

The background features a vertical split between a dark navy blue left half and a light gray right half. Concentric, thin, dark gray arcs originate from the center of the split and curve upwards and outwards, spanning across both halves. A solid yellow horizontal line is positioned on the dark left side, extending from the left edge towards the center.

Cyber Awareness

Agenda



Einleitung



Angriff
Angreifer
Werkzeuge
Leaks



Technische
Grundlagen



Schutzkonzepte
Flyover



Ich bin am „Haken“
– was jetzt?



Wer bin ich?

- M.Sc. Digitale Forensik
- Seit 2022 bei der Stawa BS tätig.
- Seit Mitte 2024 Leiter Dezernat Digitale Kriminalität bei der Stawa BS.

Links, um Informationen zu Cyber Awareness zu erhalten:

[BSI](#)

[BACS](#)



Cyber Awareness – wer braucht das?

- Seit einigen Jahren sind mehr oder weniger alle von uns digital präsent oder digital konsumierend unterwegs.
- Damit sind alle von uns für jeden potentiellen Täter auf diesem Planeten erreichbar.
- Heute ist jede und jeder ein mögliches Ziel.
- Wurde das Ziel zum Opfer, kann der Täter dieses für kriminelle Handlungen als Strohmann verwenden oder sich auf dessen Kosten bereichern.
- Ob man ein Opfer wird, kann man beeinflussen.



Angriff und Angreifer

- Was ist ein Angriff?
- Wo und was ist der Angreifer?
- Warum ich?



- Erlangte Identitäten
 - Private Daten
 - Zugangsdaten
 - Software
 - Hardware
-
- Klassiker: Ein gefundener USB-Stick wird angesteckt, um zu sehen, wem er gehört – genau das ist die Falle.



Leaks – jedem bekannt, nur nicht den Betroffenen

- Woher haben die Darknet-Marktplätze ihre Ware?
- [Liste zu bekannten Datenleaks.](#)
- Wozu kann das führen?



Im Internet spurlos unterwegs

- Jede Browsernutzung hinterlässt einen digitalen Fingerabdruck:
 - <https://amiunique.org/>
 - <https://coveryourtracks.eff.org/>
 - <https://privacy.net/analyzer/#accordion>
- Deshalb:
 - Torbrowser (den „Normalen“ auch, wenn möglich) auf Englisch betreiben.
 - Keine Fenstergrößenänderungen verwenden.
 - Im Torbrowser über das Menü regelmässig new identity erstellen.
 - Immer einen VPN oder Bridges verwenden (bridges.torproject.org), bei VPN-Nutzung einen VPN-Onion-Server verwenden.
 - Durch Klick auf das Schloss-Symbol in der Adressleiste den Verbindungsverlauf kontrollieren.
 - Sicherheitseinstellungen anpassen.



OSINT – das kann jeder, also auch die „Falschen“

- OSINT steht für Open Source Intelligence – hier geht es um sicherheitsrelevante Informationen, die frei verfügbar sind (Soziale Netzwerke jeglicher Art, das Web an sich)
 - [Maltego](#)
 - <https://inteltechniques.com/tools/index.html>
 - Achtung: hier gibt es „gefährliche“ Seiten:
 - [OSINT Framework](#)
- Timemachine des Internets: zeigt, was wer wann mal war: [Wayback](#)
- Suchmaschinen bedienen und einschätzen lernen: nicht jede Suchmaschine zeigt dasselbe! Vgl. dazu [Google](#) und [Bing](#) mit der Suche „Sopka Veracrypt“.
- IPs oder Domains auflösen und Rückschlüsse ziehen: [Talos](#).
- Leak-Databases dann und wann abfragen, z.B. hier: [Hasso-Plattner-Stiftung](#).
- Digitalen Fingerabdruck des Browsers vermeiden (wie im Darknet): [Privacy](#).



WLAN, Bluetooth, AirDrop, Hotspot – unterschätzte Gefahr

- Der Klassiker: Sync-Knopf für WPS am Router und die Party mit Fremden in der Wohngemeinschaft. Immer deaktivieren!
- Bluetooth: Einfallstor für Spyware am Smartphone (Android-Welt).
- AirDrop: Einfallstor für Spyware am Smartphone (Apple-Welt), wenn die Option „alle“ aktiviert ist.
- Hotspot: Datenverkehr kann vom Anbieter mitgeschnitten werden. Relativ unproblematisch, solange man nur surft und nur https verwendet.



Welche Malware ist wirklich gefährlich – und wie schütze ich mich davor?

- Spyware, die Kontakte und Chats ausliest, Selfies und Filmaufnahmen wegspeichert, Mikrofon und Kamera einschaltet.
- Auf jede Kamera gehört ein mechanischer Schutz.
- Keylogger schreiben Tastatureingaben (z.B. die vom Kennworttresor) mit.
- Keine Software nutzen, deren Herkunft unklar ist. Nie.
- Nach wie vor ist der Windows Defender Antivirus für die meisten Fälle ausreichend – der Faktor Mensch ist das grosse Problem.



Schutzkonzepte – Flyover

- Bequemlichkeit im falschen Moment ist toxisch.
- Man muss das eigene Konsumverhalten anpassen.
- Es braucht die Bereitschaft, für Informationen zu bezahlen.
- Daten sind immer als privat zu betrachten.
- Privates darf **nie** publiziert werden.
- Bestimmte Soft- und Hardwarekombinationen möglichst meiden.



Werbung und Werbeblocker

- Wenn etwas im Web nichts kostet, bin ich in 99% der Fälle das Produkt. Also meine Daten, mein Verhalten sind das Produkt und werden an fremde Dritte verkauft.
- Die über mich gesammelten Informationen können in falsche Hände gelangen und gegen mich verwendet werden.
- Kein Datensammler wird freiwillig publizieren, dass er gehackt wurde.



Kennwörter und 2FA – Teil 1

- Wie baue ich eine wirklich handhabbare Kennwort-Logik auf?
- So nicht: [Handelsblatt-Artikel von 2019](#)
- So auch nicht: [Kundendaten eines Kennwortmanagers gestohlen](#)
- Wenn es wirklich nicht ohne Kennwortmanager geht, dann etwas wie [Bitwarden](#) verwenden.



- Vorschlag:
 - Basis ist ein Merksatz.
 - Dazu kommt eine vierstellige Zahl (gerne länger).
 - Sowie ein oder zwei Sonderzeichen, die NLS-kompatibel sind.
 - Bestimmte Buchstaben werden getauscht, andere grossgeschrieben.
 - Es geht um die Entropie und die Anzahl der Zeichen!



- Beispiel:
 - Merksatz: „Das ist mein Kennwort für X seit diesem Vortrag“, davon erst alle Anfangsbuchstaben verwenden.
 - Ergibt „DimKfXsdV“.
 - Eine Zahl dazu nehmen (vorne, hinten, mittendrin): KEINE, die in den sozialen Medien kursiert (Geburtsjahr, Jahr, in dem das Studium beginnt usw.), hier beispielhaft 2026 folgend angefügt.
 - Ergibt „DimKfXsdV2026“.
 - Sonderzeichen (z.B. das #) dazu nehmen:
 - Ergibt „DimKfXsdV2026#“.
 - Das X ersetzen durch z.B. R bei Ricardo, E bei eBay, P bei Pensionskasse usw.



Kennwörter und 2FA – Teil 4

- Im Merksatz wird für jeden Einsatzzweck mindestens ein Wort getauscht (besser zwei). Wichtig!
- Dieses Kennwort wird nahezu immer von dem jeweiligen Anmeldesystem akzeptiert werden, es hat Sonderzeichen, Ziffern, Gross- und Kleinschreibung und eine akzeptable Länge.
- Diese Entropie ist viel zu hoch, um in einer Hashwert-Datenbank aufgefunden zu werden.
- Entscheiden, welche Dienste 2FA haben müssen: wenn der Dienst das nicht anbietet, diesen nicht nutzen.
- Wichtig: wo möglich, nur die Kombination von Kennwort und 2FA nutzen, [siehe dazu diesen Link](#).



Werkeinstellungen von Hard- und Software korrigieren

- Immer noch ist sehr viel Hardware in der Grundeinstellung „offen“.
- Oft ist auf der Unterseite des Internetzugangsgesetzes das Kennwort aufgeklebt. Nach einem Hardwarereset gilt dieses wieder.
- Immer eine Firewall verwenden, idealtypisch auf eigener Hardware (nicht beim Hoster) auf etwas wie z.B. [pfSense](#) (technisch sehr anspruchsvoll).
- Das „richtige“ Betriebssystem hält mich aus der „Schusslinie“.
- Updates jeglicher Art sind immer so zeitnah wie möglich durchzuführen.
- Malwareschutz immer aktuell halten.
- Schon länger ist auch der Fernseher ein Internetbrowser – auch ihn in die Schutzkonzepte einbeziehen.

Was gebe ich wann wem heraus?

- Zuerst eine Priorisierung durchführen: welcher digitale Dienst macht mein Leben wirklich angenehmer.
- Dann überlegen, ob man bei der Registrierung nicht mit Fake-Daten arbeiten kann.
- Beispiel: Fitbit wurde für ca. 2,1 Milliarden \$ an [Google verkauft](#).
 - Warum bezahlt Google so viel für einen Wearable-Hersteller?
 - Antwort: Wegen der Daten. Bei Fitbit werden alle Daten an den Hersteller weitergeleitet, man kann diese nur über einen Webbrowser einsehen.
 - Nach einer [Übergangsfrist](#) muss ein Fitbit-Anwender einen Google-Account haben.



Wie kann ich ausweichen?

- Über E-Mail-Anbieter wie z.B. [Proton Mail](#).
- Über VPNs wie z.B. ProtonVPN.
- Über eine Natelnummer und E-Mail-Adresse nur für Registrierungen (Twitter, Facebook, WhatsApp), die sonst für nichts genutzt wird.
- Mit durchdachter Verwendung von Unterhaltungsmedien wie Spotify und Netflix.
- Privates nur mit [Threema](#) oder iMessage (nur bei Apple verfügbar) versenden.
- Bestimmte Hardware (Natels) meiden. Siehe [Krait und Android](#).
- Bestimmte Accounts sehr vorsichtig nutzen (Google, Microsoft).



Ich bin am „Haken“ – was jetzt?

- Auf einem „vertrauenswürdigen“ Computer, Smartphone oder Tablet seine E-Mail-Kennwörter ändern.
- Erstattung einer Strafanzeige. Zeitnah!
- Sicherstellen, dass der Computer, das Smartphone oder das Tablet, mit dem man arbeitet, nicht von einer Malware infiziert ist.
- Ändern der Zugangsdaten aller weiteren Accounts, insbesondere der Kennwörter.
- Information aller Stellen, bei denen man einen Account hat. Dies dokumentieren bzw. bestätigen lassen.
- Information des Arbeitgebers, der Kollegen, des **engeren** und weiteren sozialen Umfelds, der Kunden und Lieferanten sowie der Behörden (Soziales, Steuern ...).