IT Sicherheit:
Lassen Sie sich nicht verunsichern

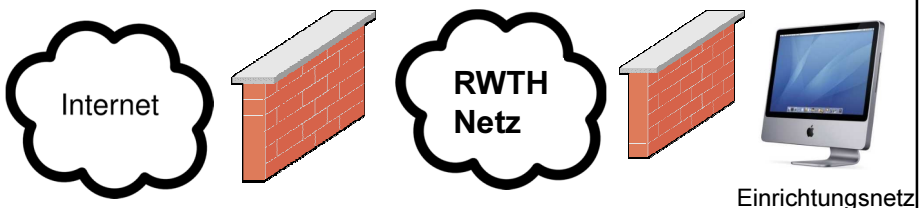
Guido Bunsen
IT Manager Security IT Center

AGENDA

- Betrieb von Firewalls
- Webfilter
- E-Mail-Filter
- Netzwerküberwachung / Blast-O-Mat
- Virenschutz-Software
- Schwachstellen-Scanner
- RWTH-VPN / Instituts-VPN
- Zertifizierungsstelle
- Beratung
- Fazit

Betrieb von Firewalls

- **Firewalls und Intrusion Prevention Systeme**
  - Separierung gefährdeter Infrastruktur vom Internet und vom Rest der Hochschule
  - Zugriffsteuerung auf Dienste
  - Abwehr von Denial of Service Angriffen (DOS)
  - Identifikation und anschließende Analyse von auffälligen Verkehrsmustern

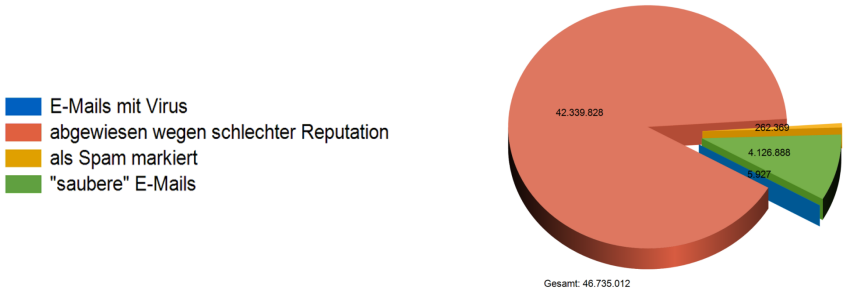


Webfilter

- **Schutz von Arbeitsplätzen vor Drive-By-Exploits bzw. schädlichen Webseiten**
  - Reputationsbasiert
  - Typischer Arbeitstag im Dezember 2014: 80 Mio. Transaktionen
  - 4 % Prozent der Zugriffe sind „verdächtig" (2 Mio. Transaktionen)
  - 0.4. Prozent der „verdächtigen" Zugriffe enthalten Schadsoftware (8.000 Transaktionen)

E-Mail-Filter

- **Reputations- und inhaltsbasierte E-Mail-Filter**
  - Schutz vor Schadsoftware in E-Mails
  - Schutz vor Spam und damit vor Überlastung der Infrastruktur und der Empfänger
  - Durchschnittszahlen pro Monat: 42 Mio abgewiesener Spam-E-Mails, Zugestellt: 3,6 Mio saubere E-Mails, 240.000 Spam-E-Mails, 15.000 E-Mails mit entfernten Viren.



Netzwerküberwachung / Blast-O-Mat

- **Identifizierung von Systemen mit Schadsoftware unerwünschtem Verhalten**
  - Beispiele: Viren, Trojaner, gestohlene WLAN- oder VPN-Accounts
  - Je nach Policy Benachrichtigung der Eigentümer, Administratoren der Deaktivierung von Ports oder Accounts.

Virenschutz-Software

- **Sophos Konsortialvertrag**
  - Nutzbar für alle Einrichtungen der RWTH Aachen University und der FH Aachen
  - Nutzbar für alle Mitarbeiter und Studierende

Schwachstellen-Scanner

- NEU / Start im Herbst 2014
- Einsatz der Software OpenVAS mit Schwachstellen-Datenbank der Firma Greenbone
- Etwa monatlicher Scan aller von außen erreichbaren Server
- Suche nach Fehlkonfigurationen (PHP, TLS, …), veralteter oder unsicherer Software
- Im Dezember enthielten von ca. 2200 gescannten Servern 10 Prozent mindestens eine schwerwiegende Sicherheitslücke
- Wann ist eine Schwachstelle „schwerwiegend": Über das Internet ausnutzbar, Exploit-Tools verfügbar, Ausnutzung einfach oder mäßig aufwändig

- Ausweitung in 2015 geplant

RWTH-VPN / Instituts-VPN

- Sichere Verbindung mit der RWTH über unsichere Netze
- Zugang für Administratoren
- Zugang für Mitarbeiter und Studierende zu ansonsten nur intern nutzbaren Dienste
- Nachteil: Bei Verlust des Passwortes erlangen auch Angreifer Zugang zu schützenswerter Infrastruktur

- 2 Ausprägungen: RWTH VPN / Instituts-VPN

Zertifizierungsstelle

- **IT Center betreibt eine Zertifizierungsstellen gemeinsam mit dem DFN Verein (DFN-PKI)**
- **Kostenfreier Zugang zu Serverzertifikaten und zu persönlichen Zertifikaten**
- **Anwendung/Nutzen:**
  - Verschlüsselter Verbindung zwischen Browser und Server in der RWTH.
  - Sichere Identifizierung des Servers.
  - Ende zu Ende Verschlüsselung von E-Mails
  - Signierung von E-Mails

Beratung

- Beratung zu Fragen der Informationssicherheit
- Unterstützung bei der Planung und Umsetzung von Sicherheitsmaßnahmen
- Unterstützung bei der Identifikation und Bewertung von Gefährdungen und Risiken, Analyse von Vorfällen

Fazit

- Die Bedrohungen nehmen zu / Mehr Präsenz in den Medien
- Wir verarbeiten immer mehr sensible Daten im Internet
- Abwehr und Schutz muss auf allen Ebenen organisiert werden

- Jeder muss sensibilisiert werden und sich beteiligen

Vielen Dank
für Ihre Aufmerksamkeit