RWTH AACHEN UNIVERSITY

Aktuelles aus der Informationssicherheit: Webserver, Vorfälle, Firewallpolicy

Jens Hektor / Guido Bunsen / Bernd Kohler

Agenda

- **Webserver-“Leichen“, Security Scans**
- **3 Vorfälle**
- **Sicherung von Webservern**
- **Aktuelle Änderung Policy, kommende Änderungen**

Webserver

- Teilweise 15 Jahre alte Anmeldungen

- Trennung HTTP / HTTPS (abgeschlossen)
- Große Anzahl nicht erreichbar („Port closed“ - Leichen)
- Aufräumen Teil I abgeschlossen (1440 -> 1095)
- Große Anzahl nicht erreichbar (Timeout – Status?)
- Aufräumen Teil II steht bevor

- Warnungen aus Securityscans zügig abarbeiten

3 Vorfälle mit Webservern

- **RWTH-IN 20160823**
  Wordpress XMLRPC bruteforce amplification

- **RWTH-IN 20160915**
  SPAM via Backdoor in Joomla-Instanz
  kryptische Kommunikation zum C&C Server

- **RWTH-IN 20160831 / DFNCERT#2016-1081908788 / CERTBund#2016091528000204 / BfV?**
  Installation Backdoor 15.12.2015 in Joomla
  Ab 31.7.2016 3 weitere Files: toter Briefkasten (Proxy)
  Opfer: US-Regierungsthinktank, weitere (?)
  Alles lief über SSL
  Interesse deutscher Behörden!

Absicherung Webserver

- **Security Scan Reports ernst nehmen!**
  Alle Instanzen aus den Scanreports waren High/Medium
- **Admin Bereiche in CMS-Systemen absichern**
  muss das weltweit erreichbar sein?
- **Virenscanner auf dem Webserver**
  Sophos erkannte alle Backdoors
  Bitte: AV-Produkte auch unter Linux einsetzen und Logs lesen
- **Möglichkeit: remote scanning**
  Mountpoint / Freigabe Richtung IT Center
  Scan der Webfiles durch IT Center
- **1500 Webinstanzen IT Center (1.1 Tbyte, 3.7M Dateien)**
  17h Scan, 15 Funde

Zentrale Firewall

- **Anstehend: Registrierung und Sperrung der Ports bis 3000 (14.10.!)**
  Vorarbeit IT Center anhand der lokalen Firewallpolicies
  Dabei wieder: Ausmistung von „Leichen“

- **Ausstehend: Einführung „Deep Inspection“ HTTP**
  Intrusion Prevention Features jetzt verfügbar
  Getestet an zentralen Webservern (www.rwth-..., …)

- **Zukunft: Aufbrechen SSL, Deep Inspection zu HTTPS-Webservern**
  Vorarbeiten: Key Management