

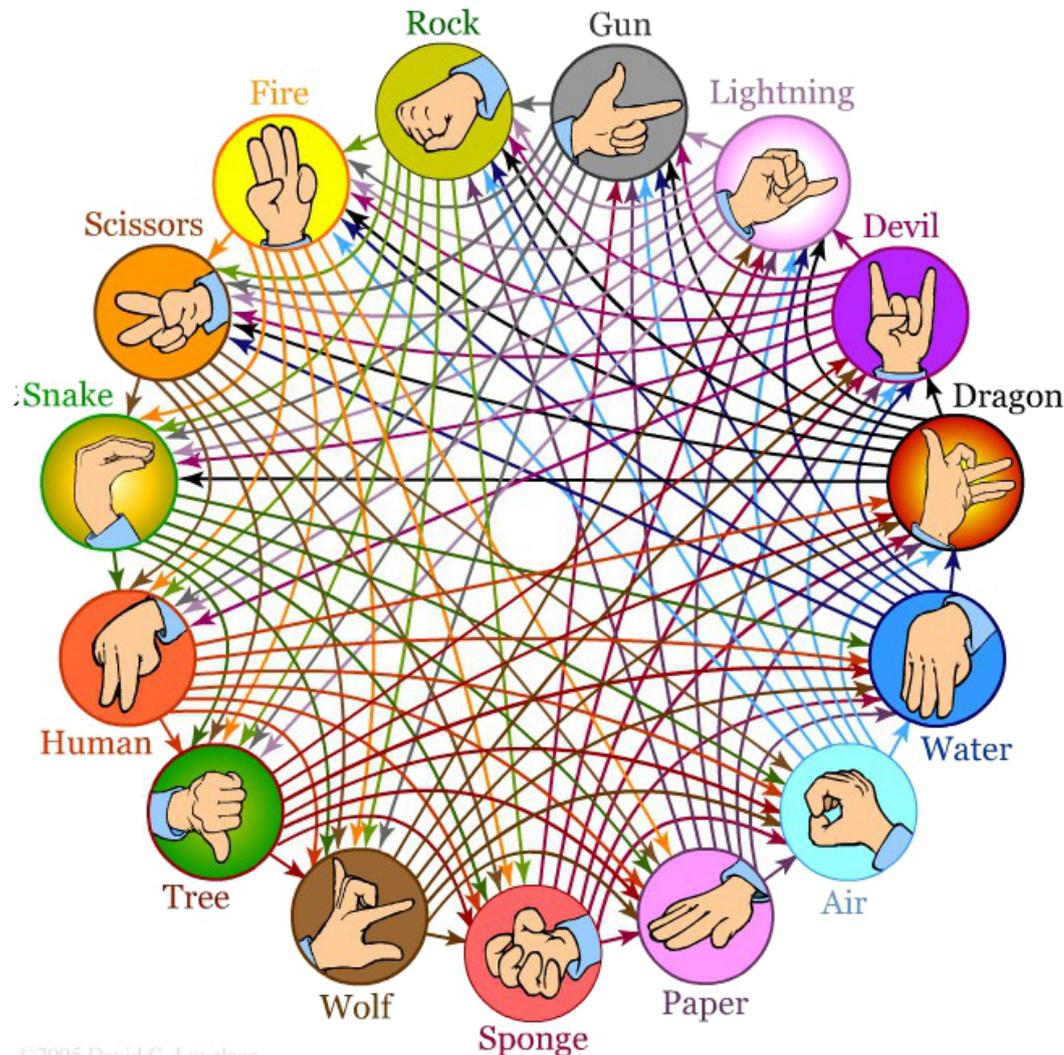


Common Vulnerability Scoring System (CVSS)

Die Kunst, Schwachstellen richtig einzuschätzen und zu bewerten

Hartmut Goebel
Diplom-Informatiker, CISSP, CSSLP
IT-Sicherheitsberater

Und nun die aktuellen Schwachstellen-Meldungen



- Extremely / Highly / Moderately / Less / Not Critical
- 1—5
- 0—99999999,99
- Low / Medium / High / Critical
- Remote Code Execution
- „wurmfähig“

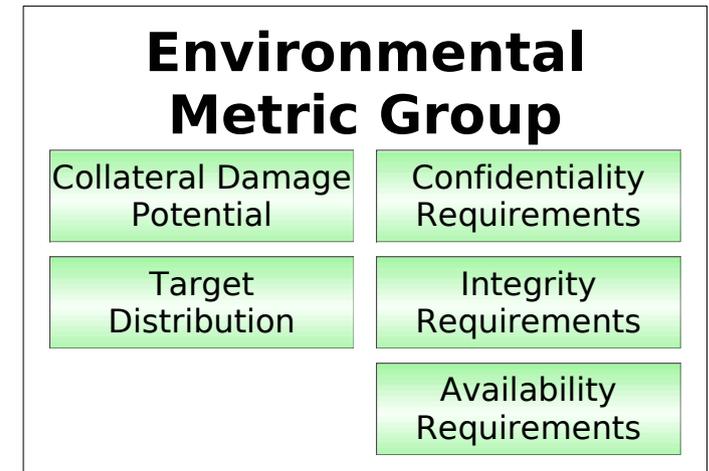
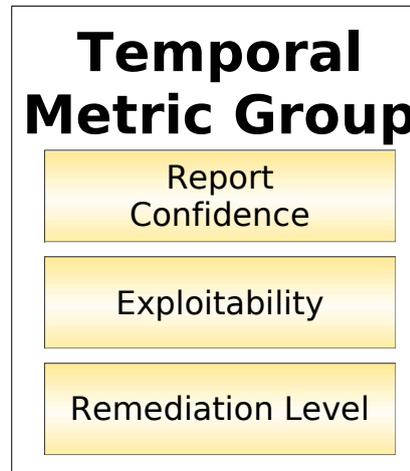
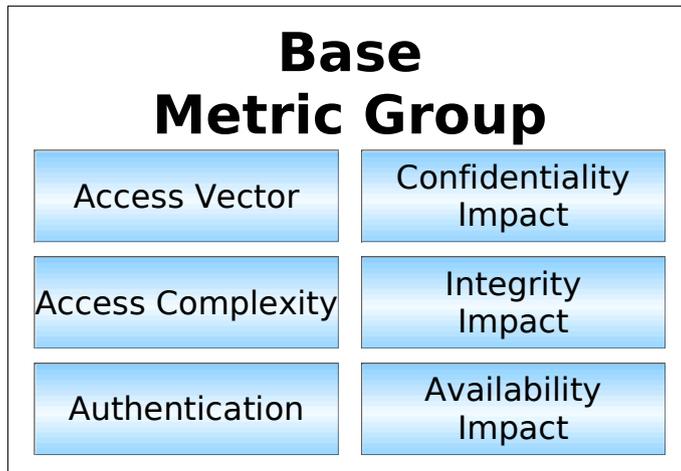
CVSS will einheitliche Bewertung schaffen

- eine handvoll Meßwerte und
- ein paar Formeln
- ergeben des Punktwert



- Endwerte 0—10
- Das ist alles

Die drei Abschnitte der CVSS-Berechnung



Berechnungstools (2)

cvss-calc

Datei Bearbeiten Ansicht Hilfe

Base Score Metrics

Exploitability Metrics

Access Vector: Network

Access Complexity: Medium

Authentication: None

Impact Metrics

Conf Impact: Complete

Integrity Impact: Complete

Avail Impact: Complete

Environmental Score Metrics

General Modifiers

Collateral Damage Potential: Not defined

Target Distribution: Not defined

Impact Subscore Modifiers

Confidentiality Requirement: Not defined

Integrity Requirement: Not defined

Availability Requirement: Not defined

Temporal Score Metrics

Exploitability: Not defined

Remediation Level: Not defined

Report Confidence: Not defined

Scoring Result

CVSS Base Score	9.3
Impact Subscore	10.0
Exploitability Subscore	8.6
CVSS Temporal Score	undefiniert
CVSS Environmental Score	undefiniert
Overall CVSS Score	9.3

 9.3

Update Scores

update automatically



www.goebel-consult.de/cvss

Was ist der *große* Nutzen?

- Egal aus welcher Quelle:
Schwachstellen werden vergleichbar
- Wechsel von Anbietern und Tools wird leichter
- Bewertungs-Policy wird *einmal* verhandelt

Beispiel einer Bewertungs-Policy

CVSS	Empfehlung der FIRST	Client	Server, Infrastruktur	Internet-Facing Server
9 – 10	Feueralarm	2 Tage	2 Tage	1 Tag
7 – 8	Binnen 7 Tagen	10 Tage	20 Tage	7 Tage
4 – 6	Next Patch Cycle	31 Tage	62 Tage	20 Tage
0 – 3	No Impact – wait for service pack			

Tipps aus der Praxis

- Bei Patchbewertung: „Remediation Level“ → „Not Defined“
- Immer mit dem Ergebnis des „temporal scores“ arbeiten
- Der "environmental score" wird pro Rechner berechnet.
- „environmental score“ vs. geschäftskritisch
- XML-Feeds

Zur Person: Hartmut Goebel



- Berater für IT-Security in komplexen Umgebungen
- Berät seit 2003 Banken, mittelständische Unternehmen und Konzerne beim Management von IT-Sicherheit

- Diplom-Informatiker, CISSP, CSSLP
- Fachautor und -Redner
- Monatliche Kolumne: www.cissp-gefluester.de

h.goebel@goebel-consult.de