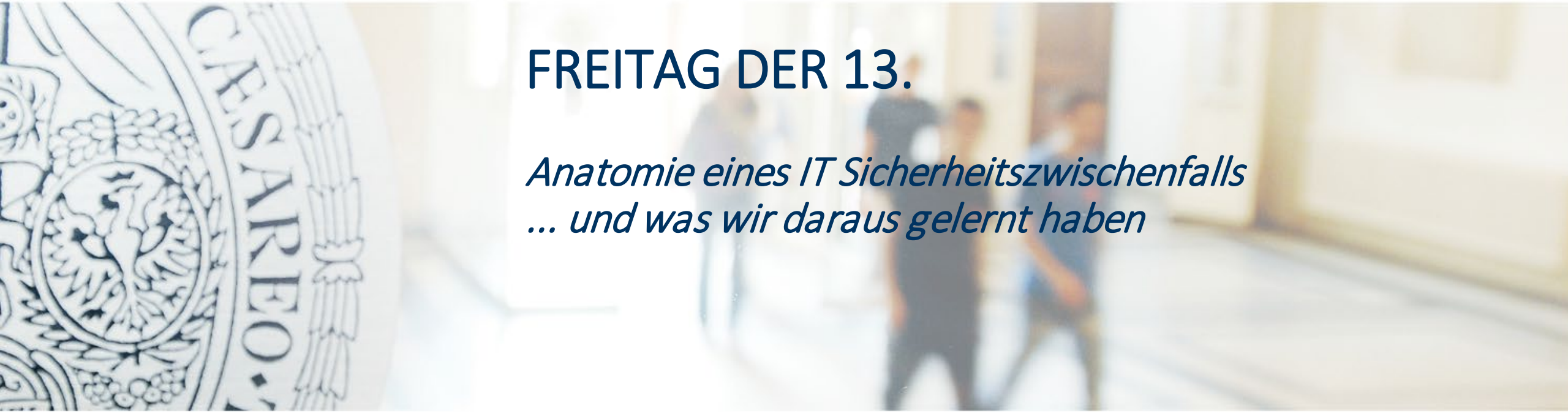
universität innsbruck

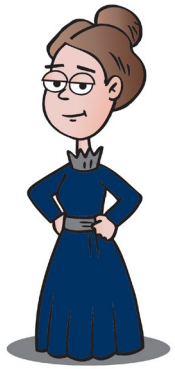


FREITAG DER 13.

Anatomie eines IT Sicherheitszwischenfalls
... und was wir daraus gelernt haben

Gegründet im Jahr 1669, ist die Universität Innsbruck heute mit mehr als 28.000 Studierenden und über 5.000 Mitarbeitenden die größte und wichtigste Forschungs- und Bildungseinrichtung in Österreich.

Teil 0
Wer wir sind



Zentraler Informatikdienst (ZID) der Universität Innsbruck

- Zentraler IT Dienstleister der Universität Innsbruck
- Serviciert ca. 5.000 Mitarbeiter:innen und 28.000 Studierende
- gesamte Bandbreite (Netzwerk, Server, Systeme, Services für Forschung, Lehre, Verwaltung)
- ... vom Datacenter und den Netzwerkkabeln
  bis zur eigenentwickelten Verwaltungssoftware
  und High Performance Computing (HPC) Lösungen
- starke lokale Infrastruktur
- ca. 130 Mitarbeiter:innen in 10 Abteilungen

Susanne Tober

- Stv. Leiterin des ZID
- Gesamtverantwortung für IT Security, Operativer Betrieb etc.
- Studium Informatik
- Software-Entwicklerin, Projekt- und Service-Managerin

Michael Redinger

- Leiter des ZID
- Studium Internationale Betriebswirtschaft (Personal & Prozesse)
- "gelernter" Systemadministrator, Netzwerkadministrator, IT Sicherheitsverantwortlicher
- IT Security Manager (ISO 27000)
- Auditor Ausbildung (ISO 19011, 20000, 27000)

Teil 1

Jetzt ist schon wieder was passiert

Kurzfassung

- Zugriff auf Uni-Netzwerk über gestohlenes Passwort von Nutzer:in
- laterale Bewegung durch Ausnutzung von Schwachstellen
- Gefahr des Zugriffs auf Zugangsdaten und Passwortinformationen
- Erkennung des Angriffs & technische Gegenmaßnahmen
- Treffen von Sicherheitsmaßnahmen (Passwortänderung)
- Rückkehr zum Regelbetrieb
- Post-Mortem Analyse

Was ist passiert

- Externer Zugriff über gestohlenes Passwort
- Scan des Datennetzes von innerhalb
- Angriff verwundbarer Systeme
- Weitere laterale Bewegungen der Angreifer

Was haben wir gemacht

- Erkennung des Angriffs bei internen Scans eines betroffenen Systems
- Analyse der betroffenen Systeme und unmittelbare Gegenmaßnahmen
- Einbeziehung externer Dienstleister
- Systematische Analyse des Angriffs (Systeme, Netzwerkverkehr etc.)
- Sicherheitsmaßnahmen (Zugänglichkeit betroffener Systeme, Backups etc.)
- Judgement Call: "soft" Reset der Passwörter

Kommunikation

- Kommunikationsstrategie - gemeinsam mit externer Unterstützung
- schnelle Information über alle Ebenen (involvierte Mitarbeiter:innen bis Rektorat)
- gezielte Einschränkung der weiteren Kommunikation
- schnelle, breite Kommunikation sobald notwendig (Passwort-Reset)
- Kommunikation zu Details bleibt eingeschränkt ("need to know")

Glück der Tüchtigen

- Erfolg ermöglicht durch schnelle Maßnahmen qualifizierter Mitarbeiter:innen
- ... unterstützt durch hochkompetente externe Partner
- ... mit dem Glück des Tüchtigen im Timing (Wochenende)

Teil 2
Was lernen wir daraus?

Externe Unterstützung („Emergency Response Service“)

- bringt viel Know-How
- bringt Routine, Sicherheit
- gibt klare Struktur und Anweisungen
- braucht kompetente lokale Partner:innen - kein Allheilmittel

Risikobasiertes IT Sicherheitsmanagement

“[A] risk-based security approach addresses security risks by first identifying and evaluating threats facing the organization. A risk-based approach is unique to each organization and addresses the individual set of needs, risks, and vulnerabilities that comprise the risk landscape of the company. A risk based approach stands in stark contrast to a compliance-driven approach, where security teams scramble to meet regulatory requirements and check off the boxes on industry-related standards.” (https://www.centraleyes.com/glossary/risk-based-security/)

Zum Beispiel

- die üblichen Maßnahmen „nach Stand der Technik“ ...
  - Zwei-Faktor-Authentifizierung (2FA)
  - Security Updates
  - Überprüfung auf Schwachstellen
- ... plus gezielte Reduktion der Angriffsfläche
  - Berechtigungen von Nutzer:innen (für Services, in Systemen)
  - Zugänglichkeit von Services

Hausaufgaben, die üblichen

- technische Systemsicherheit
- technische Netzwerksicherheit
- Log-Aufzeichnungen und Analyse

Zero Trust Security

“Zero Trust ist eine Bezeichnung für das IT-Sicherheitsprinzip „Vertraue niemandem, verifiziere jeden“. Dabei wird keinem Akteur, der auf Ressourcen zugreifen möchte, vertraut. Jeder einzelne Zugriff erfordert eine Authentifizierung.” (https://cyqueo.com/magazin/was-ist-zero-trust-das-prinzip-erklaert-verstaendlich/)

- im Gegensatz zur klassischen Perimeter-Sicherheit
- wachsende Bedeutung durch verschwimmende Unternehmensgrenzen (Cloud Computing)
- besonders bei offenen Umgebungen (Universitäten)

Zero Trust Security als

- gesamtheitlicher Ansatz
- Hinterfragen der IT Architektur
- Hinterfragen der Prozesse

Awareness & Schulung

- zentral & immer unterschätzt
- Menschen als wichtigster Angriffspunkt
  - risikobasierte IT Security!

- bei Nutzer:innen …
- … und den Mitarbeiter:innen in der IT!
  - am Stand der Technik?
  - „Verinnerlichung“ Bedeutung von IT Security in täglicher Arbeit
  - auch als Nutzer:innen!

Personal, Personal, Personal

für

- gewartete technische Systeme
- Weiterentwicklung der IT Landschaft & IT Security
- tägliche Routine (Loganalyse, Sicherheitsupdates u.v.m.)
- "schnelle Eingreiftruppe"

Externalisierung des Problems - SIEM, SOC & Co

- externe technische Lösungen sind kein Allheilmittel
- Hausaufgaben gemacht? (Logging etc.)
- passend zur lokalen Infrastruktur und zu lokalen Kompetenzen?
- Immer lokale Schnittstellen & Kompetenzen notwendig
- Auslagern & Vergessen gibt's nicht


Vielen Dank!