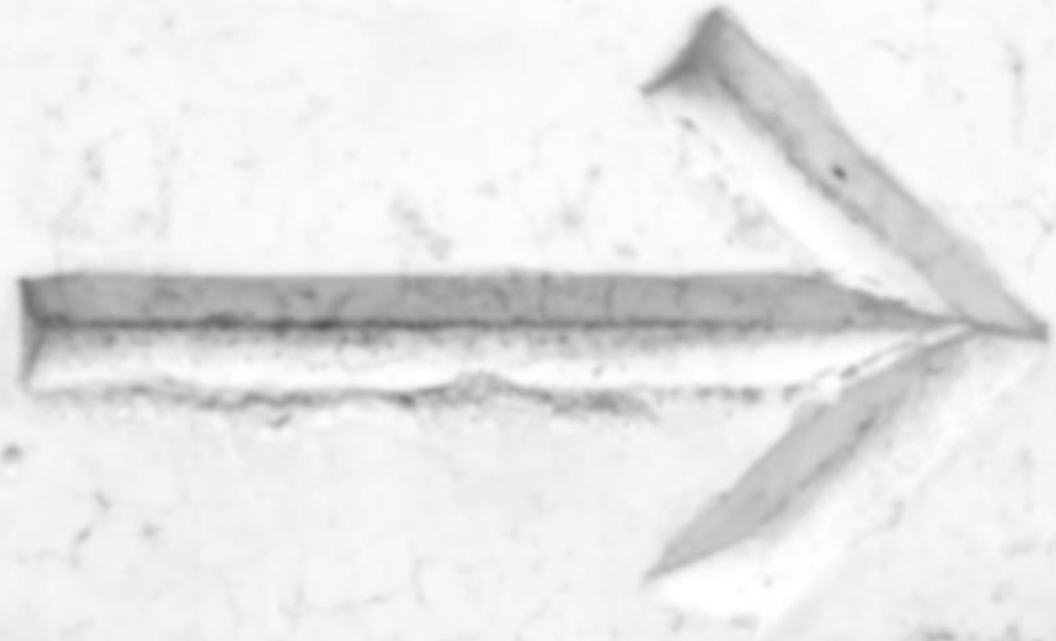
MICROMATA

Wie Hacker Systeme knacken

…. und wie Sie sich davor schützen können

AGENDA



- BadUSB Angriff
- Phishing Angriff
- Evil Twin + WPA Bruteforce
- Passwortmanager

BADUSB

Modul, welches sich als Tastatur ausgibt

Viele Betriebssysteme haben keine Standard –Protection,
um den Unterschied zwischen BadUSB und Tastatur zu erkennen

BadUSB führt Befehle auf Zielcomputer aus und ermöglicht so bestenfalls die Übernahme des kompletten Systems

Besonders effektiv in Kombination mit Social Engineering

WIE KANN ICH MICH SCHÜTZEN?

CHECKLISTE:

- ☑ Computer immer sperren, wenn man den Arbeitsplatz verlässt
- ☑ Clean Desktop Policy
- ☑ Niemals unbekannte USB Devices „ausprobieren“
- ☑ Automatische Bildschirmsperre einrichten
- ☑ Ggf. Antivirus mit Erkennungs-Feature für Peripherie-Angriffe

PHISHING ANGRIFF

Websitemanipulation:
User-Eingaben abgefangen und an den Angreifer übermittelt

Ziel: Account-Zugänge, System-Passwörter
oder sensible Informationen

Phishing = Social Engineering: menschliche Kurzschlussreaktionen provozieren,
um emotionale Reaktionen auszulösen

Künstliche Drucksituation:
Opfer hat nicht viel Zeit zum Nachdenken

WIE KANN ICH MICH SCHÜTZEN?

CHECKLISTE:

- ☑ Jede Form der Kommunikation immer im Kontext bewerten
- ☑ Bei Aufforderungen Änderungen im Konto zu tätigen immer manuell im Browser den jeweiligen Dienst öffnen und das Vorhaben validieren
- ☑ Passwortmanager: Falls ein Passwort gephisht wurde, kann es einfach gewechselt werden und keine weiteren Zugänge sind betroffen

EVIL TWIN

WLAN Router, der einen anderen Router imitiert

Das Signal des Ziel-Routers wird meistens unterdrückt, so dass nur noch der Evil Twin zu sehen ist

Geräte, welche mit dem gewohnten Router kommunizieren wechseln ihre Verbindung zum Evil Twin

gleicher WLAN-Schlüssel (WPA Key) wird beim bösen Router zum Authentifizieren verwendet

Der Schlüssel befindet sich in einem “Handshake“ Fragment

Dieses ist zwar verschlüsselt, kann aber gebrochen werden, wenn das WLAN Passwort zu schwach ist

WIE KANN ICH MICH SCHÜTZEN?

CHECKLISTE:

- ☑ Das Standard Passwort des Routers ändern
- ☑ Mit einem Passwort Generator ein neues Passwort erstellen
- ☑ Das Passwort sollte mindestens 20 Stellen haben
- ☑ Das Passwort (WPA Key) kann in einem QR Code abgespeichert werden, um Freunden/Familie einen sicheren Zugang gewährleisten zu können

PASSWORT MANAGER

Jeder Zugang hat ein einzigartiges, KRYPTISCHES PASSWORT

Eine ZENTRALE ABLAGE für alle Passwörter und Zugänge

Ein MASTER-PASSWORT für alle Zugänge, Accounts, Netzwerkverbindungen

+ Sicheres Verwalten von Zugängen und Accounts

+ Erhöhung der Netzwerksicherheit (hinsichtlich Authentifizierung)

+ Ohne Kenntnis eigener Passwörter können sie nicht weitergegeben werden

AUSBLICK UND KONTAKT

Dominique Wüst

Sergej Michel

Jens Becker

Matthias Altmann

anfrage-security@micromata.de micromata.de/it-services

FOLGEVERANSTALTUNGEN

- 03.04.2023 | 17.00 Uhr | Online
  Datensicherung / Backup
- 03.05.2023, 17.00 Uhr | Online
  Sicher im Homeoffice
- 25.05.2023 | 10.00 Uhr | Workshop
  Verhalten im Schadensfall / Notfallplanung

MICROMATA

Vielen Dank

MICROMATA GMBH

Marie-Calm-Straße 1-5

34131 Kassel

Germany