Leibniz Universität IT Services

Leibniz Universität Hannover

Aktuelle Sicherheitslage & Awareness Best Practices

LUIS-Sicherheitstage 27.02. & 28.02.2024

Inhalt

- Aktuelle Sicherheitslage
  - Phishing (E-Mail)
  - CEO-Frauds
  - Passwort-Leaks
  - Geleakte Kommunikationsverläufe + (PDF-Anhang mit) Link
  - Mail-Server-Bounce-Spam-Mails
- (Veraltete) Software auf Serversystemen
- Schwachstellen-Scans
- Maßnahmen im Ernstfall
- Best Practices Awareness

E-Mail: Phishing

- Phishing-Mails bleiben eine anhaltende, ernst zu nehmende Bedrohung
- Best Practice: Absender-Mail-Adressen anzeigen lassen
  - <Volker Epping> spammail@spam.org
  - <Volker Epping> praesident@uni-hannover.de

    → aber: auch Absender-Mail-Adressen können gefälscht sein
- **Maßnahmen**:
  - Telefonische Rücksprache halten
  - Löschen, nicht antworten, keine Login-Daten eingeben, keine Links anklicken
  - Mails als „Nur-Text“ anzeigen lassen (kein HTML)
  - Achten auf **[extern]**-Tag im Betreff
  - Ggf. **melden** (security@luis.uni-hannover.de und spam@luis.uni-hannover.de)
  - Verwendung von S/MIME-**(Nutzer-)Zertifikaten**

Phishing – Beispiel Outlook Web App

Von: IT-Support <spammail@spam.org>

Lieber E-Mail-Nutzer,

Wir migrieren alle E-Mail-Konten auf die neue Outlook Web App 2023 und daher müssen sich alle aktiven Kontoinhaber verifizieren und anmelden, damit das Upgrade und die Migration jetzt automatisch wirksam werden. Dies geschieht, um die Sicherheit und Effizienz aufgrund der neuesten empfangenen Spam-Nachrichten zu verbessern.

Um Unterbrechungen des Dienstes zu vermeiden, klicken Sie bitte auf den unten stehenden Link, um Ihre Beiträge zu aktualisieren
Outlook Web App 2023<schadhafter Link> und melden Sie sich an, um mehrere Spam-Mails zu migrieren und zu blockieren.

Wenn Sie Ihr Konto nicht innerhalb von 24 Stunden übertragen, wird Ihr Konto vorübergehend gesperrt, sodass Sie keine E-Mails empfangen/senden können.

IT-Helpdesk
Informationstechnologie

CEO-Fraud – Echtes Beispiel

- **Leider Normalität**, nicht immer einfach technisch zu filtern.
- Hier ein **echtes Beispiel** (Antworten zwischen den Nachrichten entfernt):

- Are you available? | Are you unoccupied? ← *i.d.R. im Namen von Vorgesetzten*

  „Hallo, sind Sie verfügbar? Bitte ich brauche dringend Ihre Hilfe.“
- Okay, danke für Ihre Antwort. Bitte, ich bin gerade in einer Situation. Ich hätte anrufen sollen, aber während des Treffens ist keine Kommunikation erlaubt und Sie müssen **sofort** eine Aufgabe für mich erledigen. Gibt es in Ihrer Nähe ein Lebensmittelgeschäft?
- Hallo <Name>, bist du da?
- Ok, kein Problem, Sie können mir aus der Ferne helfen. Bitte hier ist, was Sie ganz schnell für mich tun müssen. Ich benötige **Apple-Geschenkkarten**. Können Sie mir helfen, diese in einem Lebensmittelgeschäft zu kaufen? Etwaige Unannehmlichkeiten werde ich so schnell wie möglich erstatten. Lassen Sie mich wissen, um Sie über die zu kaufenden Stückelungen zu beraten. Danke
- Ok, danke, der Betrag, den ich benötige, beträgt jeweils 100 € in 6 Stücken, also insgesamt 600 €. Wenn Sie sie bekommen, rubbeln Sie einfach den **Anspruchscode** frei, machen Sie ein klares **Foto** der Karten und legen Sie sie mir hier bei. Ich werde sie später von Ihnen bekommen, aber stellen Sie sicher, dass Sie sie mir hierher schicken, sobald Sie sie erhalten haben, da ich sie **sofort** brauche. Hoffe das ist klar genug?
- Wie viele Minuten bitte?

Passwort-Leaks

- Hinweise auf geleakte Passwörter
- Beispiel: security@luis.uni-hannover.de | Se_____

- Gründe und Ursprung meist nur zu vermuten
- Mögliche Gründe
  - **Mehrfach verwendete Passwörter** + Sicherheitsvorfall bei ext. Diensten
  - Erfolgreiches Phishing
  - Schadsoftware auf Endgerät

- **Maßnahmen**:
  - Passwort identifizieren, falls verwendet: ändern
  - Kritische Accounts (z.B. Mailbox) überprüfen (oft ist Mailbox betroffen)

- Hinweise zu Passwort-Hygiene auf **LUIS-Website** unter: https://go.lu-h.de/passwoerter

Geleakte Kommunikationsverläufe I

- Beispiel:

Von: Epping, Volker <spammail@spam.org>

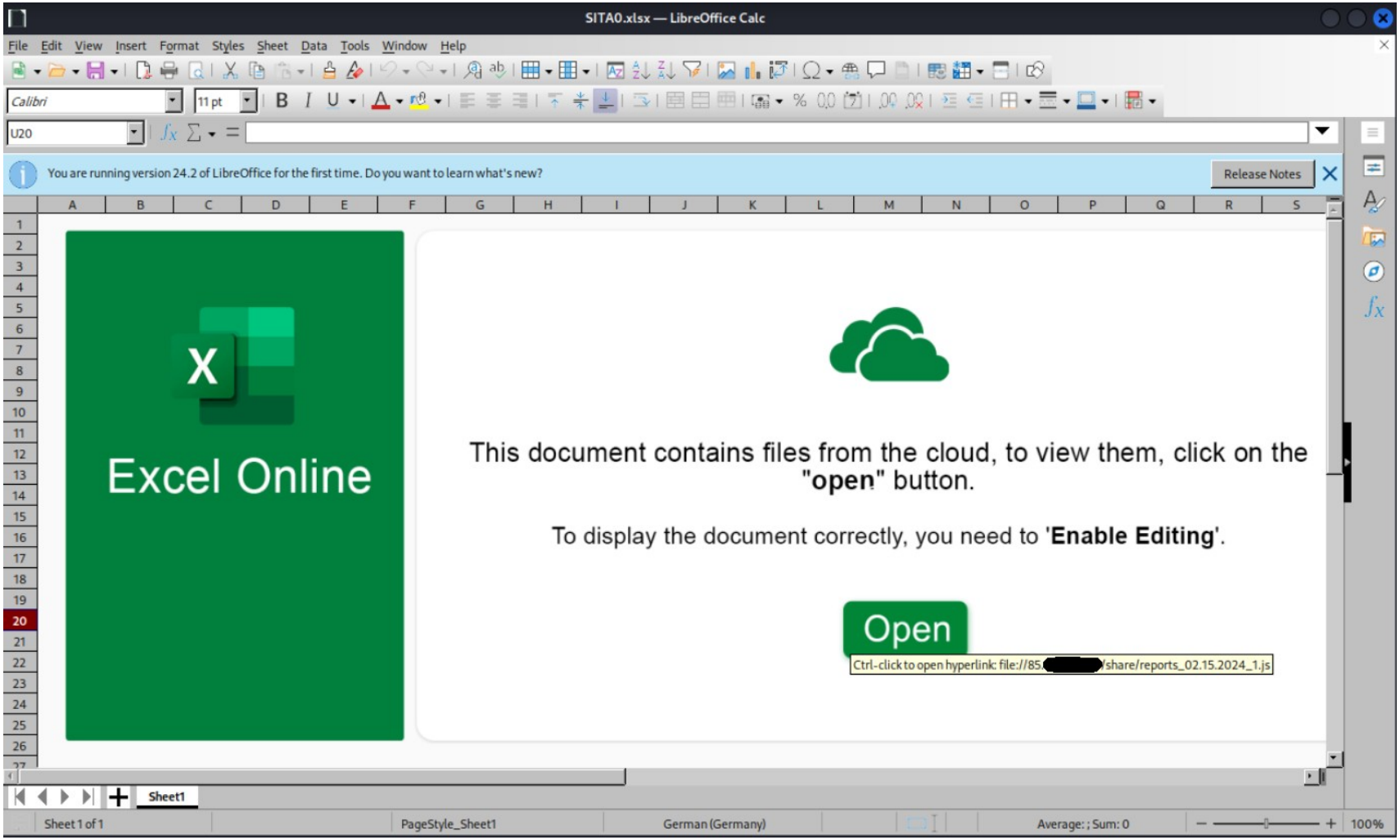
Betreff: [extern] Re: Willkommen an der LUH

Ich habe Ihnen am Vortag ein Material weitergeleitet. Sind es zu dir gekommen?

<schadhafter Link>

Willkommen an der LUH… (ab hier echte geleakte Kommunikation)

Geleakte Kommunikationsverläufe II - Anhang



Phishing – Angeblicher Mail-Server-Bounce I

Von: Mail Delivery System <Mailer-Daemon@brands.technado.co>

An: security@luis.uni-hannover.de

Betreff: [extern] Mail delivery failed: returning message to sender

Anlage: file-2 , 127 Bytes
Incoming Message Failure Delivery Status Notification_ returning message to security@luis.uni-hannover.de.eml

```
This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its
recipients. This is a permanent error. The following address(es) failed:

  security@luis.uni-hannover.de
    Domain merakiappstudio.com has exceeded the max emails per hour (188/150 (125%))
allowed.  Message discarded.
```

- Der Mail ist eine vermeintlich gesendete Mail angehängt, die dann schadhafte Links zu einem vermeintlichen Webmailer beinhaltet

  → Phishing von Zugangsdaten
- Ob die Mails tatsächlich gesendet worden sind (mit gefälschter Absender-Mail-Adresse) oder ob die Masche rein darin besteht, die Empfänger der Bounce-Mails hereinzulegen, ist unklar, beides ist jedoch möglich.

Veraltete Server-Software

- Meldungen zu veralteter Software auf Serversystemen
  - Nicht (mehr) betreute Systeme
  - Kurzfristige (Sicherheits-)Updates

- Best Practices:
  - Regelmäßige automatisierte (Sicherheits-)Aktualisierungen
  - Prüfen ob Dienste einschränkbar sind (z.B. Uni-/Instituts-Intern)

Schwachstellen-Scans

- Zentrale OpenVAS-Instanz
  - Schwachstellenmanagement
  - IP-Netzbereiche werden mit verschiedenen Tools gescannt
  - Ziel: Finden von Schwachstellen oder Fehlkonfigurationen

- Bei Interesse melden
  - Individueller Setup wird besprochen
  - Ergebnis des Scans kann als Bericht in verschiedenen Formaten bereitgestellt werden

Maßnahmen im Ernstfall

- Sofort
  - Betroffenes System **vom Netz nehmen**
  - Vorfall **melden** (LUIS-Sicherheitsteam)
- Im weiteren Verlauf
  - Kompromittiertes System bereinigen (**Flatten & Rebuild**)
  - Ändern von gespeicherten / eingegeben **Zugangsdaten**
  - Meldung von **Datenschutzverstößen** gem. Art 33 DSGVO
- Danach:
  - Prävention

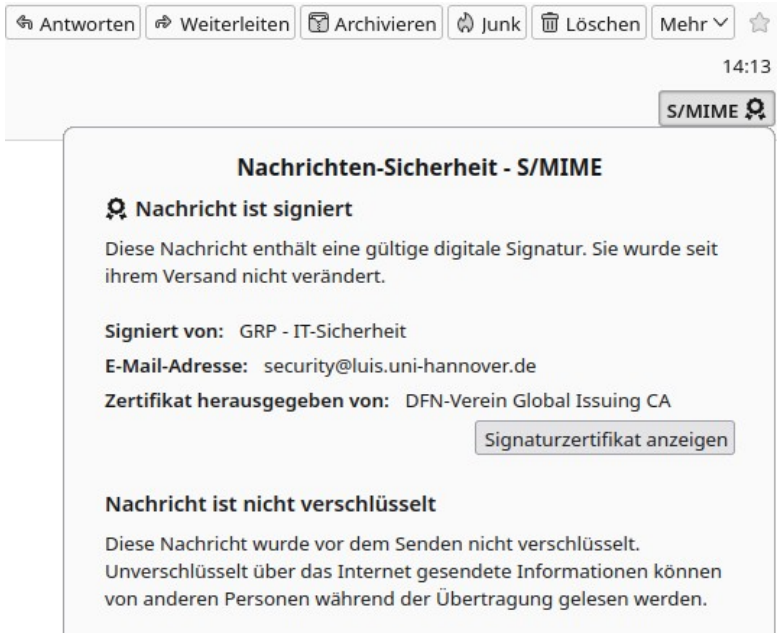
- Blick auf LUIS-Website:
  https://www.luis.uni-hannover.de/de/services/it-sicherheit/ernstfall

Best Practices Awareness

- **KeePassXC** + Browser-Plugin / Seafile
- Seafile / **Cryptomator**: Verschlüsselter Container in der Cloud
- Mail-Programm (z.B. Thunderbird) **Hauptpasswort** einrichten
- Account **ohne Admin-Rechte** (für tägliche Arbeit)
- **Virenschutz**
- Regelmäßige **Backup**s
- (Daten-/Zugangs-)Minimierung, **Need-To-Know**-Prinzip
- Geräte**verschlüsselung**
  (nur aktiv im ausgeschalteten Zustand, nicht bei zuklappen)
- Bitlocker & **TPM**
  - Empfehlung: TPM aus, Bitlocker-Passwort an
  - Falls TPM genutzt wird: zusätzlicher Authentifizierungsfaktor zwingend notwendig (min. erweiterter PIN)

Best Practices Awareness - S/MIME-Zertifikate

- Zuverlässige Möglichkeit der Verifizierung der Identität eines E-Mail-Senders
- Dienstliche E-Mail-Kommunikation soll mit digitaler Signatur erfolgen. (Genaueres im anschließenden Vortrag)
- Tipp: Nicht nur Mails, auch z.B. Git commits können signiert werden



Zusammenfassung

- Phishing(-Mails) bleiben aktuell
  - Insbesondere CEO-Frauds
  - Aber auch andere (kreativere) Maschen erwartbar
- Server-Software aktuell halten
- Schwachstellen-Scans mit OpenVAS
- Verhalten im Ernstfall
- Best Practices Awareness
- Materialien/Handreichungen:
  https://www.luis.uni-hannover.de/de/services/it-sicherheit

Fragen?