IT-Sicherheitsvorfälle an Hochschulen

seit Juni 2022 & Lessons Learned

Leonard Rapp
Security Engineer DFIR
CSIRT
G DATA Advanced Analytics GmbH

Jasper Bongertz
Principal Network Security Specialist
Head of CSIRT & Prokurist
G DATA Advanced Analytics GmbH

G DATA
advanced analytics

Inhalt

G DATA advanced analytics

01 Einleitung & Überblick

Juni 2022 – Juni 2024

G DATA
advanced analytics

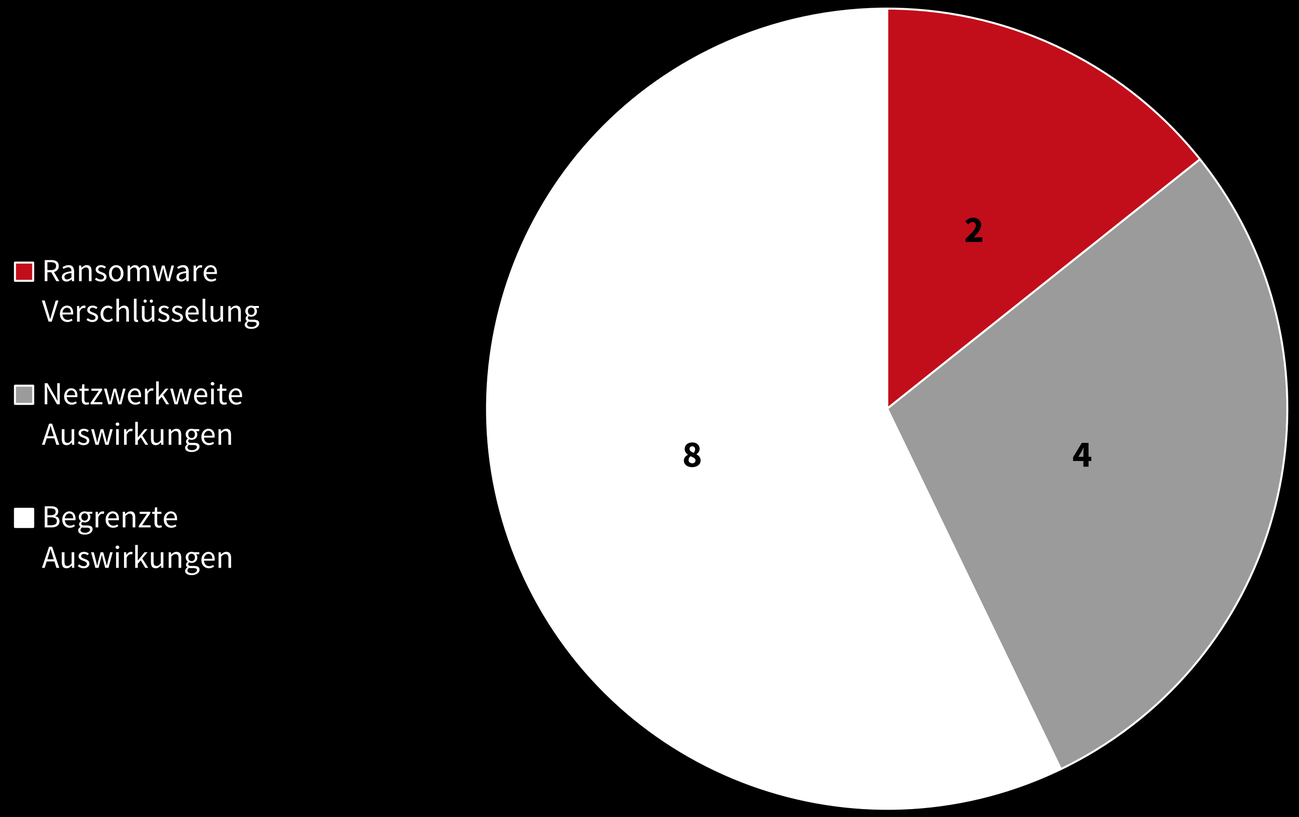
Mehrwert durch Praxiserfahrung schaffen

Keine wissenschaftlich-quantitative Studie

G DATA
advanced analytics

IT-Sicherheitsvorfälle an Hochschulen

01 Überblick über Vorfälle Juni 2022 – Juni 2024



G DATA advanced analytics

01 Überblick über Vorfälle Juni 2022 – Juni 2024

- **14** IT-Sicherheitsvorfälle
- **11** verschiedene Hochschulen
- **10** davon mit Rahmenvertrag
- **2** Hochschulvorfälle aus Kapazitätsgründen abgelehnt
- **Ca. 46%** haben Rahmenvertrag seit Juni 2022 genutzt

G DATA advanced analytics

02 Fallstudien

02 Fallstudien A - Angriffsablauf

- **Initial Access:** kompromittierte Zugangsdaten, VPN + VDI
- **Privilege Escalation:** LSASS Dump, NTDS-Dump
- **Lateral Movement:** RDP
- **Persistence:** VPN, VDI, SSH-Tunnel über TOR, Splashtop, AnyDesk, Cobalt Strike
- **Impact:** Hochschulweite Auswirkungen, keine Verschlüsselung

G DATA advanced analytics

02 Fallstudien A - Vorfallbewältigung

- Netzwerktrennung an der Firewall
  - Interne Dienste nur intern nutzbar
  - Externe Dienste nur Extern nutzbar
- Klausurphase in Präsenz überwiegend wie geplant
- Notfall-Website
- Hochschulweiter Passwort-Reset
  - Wie kontaktiert man Studierende?
  - Falsche Geburtsdaten
- Dienste hinter VPN mit verpflichtendem 2FA

G DATA advanced analytics

02 Fallstudien B - Angriffsablauf

- **Initial Access:** ???
- **Privilege Escalation:** LSASS-Dump, NTDS-Dump
- **Lateral Movement:** RDP, SSH auf ESXi
- **Exfiltration:** PowerShell + MegaSync
- **Impact:** Hochschulweite Auswirkungen, Verschlüsselung auf ESXi-Ebene, Löschen der Backups

G DATA advanced analytics

02 Fallstudien A - Vorfallbewältigung

- Großteil der Systeme verschlüsselt
- Forensik kaum möglich
- Koordination und Kommunikation herausfordernd

G DATA advanced analytics

02 Fallstudien C - Angriffsablauf

- **Initial Access:** Kompromittierte Zugangsdaten, VPN
- **Execution:** Ausnutzung von Sicherheitslücke
- **Exfiltration:** ca. 200MB LDAP-Daten
- **Discovery:** Netzwerkscans
- **Impact:** Keine Auswirkung auf Hochschulbetrieb, Datenschutzvorfall

G DATA advanced analytics

02 Fallstudien C - Vorfallbewältigung

- Frühzeitige Erkennung durch Mitarbeitende der Hochschule
- Gute Übergabe an G DATA ADAN
- Administrator hat System ohne Rücksprache mit dem Internet verbunden

G DATA advanced analytics

03 Häufige Angriffsmuster

03 Häufige Angriffsmuster – Initial Access

Überdurchschnittlich oft kompromittierte (VPN)-Konten

Hohe Anzahl an Personen mit Zugängen

G DATA advanced analytics

03 Häufige Angriffsmuster – Initial Access

Ausnutzung von Schwachstellen

Viele unterschiedliche, dezentral verwaltete Systeme
Keine zentralen Sicherheitsrichtlinien

03 Häufige Angriffsmuster – Initial Access

Wenig beschränktes Lateral Movement via RDP

Historisch gewachsen, komplexes aber flaches Netzwerk
Segmentierung extrem aufwendig

G DATA advanced analytics

03 Häufige Angriffsmuster – Initial Access

Schnelle Privilege Escalation

Historisch gewachsene, komplexe AD-Struktur
Dezentrales AD darf auf zentrale Infrastruktur zugreifen

04 Vorfallbewältigung

04 Vorfallbewältigung

- Dezentrale Organisations- und Personalstruktur
- Technologie-Diskussionen
- Viele betroffene Personen und Systeme
- Beschaffungsprozesse
- Zeitabhängige Systempriorisierung (Klausurphase, Einschreibefrist, …)

G DATA advanced analytics

04 Vorfallbewältigung

„Freiheit der Forschung und Lehre“

G DATA advanced analytics

05 Zentrale Gegenmaßnahmen

05 Zentrale Gegenmaßnahmen

- 2FA für ALLE Remote-Zugänge
- Verpflichtendes Patchmanagement
- Zentrale Strukturen (CERT / CSIRT)
- Ausreichend IT-(Security) Personal

G DATA advanced analytics

05 Zentrale Gegenmaßnahmen

Netzwerksegmentierung

- Administratives Netz mit VPN + 2FA oder Jumpserver
- Hohes Maß an Sicherheit, keine Beeinträchtigung der Nutzer
- Gezielte Überwachung möglich

G DATA advanced analytics

05 Zentrale Gegenmaßnahmen

AD-Design

- Zentrales AD separiert von dezentralen ADs
- „Wer sich nicht an zentrale Richtlinien hält, kommt nicht ins zentrale AD“
- Microsoft Tiering Modell / Enterprise Access Modell

G DATA advanced analytics

05 Zentrale Gegenmaßnahmen

Incident Response Plan

- Notfallhandbuch / Kontaktlisten Krisenstab (ausgedruckt)
- IR Rahmenvertrag & Kontaktinfo IR-Dienstleister
- Lagebildbestimmung
- Prozesse für Internet-Notfalltrennung
- Zeitabhängige Systempriorisierung
- Prozesse für Notfallbeschaffung

06 Fazit

06 Fazit

Probleme

- Hohe Anzahle Nutzende
- Viele unterschiedliche Systeme
- Dezentrale Organisationsstruktur

Lösungen

- Schaffung zentraler Strukturen und Sicherheitsrichtlinien
- 2FA für alle Remote-Zugänge
- Speziell gesichertes Managementnetzwerk
- Incident Response Plan mit zeitabhängiger Systempriorisierung

G DATA advanced analytics

Vielen Dank für Ihre Aufmerksamkeit,
bis (hoffentlich erst) nächstes Jahr!

G DATA
advanced analytics

Notfallnummer
+49 234 9762-800

Jasper Bongertz
jasper.bongertz@gdata-adan.de
+49 172 5783558

Leonard Rapp
leonard.rapp@gdata-adan.de
+49 173 2751342