«KMU SECURITY FITNESS» BY DIAG

25. April 2024, Pfäffikon

«KMU Security Fitness» by diag

diag DIENSTLEISTUNGEN AG

Lösungen für ICT-Systeme in den Bereichen Hosting, Kauf, Miete, Microsoft 365 und vCloud

Neu : Security Operations Center (SOC) mit Crowdstrike

- **Bedrohungserkennung:** Cyberbedrohungen proaktiv identifizieren und analysieren um potenzielle Sicherheitsverletzungen zu verhindern
- **Endgeräteschutz**: Schutz für (PC, Laptop,Mobile) überwacht verdächtige Aktivitäten und reagiert auf Anomalien
- **Wirtschaftlichkeit:** diag SOC bietet KMU erschwingliche und umsetzbare Lösung

diag DIENSTLEISTUNGEN AG Security Today by UCSP MOONEN COMMUNICATIONS

Was kann Cybersicherheit für Ihr Unternehmen tun?

Unsere Expertin und Experten

awareness4you

Sandra Aengenheyster

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

George Necola

freudiger IT security

Sam Freudiger

diag
DIENSTLEISTUNGEN AG

Security Today
by UCSP

MOONEN
COMMUNICATIONS

AGENDA

08:30 - 09:00 Uhr	**Begrüssung Hardy Ruoss**, Geschäftsleitung, diag Dienstleistungen AG
	Einführung George Necola, Head of Security & Network, Swiss IT Security AG
09:00 - 09:45 Uhr	**Was sind eigentlich „die Kronjuwelen des Unternehmens"?**
	Sam Freudiger, freudiger IT security B.V.
09:45 - 10:15 Uhr	**Kaffeepause**
10:15 - 11:00 Uhr	**Mit Herz, Hand und Verstand eine gesunde Sicherheitskultur aufbauen**
	Sandra Aengenheyster, awareness4you
11:00 - 11:30 Uhr	**Diskussion / Fragen**
11:30 - 13:00 Uhr	**Stehlunch / Networking**

diag DIENSTLEISTUNGEN AG

Security Today by UCSP

MOONEN COMMUNICATIONS

Einführung und Moderator

- George Necola, Head of Security & Network bei Swiss IT Security AG
- > 18-jährige Expertise in den Bereichen IT-Governance, IT-Sicherheit und Business Continuity.
- Stationen: Cembra Money Bank (ITSLT), localsearch (Swisscom Directories AG), Axon Lab AG
- Entwicklung und Umsetzung von IT-Sicherheitsstrategien, Leitung von IT-Projekten und strategische Umsetzung der IT-Sicherheit

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

diag
DIENSTLEISTUNGEN AG

Security Today
by UCSP

MOONEN
COMMUNICATIONS

Cyberangriffe machen keinen Unterschied zwischen Branchen – jedes KMU kann betroffen sein.

diag DIENSTLEISTUNGEN AG

Security Today by UCSP

MOONEN COMMUNICATIONS

https://www.youtube.com/watch?v=Rh5ycQXPOnQ

Hand aufs Herz - 10 Fragen

https://menti.com 4550 1120

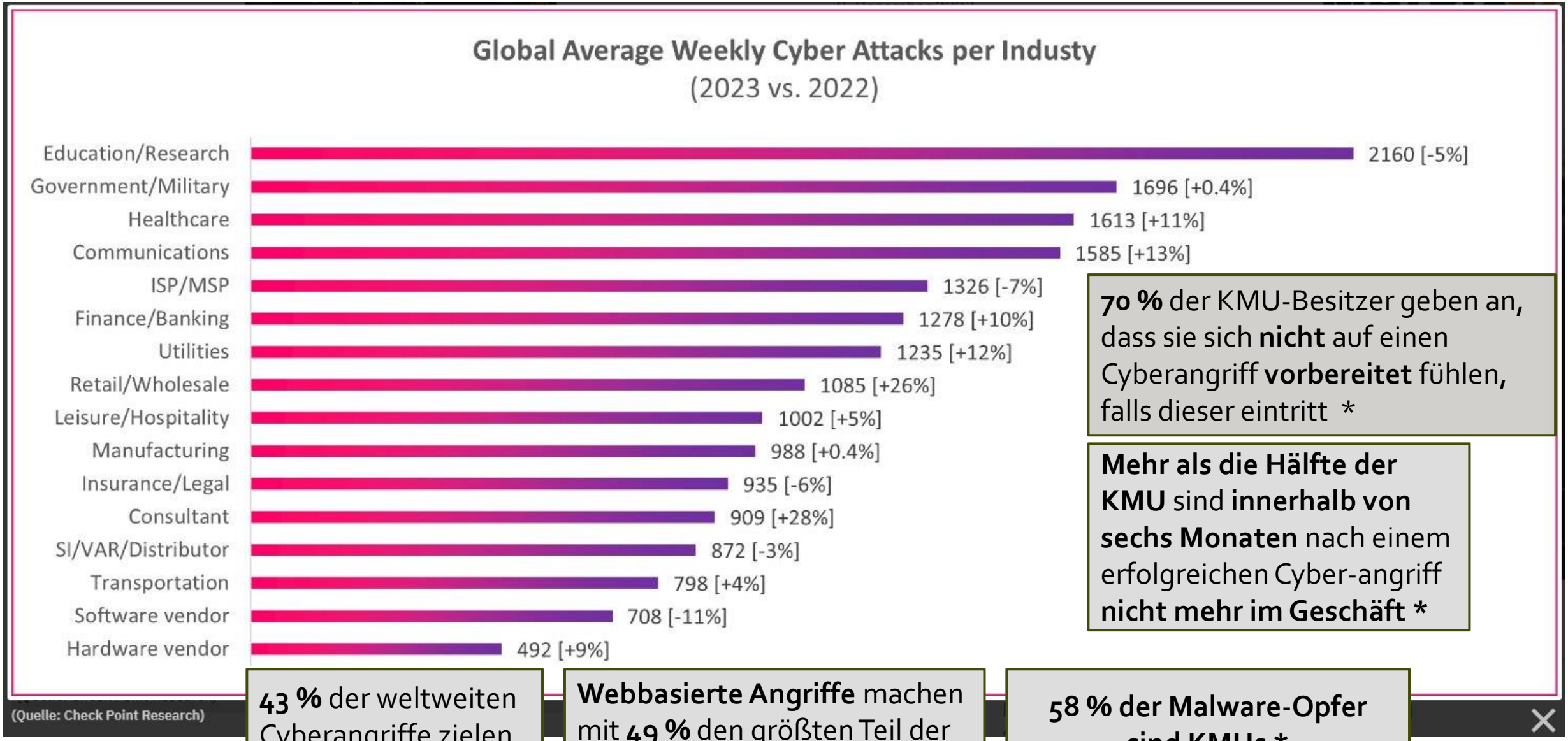
1. Wie viele Geräte nutzen Sie in Ihrem Unternehmen?
2. Wissen Sie, welche Geräte und Mitarbeiter Zugriff auf Ihre Unternehmensdaten haben?
3. Welche Arten von Daten werden in Ihrem Unternehmen verarbeitet?
4. Wo werden Ihre Daten gespeichert?
5. Wie werden Ihre Daten gesichert?
6. Haben Sie bereits eine IT-Security Beratung in Ihrem Unternehmen durchgeführt?
7. Haben Sie schon einmal eine Security- oder Awareness-Kampagne durchgeführt?
8. Wurden bereits Schulungen zum Thema IT - Sicherheit für Ihre Mitarbeiter veranstaltet?
9. Halten Sie Ihr Unternehmen für ein interessantes Ziel für Hacker?
10. Haben Sie eine Cyber Risk Versicherung abgeschlossen?

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

diag
DIENSTLEISTUNGEN AG

Security Today
by UCSP

MOONEN
COMMUNICATIONS



70 % der KMU-Besitzer geben an, dass sie sich **nicht** auf einen Cyberangriff **vorbereitet** fühlen, falls dieser eintritt *

Mehr als die Hälfte der KMU sind **innerhalb von sechs Monaten** nach einem erfolgreichen Cyber-angriff **nicht mehr im Geschäft ***

43 % der weltweiten Cyberangriffe zielen auf KMU ab. *

Webbasierte Angriffe machen mit **49 %** den größten Teil der Cyber-angriffe auf KMU aus. *

58 % der Malware-Opfer sind KMUs *

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

diag
DIENSTLEISTUNGEN AG

Security Today
by UCSP

MOONEN
COMMUNICATIONS

Ihr Unternehmen

Hardy Ruoss

Hacker

Wichtige Daten

Backup

Router nicht gepatcht

Bekannte Schwachstelle

Bekannte Schwachstelle auf der Firewall

Unbekanntes Gerät

Phishing Email

Auf dem Server keine Updates eingespielt

BANK: 1200 MITARBEITENDEN

ROLLEN	ANZAHL
• Chief Information Security Officer (CISO)	2
• Information Security Officer	5
• Enterprise Architect	4
• Risk	48
• Internal Audit	5
• External Audit	KPMG
• Security Operation Center (SOC)	6 intern, 24 extern
• IT Operations	80 intern, 120 extern
• ISO	4
• Security Architect	2
• IT Architect	4
	TOTAL 304

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

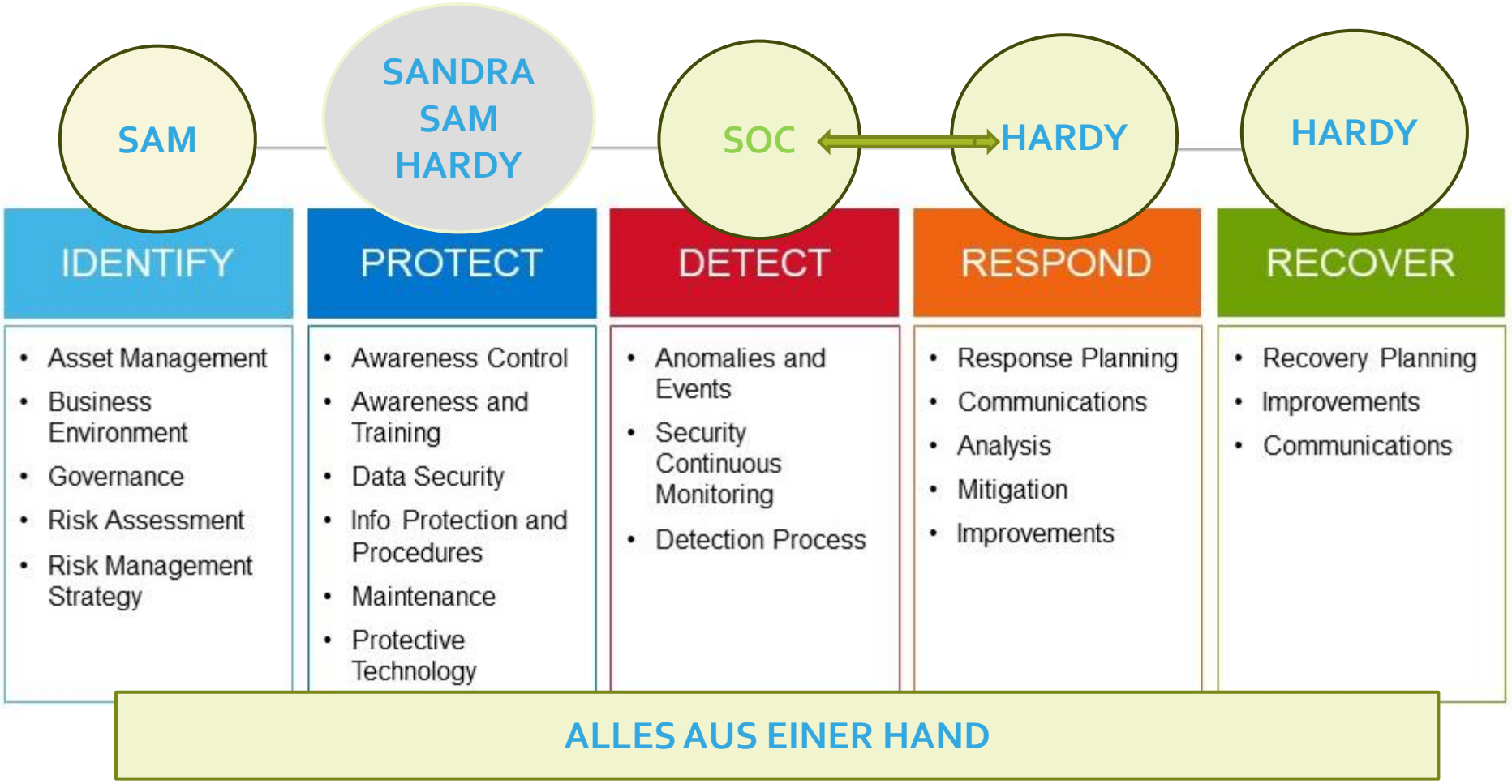
Security Today
by UCSP

diag
DIENSTLEISTUNGEN AG

Security Today
by UCSP

MOONEN
COMMUNICATIONS

Cybersicherheit im Unternehmen



SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

diag
DIENSTLEISTUNGEN AG

Security Today
by UCSP

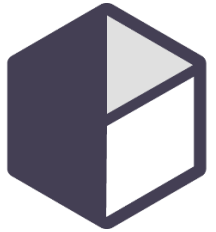
MOONEN
COMMUNICATIONS

WAS SIND EIGENTLICH „DIE KRONJUWELEN DES UNTERNEHMENS“?

freudiger **IT security** B.V.

Sam Freudiger

freudiger **IT security** B.V.



freudiger **IT security**

- Gründung 2017
- Kartographiert und analysiert IT-Cyberrisiken bei KMU
- Hauptsitz in Utrecht, Niederlande
- Niederlassung in Biel/Bienne, Schweiz
- Sam Freudiger, gebürtiger Schweizer
- Kundenreferenz CH

diag DIENSTLEISTUNGEN AG

CENDRES+ MÉTAUX

weiss comunication + design ag

diag DIENSTLEISTUNGEN AG

Security Today by UCSP

MOONEN COMMUNICATIONS

Was sind eigentlich „die Kronjuwelen des Unternehmens“?

Agenda

- Warum fallen Unternehmen Cyberattacken zum Opfer?
- «Kronjuwelen?»
- Welchen digitalen Risiken ist Ihr Unternehmen ausgesetzt?
- Wie dringen Kriminelle zu den Kronjuwelen durch? (Praxisbezogenes Beispiel)
- Was sind Schwachstellen?
- Wie verhindern Sie einen unerwünschten Zugriff? (Praxisbezogenes Beispiel)
- Was tun, wenn es zu spät ist?
- Fragen und Anmerkungen zum Thema

Warum fallen Unternehmen Cyberattacken zum Opfer?

- "Wir sind nicht interessant genug"
- "Wir haben ISO27001 – wir sind sicher"
- "Wir haben Antivirus"
- "Meine IT hat mir versichert, dass alles gut ist"
- "Wir haben nichts zu verbergen"

„Kronjuwelen?“

Was sind eigentlich die sogenannten "Kronjuwelen eines Unternehmens"?

Frage ans Publikum

Was kommt ihnen ihnen in den Sinn wenn Sie an “Kronjuwelen“ denken?

„Kronjuwelen?“

Was sind eigentlich die sogenannten "Kronjuwelen eines Unternehmens"?

- Ihre Unternehmenskernkompetenzen
- Ihre einzigartigen Fähigkeiten und Ressourcen

Also wie Sie sich von der Konkurrenz abheben und für Ihren Erfolg entscheidend ist

Unternehmen schützen und entwickeln Kernkompetenzen weiter, um die **Überlebensfähigkeit** und **Unabhängigkeit** des Unternehmens **langfristig zu sichern.**

Kronjuwelen Beispiele

- **Die schützenswerte Innovationen Ihres Unternehmens**, beispielsweise neue und verbesserte Produkte, Dienstleistungen oder Prozesse
- **Alles Rund um Ihren Kundendienst**, zum Beispiel wie Sie Kundenbindung betreiben und was macht Ihr Kundenservice aus
- **Die reibungslose betriebliche Effizienz**, wie beispielsweise wie Sie Kosten senken und Ihre Produktivität steigern
- **Ihr ureigenes Spezialwissen und Know-how** in beispielsweise technologischen Bereich, der einen Vorsprung gegenüber der Konkurrenz gibt.

Kronjuwelen dürfen nur für eine begrenzte Anzahl Personen zugänglich sein.

Welchen digitalen Risiken ist Ihr Unternehmen ausgesetzt?

Beispielsweise: Informationseingang

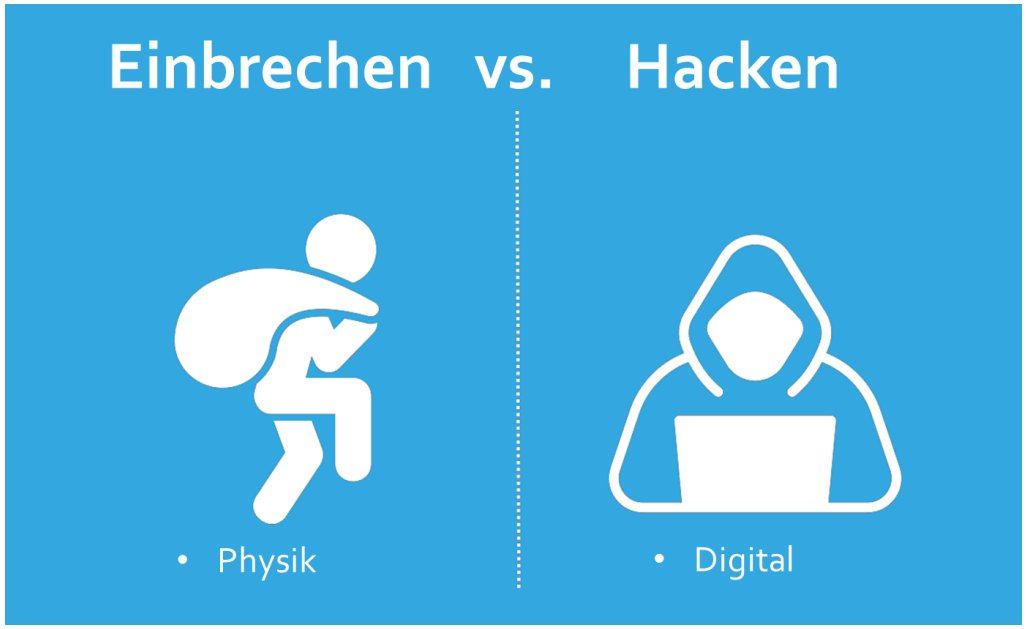
- Personalvermittler: Lebensläufe von Kandidaten
- Investment Unternehmen: Anlagestrategien, Verträge
- Bauunternehmen: CAD-Zeichnungen
- Liegenschaftsverwaltung: Mietverträge
- Gemeinde: Geburtsurkunden, Personendaten
- Hotel: Gästelisten, Bestätigungen, Offerten, Anfragen

Welchen digitalen Risiken sind Sie ausgesetzt?

- Datendiebstahl (Vertraulichkeit)
- Datenmanipulation (Integrität)
- Datenverlust (Verfügbarkeit)

Wie dringen Kriminelle zu den Kronjuwelen vor ? 1

Analogien zum 'traditionellen" Einbruch



Wie dringen Kriminelle zu den Kronjuwelen vor ? 2

Analogien zum 'traditionellen" Einbruch

Auskundschaften

- Umgebung
- Bewohner

- Website
- Social Media

Abtasten

- Schlösser kontrollieren
- Ungeschlossene Fenster / Türen

- Scannen nach offenen Ports
- Schwachstellenscan

Wie dringen Kriminelle zu den Kronjuwelen vor ? 3

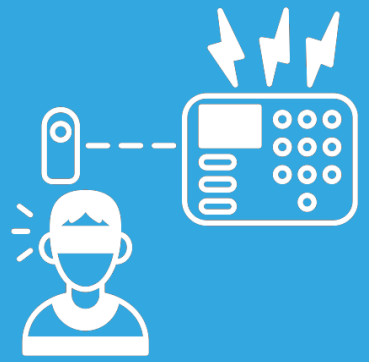
Analogien zum 'traditionellen" Einbruch

Einbrechen

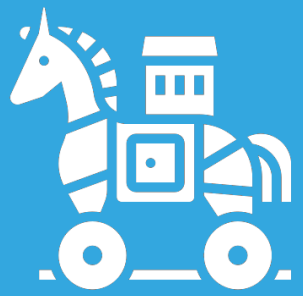
- Offenes Fenster / Türe
- Brecheisen

- Nicht aktualisierte Software
- Standard Passwort
- Wifi / Router / IOT

Zugang sichern & behalten



- Alarm ausschalten
- Knochen für den Hund



- Backdoor (Hintertür)
- Erstellen eines Benutzers

Wie dringen Kriminelle zu den Kronjuwelen vor ? 4

Analogien zum 'traditionellen" Einbruch

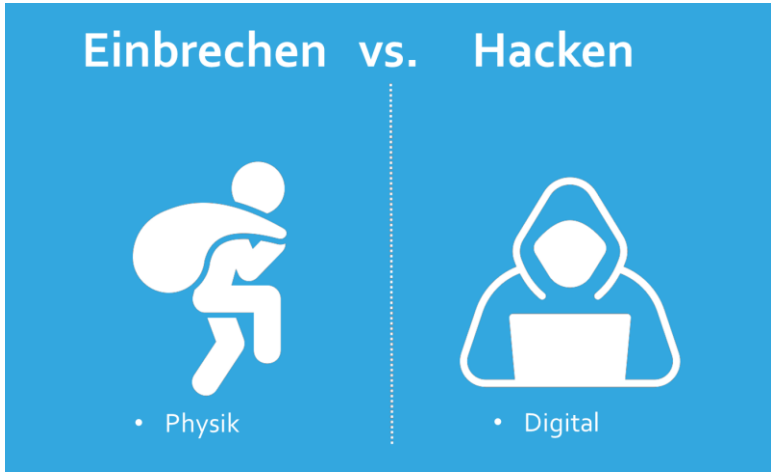
Juwelendiebstahl

Wie dringen Kriminelle zu den Kronjuwelen vor ? 5

Analogien zum 'traditionellen" Einbruch

Wie dringen Kriminelle zu den Kronjuwelen vor ? 6

Analogien zum 'traditionellen" Einbruch



- Erpressung: Lösegeldforderung
- Bereicherung: Verkauf der Daten im Darknet
- Plagiat: Intellektuelles Eigentum wird verwendet

Wo können Schwachstellen auftreten?

Frage an das Publikum

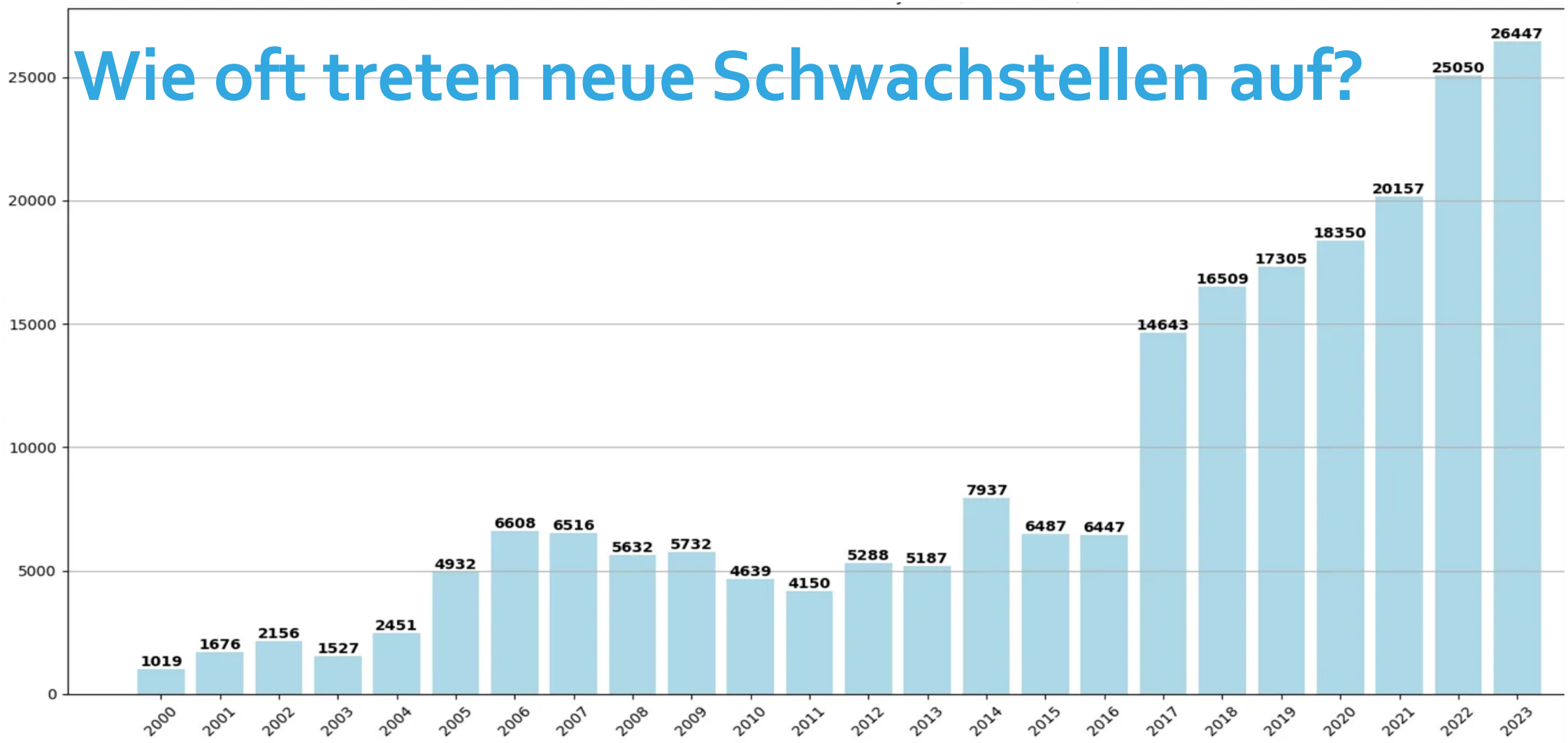
Was kommt ihnen ihnen in den Sinn wenn Sie an eine Computer-Schwachstelle denken?

Wo können Schwachstellen auftreten?

Verschiedene Gruppen von Schwachstellen

- Software Bug
- Firmware Vulnerability
- Ungesicherter Service im Netzwerk
- Schwache Authentifizierungsprozedur
- Veraltete Software oder Firmware
- Unsichere Standardkonfiguraion
- Ungenügende Netzwerksegmentation
- keine Verschlüsselung
- Kein oder ungenügendes Monitoring
- Injektierung

Wie oft treten neue Schwachstellen auf?



Qualys https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one

Wie verhindern Sie einen unerwünschten Zugriff? 1

Bei freudiger IT security machen wir das s

- Begreifen und Planen
- Gründlich Prüfen
- Verständliche Ergebnisse
- Durchblick bzw. Überblick sicherstellen

Wie verhindern Sie einen unerwünschten Zugriff? 2

Bei freudiger IT security machen wir das so

Begreifen und planen:

Ihr Unternehmen verstehen.
Ausführliche Gespräche mit allen Stakeholdern, Verantwortlichen

Wie verhindern Sie einen unerwünschten Zugriff? 2

Bei freudiger IT security machen wir das so

Gründlich Prüfen:

Wir testen was für ihr Unternehmen relevant ist.

Wie verhindern Sie einen unerwünschten Zugriff? 2

Bei freudiger IT security machen wir das so

Verständliche Ergebnisse:

Klar formulierte und umsetzbare Handlungsempfehlungen.

Wie verhindern Sie einen unerwünschten Zugriff? 2

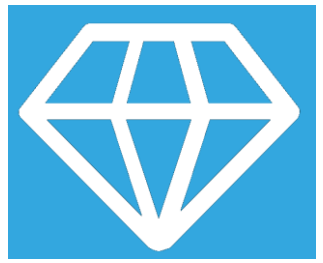
Bei freudiger IT security machen wir das so

Durchblick sicherstellen :

Wir stellen sicher, dass alle Beteiligten die Resultate und deren Bedeutung verstehen.

Was tun, wenn es zu spät ist?

- Security Incident Response Plan
- Externer DFIR-Dienstleister einschalten
- Eventuelle Meldepflicht
- Offline Backup
- Stift & Papier & FAX



Fragen und Anmerkungen zum Thema „Wie schütze ich meine Unternehmens-Kronjuwelen“

awareness4you

MIT HERZ, HAND UND VERSTAND EINE GESUNDE SICHERHEITSKULTUR AUFBAUEN

Das Herzstück Ihrer Cybersicherheit

Security Today by UCSP

awareness4you

Sandra Aengenheyster

- Leidenschaftliche Botschafterin für Cybersicherheit und IT mit fast 25 Jahren Erfahrung in diesen Bereichen
- Ev. Diplomtheologin mit Executive MBA in International Management
- Autorin, Moderatorin und Strategin für digitale Sicherheitskultur
- Umsetzerin von Sensibilisierungskampagnen für Cybersicherheit

Security Today by UCSP

Agenda

- Daten & Informationen schützen
- Drei Säulen des Schutzes
- Cybersicherheit und Sensibilisierung
- Umsetzung im Unternehmen

Security Today by UCSP

Agenda

- Daten & Informationen schützen
- Drei Säulen des Schutzes
- Cybersicherheit und Sensibilisierung
- Umsetzung im Unternehmen

Security Today by UCSP

Das ist Markus

Markus erhält einen Anruf aus der IT-Abteilung. Der Anrufer benötigt dringend Zugang zu bestimmten Daten für ein Update. Markus, der helfen möchte und den Anrufer für legitim hält, gibt die geforderten Informationen preis.

...was geschah dann?

Security Today by UCSP

Kunden-informationen

Namen, Adressen, Telefonnummern, E-Mail-Adressen und insbesondere Zahlungsinformationen, sind für die Aufrechterhaltung der Kundenbeziehungen und für Transaktionen unerlässlich.

Finanzdaten

Bankinformationen, Bilanzen, Investitionsberichte, Gehaltsabrechnungen und andere sensible Finanzunterlagen

Geschäftsgeheimnisse, geistiges Eigentum

Produktentwürfe, Patente, Geschäftsstrategien und Forschungsdaten

awareness4you

Security Today by UCSP

Agenda

- Daten & Informationen schützen
- Drei Säulen des Schutzes
- Cybersicherheit und Sensibilisierung
- Umsetzung im Unternehmen

Security Today by UCSP

Schutzbedarfe

Vertraulichkeit (Confidentiality)

Integrität (Integrity)

Verfügbarkeit (Availabilty)

Security Today by UCSP

Agenda

- Daten & Informationen schützen
- Drei Säulen des Schutzes
- Cybersicherheit und Sensibilisierung
- Umsetzung im Unternehmen

Security Today by UCSP

Cyber-Sicherheit

zielt auf die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer überlebenswichtigen Daten und Informationen. Cyber-Sicherheit meint die Sicherheit von Technologie, Organisation und Menschen sowie die Schnittstellen und Interaktion zwischen diesen.

awareness4you

Security Today by UCSP

Sensibilisierung für Cyber-Sicherheit

richtet sich insbesondere auf die Menschen, indem sie aufklärt, erklärt und trainiert. Das Ziel ist es, Gefahren zu erkennen und richtig zu reagieren. Also zu lernen, wie Technologie und Organisation (z.B. Richtlinien und Prozesse) zum Schutz vor Cyber-Kriminalität eingesetzt werden.

awareness4you

Security Today by UCSP

- Technologie
- Prozesse
- Menschen

Kommunikation & Kultur

Security Today by UCSP

Stärken oder Schwächen?

Social Engineering

Die meisten Menschen…

…sind **hilfsbereit**

…sind **höflich**

…mögen Menschen, die ihnen **ähnlich** sind

…möchten **geschätzt** werden

…sind (oder wirken) gerne **gut informiert**

…können nicht gut **„Nein"** sagen

Security Today by UCSP

Agenda

- Daten & Informationen schützen
- Drei Säulen des Schutzes
- Cybersicherheit und Sensibilisierung
- Umsetzung im Unternehmen

Security Today by UCSP

Gute technische Lösungen allein schützen nicht!

Herz

„Geht mich nichts an und hat mit mir nichts zu tun?“

Hand

„Höre nie auf zu lernen, denn Cyberkriminalität hört nie auf zu lehren“

Verstand

„Was ich nicht weiß, macht mich nicht heiß?“

awareness4you

diag DIENSTLEISTUNGEN AG

Security Today by UCSP

MOONEN COMMUNICATIONS

Beispiele Maßnahmen

Cyber-Security-Awareness-Training	x		x
Phishing-Kampagne		x	x
Phishingtool für E-Mail-Programm		x	
Escape room/ Cyber-Security Game	x	x	x
Management-Veranstaltung	x		x
Awareness Workshop Serie mit Fachbereichen	x	x	x
Simulationen realer Bedrohungssituationen		x	x
Notfallkarte			x
Info-Bundle mit Notfallhandbuch und Instruktionen			x
Poster	x		x
Give-aways	x		x
Arbeitsanweisungen			x
Brown bag session-Serie	x		x
Awareness-Tag mit Infos, Quizzes, Sprechstunde, Games	x	x	x
E-Learning		x	x
Aufbau Teams-, Slack-Kanal oder Wiki mit relevantem Content	x		x

Vorbild sein

Konkrete Umsetzung

- Regelmäßige Schulungen und Awareness-Programme für alle Mitarbeitenden
- Klare Kommunikation der Sicherheitsrichtlinien und -verfahren
- Schaffung eines sicheren Kanals für die Meldung von Sicherheitsvorfällen
- Regelmäßige Überprüfungen und Aktualisierungen der Sicherheitsmaßnahmen
- Förderung einer Kultur der Offenheit, in der Fehler als Lernchancen gesehen werden

Kommunikation

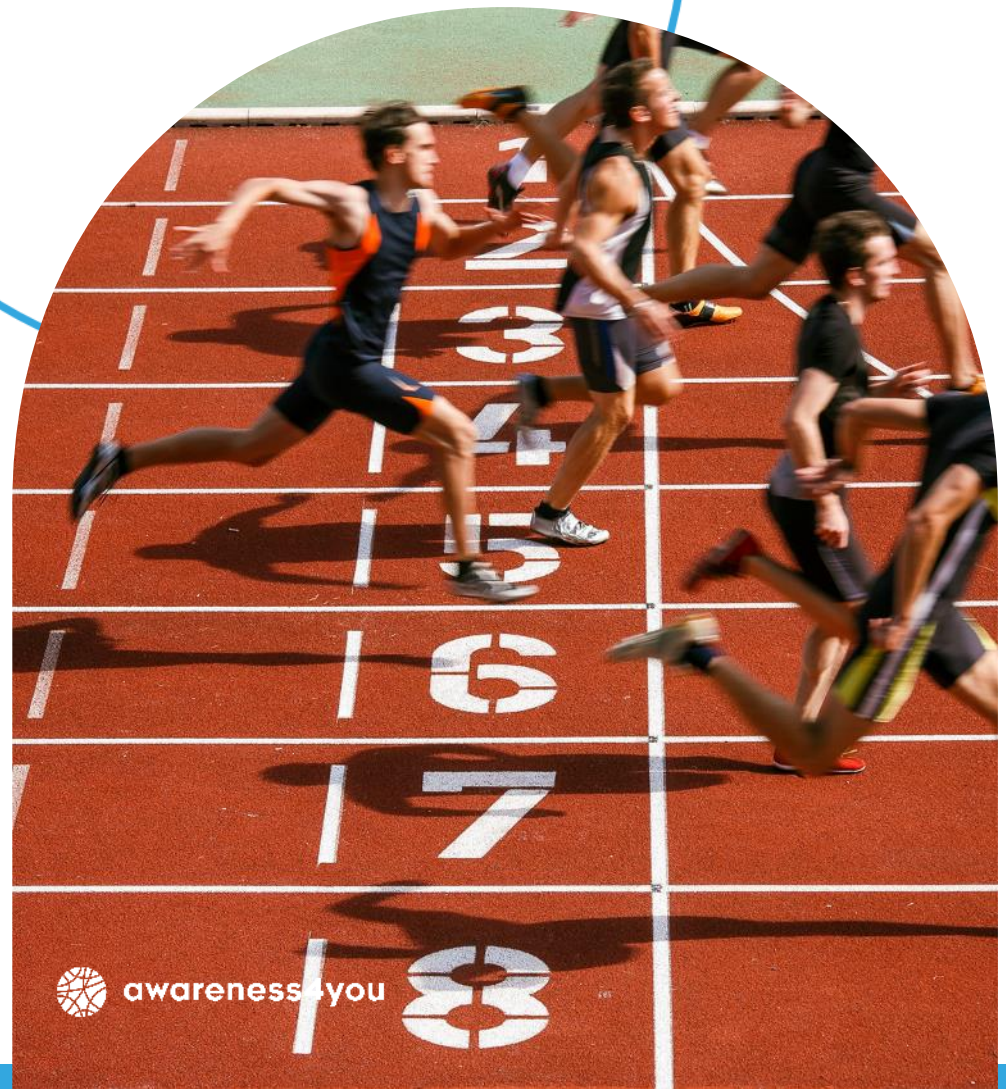
...ist ein Marathon, kein Sprint

...muss trainiert werden

...Fitness und Kondition führen zum Ziel

...Gemeinsam läuft es sich besser

Security Today by UCSP



Nach dem Rennen ist vor dem Rennen

Ziel erreicht?

Mitarbeitende

...kennen die Gefahren und Angriffspunkte von Cyberkriminellen

...wissen, wie sie im Zweifelsfall oder Ernstfall handeln müssen

...sind Verbündete im Kampf gegen Cyber-Kriminalität und handeln proaktiv in ihrem Sinne und zum Wohle des Unternehmens

Security Today by UCSP

Agenda

- Daten & Informationen schützen
- Drei Säulen des Schutzes
- Cybersicherheit und Sensibilisierung
- Umsetzung im Unternehmen
  - Resilienz des gesamten Unternehmens

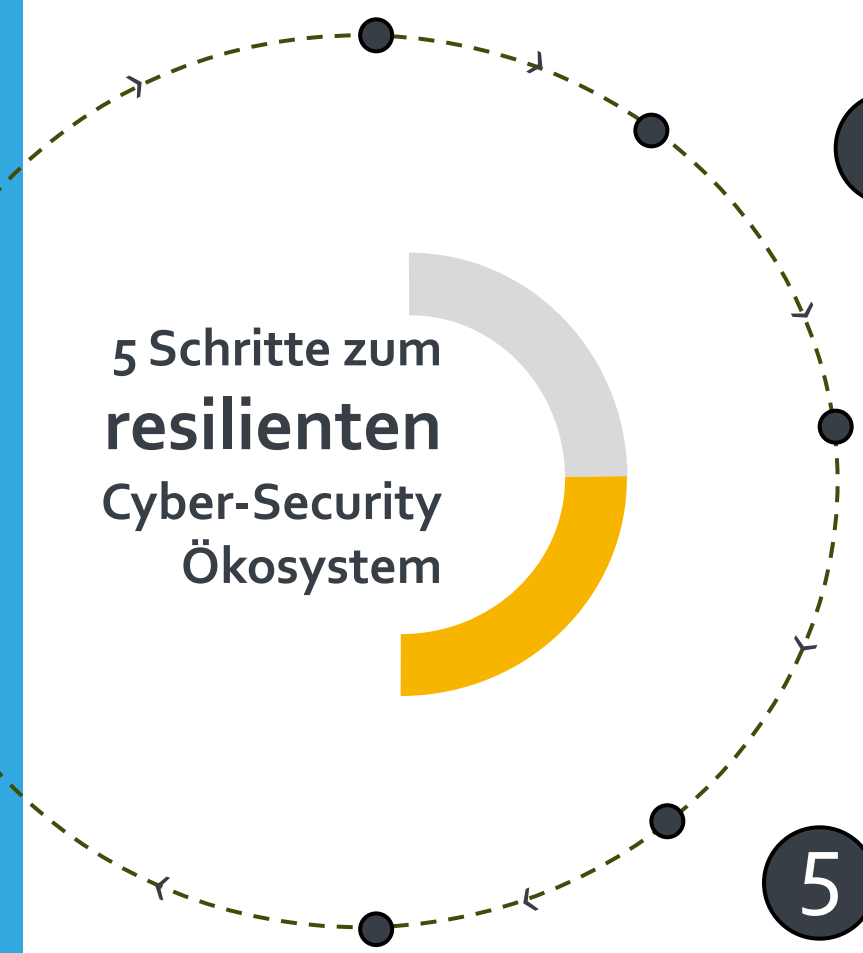
Security Today by UCSP

Resilienz

Vorbeugen, Schaden reduzieren, wiederherstellen

Link zum Buch

5 Schritte zum resilienten Cyber-Security Ökosystem



1 Ziele

Ziele definieren

- Schutzziele identifizieren & bewerten
- Risiken evaluieren
- Ausgangssituation ergeben
- Geltungsbereich definieren
- Projektteam zusammenstellen
- Vorgehensweise festlegen

2 Ist-Zustand

Maturität & Delta erheben

- Feststellung Ziele sowie Zeit- & Ressourceneinsatz
- Erhebung des Status Quo
- Soll-Ist-Vergleich: Status Quo zu avisiertem Zielbild
- Feststellung des Deltas: Status Quo zu avisiertem Zielbild
- Festlegung des beabsichtigten Aufwandes

3 Lösungen

Lösungen & Fahrplan ableiten

- Lösungsentwicklung anhand der identifizierten Handlungsfelder
- Bewertung der Lösungen (Machbarkeit, Abwägen Aufwand/Nutzen)
- Fahrplan inkl. Zeit- und Ressourcenplan erstellen

4 Maßnahmen

Maßnahmen umsetzen & Prozesse verankern

- Durchführung von Pilotprojekten, um Akzeptanz und Wirksamkeit zu testen
- Während der Umsetzung regelmäßig überprüfen, ob die Maßnahmen greifen und verstanden werden
- Konsistente Botschaften senden (Kommunikation)
- Auf Beteiligung des Kernteams achten (inkl. Management)

5 Erfolge

Ergebnisse überwachen & optimieren

- Messung des Erfolgs
- Regelmäßige Kontrolle der Situation
- Befragung Mitarbeiter und Kernteam
- Sammlung von Verbesserungsoptionen

awareness4you

Security Today by UCSP

Sandra Aengenheyster

awareness4you

www.awareness4you.de

info@awareness4you.de

Security Today by UCSP