LUIS Sicherheitstag Herbst 2022

- Aktuelle Sicherheitslage (Michael Brenner, LUIS)
- Neue Lösung für den Virenschutz (Mathias Casselt, LUIS)
- Digitale Zertifikate von GÉANT-TCS (Mathias Casselt, LUIS)
- Security-Awareness an der LUH (Jens Rademacher, CIO Büro)

Aktuelle Sicherheitslage

Zeitraum: 03.2022 – 08.2022

LUIS Sicherheitstag Herbst 2022 am 20.09.2022

DFN-CERT-Warnmeldungen

- 300 Scan / Portscan
- 9 Configuration / Amplifier
- 8 Attack / Virus
- 8 Bot
- 4 Configuration / Unencrypted Communication
- 3 Configuration / Unrestricted Access

- → 332 Warnmeldung insgesamt
- → Zeitraum: 03.2022 – 08.2022

Credential-Leaks (DFN-CERT-Meldungen)

- Regelmäßige Meldungen vom DFN-CERT zu geleakten Kennwörtern (Kombination: E-Mail-Adresse + Passwort)
- Daten unklarer Herkunft und Qualität
- Erfahrung: Daten meist älter, manchmal aber noch aktuell
- Betroffene werden vom LUIS-Sicherheitsteam kontaktiert
- → Maßnahmen: Passwort erkennen & ändern

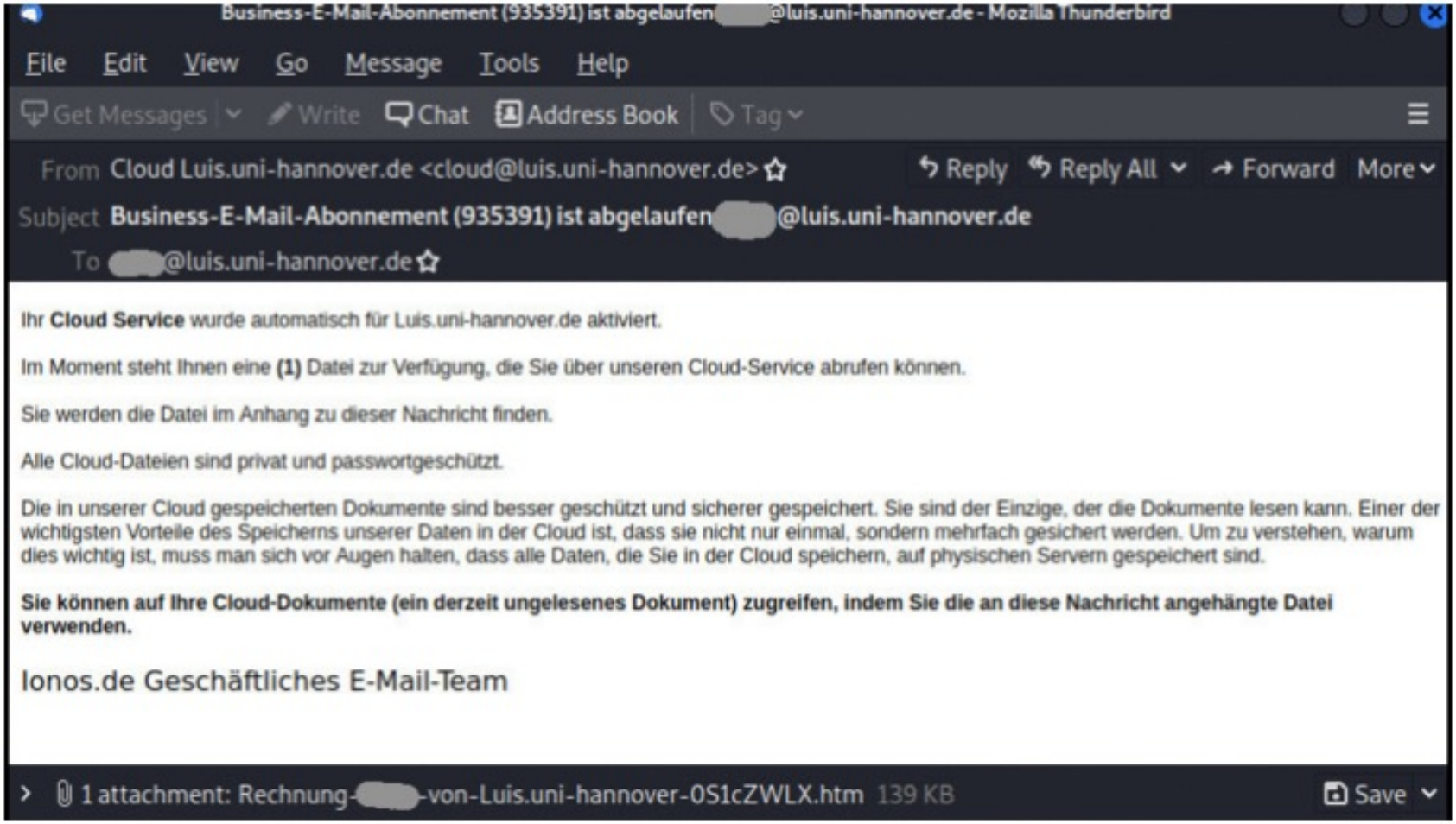
CEO-Fraud

- Phishing-Mails
- Kommen immer mal durch
- Sind oft nicht direkt schadhaft

- Kontaktaufnahme z.B. durch „Do you have some minutes?“

- Ziel: Aufforderung zum Kauf von Google Play Cards

Phishing Kampagne September



Weiteres / Kurz vermerkt

- Hackerangriff auf Uni Wuppertal
- Schwachstellen (News-Meldungen):
  - Polkit
  - Samba
  - Netatalk (NAS-Systeme)
  - Zero-Day-Lücke in Microsoft Office
- BSI-Warnung vor Einsatz von Kaspersky-Virenschutz
- Sicherheitshinweis: Krieg in der Ukraine
- Virenschutz: Sophos verlängert, neue Lösung verzögert sich

Zusammenfassung

- 332 DFN-CERT-Warnmeldungen
- (Port-)Scans mit uns absprechen
- Firewall pflegen

- Credential-Leaks

- LUIS-Virenschutz

- Anhaltende „Bedrohung“ durch:
  - CEO-Frauds
  - Ukraine-Konflikt (Sicherheitshinweis)
  - Schwachstellen in Software (allgemein)

Informationsbeschaffung

- BSI Lagebericht (~100 S.)
- ENISA Threat Landscape (~100 S.)
- NCSC Threat Intelligence Report (eher so monatlich, sehr kurz, 3-10 S.)
- NIST SP 800-150 Guide to Cyber Threat Information Sharing (~35 S.)

- Talos Cybersecurity Report
- CrowdStrike Global Threat Report
- Sophos Security Threat Report
- Intel Cyber Threat Report
- IBM Security Threat Intelligence Report
- trendmicro Threat Report
- NETSCOUT Threat Intelligence Report
- SonicWall
- Rapid7
- ...