Skript zum Vortrag

Sicherheit im Netz, Passwörter & Co.

Lunch & Learn vom 25.8.2022

Inhaltsverzeichnis:

Datum	24.8.2022
Inhalt	Sicherheit im Netz, Passwörter & Co.
Version	1.1
Autor	Bernhard Karlen
Review	Nobody

1 Wer bin ich

- Bernhard Karlen
- Wirtschaftsinformatiker mit eidg. Fachausweis
- Buchhalter mit eidg. Fachausweis
- 12 Jahre Leiter IT Bodenschatz AG
- Hobby Kitesurfer
- Genügend Informationen für einen Angriff per Mail

2 Umfang

- Versicherungen
- Sicherheit im Netz
  - Voraussetzungen
  - Virenscanner
  - Sichere Dateien
  - Angriffsmuster
  - Wie erfolgt ein Angriff
  - Gefährliche E-Mails - Grundsätze
  - Gefährliche E-Mails erkennen
  - Surfen im Netz
  - Pishing mit SMS
- Passwörter & Mehrfaktor Authentifizierung
  - Passwort Links
  - Sichere Passwörter bilden
  - Passwörter ablegen
  - Passwörter aktualisieren
  - Was macht Logindaten sicher
  - Welche 2FA/MFA gibt es
  - Welche Logins sollten 2FA/MFA geschützt werden
  - Passwörter bilden
  - Passwörter aktualisieren
  - Passwörter ablegen

3 Heute kein Thema

- Datensicherung (Office 365, iCloud, pCloud, Harddisk, NAS)
- Internetverbindungen
  - Unverschlüsselt (Freies WLAN ohne Passwort)
  - Verschlüsseltes WLAN
  - VPN
  - Natelverbindung, Heimnetz, Firmennetz
- E-Mail-Verschlüsselung SSL
- Datenschutzeinstellungen von LinkedIn, Facebook, Instagram
- Gefahren des USB-Sticks, Betrugsvarianten
- Festplattenverschlüsselung mittels Bitlocker
- Kommunikation Messenger (WhatsApp, iMessage, Signal, Threema)

4 Sicherheit im realen Leben

- Haustüren
  - Einfache Haustüren, Einbruchsschutz < 1 Minute
  - Einbruchssichere Türen > 30 Minuten
- Fenster
  - Normale Fenster sind < 1 Minute geöffnet (Stein fliegt durch die Scheibe)
  - Fenster mit Sicherheitsglas > 20 Minuten
- Abschliessbare Fenster
  - Bei gekipptem Zustand und Sicherheitsglas teilweise < 1 Minute
  - Bei geschlossenem Fenster und Sicherheitsglas > 30 Minuten
- Sicherheitskameras / Alarmanlage
  - Sie verhindern keinen Einbruch - sind aber wegen der Verfolgbarkeit eine zusätzliche Hürde für Einbrecher
- Autonummernverzeichnis
  - Autonummer im Verzeichnis sperren (Beispiel Gotthardtunnel)
- **Merke** Sicherheitsmassnahmen verhindern keinen Einbruch, sie erhöhen die Einbruchszeit. Im Idealfall ist man dann uninteressant

5 Warum eigentlich

- Verlust von Geld
- Verlust von Daten
- Reputationsschaden
- Bei Firmen auch «überlebenswichtig»

6 Versicherung

- Inzwischen bieten die meisten Versicherungen auch Cyber Versicherung für Private und Firmen an
  - Online-Konten & Kreditkarten
  - Online-Mobbing & Urheberrechte
  - Online-Shopping
  - Datenrettung, Virenentfernung & IT-Assistance

7 Sicherheit im Netz

7.1 Voraussetzungen

- Windows 10 oder 11, Mac OS X
  - immer mit Passwortschutz
  - immer als Benutzer und nicht als Administrator einloggen (Ausnahme Installationen)
  - Windows, Mac OS X und die verwendeten Programme laufend updaten
- Natel und Tablets
  - Natel und Tablets **immer mit 6-stelligem sicheren Code** versehen
  - Face ID ist besser als Fingerprint und als Code (aber Achtung beim Schlafen)
  - Natel und Tablets laufend updaten (bei billigen Geräten werden nur 2 Jahre Sicherheitsupdates geliefert)

7.2 Braucht es einen Virenscanner

- Mac OS X ☞ Nein
- Windows 10 / 11 ☞ Ja
- «Microsoft Defender» ist kostenlos und gut
- Für unsichere Benutzer ungenügend
- Grösster Fehler: abgelaufene Virensoftware

7.3 Sichere Dateien

- Es gibt keine sicheren Dateien, weil jede unsichere Datei als sichere getarnt werden kann!
- Eher als sicher gelten
  - xlsx, docx, pptx, pdf, jpg, tiff, gif
- Nicht sicher sind
  - xls, doc, ppt (viele Verschlüsselungen werden mit diesen Dokumenten initiiert)
- Gefährliche Dateien sind
  - exe, com, bat, reg, vbs, html
- Merke: Alle im Internet gelandenen Programme können böse sein

7.4 Angriffe

- Angriffe per Mail
  - Ransomware Verschlüsselungstrojaner oder Erpressungssoftware
  - Phishing Ziel des Betrugs ist es z.B. an persönliche Daten eines Internet-Benutzers zu gelangen
  - Trojaner Als gutes Programm getarntes Schadprogramm
  - Spam / Junk unerwünschte Werbemails
  - Virus Schadprogramm für Computer, selbstverbreitend, mittels Dateien, Bootsektoren
  - Würmer Schadprogramm, selbstverbreitend, ohne Dateien, Bootsektoren
  - Malware Bösartige Software
  - Spyware Schnüffelsoftware

- Webangriffe
  - SQLinjection Ausführung von bösartigem SQL Code
  - Ddos Unter (Distributed Denial of Service) versteht man einen Angriff auf Systeme mit dem erklärten Ziel, deren Verfügbarkeit zu stören
  - CodeInjection Schadcode einschleusen durch Ausnutzung einer Schwachstelle
  - BufferOverflow BufferOverflow führt dazu, dass der Speicher eines Programms überfüllt wird und dadurch etwas schädliches passieren kann
  - Brute-Force Probiert alle Passwort Kombinationen durch
- **Merke:** wir können mit unserem Verhalten viel gegen Angriffe tun

7.5 Wie erfolgt ein Angriff

- 95 % der Angriffe erfolgen per E-Mail
- Die meisten Angriffe passieren vollautomatisiert
- Alle Sicherheitslücken sind im Internet **öffentlich** zugänglich und werden umgehend in Angriffssoftware integriert (teilweise auch bevor sie öffentlich sind)
- Angriffssoftware kann gemietet werden
- Es gibt Virenbaukästen um sich Viren selber zu bauen
- Kreditkartennummer können gekauft werden
- Login Informationen können gekauft werden
- E-Mail-Adressen können gekauft werden
- Nur bei gezielten Angriffen und/oder entsprechender Komplexität übernehmen Menschen den Angriff
- In einigen Ländern sind Hacker geachtete und reiche Personen (solange sie nur im Ausland angreifen)

7.6 Gefährliche E-Mails

- Öffnen sie nur die wirklich notwendigen Mails
- Öffnen sie nur die wirklich notwendigen Anhänge
- Tippen sie den Link ab anstatt den im Mail verwendeten Link zu verwenden
  (Wenn sie die UBS auffordert das Passwort zu ändern, dann öffnen Sie den Browser und tippen www.ubs.com manuell ein)
- **Merke:** Wichtige und richtige Mails werden auch mehrmals verschickt
- **Merke:** Beim geringsten Zweifel beim Absender anrufen (aber nicht mit der Telefonnr. im E-Mail)

7.7 Gefährliche E-Mails erkennen

- Wie erkennen wir Angriffsmails?
  - Keiner E-Mail-Adresse vertrauen (die Absender E-Mail-Adresse kann gefälscht werden)
  - Schreibfehler beachten
  - Fremdsprachen beachten
  - Falsche Logos beachten
  - Der Name fehlt in der Anrede
  - Dringender Handlungsbedarf
  - Sie sollen Daten eingeben, ein Formular ausfüllen oder eine Datei öffnen
  - Achtung bei
    - DHL, UPS, Post
    - Postfinance und Banken
    - Paypal, Kreditkarten
    - Gewinnausschreibungen, Lottogewinnen, Gewinnversprechen
    - Medikamentenwerbung, Rückvergütungen,
    - etc.
  - Achtung auch vor «Social Engineering» - wie viele Daten von Ihnen sind im Internet bekannt?

7.8 Surfen im Netz

- Nur auf Seite mit https:// Surfen (http:// kann abgehört werden)
- Als Startseite www.startpage.com einrichten
- Keine Werbung anklicken
- Nur auf einem aktualisierten PC mit aktualisiertem Browser surfen
- Alle Informationen, welche im Internet erfasst werden, können verbreitet und verkauft werden (z.B. Übersetzungsdienste etc.)
- **Merke:** Vertrauliche Informationen dürfen im Internet nie erfasst werden

7.9 Pishing mit SMS

- Keiner Telefonnr. vertrauen (die Absender Telefonnr. kann gefälscht werden)
- Keine Links anwählen (dadurch kann man ein kostenpflichtiges Abo abschliessen)
- Keine Kreditkartendaten angeben

Merke: Beim geringsten Zweifel beim Absender anrufen (aber nicht mit der Telefonnr. im SMS)

8 Interessante Links

- Wurde mein Account schon gehackt?
  - https://haveibeenpwned.com
  - https://sec.hpi.uni-potsdam.de/ilc/
  - https://checktool.ch
- Beispiele von im Netz bekannten Informationen
  - https://swissleak.ch/
- Passwortcheck (aber nicht mit eigenen Passwörtern)
  - https://www.passwortcheck.ch/
- Wem folge ich bei Youtube?
  - The Morpheus Vlogs
- Nationales Zentrum für Cybersicherheit (früher Melani)
  - www.ncsc.admin.ch/ncsc/de/home.html
- Vorträge wie Hacker (Cracker) vorgehen
  - Mathias Gut, Digicomp
  - T-Systems Webinar
- Wie erkenne ich Angriffsmails
  - www.verbraucherzentrale.de
- Wie funktioniert Hacken
  - BYTEthinks

9 Passwörter & Co.

9.1 Sichere Passwörter bilden

- Anforderung
  - Mindestens 12 Stellen

	Beispiel einfach			Beispiel komplex		
Stellen	**Passwort**	**Rechenzeit**		**Passwort**	**Rechenzeit**	
8	OberwilBL	9	Minuten	F9j4lk3%	1	Tag
10	PippiKakka	22	Minuten	F9j4lk3%gz	39	Jahre
12	Ichbinsuper!	7	Monate	F9j4lk3%gz&f	402'157	Jahre
16	Ichbinsupercool%	193'759	Jahre			

  - A a 0 9 % #
  - Keine Wörter aus dem Duden
- Hilfestellung
  - Glaubenssätze oder freie Sätze
    - Ich finde Euch nett und bin froh, dass ihr keine Fragen stellt => IfEnubfdikFs?
    - Es geht mir mit jedem Tag immer besser und besser => EgmmjTibub!!
  - automatisch generieren lassen
  - Sonderzeichenproblem bei anderen Tastaturen
  - Sätze Bilden und immer nur 3 Buchstaben vom Wort nehmen
    => IchKanEsJaPro%

9.2 Passwörter ablegen

- Im Kopf
- Passwort Applikationen
  - Dashline (50 Passwörter auf einem Gerät kostenlos)
  - Apple iCloud Schlüsselbund (Face ID geschützt) für iPhone User
  - Bitwarden
  - UBS App (falls Sie ein USB Konto haben)
  - Keepass
  - Keeper Security, 1Password, Bitdefender Passwort Manager
- Auf Papier (versteckt in der Bibel auf Seite nn)
- Aber nicht im Word, Excel, Notizen (auch nicht wenn diese Passwortgeschützt sind)

9.3 Passwörter aktualisieren

Ideal wäre Wichtige Passwörter 1 x pro Jahr zu aktualisieren

9.4 Was macht Logindaten sicher?

- Unterschiedliche Passwörter
- Kein erkennbares System in den Passwörtern
- Länge und Komplexität des Passworts
- 2FA/MFA (via SMS, Authenticator, etc.)

9.5 Welche 2FA/MFA gibt es

- Passwort
- Natel per SMS
- Authentifizierungs-App (Recovery Codes) / Token
- Biometrische Daten (Face-ID, Fingerprint)
- Keys mit Fido2, Youbekey

9.6 Besonders wichtige Logins (2FA/MFA)

- Computer als Benutzer benutzen und mit Passwort schützen. Beim Surfen werden viele Passwörter gespeichert.
- Passwort vom Passwortverwaltungsprogramm → Jackpot
- E-Mail Konten → Passwort Recovery → Jackpot
- Microsoft, Apple, Google Accounts
- Banken, Kreditkartenfirmen, Paypal
- Online Shopping → Lieferung gegen Rechnung, Lieferadresse als Post 24 Schalter
- Aber auch LinkedIn, Facebook, Instagramm