its VERMITTELT TECHNOLOGIE.

InfoGuard SWISS CYBER SECURITY

«CYBER SECURITY IN DER PRAKTISCHEN UMSETZUNG»

WIE SCHÜTZE ICH MEIN UNTERNEHMEN EFFEKTIV UND WIE VERHALTE ICH MICH IM ANGRIFFSFALL?

14. Juni 2021

«Cyber Security ist vielschichtig. Ein zuverlässiger Schutz Ihrer Werte – Informationen, Mitarbeiter, Prozesse und Infrastruktur – lässt sich nur über einen strukturierten, methodischen Sicherheitsprozess erreichen.»

Franco Cerminara
Chief Consulting Officer, InfoGuard AG
Tel. +41 41 749 19 62
Mob. +41 79 308 83 16
franco.cerminara@infoguard.ch

INFOGUARD –
Der Schweizer Cyber Security Experte

InfoGuard
SWISS CYBER SECURITY

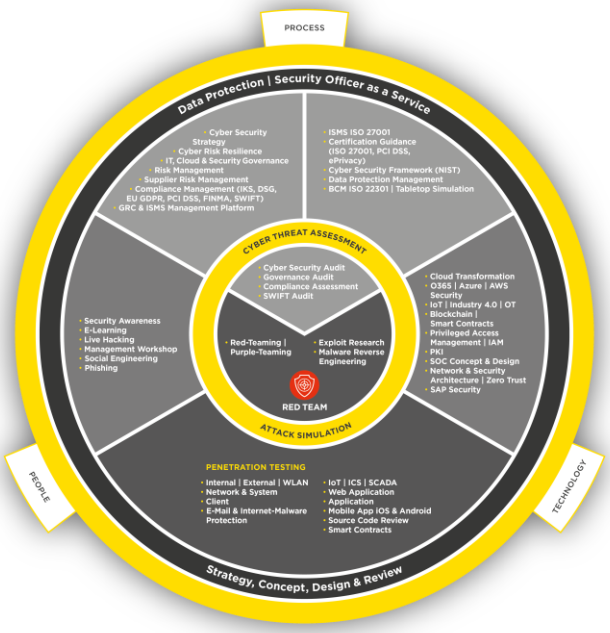
150+ SICHERHEITSEXPERTEN IN ZUG UND BERN

100% IM BESITZ DES SCHWEIZER MANAGEMENTS

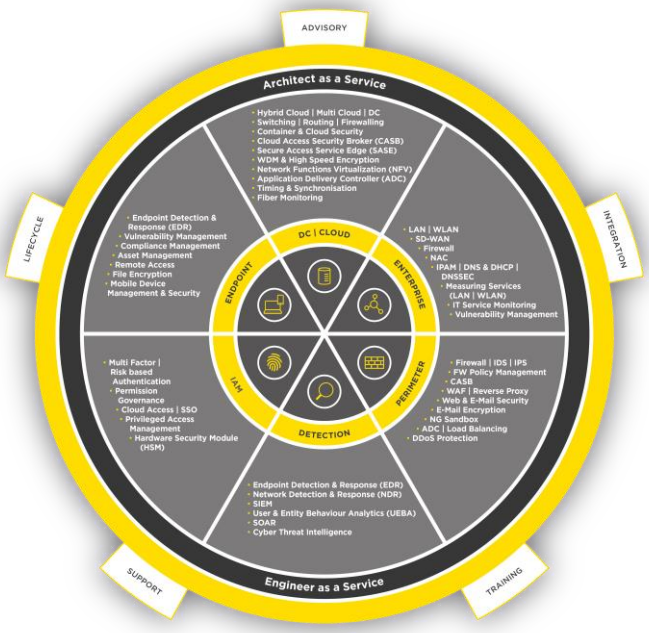
ISO 27001 ZERTIFIZIERT

SWISS CDC CYBER DEFENCE CENTER

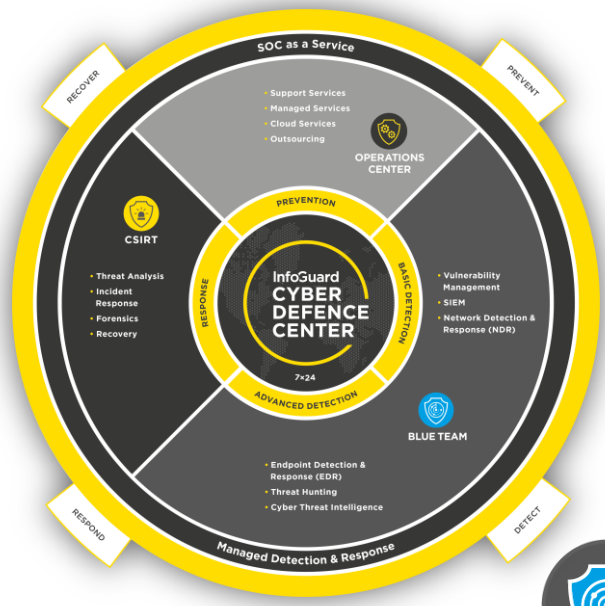
SECURITY CONSULTING SERVICES



NETWORK & SECURITY SOLUTIONS



CYBER DEFENCE SERVICES



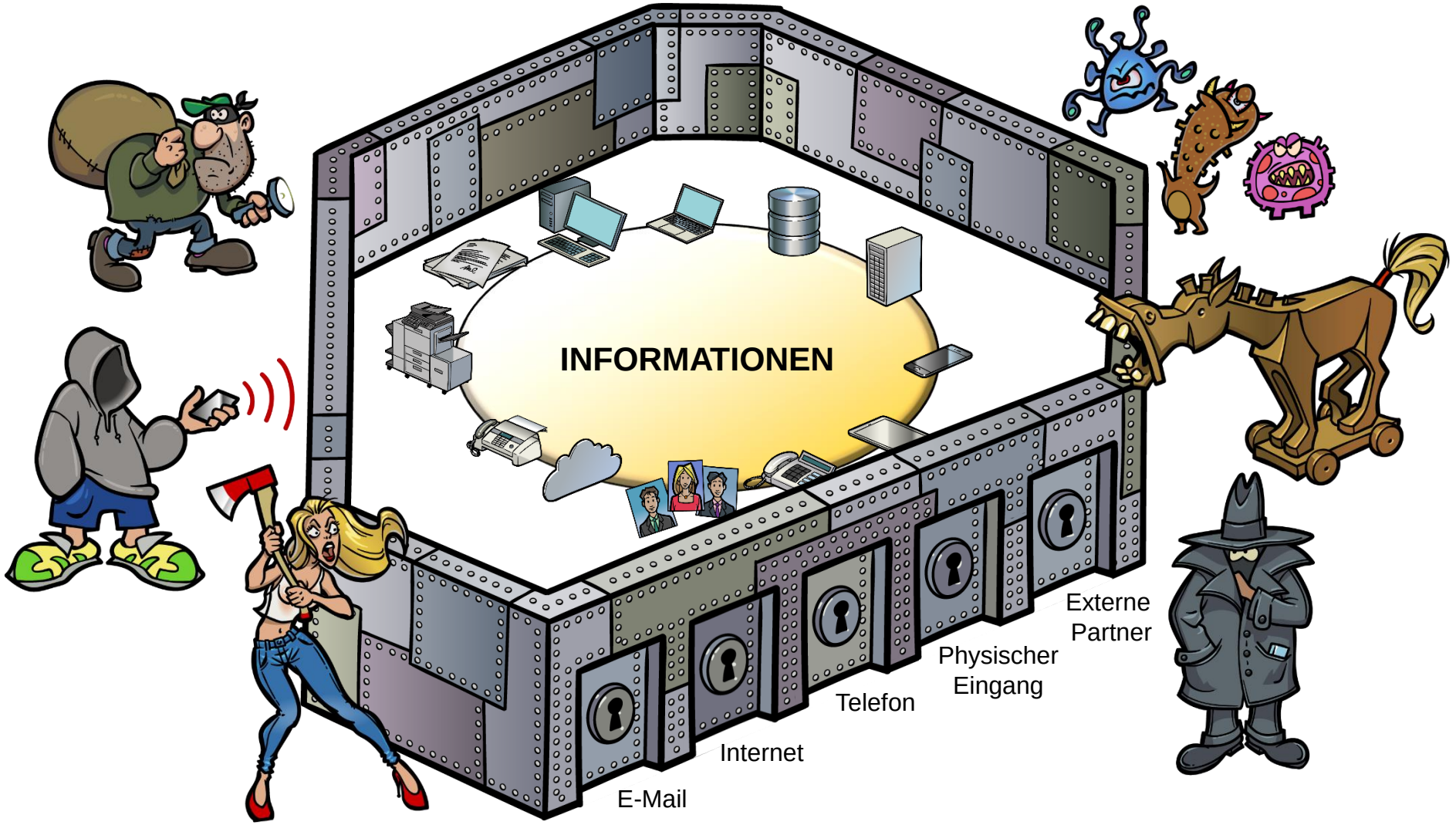
InfoGuard
RED TEAM

InfoGuard
BLUE TEAM

Agenda

- Begrüssung
- Cyber Security ist mehr als eine hohe IT-Sicherheitsmauer
- Cyberkriminalität ist Realität
- Wie schütze ich mein Unternehmen effektiv und wie verhalte ich mich im Angriffsfall?
- Q&A

Cyber Security ist mehr als eine hohe IT-Sicherheitsmauer



Cyberkriminalität ist Realität!

cash Informieren Investieren Diskutieren Depot eröffnen

Startseite > Informieren > News > Börsen Ticker > FuW: Siegfried-Halbjahresergebnis wird Spuren von Hackerangriff zeigen

FuW: Siegfried-Halbjahresergebnis wird Spuren von Hackerangriff zeigen

Seite teilen

Beim Pharmazulieferer Siegfried

Cyber-Sicherheitsvorfälle nehmen in einem alarmierenden Tempo zu und können tiefgreifende Auswirkungen auf das tägliche Funktionieren von Gesellschaft und Wirtschaft haben, sowohl online als auch offline…

Handelsblatt

IT-DIENSTLEISTER

Sabotageangriff legt Onlinebanking bei mehr als 820 Banken lahm

Angreifer haben Rechenzentren des IT-Dienstleisters der Volks- und Raiffeisenbanken mit Datenanfragen überflutet. Sensible Daten seien jedoch nicht in Gefahr gewesen.

Netzwerkverbindungen unterbrochen und sämtliche IT-Systeme einer vertieften Untersuchung unterzogen worden.

Dabei handelte es sich um eine sogenannte "Ransomware"-Attacke, bei welcher die Hacker Daten verschlüsselten und so den Zugriff des Unternehmens darauf blockierten, wie Gehler gegenüber der FuW bestätigte. Siegfried gebe aber keinen Kommentar ab, ob ein Lösegeld bezahlt wurde, um die Blockade aufzulösen.

Wie lange die vollständige Wiederherstellung brauche, konnte Gehler gegenüber der FuW nicht sagen. Priorität hätten die Produktionsanlagen. Geschäftsmail und Telefon hätten am Donnerstagmorgen noch nicht funktioniert. Immerhin verfüge Siegfried über Backups der Software, was den Wiederherstellungsprozess beschleunigen sollte.

Ausgewählte Produkte auf Siegfried

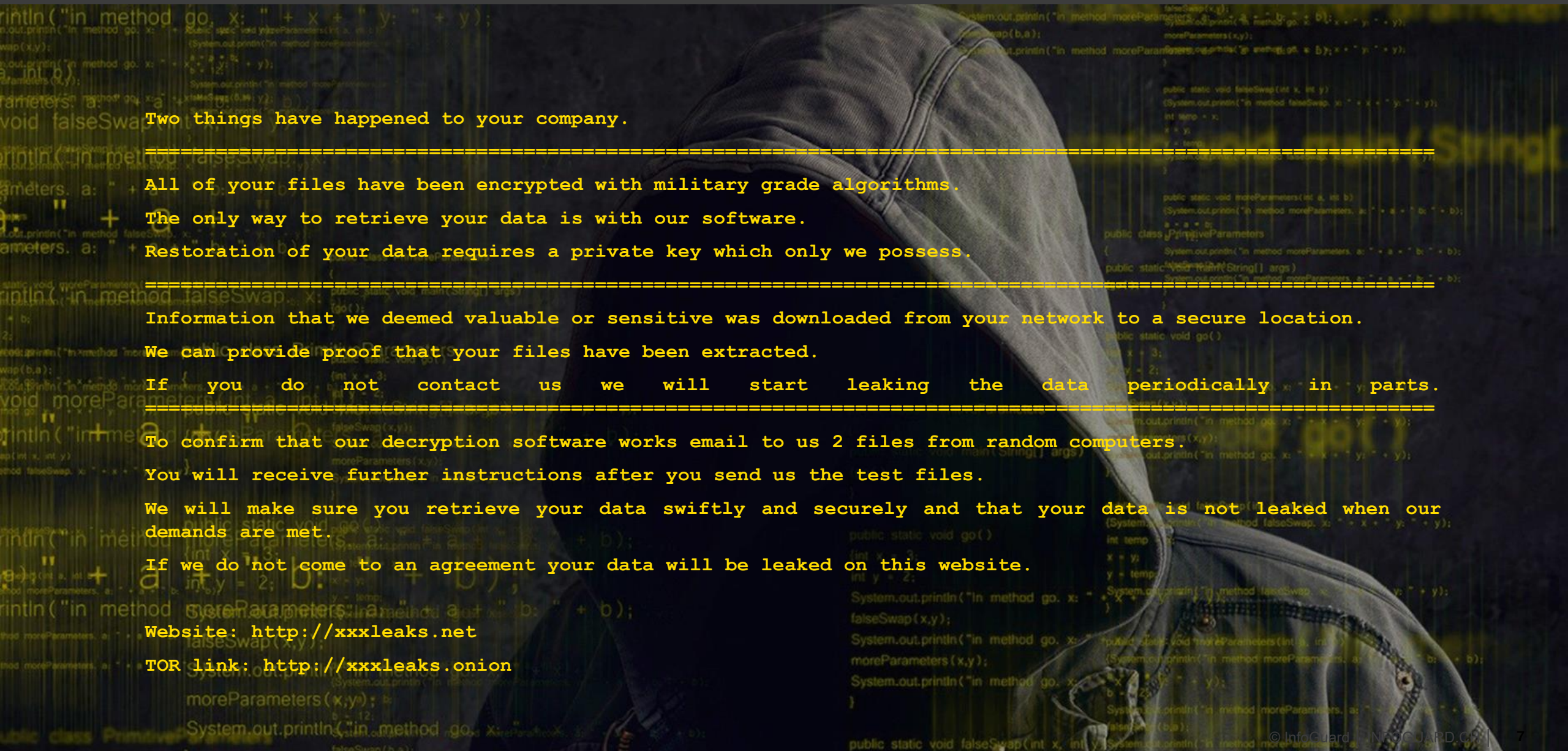
Symbol	Typ	Verfall	Strike
S7FZZU	Call-Warrant	22.09.2021	750
SAFZ0U	Call-Warrant	22.12.2021	750

presented by **UBS KeyInvest**

Dies ist keine Produktempfehlung. Weitere Produkte finden Sie auf UBS KeyInvest

Wenn der Schaden entstanden ist, hat das Sicherheitsdispositiv versagt!

InfoGuard
SWISS CYBER SECURITY



Two things have happened to your company.

==========

All of your files have been encrypted with military grade algorithms.

The only way to retrieve your data is with our software.

Restoration of your data requires a private key which only we possess.

==========

Information that we deemed valuable or sensitive was downloaded from your network to a secure location.

We can provide proof that your files have been extracted.

If you do not contact us we will start leaking the data periodically in parts.

==========

To confirm that our decryption software works email to us 2 files from random computers.

You will receive further instructions after you send us the test files.

We will make sure you retrieve your data swiftly and securely and that your data is not leaked when our demands are met.

If we do not come to an agreement your data will be leaked on this website.

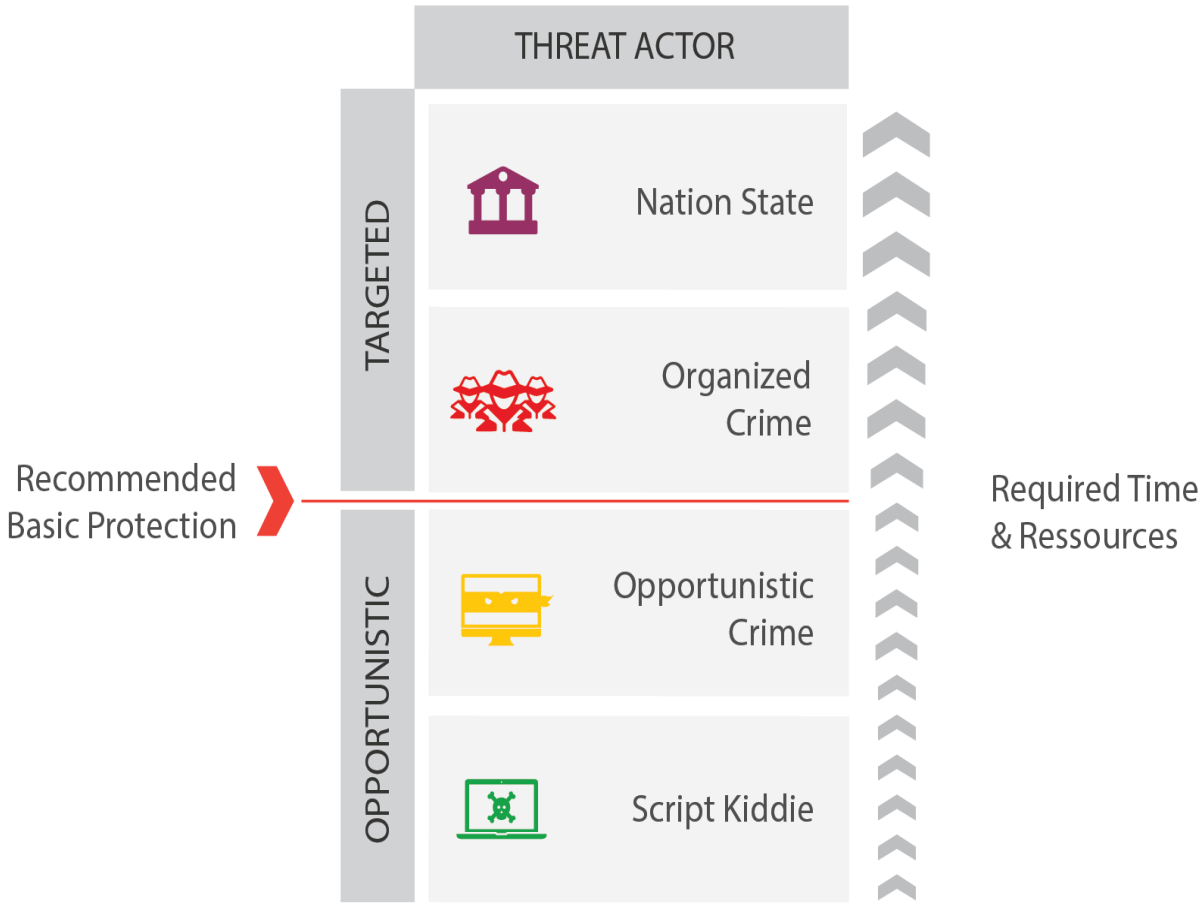
Website: http://xxxleaks.net

TOR link: http://xxxleaks.onion

Cyber Crime ist BIG BUSINESS

InfoGuard
SWISS CYBER SECURITY

Threat Actors – die Angreifer



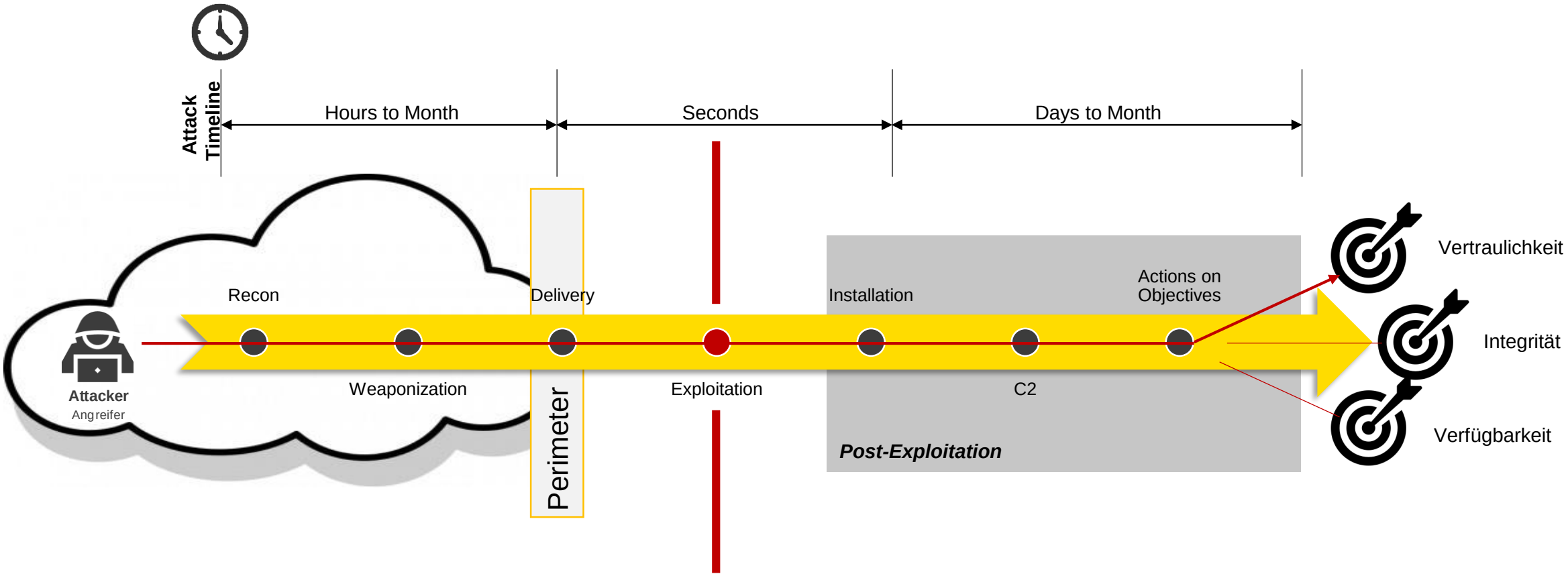
ZIELE	RESSOURCEN	VORGEHEN
• Information • Spionage • Sabotage	• Unlimitierte finanzielle Ressourcen • Zielorientiert	• Erwerb und Aufbau von Wissen • Persistente und versteckte Angriffe • Kompromittierung von Lierferanten
• Schaden • Spionage • Fear, Uncertainty and Doubt	• Grosse finanzielle Ressourcen • Möglicherweise von mehreren Firmen unterstützt	• Kauf von Wissen auf dem Schwarzmarkt • Physische Angriffe
• Finanzieller Gewinn über einen längeren Zeitraum	• Geschäftsorientiert • Agieren ähnlich wie ein KMU	• Existierende Gruppe mit einzelnen Spezialisten • Erpressung
• Ruhm • Reputation	• Minimale finanzielle Ressourcen	• Verwendung von öffentlich verfügbaren Tools

https://attack.mitre.org/groups/

InfoGuard
SWISS CYBER SECURITY

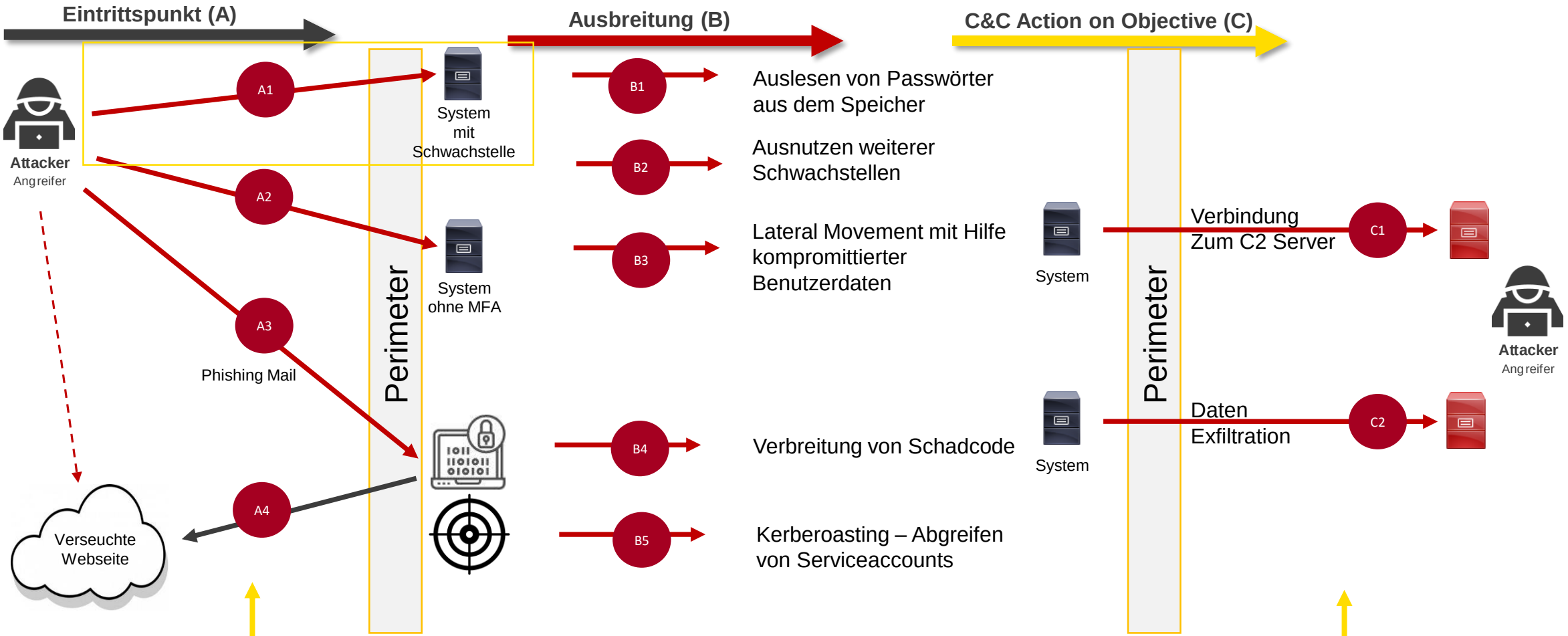
Wenn man versteht, wie die Angreifer vorgehen, kann man sein Abwehrdispositiv danach ausrichten.

Wie gehen nun Angreifer vor?



Es ist sehr wichtig die Motivation, das Vorhaben, das Vorgehen und die Instrumente der Angreifer zu verstehen, um Bedrohungen zu antizipieren, Angriffe zu verhindern und erkennen sowie im Notfall effektiv zu reagieren

Welches sind die häufigsten Eintrittspunkte?



Jegliche Interaktionen mit dem Internet sind riskant und müssen mit bedacht eingesetzt werden!

Einfallstor: E-Mail mit Beilage und Makros

InfoGuard
SWISS CYBER SECURITY

Angreifer

1 Angreifer sendet E-Mail mit schädlichem Anhang

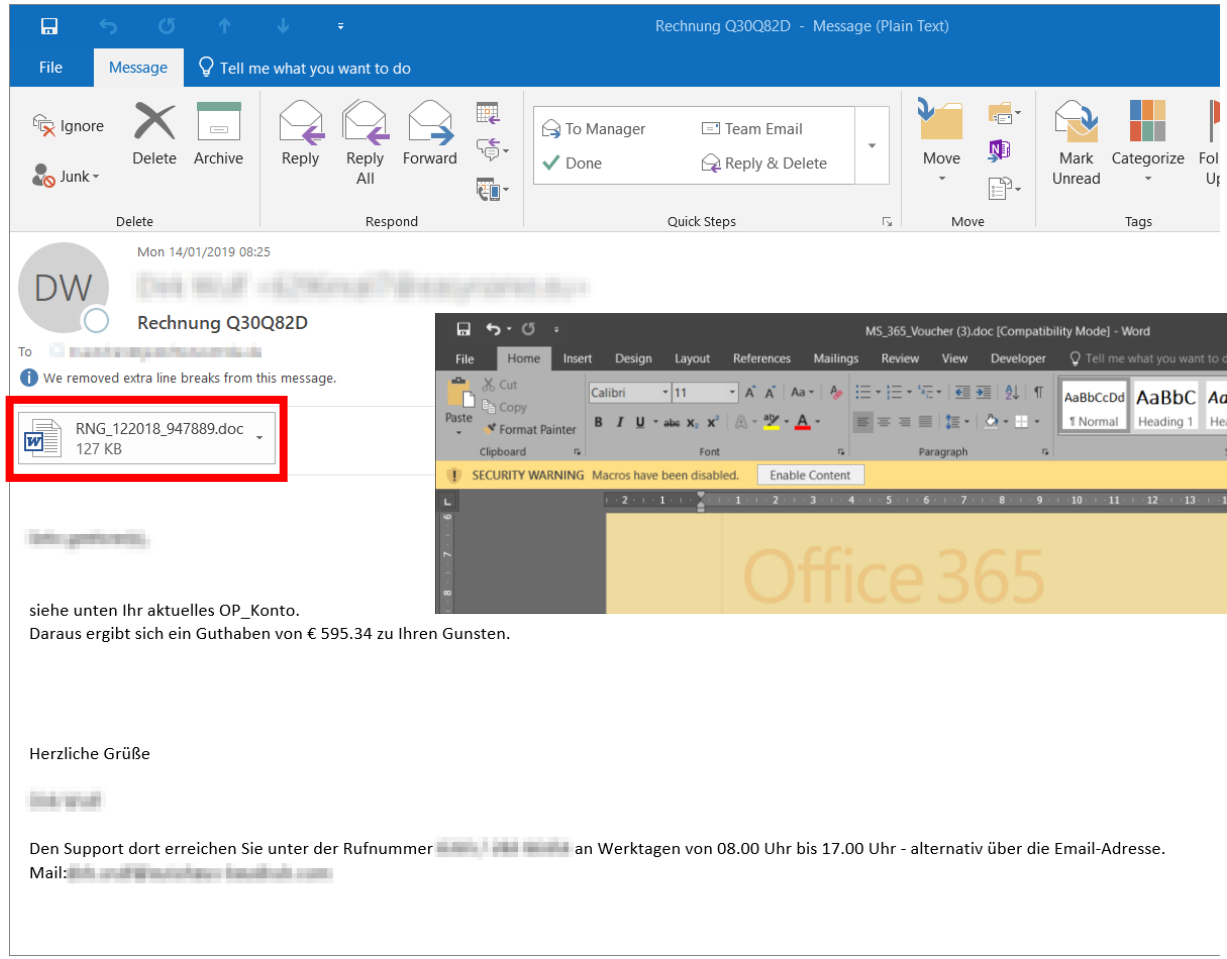
Erstes Opfer

2 Opfer liest E-Mail und öffnet schädlichen Anhang

3 Opfer ignoriert Warnmeldungen und aktiviert Makros

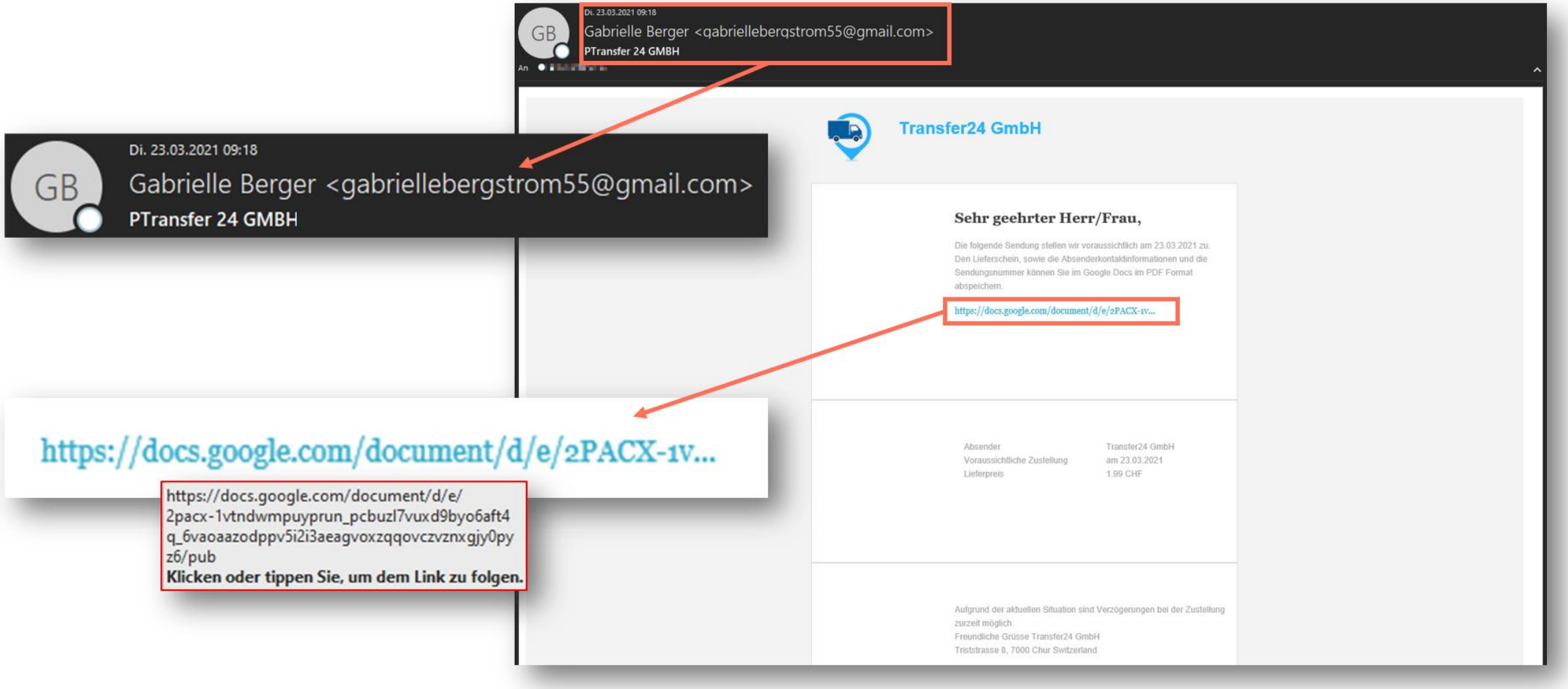
4

Angreifer installieren die Ryuk Ransomware und beginnen mit dem Verschlüsseln der Systeme



Einfallstor: E-Mail mit Link

Pandemiebedingt wird vermehrt online eingekauft. Die Wahrscheinlichkeit, dass jemand ein Paket erwartet ist gross. Diese Situation wird bei diversen Phishing-Angriffen per E-Mail und SMS aufgegriffen und ausgenutzt.

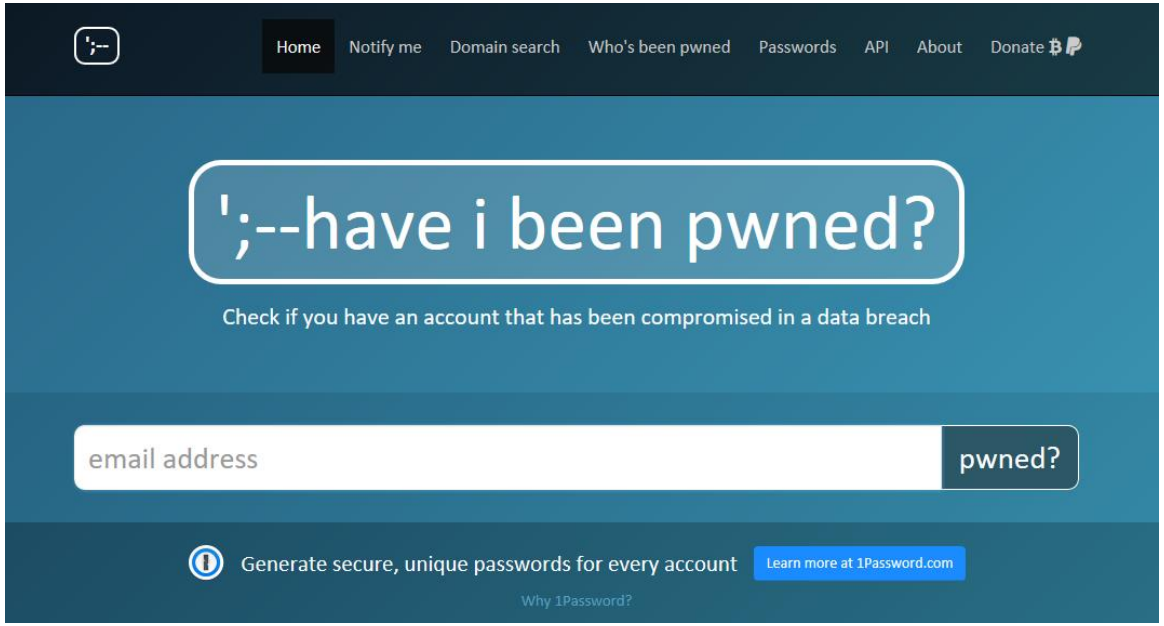


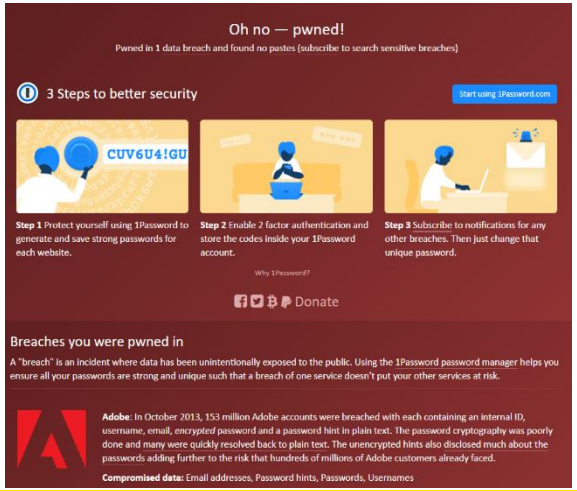
Einfallstor: Gestohlene Passwörter

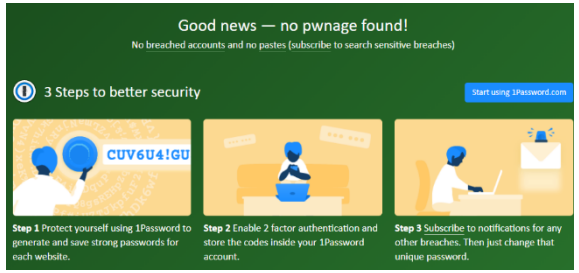
Insgesamt haben wir ca. 450 Passwörter gefunden – Beispiele:

Schaffhausen	gladiator	14binich	italia-9
Berlin71	darkn3ss	$Cudrefin2010	lolalola
Switzerland	mumuscheli	12345678910	roli77
Legendsdaddy12	Dampf	2644sara	Alfetta1800
Edith1973	04luca	aurasoma	clown
medipack	potter4137	Cara101383	freundlich
moser	seeotter	Colette	tom
null	immobilier	Hallo	leeer

Sind auch Ihre Passwörter von Diebstahl betroffen?







Immer wieder kommt es vor, dass Hacker Datenbanken von Unternehmen knacken und Zugangsdaten von Webseiten-Nutzern, Cloud-Anwendungen und sozialen Netzen entwenden. Oft wissen User nicht, wie sie herausfinden können, ob auch ihr Account vom Angriff betroffen ist. Auf diese Frage weiss "Have I Been Pwned" https://haveibeenpwned.com/ die Antwort.

Rezept aus dem Passwörter-Kochbuch

- Benutze für jede Anwendung ein anderes Passwort.
- Ein starkes Passwort besteht aus mindestens 12 Zeichen
- Berücksichtige bei der Wahl des Passworts die nachfolgenden Kategorien:
  - Grossbuchstaben (A-Z)
  - Kleinbuchstaben (a-z)
  - Zahlen (0-9)
  - Sonderzeichen (& ! ? * \ ‘ $ % : + , - < = # « @ ; > /) (_ [.] { ~ })

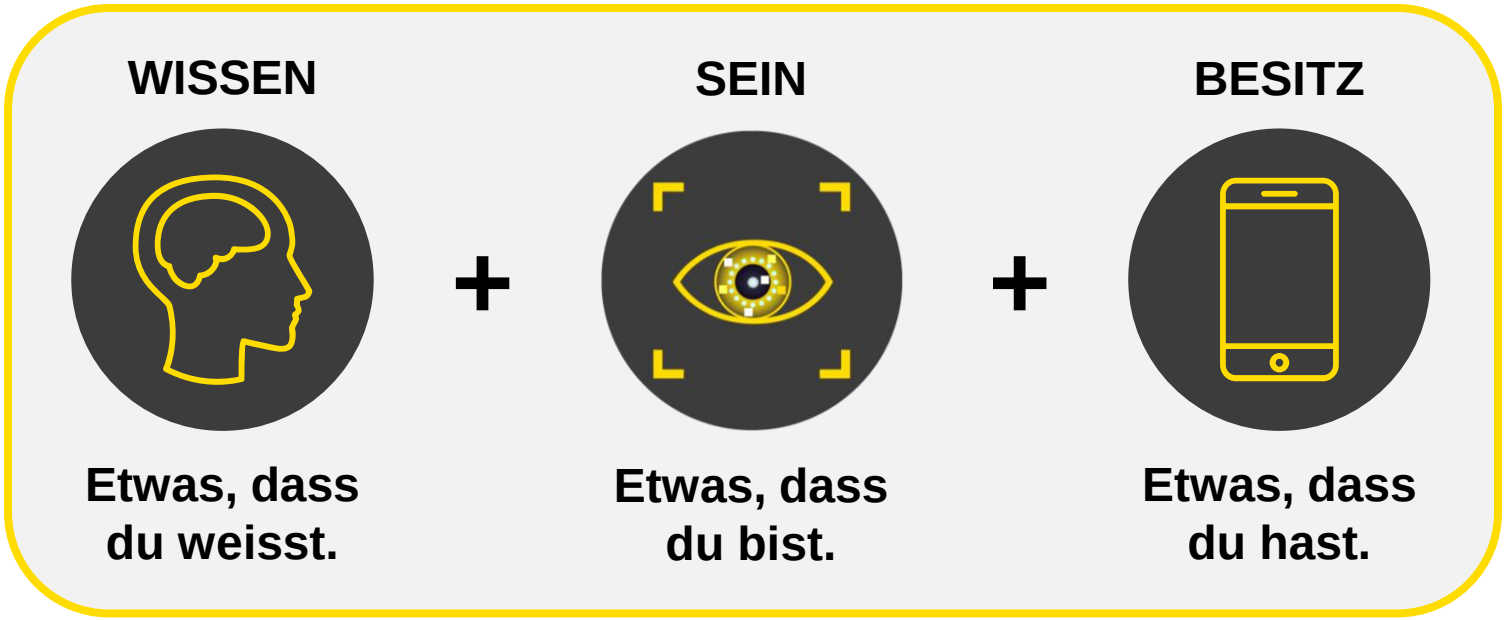
- Denke einfach einen für dich einprägsamen Satz aus.
- Nun kannst du die Anfangsbuchstaben jedes Wortes zusammensetzen und einzelne Bestandteile durch Sonderzeichen ersetzen.
- Beispiel: Mein Auto steht seit März 2021 in der Garage! > **MAs$03/21@dG!**
- Beispiel: We all live in a yellow submarine. The Beatles 1966! > **Waliays_TB66!**

Quelle: https://www.pinterest.ch/pin/511510470173669870/

Passwort Manager

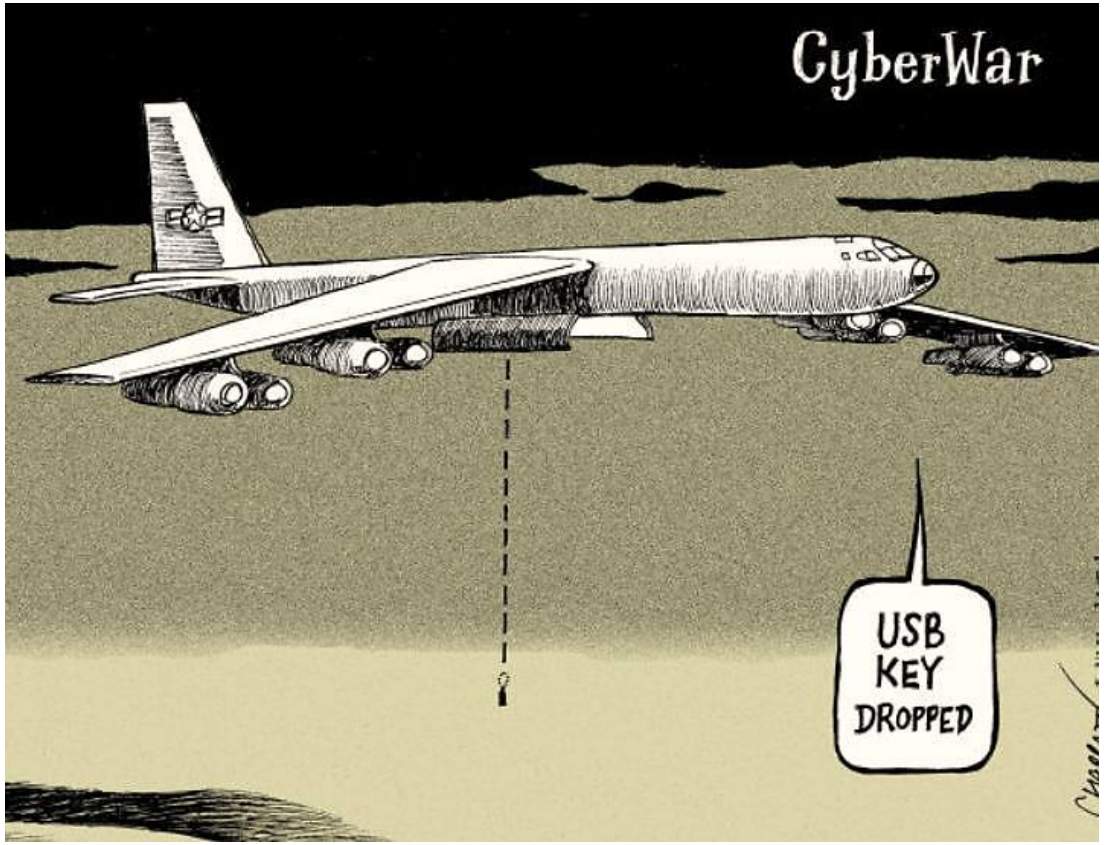
- Bessere, komplexere Passwörter
- Ständig andere Passwörter
- Schutz vor Phishing
- Mehr Komfort
- Weniger Passwörter merken
- Beruflich und privat

Multi Faktor Authentifizierung



- SMS-basierte MFA ist weniger sicher als die Verwendung einer MFA-App
- Schwache oder gestohlene Anmeldedaten sind die bevorzugte Waffe von Hackern

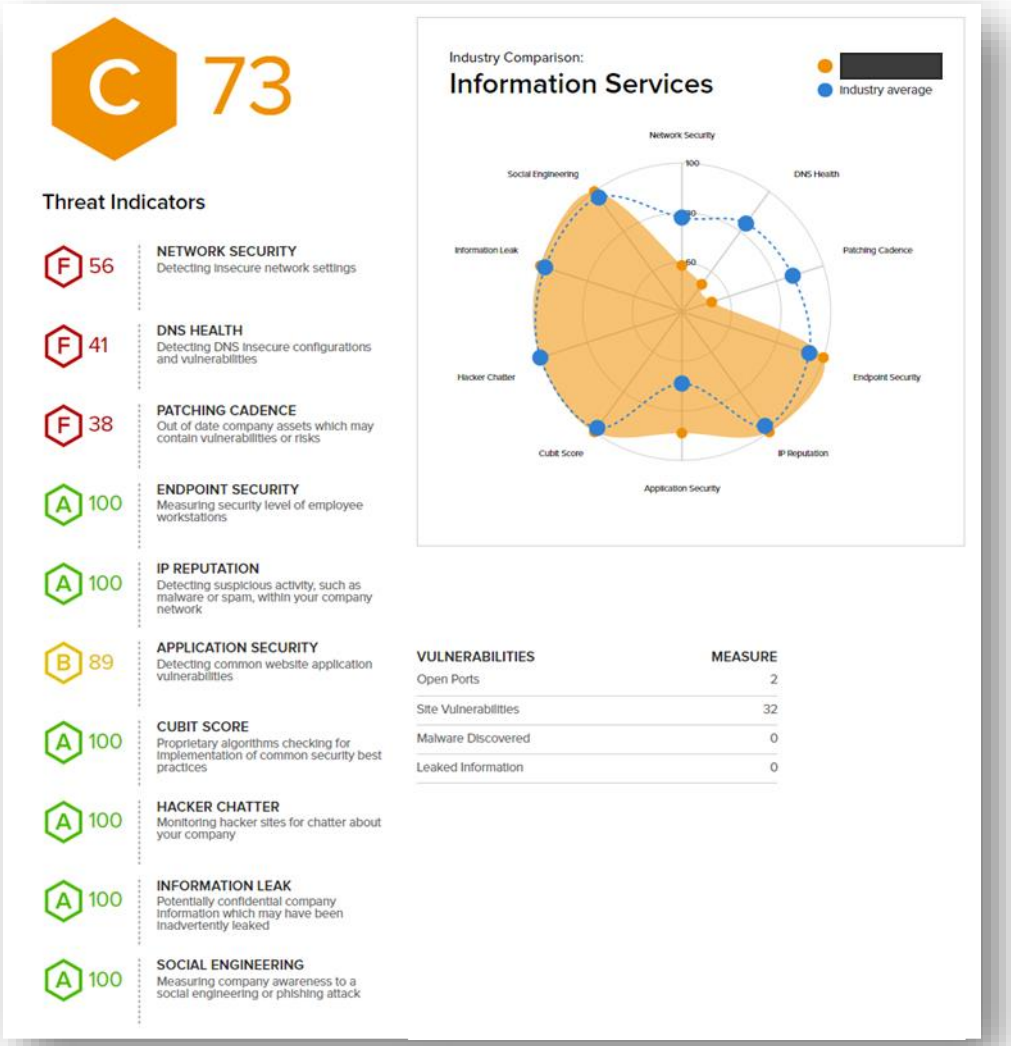
Einfallstor: USB Memory Stick

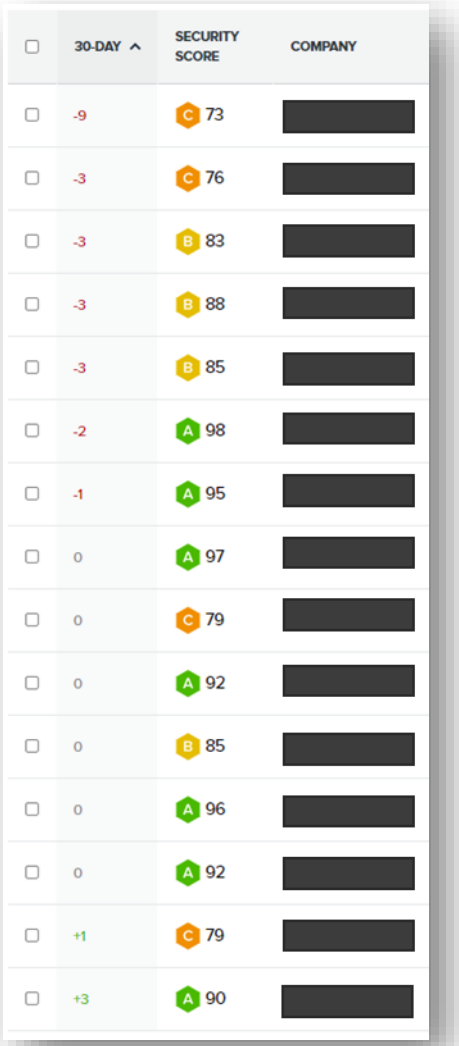


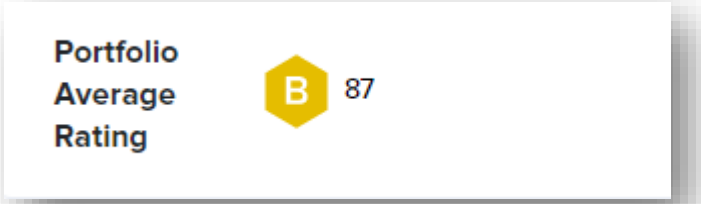
Einfallstor: Ungepatchte Systeme

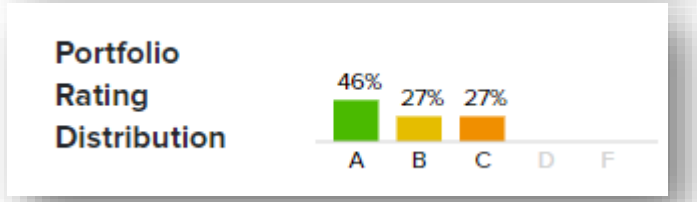
Quelle Bild: https://www.cio.com/article/3197361/wannacry-reminds-cios-to-stay-on-top-of-patching.html

Wie sieht ihr digitaler Fussabdruck aus?





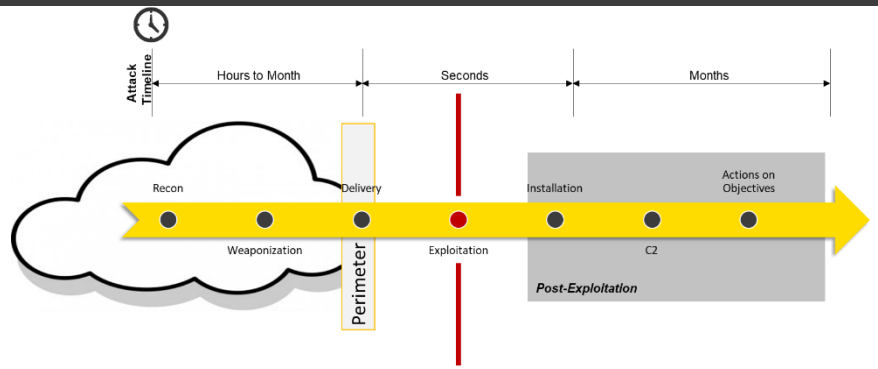




InfoGuard
SWISS CYBER SECURITY

WIE SCHÜTZE ICH MEIN UNTERNEHMEN EFFEKTIV UND WIE VERHALTE ICH MICH IM ANGRIFFSFALL?

Empfehlungen:
Zur Erinnerung - Wie läuft Angriff und Verteidigung ab?



PROTECT – Schutz vor dem Angriff
DETECT – Erkennung des Angriffs
Hier kann man den Angriff verhindern bzw. entdecken

Bewältigung des Angriffs
RESPONSE & RECOVER

Empfehlungen -
Es braucht eine umfassende Betrachtung der Cybersicherheit

InfoGuard
SWISS CYBER SECURITY

NIST CYBER SECURITY FRAMEWORK

IDENTIFY
- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT
- Access control
- Awareness and training
- Data security
- Information protection and procedures
- Maintenance
- Protective technology

DETECT
- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND
- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER
- Recovery planning
- Improvements
- Communications

CYBER DEFENCE MATURITY

Yesterday's focus

Today's focus

https://www.nist.gov/cyberframework

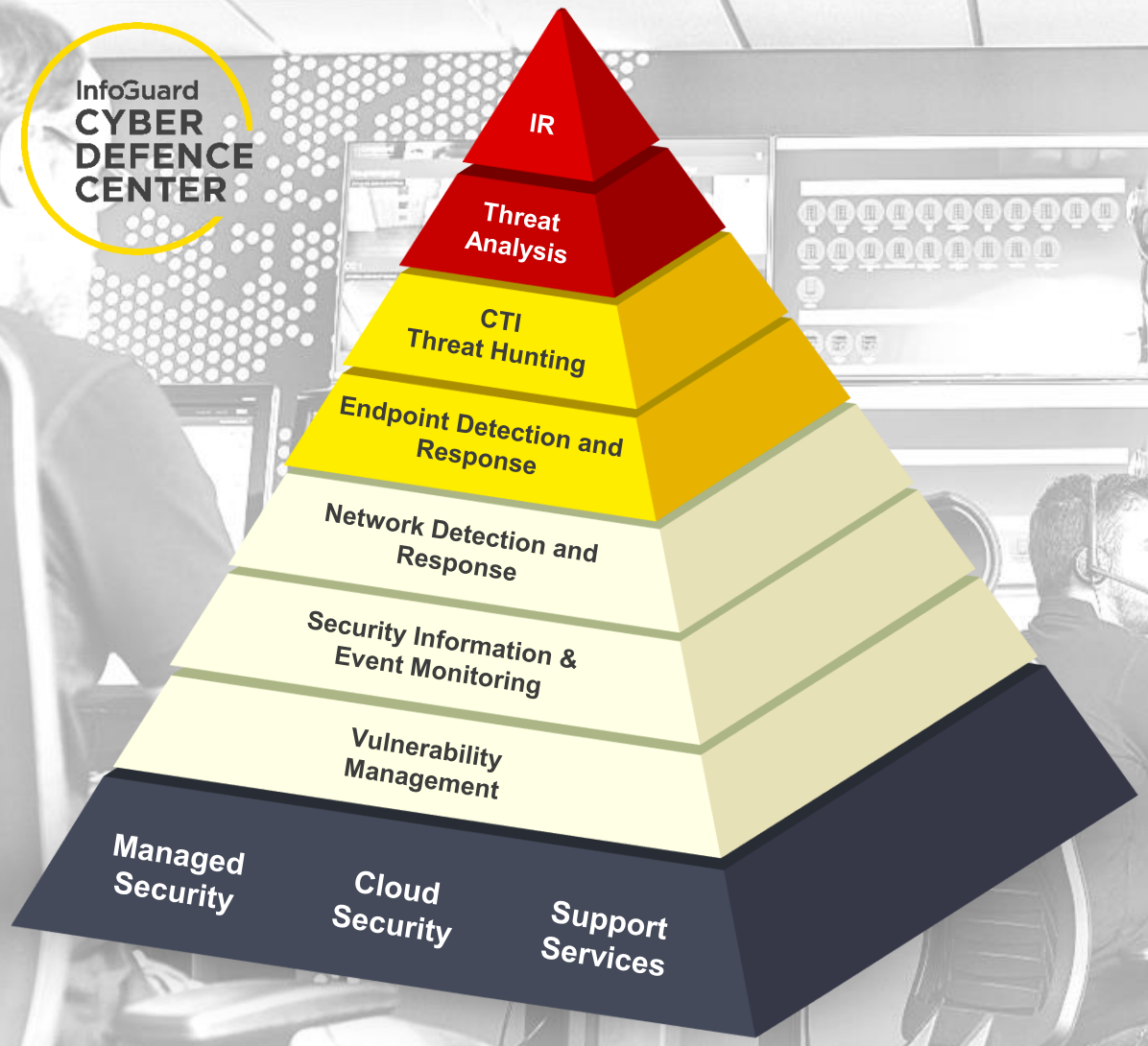
Empfehlungen – Technische Massnahmen

1. **Erhöhung** der **Detektions- und Reaktionsfähigkeiten** um Cyberangriffe zu verhindern oder die Auswirkungen der Angriffe einzudämmen.
2. Verwendung einer **Multi-Faktor-Authentisierung** (MFA) für alle externen Schnittstellen, wie beispielsweise Outlook Web Access.
3. **Einschränken und Kontrolle** von **administrativen Schnittstellen** am Perimeter.
4. Einsatz von **Web Proxy Lösungen** um den Download von riskanten Dateien wie .exe zu unterbinden.
5. Umsetzung eines **DMZ-Konzeptes** mit einer **Trusted Zone** und **Netzwerk Segmentierung**.
6. Verwendung und Umsetzung **verschlüsselter Protokollen** (FTP mit SFTP und HTTP mit HTTPS ersetzen) sowie unsichere Protokollversionen TLSv1 und SSLv3 unterbinden.
7. Einschränken von **Benutzerprivilegien** sowie Einsatz von **starken Passwörtern** (Komplexität und Minimum 12 Zeichen).
8. Am Internet exponierte Dienste kontinuierlich auf Schwachstellen überprüfen und aktualisieren - **Vulnerability und Patch Management.**

FTP: File Transfer Protocol, SFTP: Secure File Transfer Protocol, HTTP: Hypertext Transfer Protocol, HTTPS: Hypertext Transfer Protocol Secure, TLS Transport Layer Security, SSL: Secure Sockets Layer

Empfehlungen – Technische Massnahmen

InfoGuard
SWISS CYBER SECURITY



Response Services

- Incident Response / CSIRT
- Forensics
- Threat Analysis

Advanced Detection Services

- Cyber Threat Intelligence (CTI)
- Threat Hunting (TH)
- Endpoint Detection and Response (EDR)

Basic Detection Services

- Network Detection and Response (NDR)
- Security Information & Event Monitoring (SIEM)
- Vulnerability Management (VUMA)

Security Operations Services

- Managed Security
- Cloud Security
- Support Services

Empfehlungen – Organisatorische Massnahmen

1. Etablierung einer Sicherheitsorganisation (**CISO Rolle**)
2. Etablierung eines **ISMS Prozesses und Umsetzung der Sicherheitsvorgaben**
3. **Awareness** Schulungen für Mitarbeiter
4. **Incident Response** Retainer
5. Funktionierendes **Backup- und Wiederherstellungs-Konzept** (Offline)
6. **Kommunikationskonzept** (intern/extern)
7. Etablierung **Krisen- / IT Notfall-Organisation** sowie **Identifikation der kritischen Prozesse**
   a) Task-Force (Rollen und Verantwortlichkeiten)
   b) Krisenmanagement (Prozess, Checkliste, etc.)
   c) Table Top Exercises (TTX)
8. Durchführung von regelmässigen Angriffssimulationen
9. **Cyber Versicherung**

CISO: Chief Information Security Officer, ISMS: Information Security Management System, TTX: Table Top Exercise

Empfehlungen – Organisatorische Massnahmen

Wenn ein Schaden entstanden ist, braucht es eine erfahrene und schnelle Eingreiftruppe.

Initialisierung eines Incident Response (**IR) Einsatzes** am Beispiel IR-255

Ein Montag im Jahr 2020

- 03:00 Start Server- und Datenverschlüsselung in DE
- 04:00 Start Server- und Datenverschlüsselung in CH
- **09:15 Anruf bei IG – Erstbeurteilung durch Senior Analyst**
- 10:00 Austausch kommerzieller Bedienungen
- 10:30 Auftragserteilung
- 10:40 Vorbereitung des Tanium Downloads
- 10:50 Senior Analyst Unterwegs zum Kunden
- 11:00 Start Download und Installation von Tanium
- **12:00 Ankunft Analyst bei Kunden**
- 15:30 Austausch mit NCSC vor Ort beim Kunden
- 14:00 Abschluss Tanium Server Installation und Agent Rollout auf betroffenen Systeme
- 17:00 Erste wichtige Erkenntnisse zum Fall gewonnen

Vorbereitung: Bewältigungsablauf (Response und Recovery) Organisatorische Sofortmassnahmen

Krisenmanagement

Ziel: *Effizientes Management der Krise inkl. Kommunikation*

Voraussetzungen:

- *Task-Force ist definiert und erreichbar*
- *Ablauf Krisenmanagement definiert*
- *Infrastruktur für Krisenmanagement steht bereit*
- *Schnelle Kommunikation kann gewährleistet werden (z.B. Templates, klare Abläufe)*

Notbetrieb

Ziel: *Wichtigste Teilprozess laufen fast reibungslos (mit minimaler Unterbrechung) weiter*

Voraussetzungen:

- *Identifikation kritischer Prozesse (inkl. Abhängigkeiten IT-Systeme)*
- *Workaround für kritische Prozesse*

Bewältigung des Angriffs

Ziel: *Beseitigung des Angreifers*

Voraussetzungen:

- *Support ist gewährleistet (IR Retainer, Forensik, IT)*
- *Handlungsfähigkeit der erreichbaren Mitarbeitenden (z.B. Rechte)*

Wiederherstellung

Ziel: *Wiederherstellung des Services*

Voraussetzung:

- *Backup existiert*
- *Backup nicht zerstört (z.B. durch ausreichende Trennung)*
- *Backup funktioniert (z.B. wurde regelmässig getestet)*
- *Restore-Geschwindigkeit für Notbetrieb ausreichend*

Ablauf Bewältigung
Organisatorische Sofortmassnahmen

Krisenmanagement

Ziel: *Effizientes Management der Krise inkl. Kommunikation*

Was ist zu tun?

- *Task-Force (relevante Mitarbeiter) alarmieren und aufbieten*
- *Externe Unterstützung kontaktieren (Forensik, evtl. auch IT)*
- *Verhaltensregeln festlegen (Zeitpunkt der Abstimmungen)*
- *Infrastruktur für Krisenmanagement bereit stellen*
- *Kommunikation etablieren*

Notbetrieb

Ziel: *Wichtigste Businessprozess laufen (gemäss Priorität des Business)*

Was ist zu tun?

- *Kritischer ausgefallene Prozesse identifizieren*
- *Workaround für diese Prozesse etablieren bzw. Wiederherstellung der Prozesse (Abstimmung mit Bewältigung des Angriffs)*

Bewältigung des Angriffs

Ziel: *Beseitigung des Angreifers*

Was ist zu tun?

Forensik Partner (IR Team) führt durch den Prozess

- *Analyse*
- *Eindämmung*
- *Bereinigung*
- *Freigabe (inkl. Testing)*

Wiederherstellung

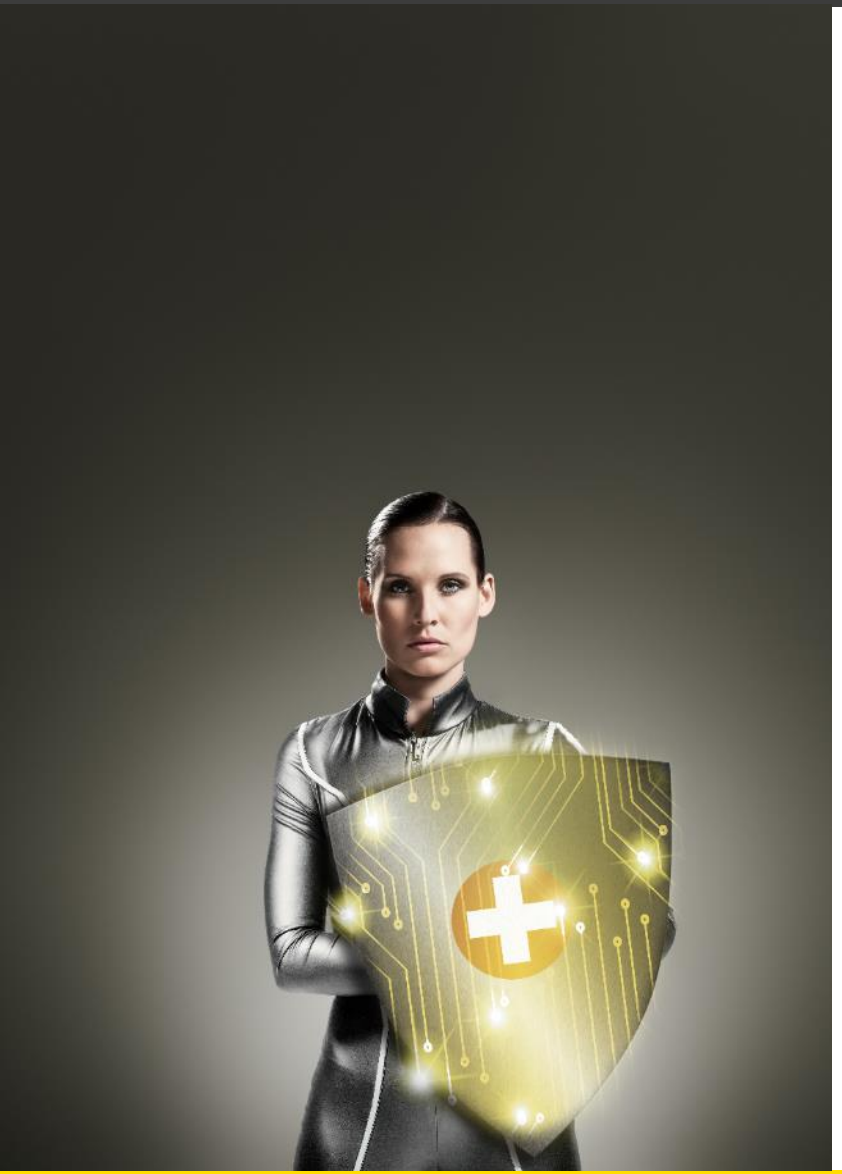
Ziel: *Wiederherstellung des Services*

Was ist zu tun?

- *Massnahmen zum Schutz vor erneutem Angriff*
- *Wiederherstellung, wenn Bereinigung erfolgreich war*
- *Wiederherstellung über Backup einspielen*
- *Wiederherstellung über Neuaufbau*

Mitarbeiterawareness: *Ihr korrektes Verhalten, ein wichtiger Schutz bei der Bekämpfung der Cyberkriminalität.*

InfoGuard
SWISS CYBER SECURITY



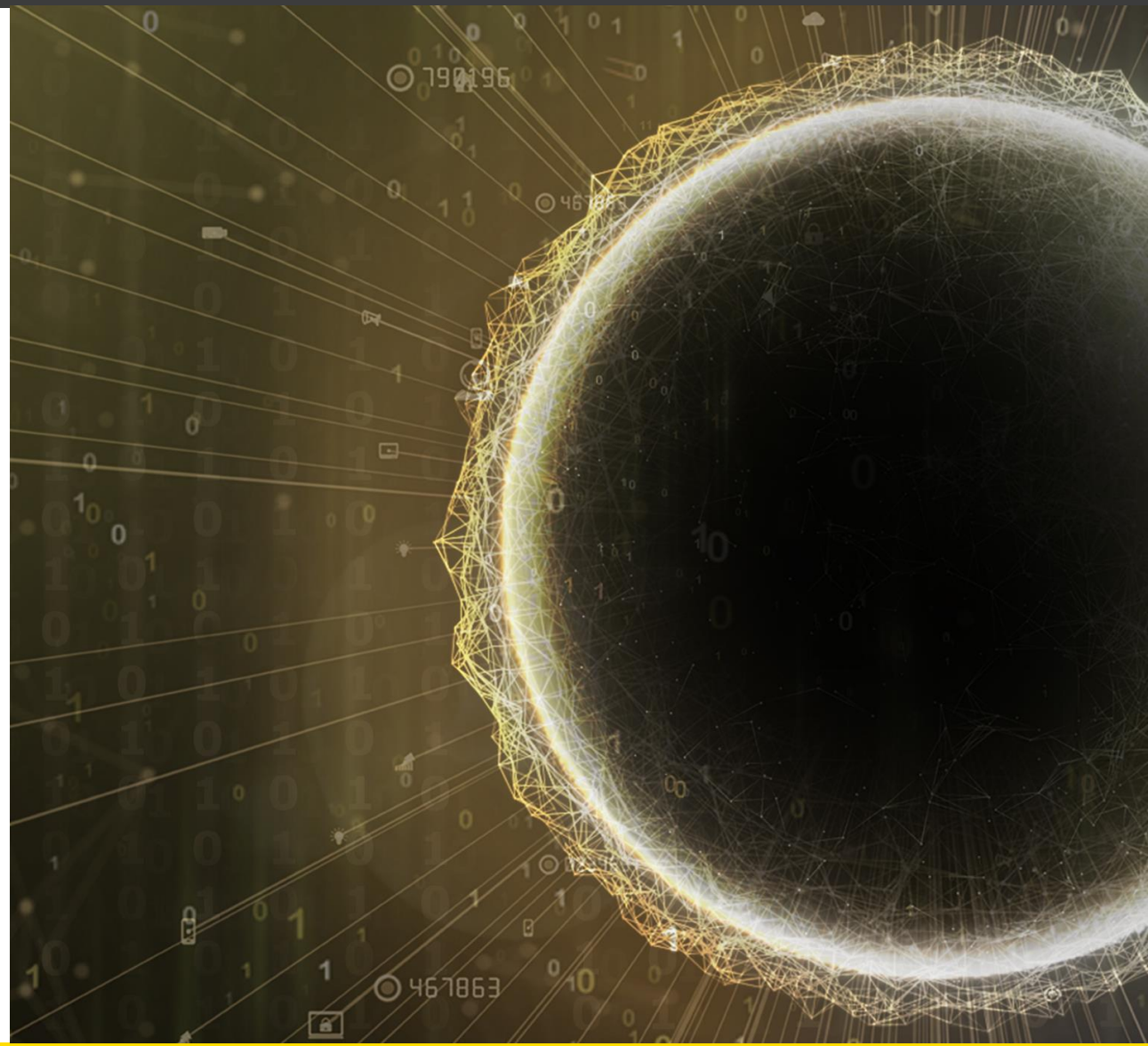
U make Sec_rity work!

- Awareness Initiative mit Branding
- Communiqué der Geschäftsleitung
- Einführungsschulung / Security Days
- Live-Hacking Show / Online Awareness Schulungen
- Know-how Transfer über das Intranet
- E-Learning
- Erklärvideos
- Themenplakate
- Sicherheitsbroschüren
- Story Telling mittels Comics und/oder Gamification
- Pre und/oder Post-Phishing Simulationen

Q&A

Fordern Sie uns heraus!

- Fragen
- Kundenanforderungen
- Nächste Schritte



InfoGuard AG
Lindenstrasse 10
6340 Baar / Schweiz

Telefon +41 41 749 19 00