Leibniz Universität IT Services

Leibniz Universität Hannover

Aktuelle Sicherheitslage

LUIS-Sicherheitstag 14.02.2023

Inhalt

- Aktuelle Bedrohungen & Herausforderungen
  - Phishing
  - Passwort-Leaks
  - Weiteres
- Verhalten bei Erhalt von Phishing-Mails mit geleakter Kommunikation
- Maßnahmen im Ernstfall

Phishing

- Unterschiedlichste Formen
  - Mailpostfach
    - Zugang abgelaufen oder Verifikation nötig
    - Geblockte Mails, Mail-Speicher voll
    - Unberechtigte Logins → bitte prüfen!
  - **Maßnahmen**:
    - Löschen, nicht antworten, keine Login-Daten eingeben, keine Links anklicken
    - Ggf. **melden** (security@luis.uni-hannover.de und spam@luis.uni-hannover.de)
- Kurzfilm: Awareness
  https://www.luis.uni-hannover.de/de/services/it-sicherheit/praevention#c14933

Phishing – Beispiel Outlook Web App

Von: <unseriöse Mailadresse.dk>

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

Passwort-Leaks

- Hinweise auf geleakte Passwörter

- 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

Weiteres: DFN-CERT – Warnmeldungen

- Bots / Schadsoftware
  - Windows: Emotet, Quakbot, Zeus
  - Aber auch **Android**: AndroidBauts
- Configuration/Unrestricted access
- Attack/Virus in Mail (False Positives)

Weiteres / Kurz vermerkt

- Sicherheitshinweis: Krieg in der **Ukraine**
- Ausgenutzte Lücke in **vmware** (Ransomware)
- IT-Dienstleister **adesso** gehackt
- Vorfälle bei **deutschen Universitäten**
- Unzulässige **Mail-Programme**

Verhalten bei Erhalt von Phishing-Mails mit geleakter Kommunikation

- Beispiel: (Phishing-Link als Antwort auf Kommunikation)

Von: Max Mustermann Uni Hannover <phishing@gmail.com>
An: Erika Musterfrau <musterfrau@uni-hannover.de>
Betreff: Re: Vortragsreihe
Inhalt:

Hi!
Hier die Vortragsfolien:
<schadhafter Link>
Dateikennwort: <Kennwort>

<bekannte Kommunikation>

- Erkennen
- **Melden** (betroffene Person weiß evtl. noch nichts vom Vorfall)

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

Zusammenfassung

- Insgesamt keine größeren Vorfälle an der LUH
- **Phishing**(-Mails) bleiben aktuell
- **Passwort-Hygiene** beachten
  - Keine Mehrfachnutzung
  - Passwort-Manager
- Verhalten im **Ernstfall**

Fragen?