FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Effektive Cybersecurity Strategien

Schützen Sie sich vor digitalen Bedrohungen

FH-Prof. DI Dr. Klaus Gebeshuber
klaus.gebeshuber@fh-joanneum.at

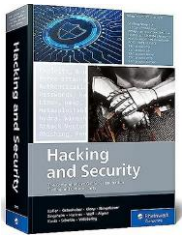
Klaus Gebeshuber

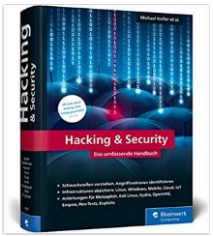
- Studium Elektrotechnik / Computer Technik TU Wien
- Industrial Software Development / Lagerlogistik

- Lehre @ FH JOANNEUM – IT & Mobile Security Kapfenberg
  - Network Technologies
  - IT-Security
  - Ethical Hacking
  - Network Security

- Forschungsthemen
  - Industrial Penetration Testing
  - Wireless Security
  - 0day hunting

- Zertifizierungen
  - OSCP, OSCE, CISSP, OSWP, CCNA, eCPPT, CSM, eMAPT





Cyber Angriffe in Österreich

15. Jan 2023	Cyberangriff auf eine Universität	Innsbruck, Tirol
Jan 2023	Cyberangriff auf einen Anbieter von Sportwetten	Admiral Sportwetten GmbH - Gumpoldskirchen
Jan 2023	Cyberangriff auf Vertriebspartner eines Telekommunikationsanbieters	Magenta Telekom - Wien
Feb 2023	Cyberangriff auf einen Hersteller von Stempeln und Lasertechnologie	Trodat / Trotec - Wels
03. Feb 2023	Cyberangriff auf eine Universität	Universität Graz
24. Feb 2023	Cyberangriff auf einen Feuerwehrausrüster	Rosenbauer - Leonding
20. Mar 2023	Instagram-Konto eines Hotels gehackt	Feuerberg Mountain Resort
Apr 2023	Cyberangriff auf einen Anbieter von Messtechnik und Automation	Anton Paar - Graz
Apr 2023	Ransomware bei einem Labor	Labor Burgenland - Eisenstadt
31. Mai 2023	Cyberangriff auf die Finanzmarktaufsichtsbehörde	FMA - Wien
21. Mai 2023	Bank von Cyberangriff betroffen	Bank99 - Wien

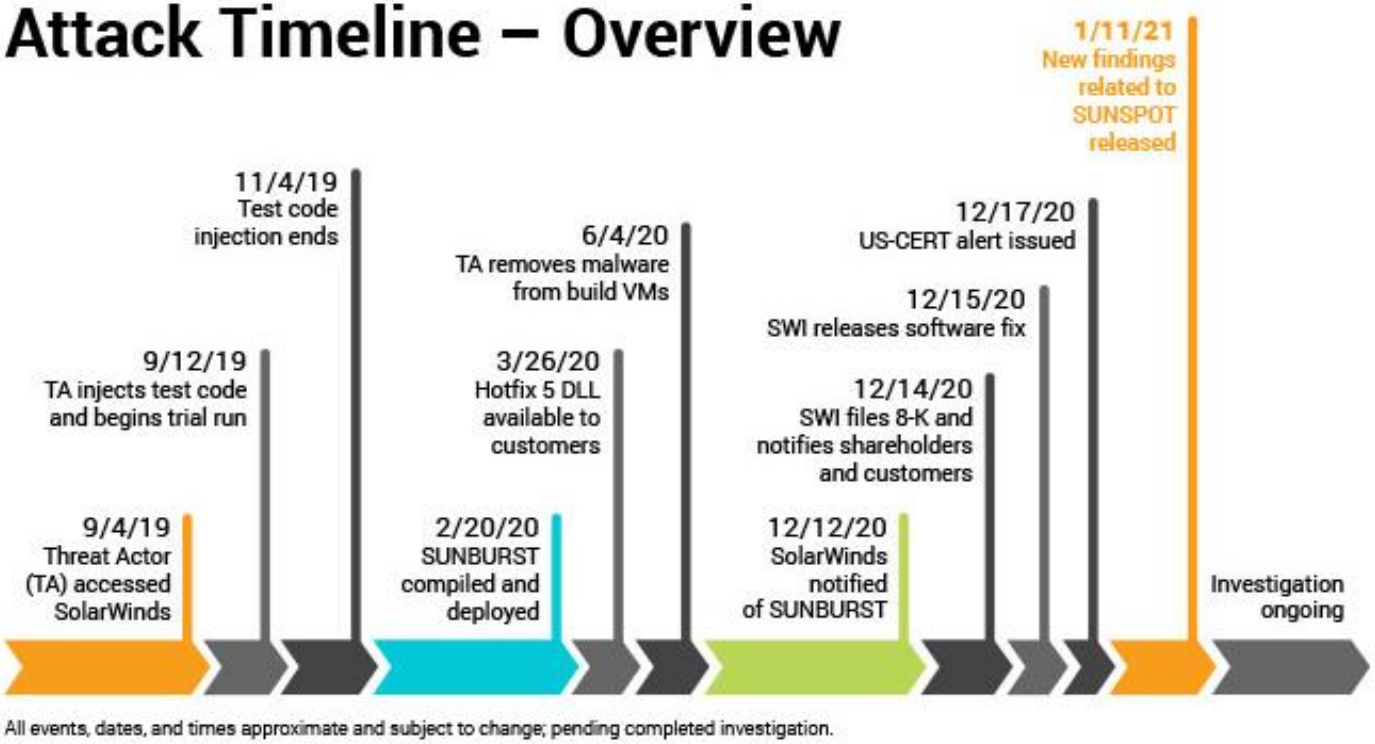
https://konbriefing.com/de-topics/cyber-angriffe.html

Cyber Angriffe in Österreich

11. Jul 2023	Online-Betrug bei einem Unternehmen	
Jul 2023	Cyberangriff auf einen Bildungsanbieter	ibis acam - Wien
25. Aug 2023	Cyberangriff auf eine berufsbildende Schule	HTL Mödling - Mödling
Sep 2023	DDoS-Angriff auf die Website einer Organisation	International Press Institute (IPI)
Sep 2023	Webshop eines Weinhändlers gehackt	Wein & Co - Vösendorf
11. Sep 2023	Unternehmer mit falscher Online-Identität betrogen	Klagenfurt
21. Sep 2023	Ransomware bei einem Unternehmen in Villach	
01. Okt 2023	Facebook-Seite eines Tierheims gehackt	Pfotenhilfe Lochen - Lochen am See
19. Okt 2023	Cyber-Zwischenfall bei einer Eisenbahngesellschaft	Westbahn - Wien
21. Dez 2023	Unbefugter Zugriff bei einer Universität	Universität Innsbruck - Innsbruck, Tirol

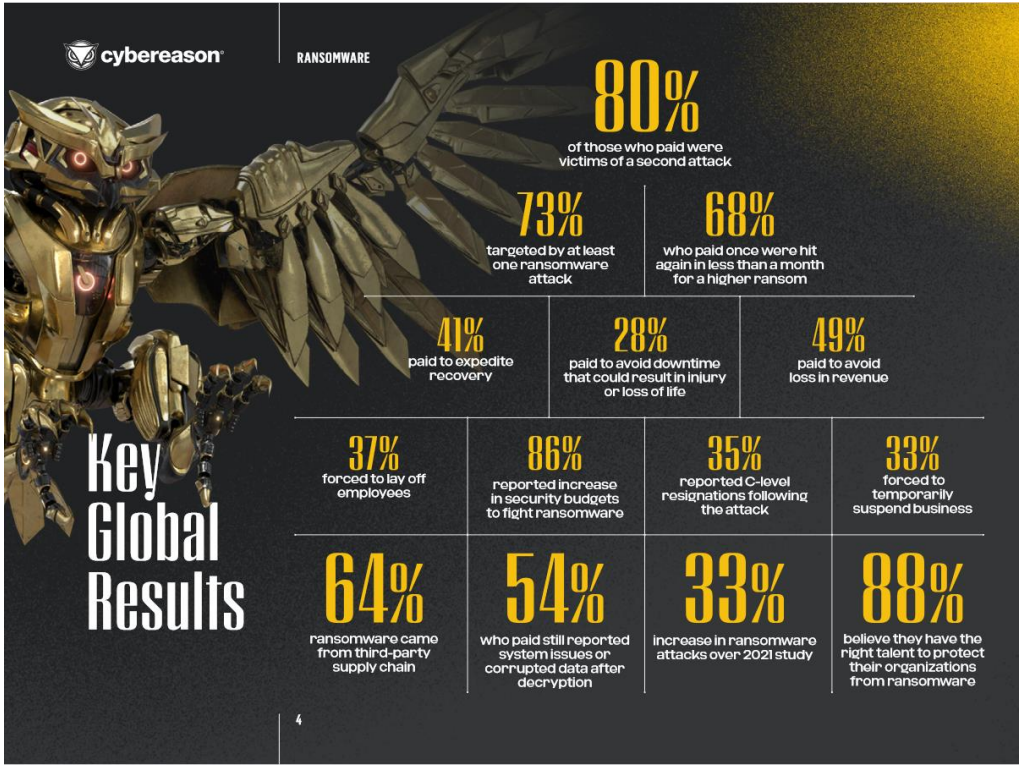
https://konbriefing.com/de-topics/cyber-angriffe.html

Supply Chain Angriffe
FireEye / Solar Winds



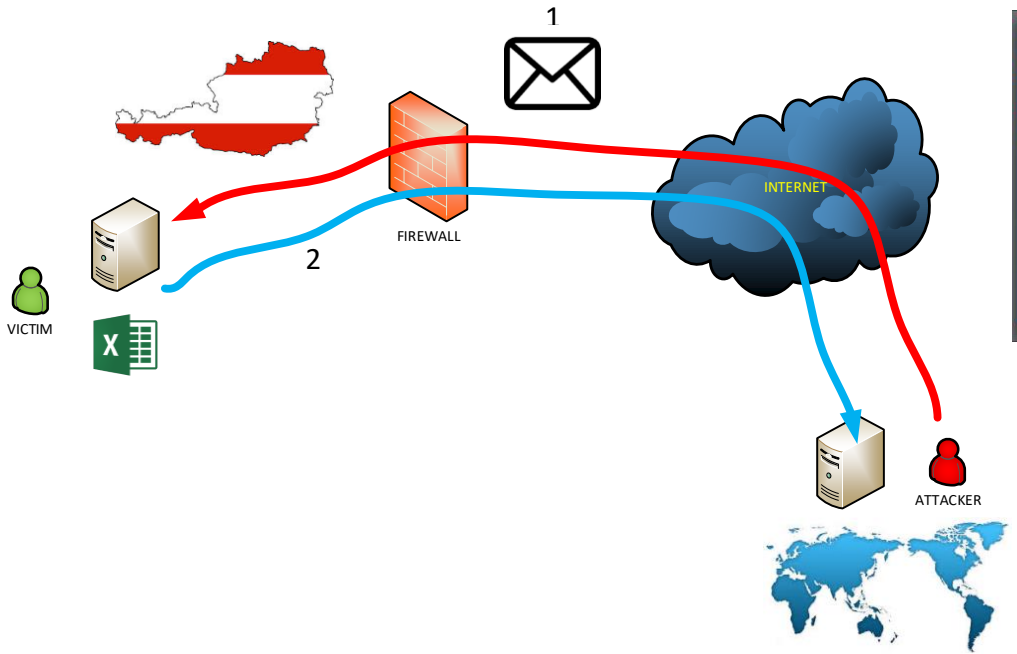
18.000 Customer
Cisco
Microsoft
Intel
Nvidia,
VMWare
AT&T,
Malwarebytes
Crowdstrike,
FireEye,...

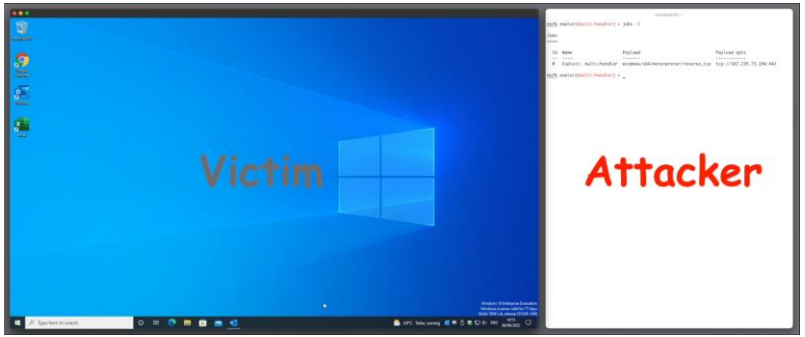
Ransomware – Sollen wir bezahlen?



 https://www.cybereason.com/hubfs/dam/collateral/reports/Ransomware-The-True-Cost-to-Business-2022.pdf

Initial Zugriff– Office Dokumente





Security Trainings

Awareness: Alle Mitarbeiter/innen - regelmäßige Termine!

- Angriffspfade vorstellen
- Phishing Attacken
- USB Sticks verteilen
- Telefon Phishing
- Physische Zutrittstests

Planspiele: Alle verantwortlichen Personen!

- Wir haben JETZT einen Ransomware Ausbruch
- Wer macht was?

Trainings für technisches Personal

Entwicklung:

- Angriffspfade vorstellen
- Secure Coding
- Secure Design
- Design Patterns

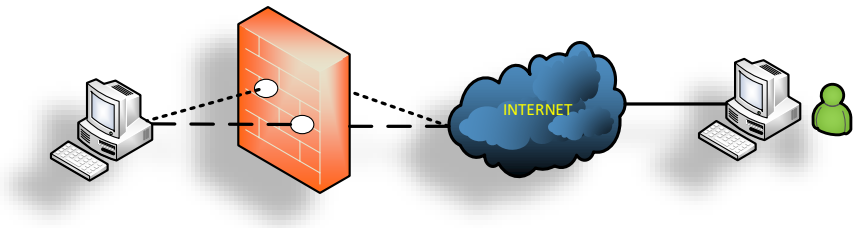
IT:

- Angriffspfade vorstellen
- Incident Response
- Monitoring, Alerting
- Angriffssimulation, Training auf einer Cyber Range

Infrastruktur – Analyse / Security Tests

Security Tests:

- Vulnerability Assessment
- Penetration Testing
- Red Team Assessments



Beispiele:

- Schwache Passwörter
- Keine Zugangs Kontrolle im Netzwerk
- Keine Netzwerk Segmentierung
- Datenverkehr aus dem Netzwerk ins Internet
- Im Netzwerk abgefangene Passwort Hashes
- Lokale Administrator Rechte
- Kein Monitoring/Alerting
- ...

Vielen Dank!