterlassene Quellen untersucht. Denkbarerweise hinterlassen ausgeführte Vorgänge aber außerhalb des Systems weitere Quellen, die in der Arbeit nicht betrachtet sind. So werden bei Vorgängen, die über ein Netzwerk wie das Internet abgewickelt werden, von Netzwerkkomponenten wie Firewalls oder Geräten zur Abrechnung beim Internetprovider eventuell bestimmte Informationen aufgezeichnet. An diese zu kommen, erfordert z.B. wegen der notwendigen Berechtigung unter Umständen die Überwindung weiterer Hürden.

Die Klassifikation gilt in der vorliegenden Form nur für die konkrete Version Windows 2003 Server. Wie schon beschrieben, konnten für Windows 2000 oder XP in stichprobenhaften Untersuchungen keine Unterschiede festgestellt werden. Jedoch ist zu erwarten, dass gerade mit neuen Versionen nicht nur zusätzliche Funktionen und damit Vorgänge hinzukommen. Denn die angekündigten wesentlichen Modifikationen bedeuten wahrscheinlich auch für die hier beschriebenen Vorgänge teilweise komplett neue Quellen mit völlig unterschiedlichen Eigenschaften während vormals hinterlassene Quellen nicht mehr erstellt werden. So ist aus Berichten zum Stand der Entwicklung ([Libb03] und [Lyma03]) der zukünftigen Windowsversion (Codename Longhorn) zu erfahren, dass z.B. das dort verwendete Dateisystem WinFS [Msdn04a] komplett als Datenbank aufgebaut werden soll. Dies würde alle Vorgänge und die Quellen in der Kategorie Dateisystem wohl entscheidend ändern.

Neben der Analyse neu auftretender Quellen, die aus der Weiterentwicklung des Betriebssystems und sonstiger Programme herrühren, wird der Computerforensiker mit einer anderen Entwicklung gegenläufigen Charakters konfrontiert werden.

So werden immer mehr Programme angeboten, die es auch nicht sehr bewanderten Benutzer ermöglichen, Quellen auf einfache Art zu löschen. Im Hinblick auf den Datenschutz sind diese Entwicklungen zwar erfreulich, für die forensische Branche gilt dies jedoch nicht. So existieren heute schon eine Vielzahl von Programmen, die das Entfernen der beim Internetsurfen hinterlassenen Quellen versprechen. Diese Funktionen werden zum Teil durch Einbettung in die normalen Anwenderprogramme eine weite Verbreitung und damit Nutzung erfahren. So

bieten z.B. die aktuellen Versionen des Webbrowsers „Opera“ heute schon eine umfassende leicht erreichbare Option „Private Daten löschen“ an, mit der sich alle Aufzeichnungen des Benutzers, wie besuchte Seiten und weiteres, mit einem einfachem Klick entfernen lassen. Zwar stellt das einfache Entfernen aus dem Dateisystem allein zunächst noch keine wirkliche Hürde für den professionellen Forensiker dar. Aber die dadurch wieder freien Festplattenbereiche werden durch nun mögliches Überschreiben auf lange Sicht die ursprünglichen Quellen unauswertbar machen. Durch die Konfrontation des Benutzers mit entsprechenden Löschbefehlen oder Optionen werden wohl viele Benutzer für dieses Problem der Aufzeichnung sensibel und treffen gegebenenfalls sogar weitergehende Vorkehrungen.

So wird schon seit Windows 2000 mit dem Befehl „cipher /w“ eine Möglichkeit mitgeliefert, die (Rest-)Fragmente gelöschter Dateien im Dateisystem durch dreimaliges Überschreiben mit unterschiedlichen Bitmustern relativ verlässlich zu entfernen. Diese Funktion ist den meisten Personen nicht bekannt. Sollte sich Microsoft aber in zukünftigen Versionen dazu entscheiden, diese Funktionalität, z.B. durch eine Systemeinstellung wie „Dateien beim Löschen endgültig entfernen“ an prominenter Stelle, leichter zugänglich zu machen oder dies sogar als Standardeinstellung zu verwenden, kommen große Probleme auf die Forensiker zu.

So ist schon die Beilegung des Programmes „Evidence Eliminator“ [Robi03] zu einer Computerzeitschrift durch das Forensikunternehmen Vogon als „struck a blow for IT Security teams and law enforcement Officers“ [Vogo02] bewertet worden.

Die Ausweitung von EDV-Anwendungen und die weitere Zunahme der Zahl von Programmversionen wird unzweifelhaft zu einer Vergrößerung der Vielfalt der Quellen der Computerforensik führen. Wegen der aus der Sicht des Datenschutzes positiv zu bewertenden Entwicklung, dem Anwender einfache Möglichkeiten zum Löschen von Quellen zur Verfügung zu stellen, könnte allerdings in konkreten Fällen der Umfang und die Qualität des relevanten computerforensisch auswertbaren Materials spürbar abnehmen. Ob dies durch immer mehr Informationen und Programme, die der Computerforensik als Hilfsmittel verfügbar gemacht werden, ausgeglichen oder überkompensiert werden kann oder sich in Zukunft der Computerforensik deutlich schwierigere Aufgaben stellen, bleibt abzuwarten. Jedenfalls sollen die erarbeitete Klassifikation und die zu ihrer Erstellung entwickelten Verfahren einen Beitrag leisten, vorhandene computerforensische Quellen möglichst umfassend auswerten zu können.

7 Anhang

7.1 Erläuterungen zu ausgewählten Informationsquellen

Um den Umfang der Quellenbeschreibungen nicht zu sprengen, sind die wichtigsten und kompliziertesten Quellen im Kapitel 4.4 oft nur kurz beschrieben und zusätzlich an dieser Stelle ausführlich erklärt. Bei der Quellenbeschreibung ist in diesem Fall jeweils auf diese Stelle verwiesen. Durch die allgemeine Erläuterung muss z.B. nicht bei jeder Quelle, die einen Registryeintrag beinhaltet, die Auswertung erklärt werden.

7.1.1 Registry

Bei der Registry handelt es sich um eine baumartige Speicherstruktur in das die meisten Windowsprogramme ihre Einstellungen und die des Benutzers speichern. Für den Durchschnittsbenutzer bleibt die Registry im Normalfall jedoch völlig verborgen, da dieser Veränderungen nur über irgendwelche Menüs vornimmt. Aber auch erfahrenen Benutzern ist zur Vorsicht geraten, wenn sie die Registry selbst manipulieren wollen. Ein falscher Eintrag oder abgeänderter Wert an kritischen Stellen kann das ganze System funktionsunfähig machen.

Eine relativ komfortables Programm für die Anzeige und Änderung bietet das mitgelieferte Programm Registrierungs-Editor regedit.exe (Abbildung 6).

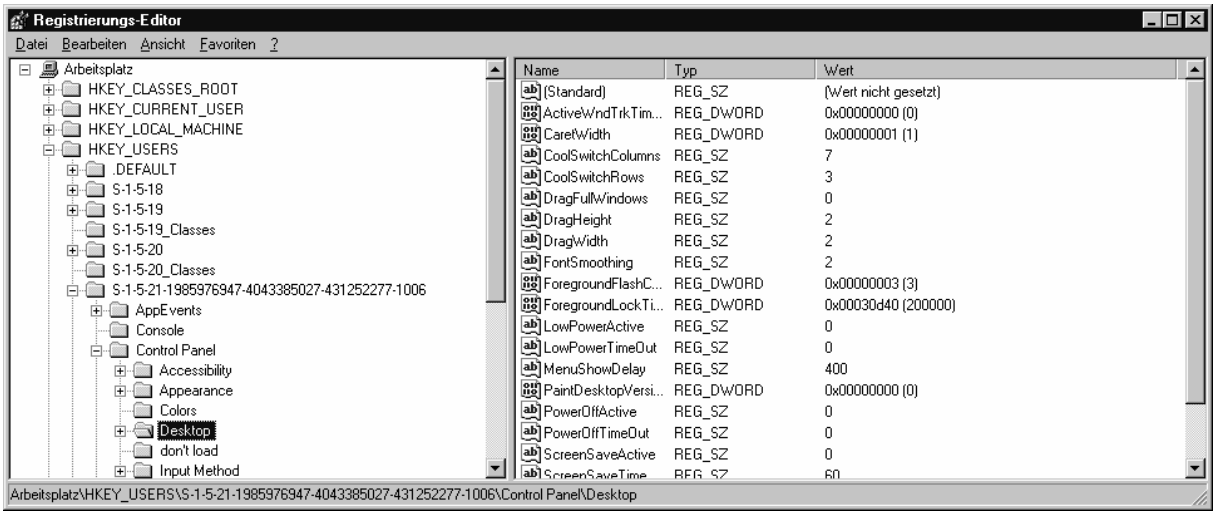


Abbildung 6: Registierungseditor regedit.exe

Wie man sieht, ist die Registry ein Baum aus Ästen („Schlüssel“) und Blättern („Wert“), die sowohl an inneren als auch den äußersten Ästen vorkommen können.

Man kann sich das ganze fast wie das Dateisystem denken. Äste als Verzeichnisse und Blätter als Dateien.

Schlüssel haben Namen, Werte sowohl einen Wertnamen als auch einen Inhalt.

Diese Inhalts-Typen werden in der Registry verwendet:

Kurzbezeichnung	**Beschreibung [Micr00a]**	**Benennung im Kontextmenü von regedit**
REG_SZ	Eine Zeichenfolge mit fester Länge.	Zeichenfolge
REG_BINARY	Binäre Daten. Die meisten Informationen zu Hardwarekomponenten sind als binäre Daten gespeichert und werden im Registrierungs-Editor im Hexadezimalformat angezeigt.	Binärwert
REG_DWORD	Daten, die mit einer Zahl von 4 Byte Länge dargestellt werden. Viele Parameter für Gerätetreiber und Dienste verwenden diesen Typ. Sie können im Registrierungs-Editor im Binär-, Hexadezimal- oder Dezimalformat angezeigt werden.	DWORD-Wert
REG_MULTI_SZ	Als mehrteilige Zeichenfolge. Direkt für Benutzer vorgesehene, lesbare Werte, die beispielsweise Listen oder verschiedene Werte enthalten, werden üblicherweise in dieser Form gespeichert. Einträge werden durch Leerzeichen, Kommas oder andere Trennzeichen voneinander getrennt.	Wert der mehrteiligen Zeichenfolge
REG_EXPAND_SZ	Eine Datenfolge mit variabler Länge. Die in diesem Datentyp gespeicherten Variablen werden aufgelöst, wenn ein Programm oder Dienst auf die Daten zugreift.	Wert der erweiterbaren Zeichenfolge

Der gesamte Registry-Baum befindet sich jedoch nicht in einer einzigen großen Datei, sondern er wird u.a. aus den Inhalten mehrerer Dateien zusammengesetzt.

Die fünf Hauptäste der Registry sind

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

Wenn ohne das Programm Regedit, z.B. bei der Offline-Analyse, zugegriffen werden muss, ist es wichtig, die Dateien zu kennen, aus denen die einzelnen Registry-Äste stammen.

Registryschlüssel	**Datei**
HKEY_CURRENT_USER	C:\Dokumente und Einstellungen\ #Benutzer#\ntuser.dat
HKEY_LOCAL_MACHINE\SAM	C:\Windows\System32\config\SAM
HKEY_LOCAL_MACHINE\Security	C:\Windows\System32\config\SECURITY
HKEY_LOCAL_MACHINE\Software	C:\Windows\System32\config\software
HKEY_LOCAL_MACHINE\System	C:\Windows\System32\config\system
HKEY_USERS\.DEFAULT	C:\Windows\\System32\config\default
HKEY_USERS\#SID des Benutzers#	C:\Dokumente und Einstellungen\ #Benutzer#\ntuser.dat

Der Hauptast HKEY_CLASSES_ROOT ist dagegen nur ein symbolischer Link zu HKEY_LOCAL_MACHINE\SOFTWARE\Classes während HKEY_CURRENT_CONFIG auf HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current zeigt.

Die Hauptäste HKEY_CURRENT_USER und HKEY_USERS enthalten je nach aktueller Anmeldung die Inhalte der ntuser.dat der jeweiligen Benutzer. Unter HKEY_CURRENT_USER findet sich der derzeitige direkt lokal am Computer eingeloggte Benutzer, unter HKEY_USERS alle derzeit am Computer verwendeten Benutzerkonten (z.B. auch für ein Konto, unter dem ein Programm mit „Ausführen als“ gestartet ist, und für Systemdienstkonten) jeweils in einem Unterschlüssel der ihrer SID (siehe Kapitel 7.2.1) entspricht.

Der Teilast HKEY_LOCAL_MACHINE\Hardware wird bei jedem Start neu erzeugt und findet sich nicht im Dateisystem.

Diese Dateien sind jedoch während des Betriebs nicht mit anderen Programmen (z.B. reinen Texteditoren) auslesbar, da sie vom System in Verwendung sind und für einen weiteren Zugriff gesperrt sind. Mit Regedit können sie jedoch angezeigt werden.

Allerdings existieren hier ähnlich wie im NTFS-Dateisystem Zugriffsbeschränkungen und Rechte.

Für Schlüssel lassen sich differenzierte Rechte vergeben, die z.B. das Lesen und Schreiben erlauben.

Unterbäume werden immer nur angezeigt, wenn der jeweilige Benutzer dafür mindestens Leserechte hat.

Selbst der Administrator hat nicht überall Zugriff. So ist der Unterschlüssel HKEY_LOCAL_MACHINE\SAM\SAM in dem die lokale Benutzerdatenbank gespeichert ist, nur vom Benutzer SYSTEM les- und änderbar.

Über einen kleinen Trick lässt sich jedoch auch darauf Zugriff verschaffen.

Man starte Regedit zeitversetzt, z.B. 1 Minute Verzugszeit, im interaktiven Modus (damit das Fenster auch angezeigt wird), mit Hilfe des Kommandos „at“ „at 16:37 /interactive regdit.exe“ (at-Befehl kann nur von Administratoren ausgeführt werden).

Dadurch erhält man einen Regedit Prozess der unter dem Konto SYSTEM läuft und man kommt somit an die bisher unzugänglichen Einträge.

Eine Auswertung nur mit einem Texteditor z.B. für die Offline-Auswertung gestaltet sich schwierig, da in einer flachen Hierarchie die Baumstruktur nicht offensichtlich ersichtlich ist (Abbildung 7).

Abbildung 7: Registrydatei im Texteditor

Leider findet sich keine Beschreibung des genauen Dateiformats, da von Microsoft der Fall der Offline-Auswertung nicht genügend berücksichtigt ist. Im laufenden Betrieb kann man entweder das mitgelieferte Regedit verwenden oder - falls man selber ein Programm schreibt - die zur Verfügung gestellten Funktionen der Windows API (Application Programming Interface) einsetzen. So gibt es zwar viele zusätzliche Tools zur Anzeige der Registry, weil sich deren Programmierer einige zusätzliche Funktionen oder einfach eine andere Art der Bedienung gewünscht haben. Aber fast alle greifen direkt auf die API Funktionen zurück und können deshalb nur die Registry eines in Verwendung befindendlichen Systems anzeigen. Dadurch sind diese für die Offline-Auswertung nicht zu verwenden, da sie nur die Registry des zur forensischen Analyse verwendeten Windowssystems anzeigen würden, nicht aber die gesicherten Registrydateien des zu untersuchenden Systems.

Es gibt allerdings das unter den verschiedensten Windowsversionen (Win 95/98/ME/NT/-2000/XP/2003) laufende Programm namens RegViewer (RegView.exe) [Leep03], das ohne die WinAPI auskommt (Abbildung 8). Bei diesem lässt sich der Dateiname des zu öffnenden Registryteils direkt angeben. Insofern könnte das Programm bei einer Offlineauswertung benutzt werden, indem die gesicherten Registrydateien auf irgendeinen Windowsrechner kopiert und ausgewertet werden.

Abbildung 8: RegViewer mit geöffneter ntuser.dat

Ansonsten könnten speziell entwickelte forensische Auswertungspakete für Windowssysteme auch eine spezielle Funktion für die Anzeige der Registry umfassen. Solche speziellen Programmpakete werden jedoch nicht untersucht.

7.1.2 Ereignisprotokoll

Im Ereignisprotokoll zeichnet das Betriebssystem Ereignisse auf. Diese Protokolle lassen sich mit dem Programm Ereignisanzeige einsehen und auswerten.

Für das Verständnis sind die Begriffe Ereignis bzw. Ereigniskennung von besonderer Bedeutung:

Ereignis: Das von Windows geführte Protokoll zeichnet einzelne Systemereignisse auf, die jedoch teilweise nur Teilvorgänge von Benutzervorgängen sind. Somit kann ein einzelner Vorgang mehrere Ereignisse auslösen. Es gibt auch Ereignisse die nicht mit Benutzerhandlungen in Verbindung stehen und deshalb für die forensische Analyse nicht von Belang sind.

Ereigniskennung: Die Ereignisprotokollierung verwendet für jedes Ereignis eine festgelegte dreistellige Nummer, um einen Ereigniseintrag eindeutig zu kennzeichnen. Insgesamt gibt es einige hundert dieser Ereignisse und damit ebenso viele Ereigniskennungen.

Standardmäßig werden 3 verschiedene Protokolle geführt, auf deren binäres Dateiformat im Kapitel 7.1.2.4 eingegangen wird:

- Anwendung (standardmäßig: C:\Windows\system32\config\AppEvent.Evt)
- Sicherheit (standardmäßig: C:\Windows\system32\config\SecEvent.Evt)
- System (standardmäßig: C:\Windows\system32\config\SysEvent.Evt)

Je nach den installierten Anwendungen können weitere Protokolle gespeichert werden. So erzeugt das Hinzufügen der Active Directory/Domänencontrollerfunktionalität zusätzlich die beiden Protokolle:

- Verzeichnisdienst (standardmäßig: C:\Windows\system32\config\NTDS.Evt)
- Dateireplikationsdienst (standardmäßig: C:\Windows\system32\config\NtFrs.Evt)

Für die forensische Analyse ist hauptsächlich das Sicherheitsprotokoll interessant, weshalb auf dieses weiter unten noch genauer eingegangen wird.

Die anderen Protokolle sind meist nützlich, um Fehler im Systembetrieb zu finden. Das System-Protokoll enthält überwiegend Meldungen, welche Dienste erfolgreich gestartet oder beendet wurden oder wo Fehler auftraten. Das Anwendungs-Protokoll kann von beliebigen Anwendungen mit dafür spezifischen Einträgen gefüllt werden. Auch im Verzeichnisdienst-Protokoll finden sich Informationen zum Start der Funktionalität des Verzeichnisdienstes. Die relevanten Einträge zum Erstellen von Benutzern usw. finden sich jedoch auch für das Active Directory im Sicherheitsprotokoll.

Zur Anzeige dieser Protokolle bietet sich die Ereignisanzeige an (Abbildung 9). Diese kann entweder über die Eingabe eventvwr.msc in der Eingabeaufforderung oder über den Eintrag Systemsteuerung\Verwaltung\Ereignisanzeige im Startmenü gestartet werden.

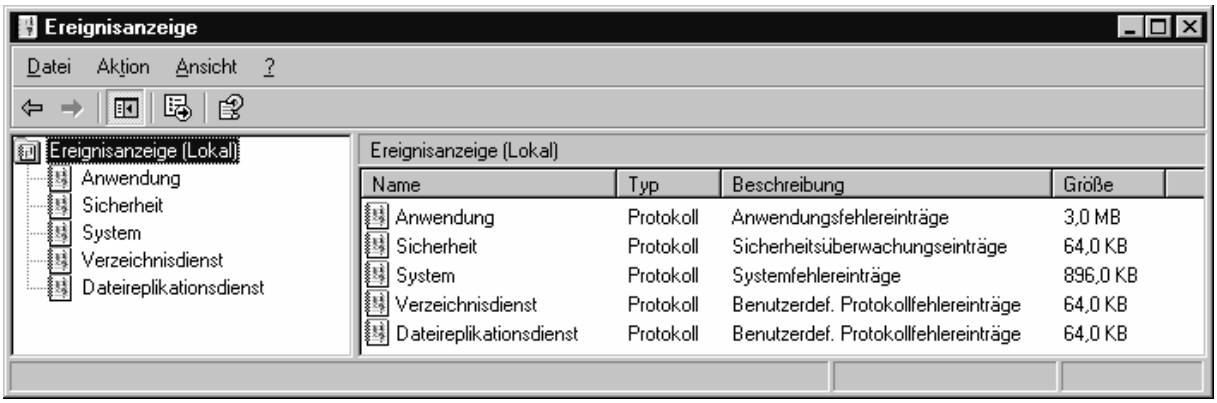


Abbildung 9: Protokolle der Ereignisanzeige

Hiermit lassen sich alle Protokolle auswählen und auslesen.

7.1.2.1 Anzeige von Einträgen

Jeder Eintrag enthält die Felder Typ, Datum, Uhrzeit, Quelle, Kategorie, Ereignis/Ereigniskennung (In Listenansicht Ereignis, in Einzelansicht Ereigniskennung), Benutzer, Computer und ein spezielles Textfeld in dem weitere Informationen vorkommen können und das je nach Ereigniskennung unterschiedlich aufgebaut ist.

Alle Felder außer dem Textfeld sind schon in der Tabellenansicht verfügbar (Abbildung 10).

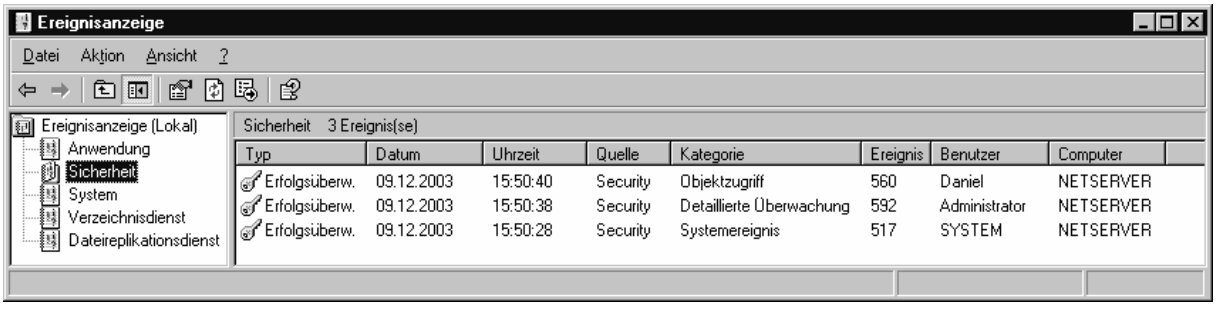


Abbildung 10: Einträge in Ereignisanzeige

Durch einen Doppelklick auf einen bestimmten Eintrag erhält man dann ein Fenster im dem noch mal alle Felder der Tabelle und zusätzlich das Textfeld mit genaueren Informationen dargestellt sind (Abbildung 11).

Mit den Buttons am rechten Rand kann man zum nächsten oder zum vorangehenden Ereignis springen oder mit letzterem den Eintrag in die Zwischenablage kopieren.

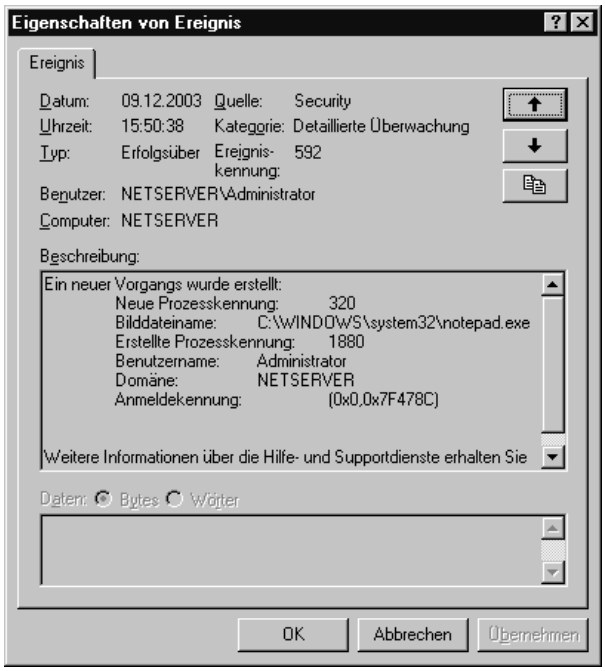


Abbildung 11: Beispiel für die Anzeige eines Ereignisses

7.1.2.2 Filterung der Einträge

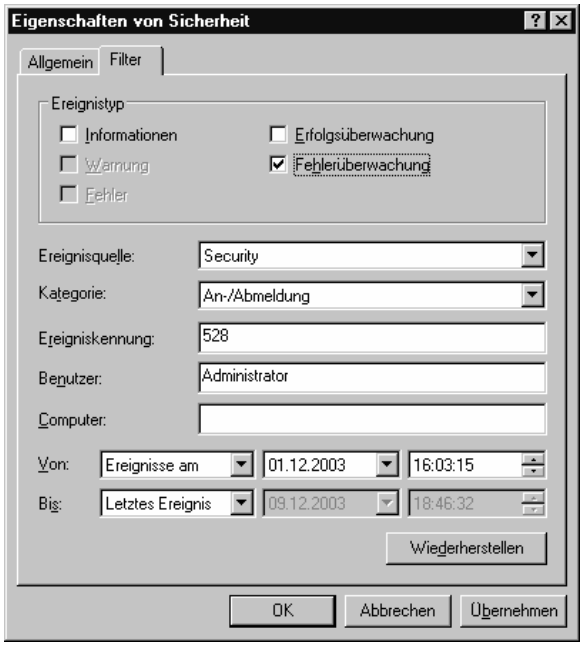


Abbildung 12: Filterung von Einträgen

Um bei vielen Einträgen nicht die Übersicht zu verlieren, kann über die Eigenschaften eines Protokolls unter der Registerkarte Filter eine sehr genaue Auswahl der anzuzeigenden Ereignisse getroffen werden (Abbildung 12). Unter anderen kann nach speziellen Ereigniskennungen, Erfolgs- oder Fehlerfällen und bestimmten Zeiträumen gefiltert werden.

Sehr viel Sinn macht es in diesem Zusammenhang, sich über das Aktions-Menü eine „Neue Protokollansicht“ zu erstellen, die dann dauerhaft mit einem wichtigen Filter spezifiziert wird. Dadurch entfällt das ständige Wechseln und neu Eingeben wichtiger Filtereigenschaften und man kann z.B. gleich die Ansicht „Alle Fehlgeschlagenen Anmeldeversuche“ oder ähnliches aufrufen.

7.1.2.3 Ereignisse

Die Protokollierung erfolgt auf der Basis von so genannten Ereignissen, die dem Ausführen von bestimmten Funktionen des Betriebssystems entsprechen. Diese Ereignisse haben zur eindeutigen Kennzeichnung eine dreistellige Identifikationsnummer, die Ereigniskennung. Dabei entspricht ein Ereignis allerdings meist nicht den im Kapitel 3.2 festgelegten Vorgängen. Wie dort schon angesprochen, korrespondieren diese Ereignisse nicht direkt mit Benutzerhandlungen, sondern stellen meist nur Teilaspekte dieser dar. Dadurch erzeugen die verwendeten Vorgänge teilweise sehr viele Ereignisse. Zudem hinterlassen verschiedene Vorgänge zum Teil Einträge derselben Ereigniskennung.

So erzeugt das Anlegen eines neuen Benutzers in der lokalen Benutzerdatenbank sowohl über die grafische Verwaltungsoberfläche als auch über den Shellbefehl net.exe nicht nur einen Eintrag der Ereigniskennung 624 für „Ein Benutzerkonto wurde erstellt“, sondern u. a. ebenso einen Eintrag 636 für das Hinzufügen des Benutzers zur Gruppe Benutzer, das automatisch vorgenommen wird.

Insofern kann hierbei durch ein einzelnes Ereignis meist noch nicht auf den verursachenden Vorgang geschlossen werden, sondern es müssen zusätzlich die dazugehörigen vorhergehenden und nachfolgenden Ereignisse miteinbezogen werden. Teilweise spielt dabei nicht nur die Ereigniskennung, also die Art des Ereignisses, sondern auch der Inhalt in dem Eintrag, für das Nachverfolgen des Vorgangs eine Rolle.

So wird beispielsweise ein Eintrag der Ereigniskennung 528, die für eine erfolgreiche Anmeldung steht, u. a. sowohl von einer lokalen Benutzeranmeldung als auch bei einer entfernten Anmeldung per Terminalserver erzeugt. Dabei hat der Eintrag im Inhaltsfeld „Anmeldetyp“ erfreulicherweise jeweils unterschiedliche Werte (siehe auch im Kapitel 7.1.2.7 unter Anmeldetypen).

Um hier dem Benutzer der Klassifikation den Rückschluss von den Quellen auf die erzeugenden Vorgänge so gut wie möglich zu erleichtern, ist auf den jeweiligen Quellenblättern, in denen die relevanten Ereigniskennungen einer Kategorie zusammengefasst sind, im Kriterium „Auswertung“ eine Entscheidungshilfe angegeben, wie mehrere Ereigniseinträge auszuwerten sind, um auf den richtigen Vorgang zu schließen.

In den folgenden Kapiteln werden Teilaspekte der Protokolleinträge etwas ausführlicher erklärt.

7.1.2.4 Dateiformat der Protokolldateien

Für die Online-Auswertung der Ereignisprotokolldateien sind im Betriebssystem die Ereignisanzeige sowie spezielle Befehle der Windows API vorhanden. Dies erleichtert dem Anwender entsprechende Aufgaben durchzuführen und macht Detailinformationen über das Format der Datei und die Kodierung der abgespeicherten Informationen entbehrlich. Dies dient auch dem Zweck, Dateizugriffe durch weitere Benutzerprogramme zu vermeiden. Während des Betriebs werden die Logdateien nämlich vom System verwendet und können deshalb nicht gleichzeitig von weiteren Programmen verwendet werden. Der Zugriff kann nur über die API erfolgen, die hier nur Befehle zum Auslesen oder Einfügen neuer Einträge zur Verfügung stellt, nicht aber um vorhandene Einträge einzeln zu löschen oder gar nachträglich zu verändern. Dies bewirkt einen gewissen Schutz vor Fälschungen.

Das Programm Ereignisanzeige bietet auch nicht die Möglichkeit, direkt andere Ereignisprotokolle zu öffnen, sondern zeigt automatisch die aktuell geführten Protokolle des Systems an. Zwar bietet sie mit dem Menüpunkt „Protokolldatei öffnen...“ im Menü „Aktion“ die Möglichkeit, andere als die aktuell geführten Protokolle zu öffnen und anzuzeigen. Jedoch funktioniert dies nur bei Protokolldateien, die zuvor mit der Funktion der Ereignisanzeige „Protokolldatei speichern unter ...“ erzeugt worden sind. Eine Suche nach anderen Tools, die auch die Protokolldateien mit dem Format der aktuell geführten Version eines anderen Systems anzeigen können, bleibt hier ergebnislos, da alle auffindbaren Programme die genannten API-Funktionen nutzen. Damit sind sie für die Offlineauswertung der Protokolldateien aber unbrauchbar, da die API automatisch nur die Einträge des auf dem eigenen System verwendeten Protokolls ausliest und keine Wahl der zu öffnenden Dateien zulässt. Es mag jedoch z.B. im Umfang forensischer Programmpakete Programme geben, die diese Funktionen mitbringen.

Insbesondere für die Offline-Auswertung ist es erforderlich, die Ereignisprotokolldateien mit einem Standardwerkzeugen auszuwerten. Als Werkzeuge für die Betrachtung von Binärdateien eignen sich Hexeditoren wie z.B. Winhex [Xway04]. Um die Anzeige interpretieren zu können sind bei einer solchen Untersuchung Informationen über das Format der Dateien und die Kodierung der abgespeicherten Informationen unentbehrlich.

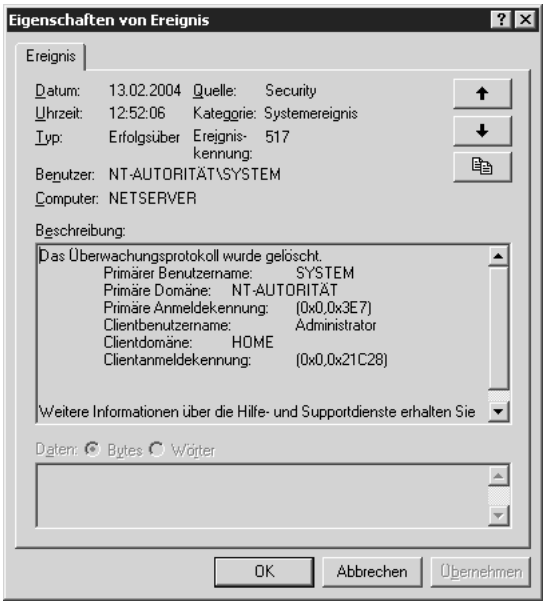


Abbildung 13: Ansicht in Ereignisanzeige

Anschließend sind die wichtigsten Informationen zur Auswertung der Ereignisprotokolldateien dargestellt. Hier sind zunächst zum Vergleich zwei Darstellungen zum Sicherheitsprotokoll abgebildet. In der linken Abbildung sieht man den ersten Eintrag des Sicherheitsprotokolls in der Ereignisanzeige (Abbildung 13), der sich nach dem Löschen aller Einträge als erster Eintrag über den Vorgang „Systemprotokoll löschen“ im Sicherheitsprotokoll befindet. Darunter ist die Darstellung der dahinter stehenden Protokolldatei SecEvent.Evt im Hexeditor (Abbildung 14) abgebildet.

Ein kurzer Vergleich zeigt, dass nur einige der Daten im Klartext in der Datei vorhanden sind. So finden sich die Werte aus dem Feld Beschreibung in der Datei wieder, allerdings ohne die erklärende Beschriftung. Dagegen können z.B. die Zeitangaben nicht im Klartext abgelesen werden.

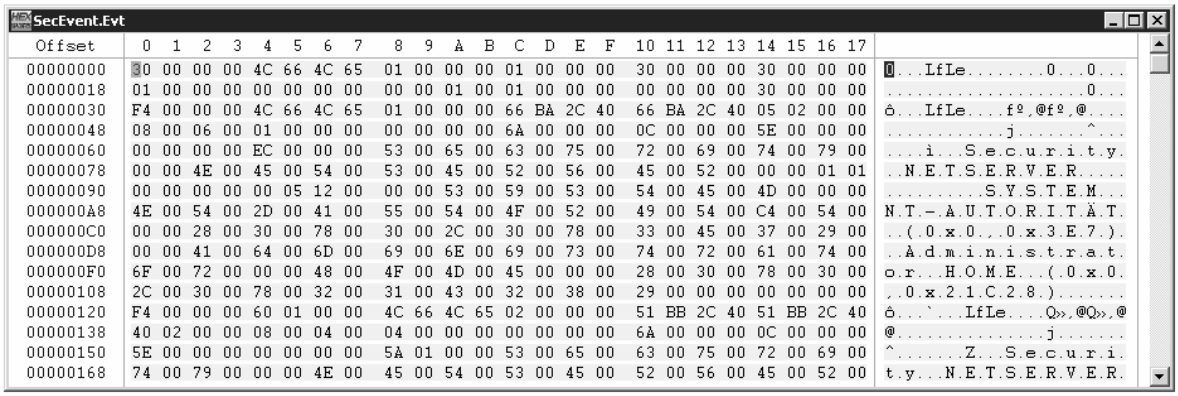


Abbildung 14: Ansicht im Hexeditor

Im Internet findet sich als Beschreibung die Datenstruktur, die die API bei der Funktion ReadEventLog für einen Eintrag zurückliefert [Msdn04b]. Dieser sieht folgendermaßen aus:

```
typedef struct _EVENTLOGRECORD {
  DWORD Length;
  DWORD Reserved;
  DWORD RecordNumber;
  DWORD TimeGenerated;
  DWORD TimeWritten;
  DWORD EventID;
  WORD EventType;
  WORD NumStrings;
  WORD EventCategory;
  WORD ReservedFlags;
  DWORD ClosingRecordNumber;
  DWORD StringOffset;
  DWORD UserSidLength;
  DWORD UserSidOffset;
  DWORD DataLength;
  DWORD DataOffset;
} EVENTLOGRECORD,
*PEVENTLOGRECORD;
```

Diese lässt sich nicht nur für die Übernahme der Daten von der API, sondern nach dem Ergebnis der Untersuchung auch auf die Einträge in der Datei anwenden. Am Anfang der Datei befinden sich ergänzend zu den Einträgen der Ereigniskennungen einige allgemeine undokumentierte Informationen. Diese werden hier jedoch nicht unbedingt benötigt.

Der Beginn eines Eintrages liegt jeweils 4 Byte vor dem Auftreten des Eintrags „LfLe“. Allerdings gehört das erste auftretende „LfLe“ noch zum Vorspann der Datei.

Alle Zahlenwerte sind im Little Endian [Curr01] Format kodiert. Das heißt bei Werten, die mehrere Bytes umfassen, dass das niederwertige vor dem höherwertigen Byte steht. Somit entspricht z.B. der Hexwert 1234 in der Ansicht im Hexeditor, dem Dezimalwert {((3x16+4)x16+1)x16+2}=850.

Die ersten 4 Bytes entsprechen dem Wert Length des Eintrages.

Die weiteren 4 Bytes mit dem Eintrag „LfLe“ entsprechen dem Reserved-Wert.

Die nachfolgenden 4 Bytes entsprechen der RecordNumber. Diese wird fortlaufend beginnend bei 1 durchnummeriert. Wenn allerdings schon Daten des Protokolls überschrieben wurden, hat die kleinste vorhandene RecordNumber einen höheren Wert als 1.

Danach folgen die beiden Zeiteinträge TimeGenerated und TimeWritten. Zur Interpretation der Zeitangaben ist zu sagen, dass diese als Zahl der Sekunden seit 00:00 Uhr des 01.01.1970 in GMT (Greenwich Mean Time) angegeben sind. Hierbei sind die Schaltjahre zu berücksichtigen (alle Jahre, die durch 4 aber nicht durch 100 ohne Rest teilbar sind).

Hier ein Beispiel für die Kodierung des 16.02.2004, 01:00:00 Uhr (Mitteleuropäische Zeit):
Zu berücksichtigen sind 34 Jahre, 7 Schalttage (Schaltjahre 72,76,80,84,88,92,96 ohne 2000), 31 Tage (Januar) und 16 Tage; Die eine Stunde ist wegen der Zeitdifferenz zur GMT nicht zu berücksichtigen.
{34 Jahre * 365 Tage/Jahr + 7 Tage + 31 Tage + 16 Tage} = 12464 Tage;
12464 Tage * 24 Stunden/Tag * 60 Minuten/Stunde * 60 Sekunden/Minute = 1076889600 Sekunden in Dezimaldarstellung;
Dieser Zahlenwert ergibt in Hexdarstellung 40 30 08 00.
In Little Endian Hex-Darstellung entspricht dies 00 08 30 40.

Es folgt die Ereigniskennung (EventID), die die Art des Ereignisses kennzeichnet und damit entscheidend für richtige Interpretation der späteren Texteinträge ist.

Die in der Ereignisanzeige in der Beschreibung angezeigten Feldnamen sind in der Datei nicht abgespeichert. In der Datei finden sich ausschließlich die variablen Werte. Um diese Werte richtig zu interpretieren, lassen sich die Feldnamen über die Ansicht eines der EventID entsprechenden Ereigniseintrags in der Ereignisanzeige ermitteln. Die Zahl der so zu interpretierenden Werte befindet sich in Numstrings.

In EventType findet sich für Sicherheitsprotokolleinträge die Information, ob es ein Eintrag für einen Fehler- oder Erfolgsfall war. Hierbei ist der Wert 1 für einen Fehler, der Wert 8 für einen Erfolg, vergeben.

Der Wert EventCategory entspricht der Ereigniskategorie. Folgende Werte entsprechen den Kategorien:

Wert für Eventcategory	**Ereigniskategorie**
01	Systemereignis
02	An/Abmeldung
03	Objektzugriff
04	Berechtigungen
05	Detaillierte Überwachung
06	Richtlinienänderung
07	Kontenverwaltung
08	Verzeichnisdienstzugriff
09	Kontoanmeldung

7.1.2.5 Entstehungsbedingungen und Lebensdauer von Einträgen

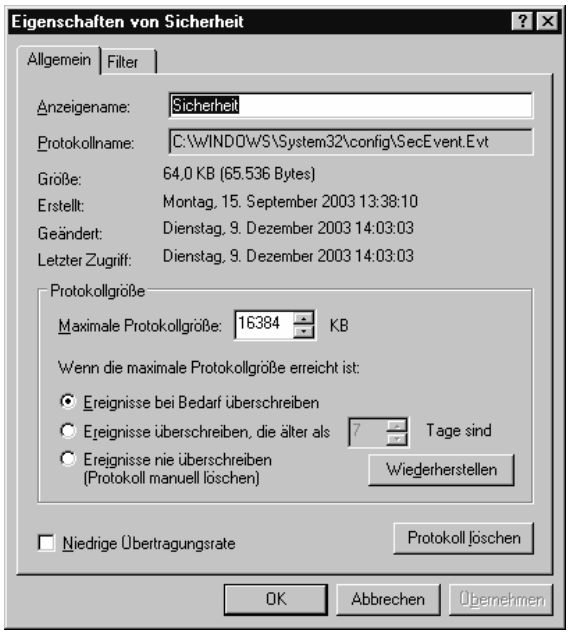


Abbildung 15: Protokolleigenschaften

Über einen Aufruf der Eigenschaften des Protokolls (Abbildung 15) lässt sich der Pfad- und Dateiname des Protokolls ablesen. Außerdem kann man hier für jedes Protokoll getrennte Einstellungen bezüglich dessen Größe und Überschreibungseigenschaften vornehmen, die Auswirkungen auf die Entstehung von Einträgen und deren Lebensdauer haben.

Vergröbert betrachtet ist das Ergebnis der Bewertung der Lebensdauer von Protokolleinträgen unabhängig von anderen Vorgängen. Denn die Einträge bleiben zunächst generell bestehen, auch wenn entsprechende weitere Vorgänge durchgeführt werden, insbesondere auch bei der Aufhebung eines erzeugten Systemzustandes durch den korrespondierenden aufhebenden Vorgang.

Differenziert betrachtet hängt die Lebensdauer vorhandener Einträge jedoch von der eingestellten "Maximalen Protokollgröße" (Standard 16384 KB) und dem Umfang weiterer eintref-

fender Einträge ab. Letzteres hängt wiederum davon ab, welche Überwachungsmöglichkeiten aktiviert sind. So wird sich ein Protokoll mit maximaler Größe einiger Megabytes, bei dem nur Benutzeranmeldungen protokolliert werden, nur relativ langsam füllen. Wenn jedoch alle Dateizugriffe der gesamten Festplatte aufgezeichnet werden sollen, ist der Speicherplatz schnell verbraucht. Die Quelle wurde deshalb mit dem Standardwert „Bedingt abhängig von anderen Vorgängen“ bewertet.

Für die Einstellung des Aufzeichnungsverhaltens bei Erreichen der eingestellten Protokollgröße stehen folgende Optionen zur Verfügung:

- Bei der Auswahl "Ereignisse bei Bedarf überschreiben" (Standardeinstellung) werden die ältesten Einträge durch die neuesten ersetzt.
- Bei der Auswahl "Ereignisse überschreiben, die älter als [x] Tage sind", werden die Einträge frühestens nach x Tagen gelöscht.
- Schließlich gibt es noch die Option "Ereignisse nie überschreiben" bei der Einträge nur manuell gelöscht werden.

Bei einer Aktivierung der ersten Option können andere Vorgänge irgendwann das Entfernen des Eintrages aus dem Protokoll bewirken. Man sollte diese Eigenschaft berücksichtigen, da dadurch das Protokoll unbeabsichtigt verändert werden kann und dies insbesondere eine Methode zur Vertuschung eines Vorgangs darstellt. Wenn man es schafft so viele spätere Einträge zu erzeugen, wird bei aktivierter Einstellung "Ereignisse bei Bedarf überschreiben" irgendwann der Eintrag, der wichtige Hinweise geben würde, von den neuen unbedeutenden ersetzt.

Bei der Aktivierung einer der beiden letzten Optionen hängt dagegen die Entstehung von neuen Einträgen von der Protokollgröße und vorausgegangenen Vorgängen und deren Protokollierung ab. Bei der dritten Option werden beim Erreichen der maximalen Protokollgröße keine neuen Einträge angelegt. Gleiches gilt bei der zweiten Option, sobald keine Einträge mehr vorhanden sind, deren minimale Aufbewahrungszeit überschritten ist. Somit besteht die Gefahr, dass ein Angreifer erst mit nichts sagenden Einträgen das Protokoll füllt und dann, nachdem nichts mehr protokolliert werden kann, seine eigentlich geplanten Vorgänge unprotokolliert durchführen kann. Da die Protokollierung nach der Alterung der Einträge bei der zweiten Option wieder aufgenommen wird, bleibt hier das Erkennen des Fehlens von Protokolleinträgen unsicher.

Wesentlich ist in diesem Zusammenhang deshalb die Einstellung in den Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen namens „Überwachung: System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können“ (standardmäßig deaktiviert). Diese verhindert bei Aktivierung in Kombination mit den beiden letzten Optionen durch das Herunterfahren des Systems das Ausführen von Vorgängen, die wegen fehlender Speicherkapazität nicht mehr protokollierbar wären. Dadurch ergibt sich aber die Möglichkeit einer „Denial of Service“-Attacke. Diese Einstellung ist somit nur bei Systemen praktikabel, bei denen es wichtiger ist, dass für alle durchgeführten zu protokollierenden Vorgänge auch Einträge erstellt werden als dass sie unterbrechungsfrei laufen.

7.1.2.6 Spezielles zum Sicherheitsprotokoll

Während bei den zwei Protokollen „System“ und „Anwendungen“ schon durch das System selber respektive die installierten Anwendungen vorgegeben wird, was für Einträge hier erstellt werden, lassen sich für das Sicherheitsprotokoll die Kategorien der überwachten Ereignisse selbst auswählen.

Dies geschieht über die Einstellungen in den Überwachungsrichtlinien (Abbildung 16).

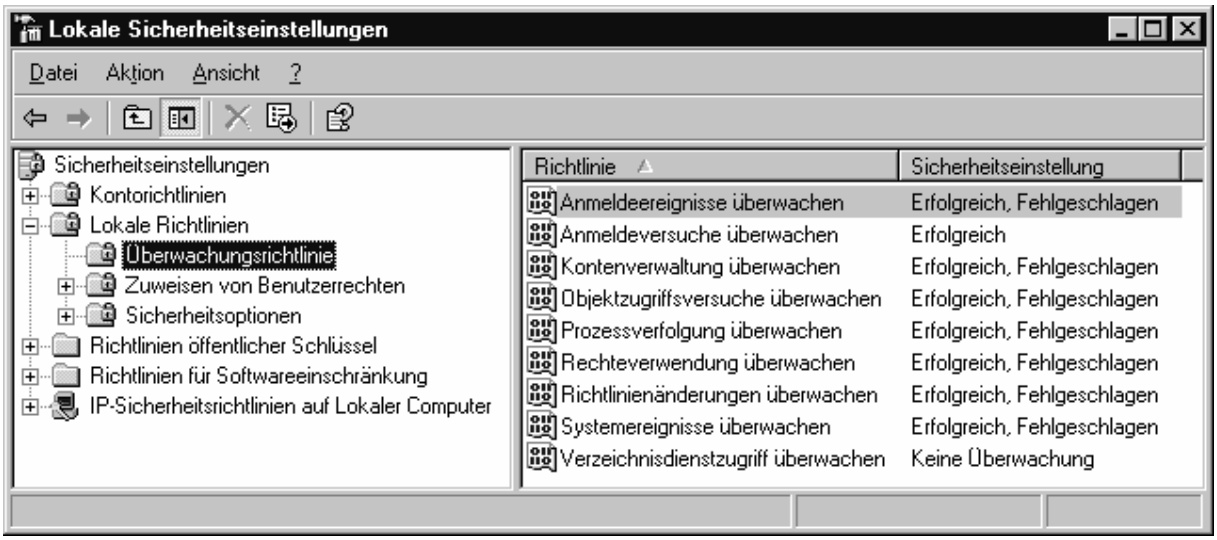


Abbildung 16: Lokale Sicherheitseinstellungen

Hier lässt sich für jede der Kategorien auswählen, ob erfolgreiche, fehlgeschlagene, beide oder keines dieser Ereignisse aufgezeichnet werden sollen. Die Standardeinstellungen werden danach unterschieden, ob der Rechner ein Domänencontroller ist oder nicht. Zu beachten ist dabei, dass die Kategorien zum Teil in der Ereignisanzeige und in den Überwachungsrichtlinien unterschiedlich benannt sind.

Bezeichnung der Kategorie im Sicherheitsprotokoll	**Bezeichnung der Kategorie in den Überwachungsrichtlinien**	**Standardmäßig aktiviert**	
		Normaler Rechner	**Domänen-controller**
An-/Abmeldung	Anmeldeereignisse überwachen	Erfolgreich	
Kontoanmeldung	Anmeldeversuche überwachen	Erfolgreich	
Kontenverwaltung	Kontenverwaltung überwachen	Keine Überwachung	Erfolgreich
Objektzugriff	Objektzugriffsversuche überwachen	Keine Überwachung	
Detaillierte Überwachung	Prozessverfolgung überwachen	Keine Überwachung	
Berechtigungen	Rechteverwendung überwachen	Keine Überwachung	
Richtlinienänderung	Richtlinienänderung überwachen	Keine Überwachung	Erfolgreich
Systemereignis	Systemereignisse überwachen	Keine Überwachung	Erfolgreich
Verzeichnisdienstzugriff	Verzeichnisdienstzugriff überwachen	Keine Überwachung	Erfolgreich

Die Kategorie „An-/Abmeldung“ ist im folgenden Kapitel 7.1.2.7 noch genauer beschrieben. Bei der Richtlinie „Objektzugriffsversuche überwachen“ ist zu beachten, dass abweichend von den anderen Richtlinien zusätzlich zur Aktivierung der allgemeinen Einstellung noch für

jedes Objekt, das einbezogen werden soll, festgelegt werden muss, welche Einzelhandlungen protokolliert werden sollen. Näheres dazu im Kapitel 7.1.2.8 „Kategorie Objektzugriff“.

Insgesamt betrachtet ist die Bedeutung der Kategorien sehr unterschiedlich. So finden sich in der Kategorie „Berechtigungen“ trotz des interessanten Titels keine wichtigen Ereignisse, die den untersuchten Vorgängen zuzuordnen wären. Für diese Kategorie ist deshalb kein Quellenblatt angelegt.

Aber auch in den Kategorien, für die Quellenblätter existieren, werden nur die Ereignisse beschrieben, die von den untersuchten Vorgängen erzeugt werden und für diese charakteristisch und auswertbar sind. Es existieren damit weitere Ereignisse, die aber wegen fehlender Relevanz für die forensische Analyse nicht beschrieben sind.

Eine Liste von Ereigniskennungen mit einer kurzen englischen Beschreibung findet sich nach Kategorien geordnet unter [Tech04a]. Die auf den Quellenblättern beschriebenen Ereigniskennungen sind mit einer Kurzbeschreibung versehen, die der deutschen Microsoft Onlinehilfe (Indexsuche beim Windows Server 2003 mit dem Stichwort „Überwachungsrichtlinieneinstellungen“ durchführen und dann die jeweilige Kategorie aufrufen) entnommen ist.

Bei der Verwendung dieser Hilfen muss beachtet werden, dass die Zuordnung der Ereignisse zu den Kategorien nicht immer korrekt ist. So finden sich die Ereigniskennungen 682 und 683 in der Hilfe sowohl bei „Anmeldeversuche überwachen“ als auch bei „Anmeldeereignisse überwachen“. Jedoch zeigt die Ereignisanzeige für diese Ereigniskennungen eindeutig die Kategorie „An-/Abmeldung“ an und diese Ereigniskennungen werden nur bei Aktivierung von „Anmeldeereignisse überwachen“ erzeugt. Weiterhin gehört die Ereigniskennung 565 nicht wie angegeben zur Kategorie „Objektzugriff“, sondern zur Kategorie „Verzeichnisdienstzugriff“. Die Aktivierung der Protokollierung und die Anzeige der Kategorie des Protokolleintrages handhabt das System widerspruchsfrei. Auf den Quellenblättern sind die in der Dokumentation fehlerhaft zugeordneten Ereigniskennungen nach dem Verhalten des Systems und nicht nach der Beschreibung eingeordnet.

Bei der Festlegung der zu überwachenden Kategorien ist eine Regel zu beachten, die eigentlich bei allen Arten von Protokollierungen und auch in vielen anderen Bereichen gilt: „Weniger ist mehr“. Wenn man sich alle möglichen Ereignisse protokollieren lässt, ergibt sich eine Unmenge von Informationen, die sich meist nicht mehr sinnvoll auswerten lässt. Außerdem setzt die Protokollierung die Systemgeschwindigkeit herab. Die Problematik des Überschreibens von älteren Nachrichten und die Unterdrückung der Aufzeichnung neuer Ereignisse ist in Kapitel 7.1.2.5 bereits dargestellt. Diese Problematik verschärft sich natürlich dann, wenn sehr viel protokolliert wird, weil dadurch bei unveränderter Protokollgröße abhängig von den Protokolleinstellungen die schon beschriebenen negativen Auswirkungen auf die Entstehung und Lebensdauer der Einträge verstärkt auftreten.

Um dennoch bei umfangreichen Anforderungen an die Protokollierung die Flut der Protokolleinträge bewältigen zu können, insbesondere wenn mehrere Rechner im Netzwerk zu überwachen sind, gibt es spezielle Programme, die über ausgefeilte Suchfunktionen und zum Teil automatische Melde- und Auswertungsfunktionen verfügen. Ohne näher auf deren Funktionalität einzugehen, werden einige dieser Programme zum weiteren Nachschlagen hier genannt.

- Event Alarm & Event Analyst [Dori03]
- Event Log Manager [Tnts03]
- LogCaster [Ripp03]

7.1.2.7 Kategorie An-/Abmeldung

Folgende Liste stammt aus der Onlinehilfe des Betriebssystems (Indexsuche, unter „Überwachungsrichtlinieneinstellungen“ und dann darunter „Anmeldeereignisse überwachen“), kann aber in ähnlicher Form auch im Internet nachgelesen werden [Tech04b].

Anmeldeereignisse	
Ereigniskennung	**Beschreibung**
528	Ein Benutzer hat sich erfolgreich an einem Computer angemeldet. Informationen zum Anmeldetyp finden Sie in der Tabelle mit den Anmeldetypen weiter unten.
529	Anmeldefehler. Ein Anmeldeversuch erfolgte mit einem unbekannten Benutzernamen oder einem bekannten Benutzernamen mit einem falschen Kennwort.
530	Anmeldefehler. Ein Anmeldeversuch erfolgte, wobei sich das Benutzerkonto außerhalb der zulässigen Zeit anzumelden versuchte.
531	Anmeldefehler. Ein Anmeldeversuch erfolgte mit einem deaktivierten Konto.
532	Anmeldefehler. Ein Anmeldeversuch erfolgte mit einem abgelaufenen Konto.
533	Anmeldefehler. Ein Anmeldeversuch erfolgte durch einen Benutzer, der sich nicht an diesem Computer anmelden darf.
534	Anmeldefehler. Der Benutzer hat beim Anmelden einen unzulässigen Anmeldetyp verwendet.
535	Anmeldefehler. Das Kennwort für das angegebene Konto ist abgelaufen.
536	Anmeldefehler. Der Anmeldedienst ist nicht aktiv.
537	Anmeldefehler. Der Anmeldeversuch ist aus anderen Gründen fehlgeschlagen. Anmerkung: In manchen Fällen ist der Grund für das Fehlschlagen der Anmeldung nicht bekannt.
538	Der Abmeldevorgang wurde für einen Benutzer durchgeführt.
539	Anmeldefehler. Das Konto wurde während des Anmeldeversuchs gesperrt.
540	Ein Benutzer hat sich erfolgreich an einem Netzwerk angemeldet.
541	Die Hauptmodusauthentifizierung per Internetschlüsselaustausch (Internet Key Exchange, IKE) wurde zwischen dem lokalen Computer und der aufgeführten Peerkennung (die eine Sicherheitszuordnung herstellt) durchgeführt, oder der Schnellmodus hat einen Datenkanal eingerichtet.
542	Ein Datenkanal wurde beendet.
543	Der Hauptmodus wurde beendet. Anmerkung: Dies kann auf das Ablaufen der Sicherheitszuordnung (standardmäßig acht Stunden), auf Richtlinienänderungen oder die Peerbeendigung zurückzuführen sein.
544	Die Hauptmodusauthentifizierung schlug aufgrund eines ungültigen Zertifikats des Peers oder einer unbestätigten Signatur fehl.
545	Die Hauptmodusauthentifizierung schlug aufgrund eines Kerberos-Fehlers oder eines ungültigen Kennwortes fehl.
546	Die IKE-Sicherheitszuordnung schlug fehl, weil der Peer eine ungültige Anfrage gesendet hat. Ein Paket mit ungültigen Daten wurde empfangen.
547	Bei einem IKE-Handshake ist ein Fehler aufgetreten.
548	Anmeldefehler. Die Sicherheitskennung (Security ID, SID) einer vertrauenswürdigen Domäne stimmt nicht mit der Kontodomänen-SID des Clients überein.
549	Anmeldefehler. Alle SIDs, die nicht vertrauenswürdigen Namespaces entsprechen, wurden während einer strukturübergreifenden Authentifizierung herausgefiltert.
550	Eine Benachrichtigung, die auf einen Dienstverweigerungsangriff hinweisen könnte.
551	Ein Benutzer hat den Abmeldevorgang gestartet.
552	Ein Benutzer hat sich mit expliziten Anmeldeinformationen erfolgreich an einem Computer angemeldet, wobei er bereits als ein anderer Benutzer angemeldet ist.
682	Ein Benutzer hat erneut eine Verbindung zu einer getrennten Terminalserversitzung hergestellt.
683	Ein Benutzer hat eine Terminalserversitzung getrennt, ohne sich abzumelden. Anmerkung: Dieses Ereignis wird generiert, wenn ein Benutzer mit einer Terminalserversitzung über das Netzwerk verbunden ist. Es wird auf dem Terminalserver angezeigt.

Die einzelnen Ereigniskennungen haben dann wie oben beschrieben alle die selben Felder, aber der Inhalt der Beschreibung weicht von Kennung zu Kennung ab.

Ein Bespiel für einen Eintrag der Ereigniskennung 528 (Ein Benutzer hat sich erfolgreich an einem Computer angemeldet) ist:

```
Ereignistyp:      Erfolgsüberw.
Ereignisquelle:   Security
Ereigniskategorie:      An-/Abmeldung
Ereigniskennung:  528
Datum:            19.11.2003
Zeit:       12:57:09
Benutzer:         NETSERVER\Administrator
Computer:   NETSERVER
Beschreibung:
Erfolgreiche Anmeldung:
      Benutzername:     Administrator
      Domäne:           NETSERVER
      Anmeldekennung:         (0x0,0xDE8E)
      Anmeldetyp: 2
      Anmeldevorgang:   User32
      Authentifizierungspaket:      Negotiate
      Name der Arbeitsstation:      NETSERVER
      Anmelde-GUID:     -
      Aufruferbenutzername:   NETSERVER$
      Aufruferdomäne:   HOME
      Aufruferanmeldekennung: (0x0,0x3E7)
      Aufruferprozesskennung: 504
      Übertragene Dienste: -
      Quellnetzwerkadresse:   127.0.0.1
      Quellport:  0


Weitere Informationen über die Hilfe- und Supportdienste erhalten Sie
unter http://go.microsoft.com/fwlink/events.asp.
```

Insofern kommen pro Ereigniskennung viele zusätzliche Feldwerte hinzu. Auf all diese konnte im Rahmen der Diplomarbeit nicht eingegangen werden, wenn sie von hoher Wichtigkeit sind werden diese Felder jedoch bei der jeweiligen Quellenbeschreibung im Kriterium „Informationsgehalt“ genannt.

Während die meisten wichtigen Felder - wie Benutzername oder Quellnetzwerkadresse - selbsterklärend sind, gebraucht es für das Verstehens der Information „Anmeldetyp“ noch weiterer Erklärungen, da diese nicht im Klartext vorliegt, sondern nur als Zahl kodiert ist:

Anmeldetypen

Die Anmeldetypen sind als Zahl kodiert die eine Aussage darüber gibt, auf welche Art sich ein Benutzer eingeloggt. Diese Anmeldetypkennzahl kommt z.B. bei den Ereigniskennungen 528 und 538 vor.

Folgende Liste stammt aus der Onlinehilfe des Betriebssystems:

Anmeldetyp	Anmeldetitel	Beschreibung
2	Interaktiv	Ein Benutzer hat sich an seinem Computer angemeldet.
3	Netzwerk	Ein Benutzer oder ein Computer hat sich über das Netzwerk an seinem Computer angemeldet.
4	Batch	Der Batchanmeldungstyp wird von Batchservern verwendet, wobei Prozesse im Auftrag eines Benutzers ohne dessen direktes Eingreifen ausgeführt werden.
5	Dienst	Ein Dienst wurde vom Dienststeuerungs-Manager gestartet.
7	Entsperren	Die Sperrung dieser Arbeitsstation wurde aufgehoben.
8	Netzwerkklartext	Ein Benutzer hat sich über das Netzwerk an seinem Computer angemeldet. Das Kennwort des Benutzers wurde ohne Hashformat an das Authentifizierungspaket übergeben. Die integrierten Authentifizierungspakete führen ein Hashing der Anmeldeinformationen durch, bevor diese über das Netzwerk gesendet werden. Die Anmeldeinformationen werden nicht unverschlüsselt (dies wird auch als Klartext bezeichnet) im Netzwerk übermittelt.
9	Neue Anmeldeinformationen	Ein Anrufer hat sein aktuelles Token dupliziert und neue Anmeldeinformationen für ausgehende Verbindungen angegeben. Die neue Anmeldungssitzung hat die gleiche lokale Identität, verwendet jedoch andere Anmeldeinformationen für andere Netzwerkverbindungen.
10	RemoteInteractive	Ein Benutzer hat sich unter Verwendung von Terminaldienste oder Remotedesktop remote an diesem Computer angemeldet.
11	CachedInteractive	Ein Benutzer hat sich an diesem Computer mit Netzwerkanmeldeinformationen angemeldet, die lokal auf dem Computer gespeichert waren. Der Domänencontroller wurde nicht kontaktiert, um die Anmeldeinformationen zu überprüfen.

7.1.2.8 Kategorie Objektzugriff

Wie schon weiter oben erwähnt, reicht es bei dieser Ereigniskategorie für die wichtigsten Ereignisse nicht nur allgemein die Protokollierung aktiviert zu haben, sondern es ist für jedes Objekt eigens die Einstellung für die Überwachung zu setzten. Objekte in diesem Zusammenhang sind sowohl Ordner und Dateien, Registryschlüssel als auch Spezialfälle wie Drucker. Für Ordner und Registryschlüssel ist jedoch die Möglichkeit der Vererbung gegeben, das heißt die Einstellungen auch für alle Unterordner oder enthaltenen Dateien respektive Unterschlüssel zu übernehmen. Ordner und Dateien sind jedoch nur überwachbar, wenn sie sich auf einer NTFS-Partition befinden.

Allgemein erfolgen die Einstellungen über die Eigenschaften des Objekts. Diese können über den Explorer oder im Falle der Registry über Berechtigungen mit dem Programm Registrierungseditor (regedit.exe) aufgerufen werden. In der Registerkarte „Sicherheit“ ist mit „Erweitert“ ein neues Fenster aufzurufen, in dessen Registerkarte „Überwachung“ sich durch Hinzufügen eines Benutzers oder einer Gruppe für diese eigene Einstellungen zur Protokollierung möglich sind (Abbildung 17). Die zur Verfügung stehenden Einstellungen, hängen wiederum von dem zu überwachenden Objekt ab. Während für ein Druckerobjekt noch überschaubare sechs verschiedene überwachbare Zugriffsarten existieren, sind es bei Ordnern schon 14 verschiedene, die auch noch nach erfolgreichem oder fehlgeschlagenem Zugriff unterschieden werden können (Abbildung 18).

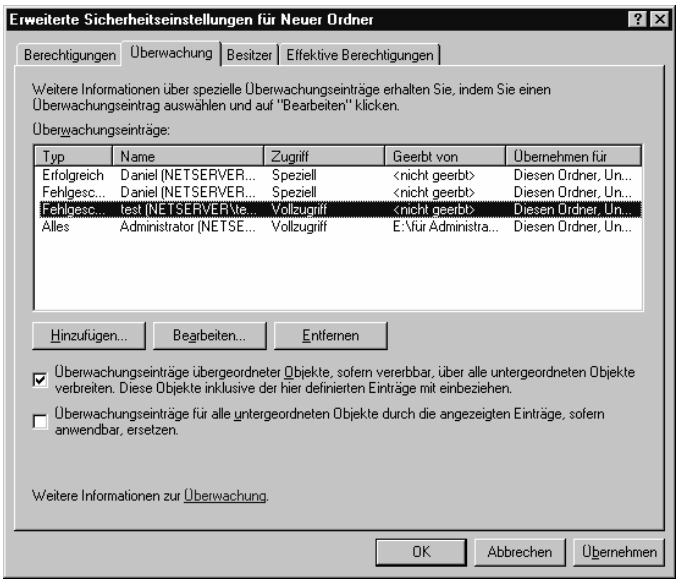


Abbildung 17: Überwachungseinstellungen

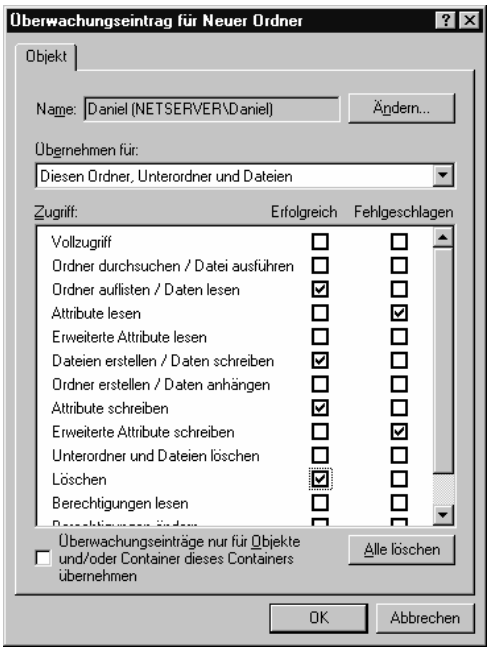


Abbildung 18: Überwachungseintrag

Diese entsprechen den normalen NTFS-Berechtigungen, die auch die Erlaubnis für Zugriffe auf Dateien oder Ordner regeln. Eine Erklärung dieser Zugriffsarten findet sich zum Beispiel unter [Tech04c].

Während zu der Kategorie „Objektzugriff“ zwar insgesamt 41 Ereigniskennungen gehören (komplette Liste in Onlinehilfe unter Windows Server 2003 über Indexsuche, unter „Überwachungsrichtlinieneinstellungen“ und dann darunter „Objektzugriffsversuche überwachen“ oder teilweise unter [Tech04d]), sind für die eigentlichen Objektzugriffe nur die Ereigniskennungen 560, 562 und 567 interessant.

In der Ereigniskennung 560 wird die Erstellung eines Handle zu einem bestimmten Objekt mit bestimmten Berechtigungen dokumentiert, in 567 die Ausführung dieser Rechte auf das Objekt und in 562 die Schließung dieses Handle. Dabei zeigt 560 eventuell die Anforderung mehrerer Rechte in einer Ereigniskennung an, die nacheinander benutzt werden. So kann 567, die immer nur für die Ausübung eines Rechtes steht, wegen mehrfacher Ausführung eines oder verschiedener Rechte mehrmals für dasselbe Handle vorkommen. Diese Ereigniskennungen treten in der Reihenfolge 560, 567 und dann 562 auf, wobei sie nicht direkt aufeinander folgen müssen, also dazwischen wiederum andere Einträge stehen können.

Die Aussagekraft dieser Protokolleinträge über die wirklich ausgeübten Vorgänge im Dateisystem wie „Datei kopieren“ ist allerdings nur gering, da in der Granularität der oben beschriebenen NTFS-Berechtigungen aufgezeichnet wird und die Verbindung zu den Benutzervorgängen erst hergestellt werden müsste.

So erzeugt der Vorgang „Datei kopieren“ mit dem copy Befehl zirka 20 Einträge von den Ereigniskennungen 560, 562 und 567, für die exemplarisch folgend jeweils ein Beispiel angegeben ist.

Ereigniskennung 560:

```
Ereignistyp:      Erfolgsüberw.
Ereignisquelle:   Security
Ereigniskategorie:      Objektzugriff
Ereigniskennung:  560
Datum:            22.01.2004
Zeit:       16:36:29
Benutzer:         NETSERVER\Administrator
Computer:   NETSERVER
Beschreibung:
Geöffnetes Objekt:
      Objektserver:     Security
      Objekttyp:  File
      Objektname: E:\für Administrator überwachter Ordner
      Handlekennung:    88
      Vorgangskennung:  {0,319181}
      Prozesskennung:   2952
      Abbilddateiname:  C:\WINDOWS\system32\cmd.exe
      Primärer Benutzername:  Administrator
      Primäre Domäne:   NETSERVER
      Primäre Anmeldekennung: (0x0,0xE4BA)
      Clientbenutzername:     -
      Clientdomäne:     -
      Clientanmeldekennung:   -
      Zugriffe:   SYNCHRONIZE
                  Daten lesen (oder Verzeichnis auflisten)

      Rechte:     -
      Beschränkte SID-Anzahl: 0
      Zugriffsmaske:    0x100001


Weitere Informationen über die Hilfe- und Supportdienste erhalten Sie unter
http://go.microsoft.com/fwlink/events.asp.
```

Ereigniskennung 567:

```
Ereignistyp:      Erfolgsüberw.
Ereignisquelle:   Security
Ereigniskategorie:      Objektzugriff
Ereigniskennung:  567
Datum:            22.01.2004
Zeit:       16:36:29
Benutzer:         NETSERVER\Administrator
Computer:   NETSERVER
Beschreibung:
Objektzugriffsversuch:
      Objektserver:     Security
      Handlekennung:    88
      Objekttyp:  File
      Prozesskennung:   2952
      Abbilddateiname:  C:\WINDOWS\system32\cmd.exe
      Zugriffe:   Daten lesen (oder Verzeichnis auflisten)

      Zugriffsmaske: 0x1


Weitere Informationen über die Hilfe- und Supportdienste erhalten Sie unter
http://go.microsoft.com/fwlink/events.asp.
```

Ereigniskennung 562:

```
Ereignistyp:      Erfolgsüberw.
Ereignisquelle:   Security
Ereigniskategorie:      Objektzugriff
Ereigniskennung:  562
Datum:            22.01.2004
Zeit:       16:36:29
Benutzer:         NETSERVER\Administrator
Computer:   NETSERVER
Beschreibung:
Geschlossenes Handle:
      Objektserver:     Security
      Handlekennung:    88
      Prozesskennung:   2952
      Abbilddateiname:  C:\WINDOWS\system32\cmd.exe


Weitere Informationen über die Hilfe- und Supportdienste erhalten Sie unter
http://go.microsoft.com/fwlink/events.asp.
```

An der "Handlekennung" kann abgelesen werden, welche Einträge 560, 567 und 562 zusammengehören, da diese jeweils hier denselben Wert haben. Aus „Prozesskennung“ sieht man die Prozessnummer des zugreifenden Prozesses. Allerdings kann man hieraus noch nicht unterscheiden, welche Tupel der Ereigniskennungen 560, 567 und 562 zum selben Benutzervorgang gehören, da nicht für jeden Benutzervorgang ein neuer Prozess und somit eine neue Prozesskennung erstellt wird. So bleibt derselbe Explorerprozess normalerweise für die gesamte Benutzersitzung erhalten. Denn hier wird nicht für jedes Explorerfenster ein eigener Prozess gestartet, sondern die Fenster werden von dem Explorerprozess verwaltet, der auch die Taskleiste ab dem Start der Benutzersitzung anzeigt. Und auch die einzelnen Shellbefehle sind so nicht nachvollziehbar, da viele Befehle wie dir oder copy keine eigenständigen Programmdateien sind, sondern Teil der Eingabeaufforderung (cmd.exe) sind und so im Feld „Abbilddateiname“ angezeigt werden. Somit bleibt auch hier die Prozesskennung gleich solange die Vorgänge in derselben Eingabeaufforderung durchgeführt werden. Nur bei speziellen anderen Programmen wie z.B. xcopy.exe, die pro Vorgang gestartet werden und nach der Ausführung enden, wird bei jedem Start eine neue Prozesskennung angelegt.

Während man aus der Ereigniskennung 560 unter „Objektname“ die betroffene Datei, unter „Abbilddateiname“ das zum Zugriff verwendete Programm (im Beispiel oben wegen copy-Befehl C:\WINDOWS\system32\cmd.exe), das „Datum“, die „Zeit“ und den ausführenden „Benutzer“ erkennen kann, bringt die Angabe unter „Zugriffe“ nur indirekte Informationen zum genauen Vorgang. Die anderen Ereigniskennungen 562 und 567 liefern hierbei auch nicht mehr Informationen.

Für einen Vorgang werden oft mehrere Tupel von Ereigniskennungen 560, 567 und 562 angelegt.

In den Einträgen mit der Ereigniskennung 560 finden sich im Feld „Zugriffe“ z.B. folgende Angaben:

```
SYNCHRONIZE
     Daten lesen (oder Verzeichnis auflisten)
```

```
READ_CONTROL
     SYNCHRONIZE
     Daten lesen (oder Verzeichnis auflisten)
```

```
     EA lesen
     Attribute lesen
```

```
DELETE
     READ_CONTROL
     SYNCHRONIZE
     Daten schreiben (oder Datei hinzufügen)
     Daten anhängen (oder Unterverzeichnis hinzufügen oder Pipeinstanz
      erstellen)
     EA schreiben
     Attribute lesen
     Attribute schreiben
```

```
SYNCHRONIZE
     Attribute schreiben
```

Mit diesen Informationen lassen sich aber noch keine aussagekräftigen Folgerungen über den eigentlich ausgeführten Vorgang anstellen. Denn an den dargestellten Einträgen der Ereigniskennungen ist ersichtlich, dass ein Vorgang keine exklusiven Einzeloperationen besitzt, sondern die Einzeloperationen Teil mehrerer Vorgänge sind. Und auch das gemeinsame Auftreten der Einträge in bestimmter Reihenfolge lässt allein noch keine allgemeingültigen Schlüsse zu, da z.B. derselbe mit dem Explorer durchgeführte Vorgang zum Teil andere Einträge in anderer Reihenfolge anlegt als der mit den Shellbefehlen.

Die weitere Untersuchung dieser Eintragsmuster führt zu dem Ergebnis, dass die Zuordnung von Sicherheitsprotokolleinträgen der Kategorie „Objektzugriffe“ zu den verursachenden Vorgängen für das Dateisystem ausgesprochen komplex ist. Unter Abwägung des zu erwartenden Nutzens ist davon auszugehen, dass bei der computerforensischen Analyse in der Praxis wegen des damit verbundenen Aufwandes darauf verzichtet werden muss, die exakte Art des Datei- oder Verzeichniszugriffs aufzuklären. Das heißt sich darauf zu beschränken, mit sehr geringem Aufwand aus den Feldinhalten wie oben beschrieben zu ermitteln, auf welche Datei oder welches Verzeichnis zu welcher Zeit von welchem Benutzer mit welchem Programm zugegriffen worden ist.

Bei der Überwachung der Registry sind die ausgeführten Operationen nach der gleichen Einteilung protokollierbar wie die Berechtigungen vergeben werden können. Da diese mit „Wert abfragen“, „Wert festlegen“, „Unterschlüssel erstellen“, „Unterschlüssel auflisten“ und „Löschen“ auch den ausführbaren Vorgängen entsprechen, ist hierbei die Zuordnung wesentlich leichter. Eingestellt werden kann die Überwachung aber nicht für einzelne Werte, sondern nur den gesamten Schlüssel.

7.1.3 Leistungsüberwachung

Unter Systemsteuerung/Verwaltung/Leistung bzw. durch Ausführen von perfmon.msc wird ein Programm gestartet, in dem sich verschiedene Arten der Leistungsüberwachung finden, die auch für eine forensische Analyse von Belang sein können. Allgemein lassen sich hier für Zustände verschiedenster Systemkomponenten Protokolle anlegen und Warnungen bzw. Aktionen für das Über- oder Unterschreiten von Grenzwerten festlegen.

Diese Quellen fallen aus dem sonstigen Rahmen, weil sie zwar theoretisch Informationen zu den unterschiedlichsten Vorgängen liefern, praktisch aber in vielen Fällen wenig forensische Aussagekraft besitzen. Sie müssen außerdem im Voraus aktiviert werden, bieten dazu aber im Vergleich zur Sicherheitsprotokollierung eine fast unüberschaubare Menge von Einstellmöglichkeiten. Auch ist es für eine Analyse zurückliegender Vorgänge sehr unwahrscheinlich, dass ein Leistungsprotokoll mit genau den dafür erforderlichen Einstellungen aktiv gewesen ist. Aus diesen Gründen ist eine Beschreibung des Leistungsmonitors auf den Quellenblättern nicht zweckmäßig.

Während sich im „Systemmonitor“ (Abbildung 19) ausgewählte aktuelle Daten anzeigen lassen, ist über „Leistungsprotokolle und Warnungen“ eine Aufzeichnung dieser Daten möglich. Unter „Leistungsprotokolle und Warnungen“ sind folgende drei Punkte zusammengefasst:

Leistungsindikatorenprotokolle

Protokolle der Ablaufverfolgung

Warnungen

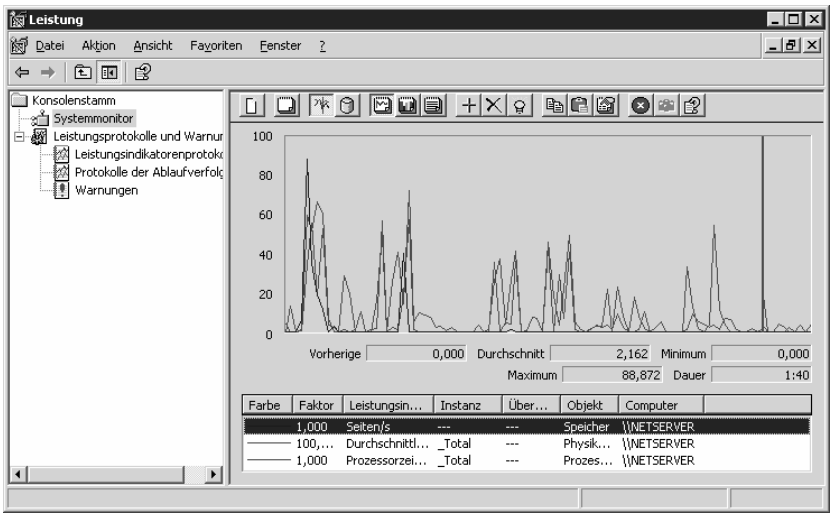


Abbildung 19: Leistungsmonitor

Da die Überwachungsmöglichkeiten im Systemmonitor, im Leistungsindikatorenprotokoll und in den Warnungen identisch sind, wird ein entsprechender Überblick der zur Überwachung zur Verfügung stehenden Objekte nachfolgend nur einmal gegeben.

Während die eigentliche Funktion des Leistungsmonitors mehr der Performanceanalyse und Optimierung sowie dem Auffinden von Flaschenhälsen dient, lassen sich hier natürlich in bestimmten Fällen auch Informationen auffinden, die für forensische Untersuchungen von Belang sind. Jedoch sind die Einstellmöglichkeiten und vor allem die daraus möglichen Kombinationen schier endlos. Für die Überwachung stehen zirka 30 Objekte zur Verfügung. Beispiele für Objekte sind Prozessor, Speicher und physikalischer Datenträger oder auch das Internet Protokoll IPv4. Je nach installierten Komponenten stehen hier eventuell zusätzliche Objekte zur Verfügung. Die Objekte bestehen wiederum aus ungefähr 5-20 einzelnen Indikatoren, die die einzelnen zu protokollierenden Aspekte darstellen.

So besitzt das Objekt über das Internet Protokolls IPv4 siebzehn einzelne Indikatoren, bei denen außer typischen Punkten wie „Datagramme empfangen/s“ und „Datagramme gesendet/s“ auch sehr spezielle Aufzeichnungsmöglichkeiten wie „Fragment-Zusammensetzungsfehler“ oder „Erhaltene Datagramme, Vorspannfehler“ gegeben sind.

So kann die Protokollierung in Spezialfällen mit günstig gewählten Protokollierungseinstellungen zwar ergiebig sein. Jedoch würde es über den Umfang der Arbeit weit hinausgehen, hier entsprechende Schemata für die Aufklärung der verschiedensten Fälle festzulegen. Hier müssten nicht nur die zirka 300 (30 Objekte á ~10 Indikatoren) einzelnen Indikatoren, sondern auch noch ihre verschiedenen Kombinationen berücksichtigt werden, da sich teilweise erst damit verwertbare Hinweise ergeben. Dazu müssten dann im Fall einer Aufzeichnung, die nachfolgend beschrieben wird, auch noch jeweils passende Aufzeichnungsintervalle und eventuelle Warnungen und Aktionen festgelegt werden.

Da der Systemmonitor zur Onlineanzeige sehr einfach zu bedienen ist und die direkten Auswirkungen sofort ersichtlich sind, wird auf eine Beschreibung der Bedienung hier verzichtet. Vielmehr wird nun ausschnittsweise beschrieben, welche Optionen beim Anlegen einer neuen Einstellung für die Protokolle und Warnungen (über Kontextmenü) wählbar sind.

Leistungsindikatorenprotokolle:

Abbildung 20: Leistungsindikatorenprotokoll

Außer den weiter unten beschriebenen protokollierbaren Indikatoren lässt sich hier das Zeitintervall für die Aufzeichnung bestimmen (Abbildung 20). Unter der Registerkarte „Protokolldateien“ ist aus den Formaten Text (Komma getrennt oder Tabulator getrennt), Binär oder SQL-Datenbank auszuwählen. Unter „Zeitplan“ lässt sich auswählen, ob Anfang und Ende der Aufzeichnung manuell ausgelöst werden müssen oder vorbestimmte Zeiten verwendet werden.

Über die Schaltfläche „Objekte hinzufügen“ stehen hier die oben bereits teilweise beschriebenen Objekte zur Wahl der Aufzeichnung zur Verfügung (Abbildung 21). Über „Leistungsindikatoren hinzufügen“ ist noch eine genauere Auswahl der Teilaspekte eines Objekts möglich (Abbildung 22).

Eine Auswertung kann bei aufgezeichneten Textdateien mit beliebigen Texteditoren und bei Verwendung einer Datenbank mit den entsprechenden Abfrageprogrammen erfolgen, da die Informationen damit in diesen beiden Fällen im Klartext angezeigt werden. Für die Auswertung der im Format Binär angelegten Aufzeichnungen kann eine Umwandlung in die Textformate über den Befehl relog.exe erfolgen. So erzeugt z.B. der Aufruf relog.exe #Binärdatei# -f csv –o #Textdatei# eine neue Datei, in der die Werte durch Kommas getrennt sind und sich

mit dem Texteditor im Klartext anzeigen lassen. Eine genaue Beschreibung zur Bedienung gibt es durch Aufruf von relog.exe /?.

Abbildung 21: Objekte hinzufügen

Abbildung 22: Leistungsindikatoren hinzufügen

Eine Liste von Leistungsobjekten und deren Indikatoren, allerdings mit englischen Bezeichnungen, findet sich unter [Tech04e].

Protokolle der Ablaufverfolgung

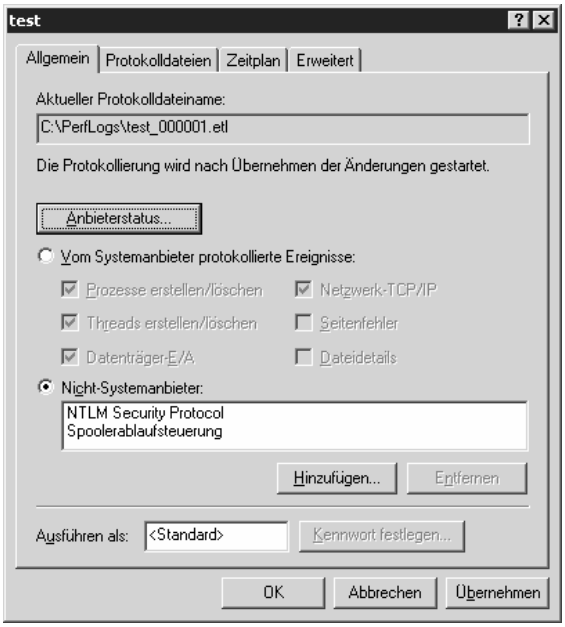


Abbildung 23: Protokoll der Ablaufverfolgung

Die Verfahrensweise für „Protokolle der Ablaufverfolgung“ unterscheidet sich deutlich von der für Leistungsindikatorprotokolle (Abbildung 23). Während beim Letzteren der Dienst Daten vom System abhängig vom eingestellten Aktualisierungsintervall erhält, werden bei der Ablaufverfolgung Daten beim Eintreten eines bestimmten Ereignisses aufgezeichnet. Folglich gibt es auch keine Eingabemöglichkeit für ein Aktualisierungsintervall. Darüber hinaus stehen hier wesentlich weniger überwachbare Ereignisse zur Verfügung. Wie man der Abbildung entnehmen kann, bieten sich die sechs vom Systemanbieter protokollierten Ereignisse und abhängig von den installieren Komponenten einige weitere Protokolliermöglichkeiten von Nicht-Systemanbietern. Nicht vergessen werden darf hier, ein Konto mit Administratorenrechten im Eingabefeld „Ausführen als“ in der Registerkarte „Allge-

mein“ einzutragen, da die Erzeugung des Protokolls sonst nicht gestartet werden kann. Hier wird immer erst im Binärformat aufgezeichnet; mit dem mitgelieferten Programm tracerpt.exe ist es jedoch möglich, aus diesen Dateien normale Textdateien (Standard: dumpfile.csv) zu erzeugen und auch gleich eine Zusammenfassung zu erhalten (Standard: summary.txt). Eine Beschreibung zur Bedienung gibt es durch Aufruf von tracerpt.exe /?.

Warnungen

Es stehen die gleichen Überwachungsmöglichkeiten wie bei Leistungsindikatoren zur Verfügung (Abbildung 24). Außer dem obligatorischen Zeitplan, kann gewählt werden, was bei Erreichen des Limits zu tun ist (Abbildung 25). So kann ein Eintrag im Ereignisprotokoll für Anwendungen erzeugt werden, eine Nachricht über das Netzwerk versandt werden, ab jetzt die Aufzeichnung eines Leistungsprotokolls veranlasst werden oder ein beliebiges Programm ausgeführt werden.

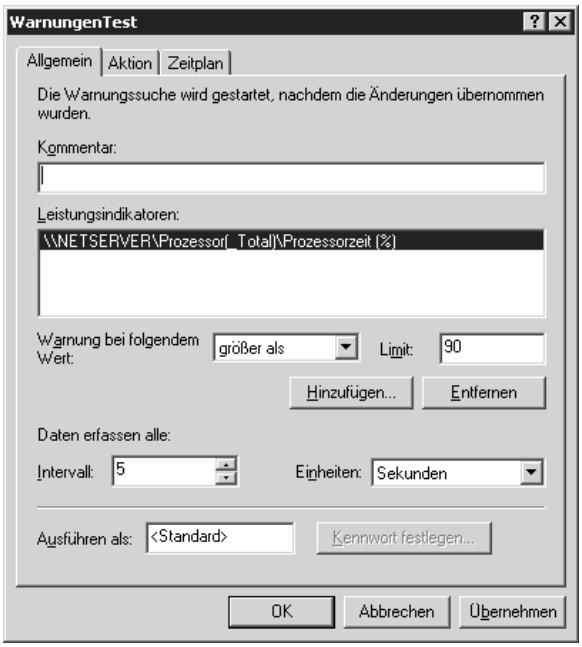


Abbildung 24: Eigenschaften von Warnungen I

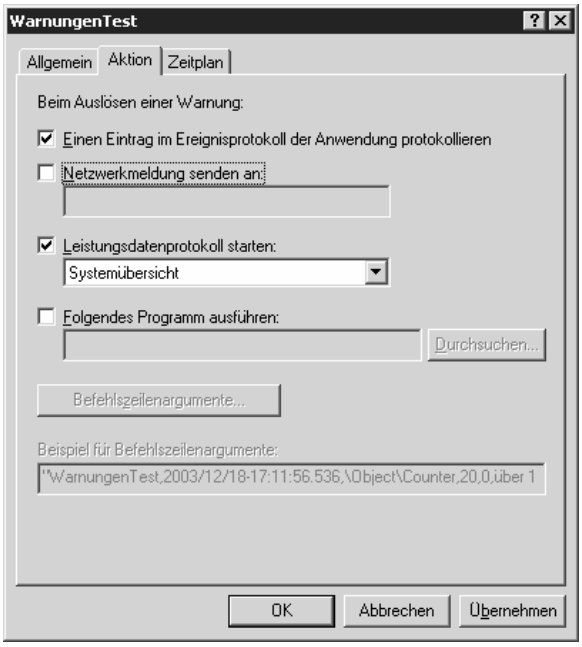


Abbildung 25: Eigenschaften von Warnungen II

7.2 Informationen für die Auswertung ausgewählter Quellen

Für verschiedene Quellen sind mitunter zu einzelnen Aspekten nähere nichttriviale Informationen nötig, die aufgrund des hohen Platzbedarfs oder zur Vermeidung von Wiederholungen nicht auf den Quellenblättern untergebracht werden.

7.2.1 Security Identifier (SID)

Die Vergabe und Ausübung von Rechten für Benutzer und Benutzergruppen erfolgt betriebsystemintern nach einer Identifikation auf der Grundlage von einem speziellen Security Identifier (SID) und nicht ihrem Benutzer- oder Gruppennamen.

So wird z.B. beim Anlegen eines Benutzers ein neuer SID kreiert und dann für die Vergabe und Überprüfung von Benutzerrechten verwendet. Dies hat weit reichende Folgen. Wenn z.B. für einen Benutzer Berechtigungen (z.B. auf Ordner) vergeben werden und dieser später gelöscht wird, kann auch durch nochmaliges Anlegen eines neuen Benutzers mit gleich lautendem Benutzernamen dieser keinen Zugriff auf den Ordner erlangen, da er nun eine neuen SID besitzt.

Es gibt sowohl Benutzer als auch Gruppen die auf allen Installationen des Betriebsystems vorhanden sind, weil es sich um interne vom System verwendete Benutzer bzw. Gruppen handelt. Eine Liste dieser findet sich unter [Tech04f].

Ein konkretes Beispiel für eine SID eines Benutzers ist S-1-5-21-1985976947-4043385027-431252277-1004. Nachfolgend werden die einzelnen Bestandteile erklärt.

Allgemein ist eine SID von der Form S-x-y, S-x-y-z oder S-1-5-21-a-b-c-d, wobei x, y, z, a, b, c, d verschieden lange Nummernblöcke darstellen können.

Für normale Benutzerkonten kommt nur das dritte angegebene Schema in Frage. Man erkennt diese am Beginn mit S-1-5-21. Die weiteren Nummern a, b, c sind 9 oder 10 Zeichen lang und bezeichnen den einzelnen Computer oder die Domäne. Dieser Wert wird bei der Installation zufällig erzeugt und stimmt alle Benutzer eines Computers oder einer Domäne überein. Am Wert von d kann man weiterhin schon Rückschlüsse auf den Benutzer machen.

Im Falle eines Wertes von 500 handelt es sich um den Administrator, dessen Benutzerkonto automatisch erstellt wird. Weitere über die Benutzerverwaltung angelegte Benutzer werden aufsteigende Werte angefangen bei 1000 und folgende vergeben. Insofern lässt sich an der SID erkennen, dass ein Benutzerkonto mit kleinerer Nummer zeitlich vor einem Konto mit größerer Nummer eingerichtet worden ist.

Für einen bestimmten Benutzernamen kann dessen SID mit dem Programm user2sid oder in der umgekehrten Richtung mit sid2user (beide [Rudn98]) aus der Benutzerdatenbank auf dem Computer abgefragt werden.

7.2.2 Global Unique Identifier (GUID)

Im Active Directory wird die Identität jedes Objektes durch eine global eindeutige Kennung (GUID) repräsentiert. Dies ist eine 128 Bit lange Nummer, die bei der Erstellung des Objektes u. a. aus der aktuellen Zeit und der MAC-Adresse des erzeugenden Systems erstellt wird.

Während die SID nur innerhalb der Domäne in jedem Fall eindeutig ist, ist die GUID in allen Domänen eindeutig.

Bei der Anzeige wird die GUID von Windows mit geschweiften Klammern und einigen Bindestrichen dargestellt, z.B. {BF967ABA-0DE6-11D0-A285-00AA003049E2}.

7.2.3 Namen von wichtigen Prozessen

Um aus der Auflistung der laufenden Prozesse mit der Quelle „Aktuell laufende Prozesse“ richtige Aussagen treffen zu können, ist es nötig sowohl die meisten Standardprozessnamen zu kennen als auch über deren Startverhalten Bescheid zu wissen.

Angezeigter Name	Prozessinformationen	Standardmäßig gestartet?
Cidaemon.exe	Gehört zum Indexdienst	nur wenn Index-dienst gestartet
Cisvc.exe	Gehört zum Indexdienst	nur wenn Index-dienst gestartet
cmd.exe	Eingabeaufforderung In Zusammenhand mit dem Aufruf von Tasklist wird ja eine Shell gestartet. Somit kommt dann auch die Eingabeaufforderung in der Ausgabe vor.	Nein
Csrss.exe	**C**lient/**S**erver **R**untime **S**erver **S**ubsystem. Fenster und Grafikausgabe	Ja
Dfssvc	Distributed File System.	Ja
Explorer.exe	Der Windows Explorer ist nicht nur das grafische Werkzeug zur Dateiverwaltung sondern auch für das Startmenü und die Taskleiste zuständig. Deswegen läuft dieser Prozess immer, auch wenn kein eigenes Explorer-Fenster angezeigt wird.	Ja
Inetinfo.exe	Internet Information Server: Der mitgelieferte Webserver.	Wenn IIS gestartet
Leerlaufprozess/System Idle Prozess	Leerlaufprozess der nichts tut	Ja
Lsass.exe	Sicherheitsdienst (**L**ocal **S**ecurity **A**uthority **S**ubsystem) zuständig für Anmeldung und Berechtigungen	Ja

Msdtc.exe	**M**icro**s**oft **D**istributed **T**ransaction **C**oordinator	Wenn Internet Information Server installiert
Scvhost.exe	Dieses Prozessname wird verwendet wenn Prozesse aus DLL-Dateien gestartet werden. Mit dem Befehl Tasklist /svc lassen sich die dahinterliegenden Dienste anzeigen, wobei sich hinter einer Instanz von svchost mehrere verschiedene Dienste verbergen können	Ja, mehrere Instanzen
Smss.exe	Session Manager	Ja
Spoolsv.exe	Für das Drucken zuständig	Nur wenn Drucker installiert
System	Systemprozess Kernel	Ja
Tasklist.exe	Der Shell-Befehl um die laufenden Prozesse anzuzeigen. Wenn man mit ihm die Prozesse ausgibt taucht er selber auch mit auf.	Nein
Taskmgr.exe	Windows Task-Manager. Wenn man über diesen die laufenden Prozesse anzeigt taucht dieser eben auch in der Liste auf.	Nein
Winlogon.exe	Benutzeranmeldung	Ja
Wmiprvse.exe	WMI Provider Service	Ja
Wuauclt.exe	Client für automatische Updates Automatische Updates sind zwar standardmäßig aktiviert. Allerdings läuft deswegen dieser Prozess noch nicht dauerhaft. Er bleibt nur gestartet, wenn sich Updates finden und er diese zur Installation anbietet.	Nein

Zu bedenken ist jedoch, dass auf vielen Systemen oft standardmäßig kleine Hilfsprogramme (z.B. Grafikkartenutility) gestartet werden, die dann in der Taskleiste links neben der Uhrzeitanzeige residieren. Es kann also völlig normal sein, wenn ohne offene Programmfenster weitere Prozesse aufgelistet werden. Dies darf somit nicht als automatischer Hinweis auf einen Trojaner oder ähnliches gewertet werden.

Um bei den eigenen Systemen den Überblick zu behalten, empfiehlt es sich daher den Normalzustand mit allen gestarteten Programmen zu notieren, um spätere Abweichungen feststellen zu können.

Das Vorgehen zur Auswertung findet sich auf dem Quellenblatt „Aktuell laufende Prozesse“.

Weitere Namen von Anwendungsprogrammen zu nennen, würde hier zu weit führen. Es gibt jedoch im Internet Übersichten, wo viele bekannte Programme eingetragen sind. Solche Übersichten findet man beispielsweise unter den Adressen [Rege03] und [Answ03].

Allerdings darf man sich nicht täuschen lassen und den Namen blind vertrauen, da von den Programmen einfach der Dateiname angezeigt wird, welcher sich durch simples Umbenennen ändern lässt.

Auch wäre es möglich gerade die standardmäßig laufenden Prozesse durch manipuliere Versionen mit extra Funktionalität zu ersetzen, so das kein weiterer Prozess angezeigt wird.

7.3 Konfiguration des Testsystems

Falls einige Quellen sich nicht wie beschrieben verhalten, kann das außer an möglichen Fehlern in dieser Beschreibung auch auf andere Einstellungen bzw. unterschiedliche Systemdateien zurückzuführen sein.

Hier finden sich alle wichtigen Abweichungen, die an der Standardinstallation vorgenommen worden sind. Insofern ist der Grund für ein abweichendes Verhalten eventuell dadurch zu finden, dass die verschiedenen Systemkonfigurationen verglichen werden.

Ausgangspunkt ist die Neuinstallation der deutschen Version von Windows 2003 Server auf einer primären NTFS Partition.

Treiber:

Der Rechner selbst ist ein Pentium II System mit Intel BX- Chipsatz. Erforderliche Treiber kommen alle von Microsoft selbst (Installations-CD oder von der Windows Update Internetseite) Zu nennen sind hierbei der Grafikkartentreiber STB Velocity 128, der Treiber für eine Netzwerkkarte mit Realtek RTL8139 Chip und der Treiber für die Soundkarte mit Aureal Vortex 8820 Chip. Als Drucker ist ein HP OfficeJet G55 auch über den von Windows bereitgestellten Treiber installiert.

Sonstige Angaben über installierte Treiber zu Standardkomponenten wie paralleler und serieller Schnittstelle, USB-Controller, etc würde zu weit führen.

Wichtige Updates:

Es sind alle bis 27.10.2003 verfügbaren wichtigen Updates mit der „Windows Update“ Funktion aus dem Internet installiert. Um für die weiteren Untersuchungen mit einer gleich bleibenden Konfiguration zu arbeiten, sind keine neueren Updates mehr installiert.

KB822925

KB823559

KB824105

KB824146

KB819696

KB828750

WM819636

WM828086

Einstellungen:

Die Überwachungsrichtlinien sind für alle Kategorien auf die Optionen „Erfolgreich“ und „Fehlgeschlagen“ gesetzt.

Programminstallationen:

Über die Serververwaltung sind folgende Serverfunktionen aktiviert:

Dateiserver

Druckserver

Anwendungsserver (IIS, ASP.Net)

Terminalserver

Nach den abgeschlossenen Tests zu der lokalen Benutzerverwaltung ist folgende Funktionalität für weitere Untersuchungen hinzugekommen:

Domänencontroller (Active Directory)

Von der Windows CD sind installiert:

Indexdienst

Netzwerkwerkmonitorprogramme (Unterkomponente von Verwaltungs- und Überwachungsprogramme)

Von anderen Herstellern:

ActiveState – ActivePerl – Version 5.8.0 Build 806

Adobe - Acrobat Reader - Version 5.0.1.27.03.2001

Elcomsoft - Advanced Registry Tracer - Version 1.67 SR2

Scooter Software – Beyond Compare - Version 2.0.2

Zusätzlich sind zwar auch noch andere Programme wie z.B. Filemon oder Regmon verwendet, die aber keine Installation erfordern und das System nicht verändern.

C Literaturverzeichnis

[Answ03] AnswearsThatWork.com: Task List Programms, AnswearsThatWork.com, 2003, http://www.answersthatwork.com/Tasklist_pages/tasklist.htm

[Baum02] Baumgarten, U.: Systemarchitekur Betriebsysteme, Technische Universität München, Institut für Informatik, München, 2002, http://wwwspies.informatik.tu-muenchen.de/lehre/vorlesung/SS02/babs

[Baum02a] Baumgarten, U.: Betriebssysteme, Technische Universität München, Institut für Informatik, München, 2002, http://wwwspies.informatik.tu-muenchen.de/lehre/vorlesung/SS02/babs/BS-Kapitel1.pdf

[Bosw01] Boswell, W.: Insider Windows 2000 Server, Markt+Technik Verlag, München, 2001, ISBN: 3-8272-5686-0

[Bosw03] Boswell, W.: Understanding Active Directory Services, 10.10.2003, http://www.informit.com/isapi/product_id~%7B2E8FF243-558D-41CE-BCE0-FCF85CBF4155%7D/element_id~%7BC328BE5D-F8F8-4B93-9D4C-43D0CD26A194%7D/st~%7B6EB673C6-2B46-498B-A653-803F5FC3AA6E%7D/content/articlex.asp

[BrAn01] Bryson C. and M. Anderson: Shadow Data - The Fifth Dimension of Data Security Risk, New Technologies Inc., 15.08.2001, http://www.forensics-intl.com/art15.html

[Broc88] Brockhaus: Brockhaus-Enzyklopädie, F.A. Brockhaus GmbH, Mannheim, 19. Auflage, 1988, ISBN für das Gesamtwerk: 3-7653-1100-6

[Bund02] Bundeskriminalamt: Bundeslagebild IuK-Kriminalität 2002, Bundeskriminalamt, 03.11.2003, http://www.bka.de/lageberichte/iuk/bundeslagebild_IuK_Kriminalitaet_2002.pdf

[Bund02a] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzhandbuch, Bundesamt für Sicherheit in der Informationstechnik, Mai 2002, http://www.bsi.de/gshb/deutsch/menue.htm

[Bund02b] Bundesamt für Sicherheit in der Informationstechnik, Leitfaden IT-Sicherheit, Bundesamt für Sicherheit in der Informationstechnik, 2002, http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf

[Carr04] Carr, J.: Child abuse, child pornography and the internet – Executive Summary, NCH -National Children's Home, Januar 2004, http://www.nchafc.org.uk/downloads/children_internet_report_summ.pdf

[Digi03] Digital Forensic Research Workshop, DFRWS Home Page, Digital Forensic Research Workshop, 2003, http://www.dfrws.org/

[Dori03] Dorian Software Creations: Event Management Software - Dorian Software Provides Event Log Management Software Solutions, Dorian Software Creations, Atlanta, 2003, http://www.doriansoft.com

[Curr01] Curran, J.: Little Endian vs. Big Endian, 05.04.2001, http://www.noveltheory.com/TechPapers/endian.asp

[Elco03] Elcomsoft: Advanced Registry Tracer, 2003, http://www.elcomsoft.com/art.html

[FaVe02] Farmer D. und W. Venema: Computer Forensics Column, 2002, http://www.porcupine.org/forensics/column.html

[Gerb03] Gerbier, E.: AFICK (another file integrity checker), 10.12.2003, http://afick.sourceforge.net/

[Gesc03] Geschonneck, A.: computer-forensic.org: Die Website zum Buch 'Computer Forensik', 2003, http://computer-forensik.org/

[Gtsl02] GTS Learning: Windows 2000 Architecture, findTutorials.com, 28.03.2002, http://tutorials.findtutorials.com/read/query/windows 2000 architectur/id/379

[Guid04] Guidance Software, Encase Forensic Edition, Guidance Software, Pasadena http://www.guidancesoftware.com/products/EnCaseForensic/index.shtm

[HaBe96] Hallam-Baker P. and B. Behlendorf: Extended Log File Format, W3C, 23.03.1996, http://www.w3.org/TR/WD-logfile

[Hart01] Hartmann, M.: Windows XP Architektur, IDG Interactive GmbH, Redaktion tecChannel.de, München, 27.09.2001, http://www.tecchannel.de/betriebssysteme/602/14.html

[Heis03] Heise Online: Computerkriminalität geht nur scheinbar zurück, c´t, Heise Online, Hannover, 21.05.03, http://www.heise.de/newsticker/data/anm-21.05.03-000/

[Hone03] Honeynet Project: The Honeynet Project Whitepapers, Honeynet Project, 2003, http://www.honeynet.org/papers/index.html

[Inte03] International Business Machines: Log File Formats, International Business Machines, 2003, http://as400bks.rochester.ibm.com/tividd/td/ITWSA/ITWSA_info45/en_US/HTML/guide/c-logs.html#ncsa

[Iwat02] Iwata, E.: Enron case could be largest corporate investigation, USA Today, Gannet Co. Inc., 18.02.2002, http://www.usatoday.com/tech/news/2002/02/19/detectives.htm

[Inte03] International Journal of Digital Evidence, Archives, International Journal of Digital Evidence, 2003, http://www.ijde.org/archives_home.html

[Libb03] Libbenaga, J.: Why Longhorn is going to be different, The Register, Situation Publishing, 28.10.2003, http://www.theregister.co.uk/content/archive/33620.html

[Leep03] Lee, P.: General Paul Lee Project - Soft - Registry Viewer, 2003, http://paullee.ru/regstry.html

[Lyma03] Lyman, J.: New WinFS File System Key to Microsoft's Longhorn, TechNewsWorld, ECT News Network, Encino, 14.10.2003, http://www.technewsworld.com/perl/story/31856.html

[Micr96] Microsoft: Microsoft Index Server: Kataloge, Microsoft, 1996, http://www.ms-net.uni-kiel.de/suchen/help/cathlp.htm

[Micr00] Microsoft: Microsoft IIS Log File Format, Microsoft, 28.02.2000, http://www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/moc07_15.htm

[Micr00a] Microsoft: Struktur der Registrierung, Microsoft, 2000, http://www.microsoft.com/windows2000/de/server/help/sag_ntregconcepts_mply.htm

[Micr03] Microsoft: IIS Log File Naming Syntax, Microsoft, 20.05.2003, http://support.microsoft.com/default.aspx?scid=kb;en-us;242898

[MiPr00] Microsoft Press Deutschland: Microsoft Windows 2000 Server, Microsoft Press Deutschland, 2000, ISBN: 3-86063-278-7

[Msdn04] MSDN Microsoft Developer Network: MSDN Home Page, MSDN Microsoft Developer Network, 2004, http://msdn.microsoft.com

[Msdn04a] MSDN Microsoft Developer Network: WinFS, MSDN Microsoft Developer Network, 2004, http://msdn.microsoft.com/Longhorn/understanding/pillars/WinFS/default.aspx

[Msdn04b] MSDN Microsoft Developer Network: EVENTLOGRECORD, MSDN Microsoft Developer Network, 2004, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/eventlogrecord_str.asp

[Nati03] National Security Agency: Security Recommendation Guides, National Security Agency, Maryland, 2003 http://www.nsa.gov/snac/

[NewT03] New Technologies Inc.: Forensic & Security Software, New Technologies Inc., 2003, http://www.forensics-intl.com/tools.html

[NewT03a] New Technologies Inc.: New Technologies, Inc. - Home Page, New Technologies Inc., 2003, http://www.forensics-intl.com

[NewT03b] New Technologies Inc.: Recent Articles from the Legal Press, New Technologies Inc., 2003, http://www.dataforensics.com/articles.html

[NewT03c] New Technologies Inc.: Computer Forensics In Action, New Technologies Inc., 2003, http://www.dataforensics.com/cases.html

[NewT03d] New Technologies Inc.: Unallocated File Space Defined, New Technologies Inc., 2003, http://www.forensics-intl.com/def8.html

[NewT03e] New Technologies Inc.: File Slack Defined, New Technologies Inc., 2003, http://www.forensics-intl.com/def6.html

[Phra03] Phrack: Phrack ...a Hacker magazine by the community, for the community...., Phrack, 2003, www.phrack.org

[Rege03] Reger, A.: Processes in Windows NT/2000/XP, 2003, http://www.reger24.de/prozesse.html

[Ripp03] Rippletech: LogCaster - Windows Server and Application Monitoring and Management, Rippletech, Conshohocken, 2003, http://www.rippletech.com/products/LogCaster/Prod_LC_Overview.htm

[Robi03] Robin Hood Software: Evidence Eliminator, Robin Hood Software Ltd., Nottingham, 2003, http://www.evidence-eliminator.com

[RuCo03] Russinovich, M. und B. Cogswell: Filemon for Windows, Sysinternals, 09.07.2003, http://www.sysinternals.com/ntw2k/source/filemon.shtml

[RuCo03a] Russinovich, M. und B. Cogswell: Regmon for Windows, Sysinternals, 13.06.2003, http://www.sysinternals.com/ntw2k/source/regmon.shtml

[RuCo04] Russinovich, M. und B. Cogswell: Process Explorer, Sysinternals, 09.01.2004, http://www.sysinternals.com/ntw2k/freeware/procexp.shtml

[Rudn98] Rudnyi, E.: user2sid and sid2user, 1998, http://www.chem.msu.su/~rudnyi/NT/

[Sage00] Sager, I. u.a.: Cyber Crime, Business Week, The McGraw-Hill Companies Inc., 21. Februar 2000, http://www.businessweek.com/2000/00_08/b3669001.htm

[Scoo03] Scooter Software Inc.: Beyond Compare, 2003, http://www.scootersoftware.com/moreinfo.php

[Tech04] Technet: Microsoft Technet: Home, Microsoft Technet, 2004, http://www.microsoft.com/technet/default.mspx

[Tech04a] Technet: Appendix E Security Event Messages, Microsoft Technet, 2004, http://www.microsoft.com/technet/prodtechnol/winxppro/reskit/prnf_msg_efgd.asp

[Tech04b] Technet: Logon Events, Microsoft Technet, 2004, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/prnf_msg_pfjj.asp

[Tech04c] Technet, Permissions for files and folders, Microsoft Technet, 2004, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/acl_special_permissions.asp

[Tech04d] Technet, Object Access Events, Microsoft Technet, 2004, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/prnf_msg_pyzc.asp

[Tech04e] Technet, Coutners by Object, Microsoft Technet, 2004, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/counters1_lkxw.asp

[Tech04f] Technet, Appendix J Well-Known Security Identifiers, Microsoft Technet, 2004, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/prnc_sid_cids.asp

[Tnts03] TNT Software: ELM Log Manager 3.1, TNT Software, Vancouver, 2003, http://www.tntsoftware.com/Products/ELM/

[Varc03] Varchaver, N.: The Perils of E-Mail, Fortune Magazine, 03.02.2002, http://www.fortune.com/fortune/technology/articles/0,15114,418678,00.html

[VCAM02] de Vel, O., M. Corney, A. Anderson und G. Mohay: Language and Gender Author Cohort Analysis of E-mail for Computer Forensics, Defence Science and Technology Organisation, Edinburgh und Faculty of Information Technology, Queensland University of Technology, Brisbane, 2003, http://www.dfrws.org/dfrws2002/papers/Papers/Olivier_DeVel.pdf

[Vogo02] Vogon International Limited: Irresponsible reporting or Privacy for the Paranoid?, Forensic Bulletin – The Smoking Gun, Volume 4, Issue 1, Vogon International Limited, Januar 2002, http://www.vogon-computer-evidence.com/forensic_bulletin-24/forensic_bulletin_24_2.htm

[Vogo03] Vogon International Limited: Forensic Bulletin Online, Vogon International Limited, 2003, http://www.vogon-international.com/computer%20evidence/bulletin-00.htm

[Xway03] X-Ways, X-Ways Trace: Browser-Logdatei und Papierkorb entschlüsselt..., X-Ways AG, Bünde, 28.10.2003, http://www.x-ways.net/trace/index-d.html

[Xway04] X-Ways, WinHex: Software für Computerforensik und Datenrettung, Hex-Editor und Disk-Editor, X-Ways AG, Bünde, 05.02.2004, http://www.x-ways.net/winhex/index-d.html