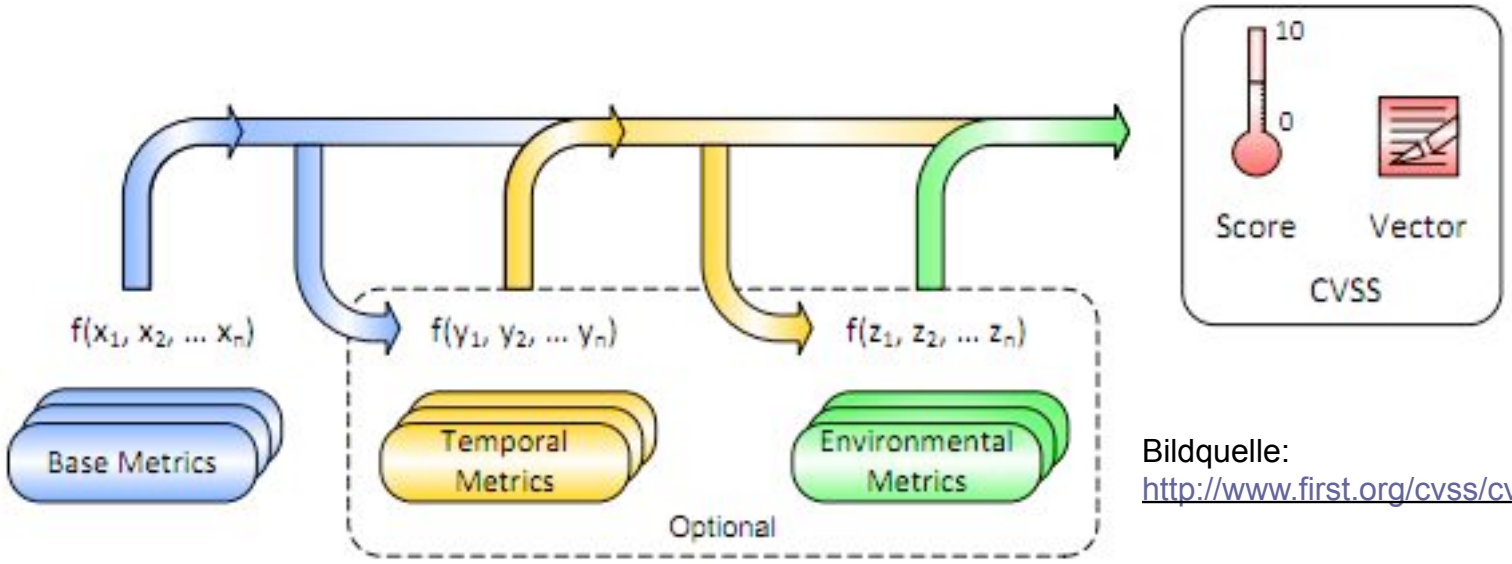
Common Vulnerability Scoring System v2 (CVSS2)

- 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.

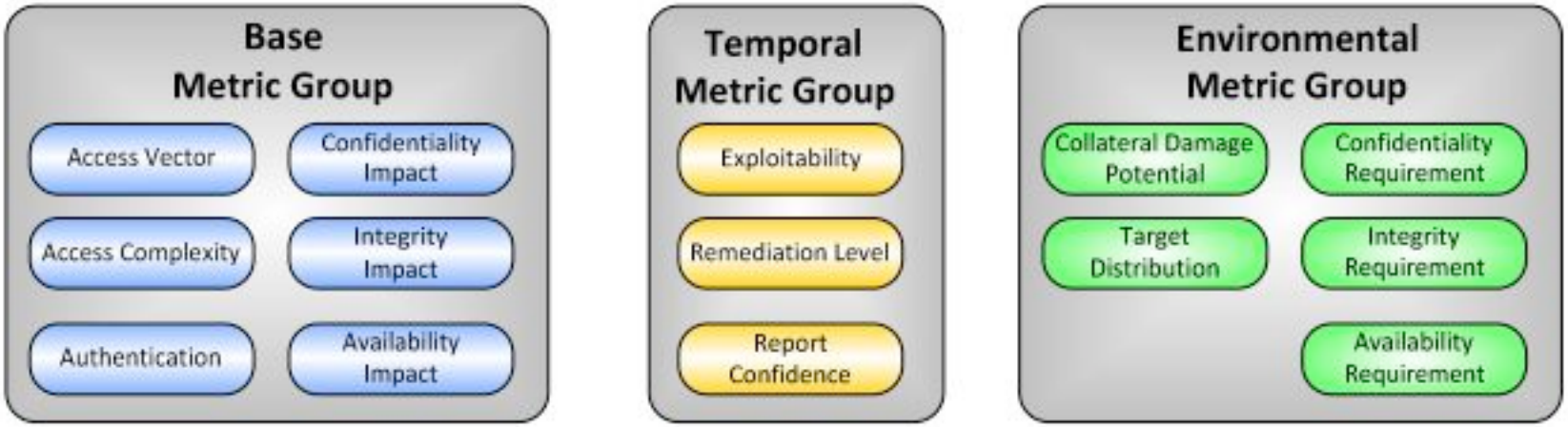


Bildquelle:
http://www.first.org/cvss/cvss-guide.html

  - 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, ... ?



Bildquelle: http://www.first.org/cvss/cvss-guide.html

Beispiel: Microsoft November-Patchday 2012

- Microsoft Security Bulletin MS 12-075 vom 13.11.2012:
  - Remote-Code-Ausführung bei Dokumenten und Webseiten mit eingebetteten “bösartigen” TrueType-Schriftarten.
  - Anwender muss Dokument/Webseite (nur/immerhin) öffnen
  - Fehler in Windows-Kernelmodus-Treiber, d.h. Kompromittierung impliziert Privilege Escalation
  - Betrifft Windows XP / 2003 / Vista / 7 / 2008 inkl. aktueller Service Packs
- CVSS2 Base Score: 10
  - Über Netz trivial ausnutzbar durch verfügbare “bösartige” TTFs
  - Angreifer muss nicht authentifiziert werden
  - Zielsystem wird komplett kompromittiert (= keinerlei CIA mehr)
- Environmental Score <= Temporal Score <= Base Score, z.B.:
  - Patchverfügbarkeit reduziert praktisches Risiko
  - Organisationen ohne Windows-Maschinen sind nicht anfällig

Einschub: Analyse von “zero-day” Exploits

- “Before we knew it - An empirical study of zero-day attacks in the real world”, Bilge/Dumitras, Oktober 2012
  http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf

- Wie lange werden Sicherheitslücken ausgenutzt, bevor sie allgemein bekannt (und beseitigt) werden?
  - Untersuchung für 11 Millionen Windows-PCs mit Symantec-Software
  - Dauer schwankt zwischen 19 Tagen und 30 Monaten
  - Durchschnitt liegt bei 312 Tagen (!)

- Wie wirkt sich die Veröffentlichung einer Sicherheitslücke aus?
  - Anzahl an Malware-Varianten steigt um das bis zu 85.000-fache
  - Anzahl beobachteter Angriffe steigt um das bis zu 100.000-fache

- Mehrwert und Seiteneffekte von “Full Disclosure”?