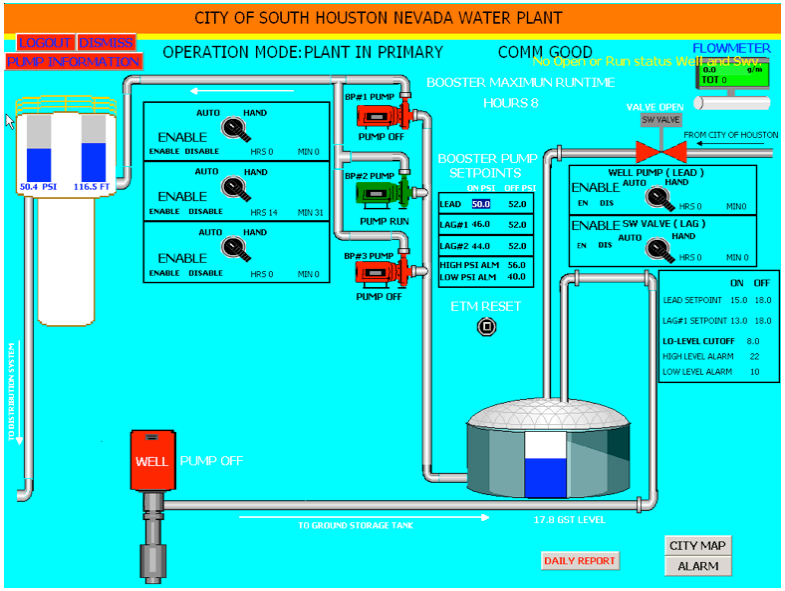
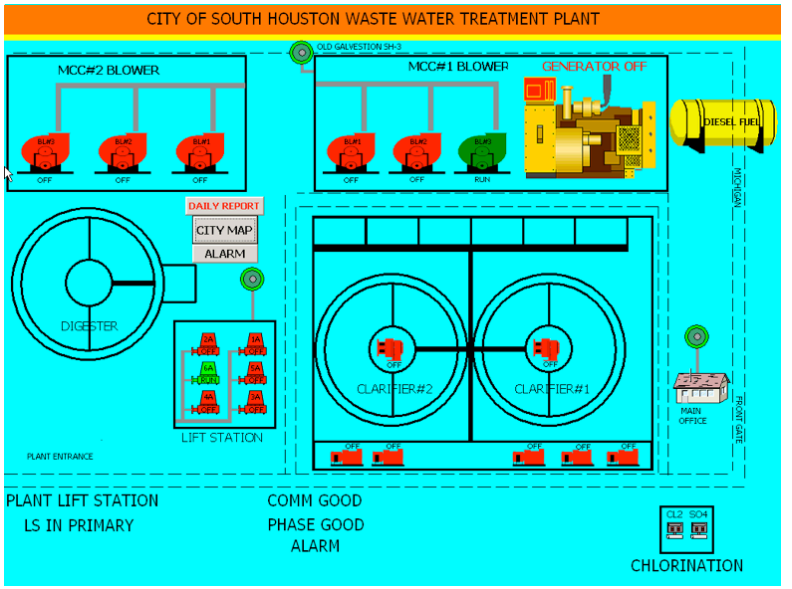
Angriff auf US-Wasserversorgung [November 2011]

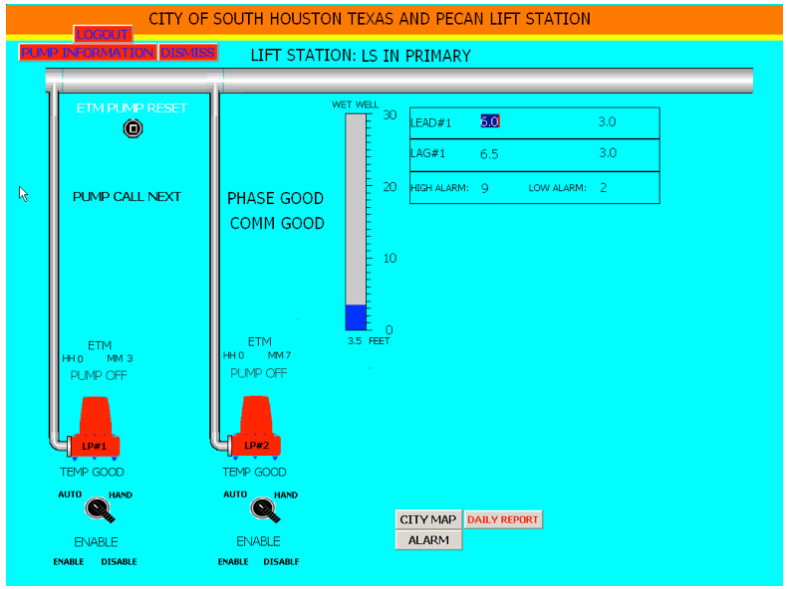
- Angreifer (mit IP-Adressen aus Russland) erlangen Zugang zu Steueranlagen eines amerikanischen Wasserversorgungs-unternehmens in Springfield, Illionois.
  - Vermutlich mit Default-Passwörtern des Anlagenherstellers
- Eine Wasserpumpe wird öfters schnell aus-/eingeschaltet und geht kaputt.
- Heimatschutzbehörde DHS spricht von „*minor glitches in remote access*“ und „*there is no credible corrobated data that indicates a risk to critical infrastructure entities*“.

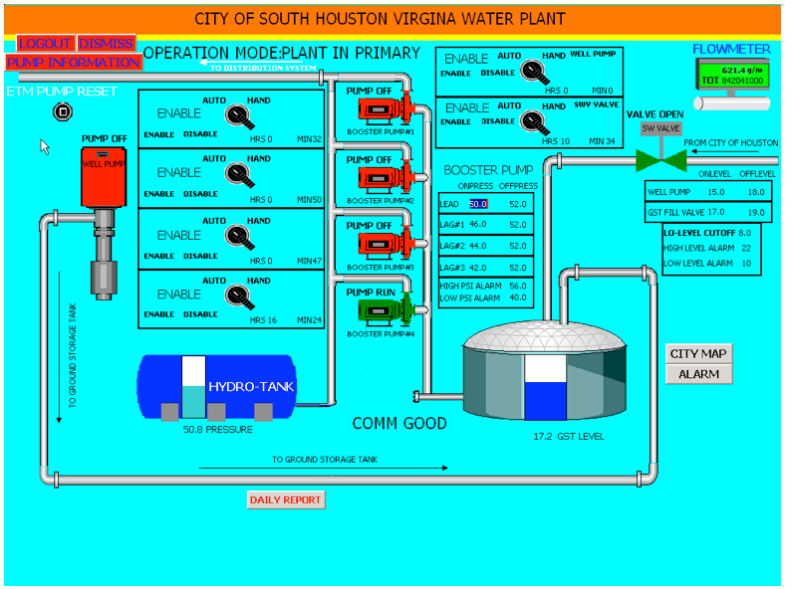
- Diese Aussage provoziert weiteren Angriff, der auf desolaten Zugriffsschutz und Probleme mit ans Internet angebundenen SCADA-Systemen hinweisen soll: `http://pastebin.com/Wx90LLum`

(Angebliche) Screenshots der Steueranlagensoftware







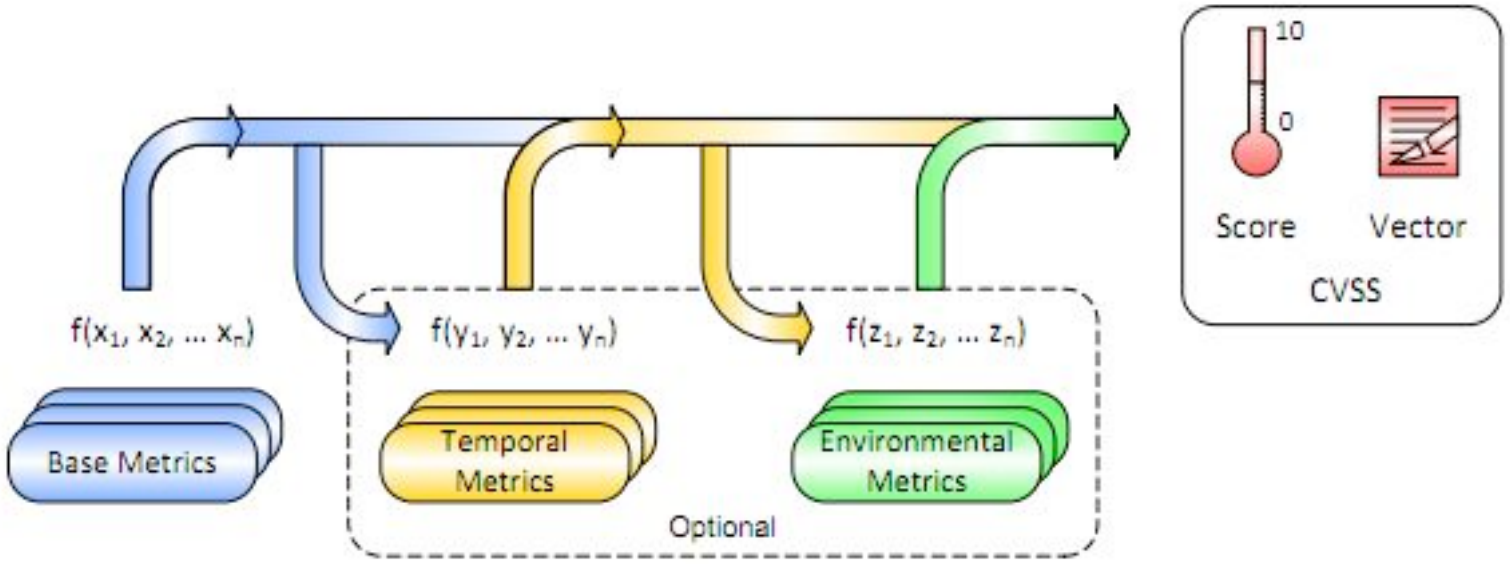


Microsoft Windows „Reference Counter Overflow“

- Fehler in der IP-Stack-Implementierung von Windows Vista, Windows 7 und Windows Server 2008.
- UDP-Pakete an einen Port, auf dem kein Dienst läuft, führen zu einem Integer-Overflow.
- Angreifer kann dadurch beliebigen eigenen Code ausführen.
- Vgl. „Ping of Death“ u. ähnl.
- Höchstwert 10.0 im CVSS2 Base Score
- http://technet.microsoft.com/en-us/security/bulletin/ms11-083

Common Vulnerability Scoring System v2 (CVSS2)

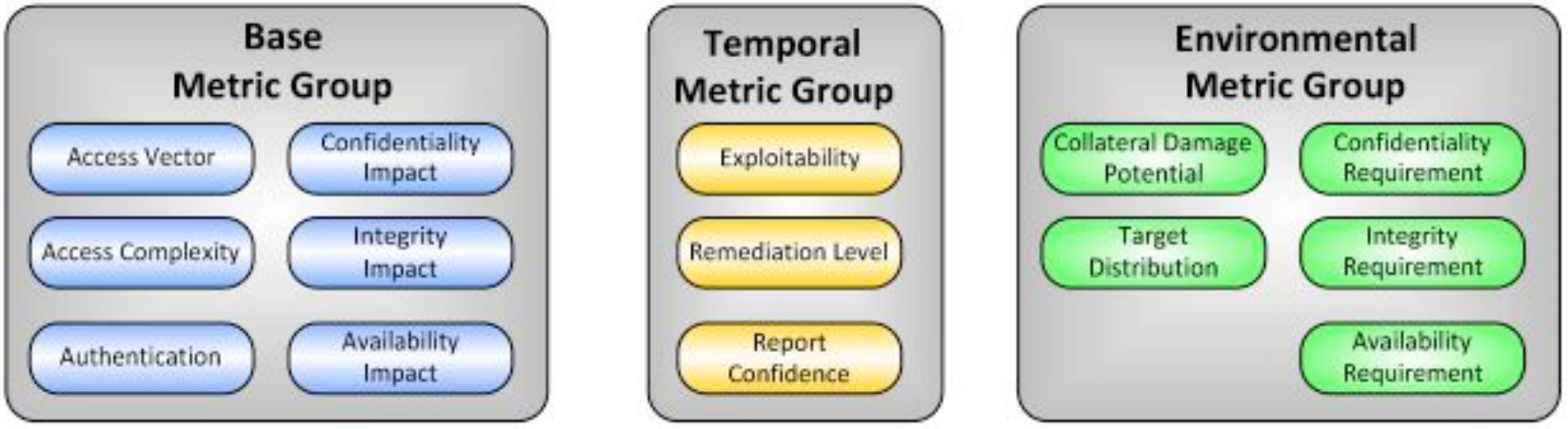
- Beurteilung der Kritikalität von bekannten Verwundbarkeiten; z.B. zur Priorisierung von Gegenmaßnahmen.
- Drei Gruppen von Bewertungskennzahlen:
  - Base Metrics: Grundlegende Eigenschaften der Verwundbarkeit
  - Temporal Metrics: Zeitabhängige Eigenschaften der Verwundbarkeit
  - Environmental Metrics: Szenarienspezifische Eigenschaften der Verwundb.



  - Base Metrics werden oft von Herstellern / Sicherheitsunternehmen veröffentlicht

CVSS2: Ausgewählte Einzelangaben

- Base Metrics:
  - Access Vector: Lokal, selbe Domäne oder über Netz?
  - Access Complexity: Trivial, anspruchsvoll, sehr schwierig?
  - Authentication: Muss sich der Angreifer authentifizieren, um den Angriff durchführen zu können? (Nein; einmalig; mehrfach)
- Temporal Metrics:
  - Exploitability: Kein Exploit bekannt, Proof of Concept, ..., Wurm?
  - Remediation Level: Offizieller Bugfix verfügbar, Workaround bekannt, ... ?



CVSS2: Beispiel „Reference Counter Overflow“

- Base Score gibt Maximalwert vor
- Hier: 10.0, da trivial remote und ohne Authentifizierung ausnutzbar, Maschine wird vollständig kompromittiert

- CVSS2 Score kann unter Einbezug von temporal und environmental metrics nur abnehmen, z.B.
  - sobald Patch verfügbar ist
  - falls eine Organisation keine anfälligen Windows-Maschinen im Einsatz hat