

Anti-Virus in the Cloud

eicar working group 2, 17.11.2009

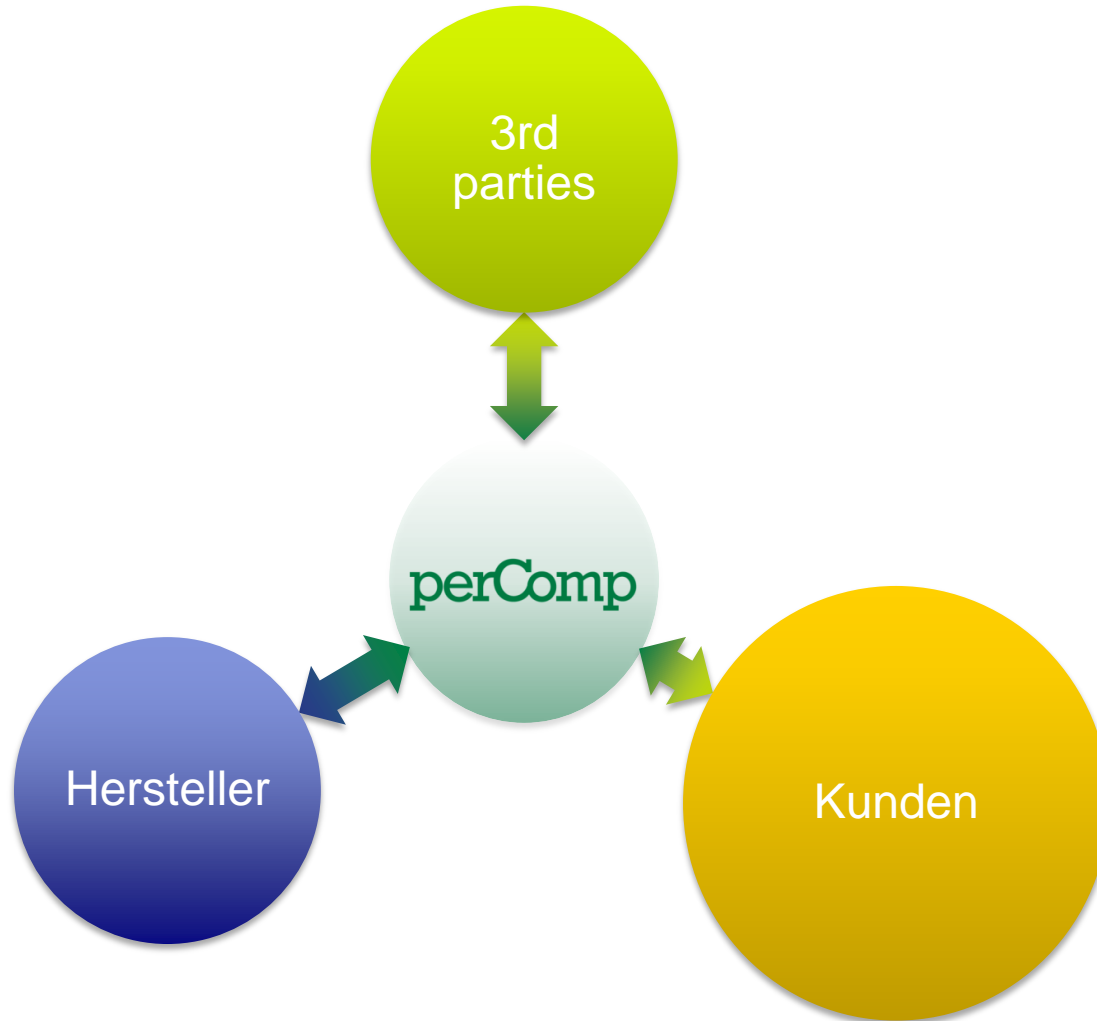
Tonke Hanebuth, perComp-Verlag

th[at]percomp.de www.percomp.de

Agenda

- perComp-Verlag
- Probleme des klassischen Anti-Virus
- Was ist Antivirus in the Cloud?
- Was macht die Cloud?
- Beispiel
- Vorteile der Cloud
- Probleme der Cloud
- Zusammenfassung

perComp-Verlag

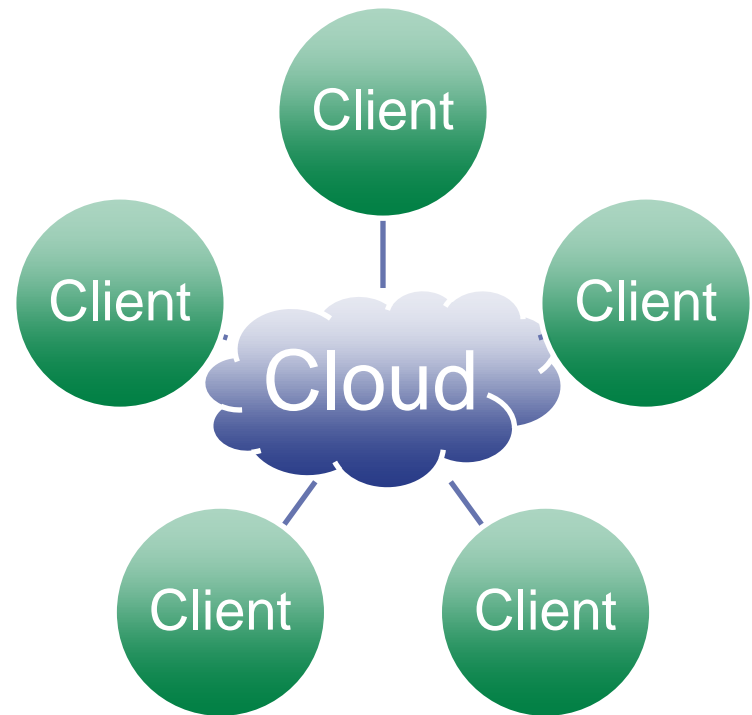


Probleme des klassischen Anti-Virus

- Entwicklung
 - steigende Anzahl Malware
 - komplexe Malware
 - serverseitige Polymorphie
 - hohe Anzahl
 - kurze Lebensdauer
- Auswirkungen
 - Performance
 - große Virus-Definitionen
 - Latenzzeiten bei Auslieferung von Virus-Signaturen
 - Fehlalarme

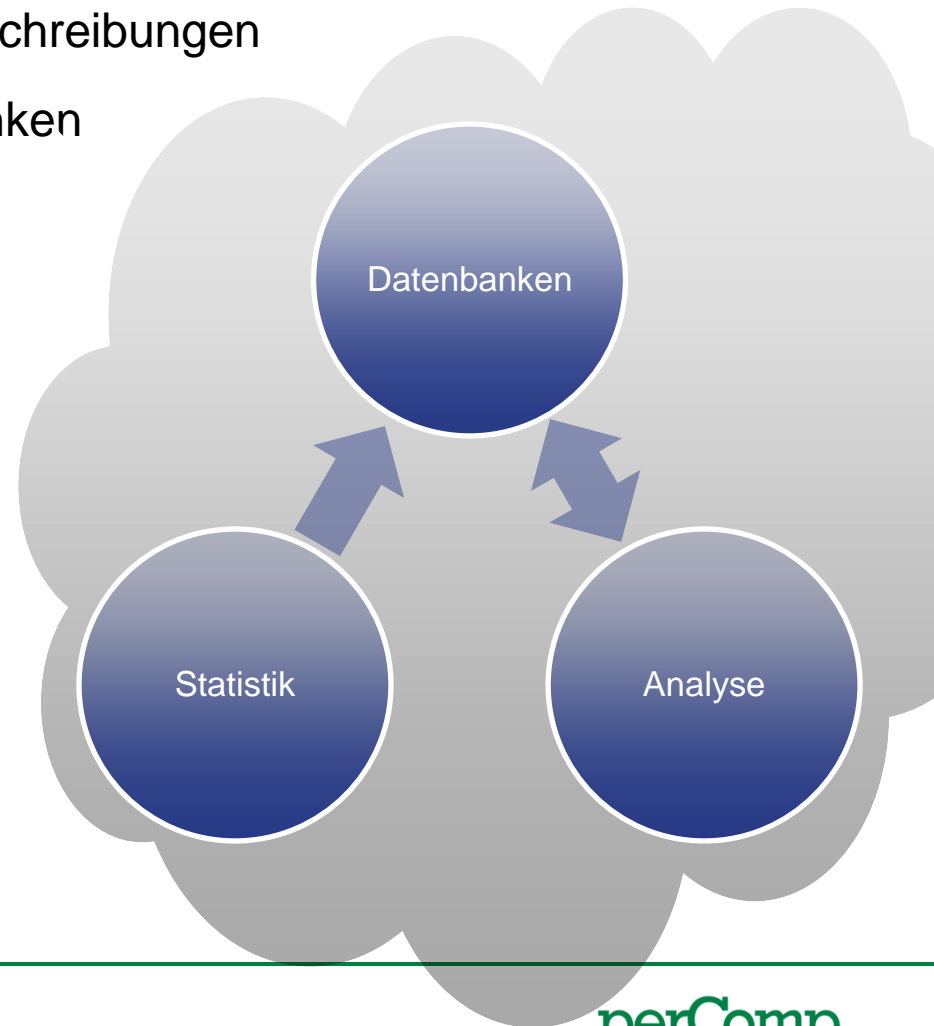
Was ist Antivirus in the Cloud?

- nicht: Managed Security Service (Cloud Computing)
 - E-Mail-Scanning bei xSP
 - Scanning-Service
 - Online Backup
- nicht: Security für Cloud Computing
 - AM- / Spam-Scanner für Web-Mail
 - verschlüsseltes Online-Backup
- Cloud-based Security ist:
 - Informationsaustausch
 - Vorhalten von Bewertungen für
 - Binaries, URLs, E-Mails

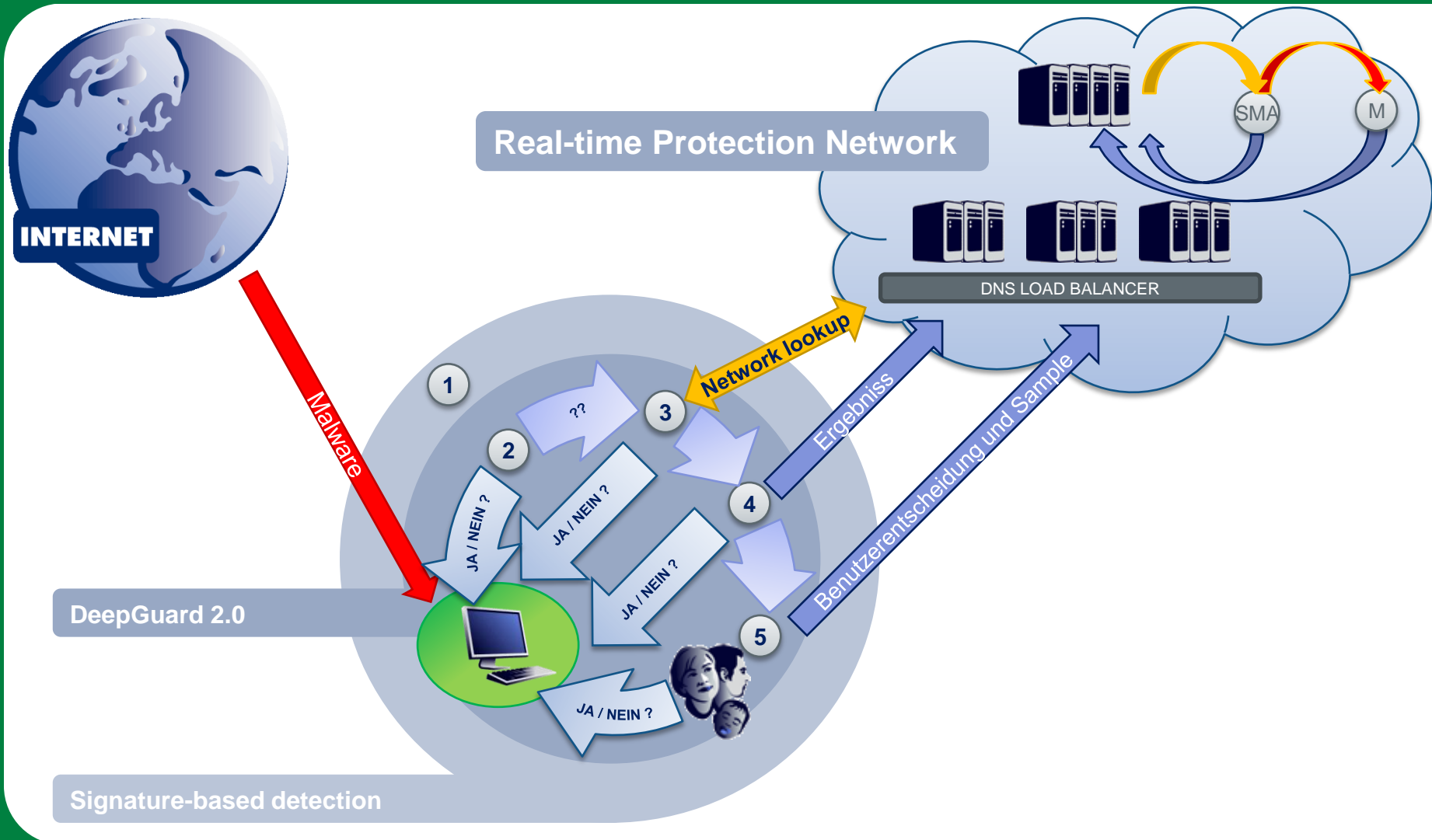


Was macht die Cloud?

- Klassifikation von Objekten
 - Risiko (gut – böse / unbekannt), Beschreibungen
- Auslagern und Vorhalten von Datenbanken
 - Blacklisting
 - Whitelisting
 - Entpack-Routinen
 - Erkennungs-Signaturen
 - Reinigungs-Routinen
- Sammeln von Statistik-Daten
 - Reputation
- Sammeln von Samples
 - Analyse



Beispiel F-Secure Real-time Protection Network



Vorteile der Cloud

- Updates schnell verfügbar
- schnelles beheben von Fehlalarmen
- größere Datenbanken
 - Blacklisting
 - Whitelisting
 - Signaturen
- Entlastung des Clients
- Sammeln von Statistik-Daten
 - Produktverbesserung
 - Reputation - Bewertung von Samples
- Sammeln von Samples

Probleme der Cloud

- Updates reaktiv
- Erstellen von Updates langsam
- kein Schutz bei Ausfall durch
 - Fehlkonfiguration
 - Netzwerkstörung
 - Serverausfall
 - Manipulation
 - Reputation, Man-in-the-Middle, DNS, DoS
- Performance
- Scannen weniger Dateien
- Sammeln von Statistik-Daten
 - Datenschutz
 - Fehlinterpretation (Rauschen)
- Sammeln von Samples

Zahlen zu F-Secure Deepguard

- Testergebnisse
 - Anfragen : 12 / 4 Stunden
 - Anzahl HTTP-Pakete: 4
 - Antwortzeit: < 100 ms
 - Datenvolumen: < 1000 Byte

Zusammenfassung

- Der klassische Anti-Virus wird nicht ersetzt.
- Zusätzliche heuristische Komponente mit möglicher Verbesserung der Reaktionszeiten auf neue Bedrohungen.
- Mögliche Verbesserung der Scan-Zeiten durch Whitelisting.
- Die Entlastung des Clients durch Reduktion der Virus-Signaturen enthält das Risiko einer schlechteren Erkennung.

Fragen?

