Hochschule Zittau/Görlitz
UNIVERSITY OF APPLIED SCIENCES

Hochschulrechenzentrum

Sicherheitsmaßnahmen im Hochschulnetz

Das Hochschulrechenzentrum

- erbringt Dienstleistungen für die Hochschule Zittau/Görlitz
  - Bereitstellung, Betrieb und Wartung der Netzinfrastruktur
  - Bereitstellung von Datenkommunikationsdiensten
  - Zentrale Arbeitsplatz- und Nutzerbetreuung
  - Bereitstellung und Betrieb zentraler IT-Ressourcen
  - Beratung, Unterstützung und Durchführung zentraler Beschaffungen für Hard- und Software
  - Grafik-, Druck- und Kopierleistungen

Bedrohungslage

Hochschule als attraktives Angriffsziel

- Hohe Anzahl an Rechnern / Servern, sehr schnelle Internetanbindung
  - Angriffe von gekaperten Rechnern, (D)DoS
- Große Anzahl an Benutzern, Mailadressen
  - Identitätsdiebstahl / Missbrauch, Zugang zu (sensiblen) Daten etc.
  - Gezielte Angriffe, z.B. Verschlüsselungstrojaner
- Datendiebstahl, Spionage
  - Forschungsdaten, MA- / ST-Daten, Vertrags- / Verwaltungsdaten
- Sabotage
  - Schaden bei Nichtverfügbarkeit von Diensten, Imageschaden

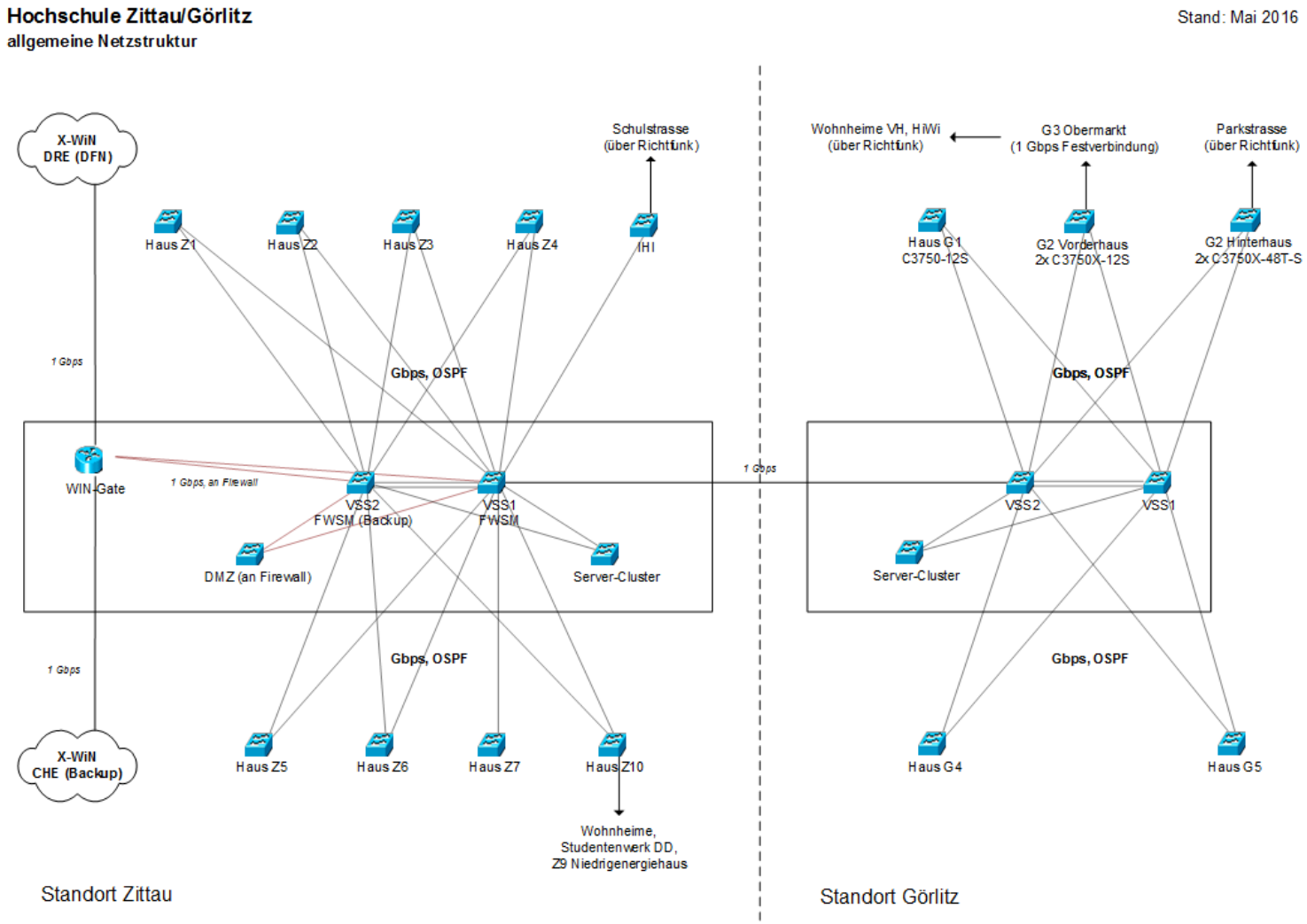
Angriffe bisher:

- Netz-Scans, Phishing-Angriffe, Trojaner-Mails (Viren / Ransomware etc.)

Sicherheitsmaßnahmen an der HSZG

- Proaktive Maßnahmen durch Nutzung von Diensten des DFN e.V.
  - Automatische Warnmeldungen
  - DFN Mailsupport (SPAM-Schutz / Antivirus)
  - DFN PKI (sichere elektronische Kommunikation)
  - Meldungen zu Schwachstellen / Advisories
- Technische Maßnahmen
  - Perimeterschutz, Sicherheitszonen
  - Antivirenschutz (Sophos Landeslizenz)
  - Updateservice, Arbeitsstationsmanagement
  - IDS/SIEM im Testbetrieb, Schwachstellen-Scans (intern / extern)
  - Backup (Mailbox, Home-Laufwerk)
- Betrieb sicherer Dienste
  - Zugangsschutz, Verschlüsselung (Transport/Daten: VPN/WLAN/VoIP)
  - Verfügbarkeit: Redundanz, Klimatisierung, USV, Monitoring

Netzstruktur der HSZG



Weitere Sicherheitsmaßnahmen

Organisatorische Maßnahmen

- Informationssicherheitsmanagement
  - Informationssicherheitsteam neu gegründet
  - Sicherheitskonzept in Arbeit
  - Informationsbereitstellung / Policies festlegen
  - Informationssicherheitsbeauftragten berufen

Was kann der Nutzer tun:

- Aufmerksam sein (Angriffe werden gezielter), Verdächtiges Melden
- Dienste nutzen (Antivirus, SPAM-Filter, Verschlüsselung, Backup)
- Updates einspielen (Antivirus, Betriebssystem, Browser / -Plug-Ins)
- Policies beachten (Passwortrichtlinie, Cloud-Nutzung etc.)
- Kollegen sensibilisieren (Bildschirmsperre, herumliegende Dokumente)

Fazit

Fazit:

- Es gibt keinen 100%igen Schutz; technische / organisatorische Maßnahmen treffen, um Bedrohung zu minimieren
- **Sensibilisierung / Awareness wichtig**

Fragen?

jederzeit an: hrz-service@hszg.de

weitere Infos: https://hrz.hszg.de