Herzlich Willkommen

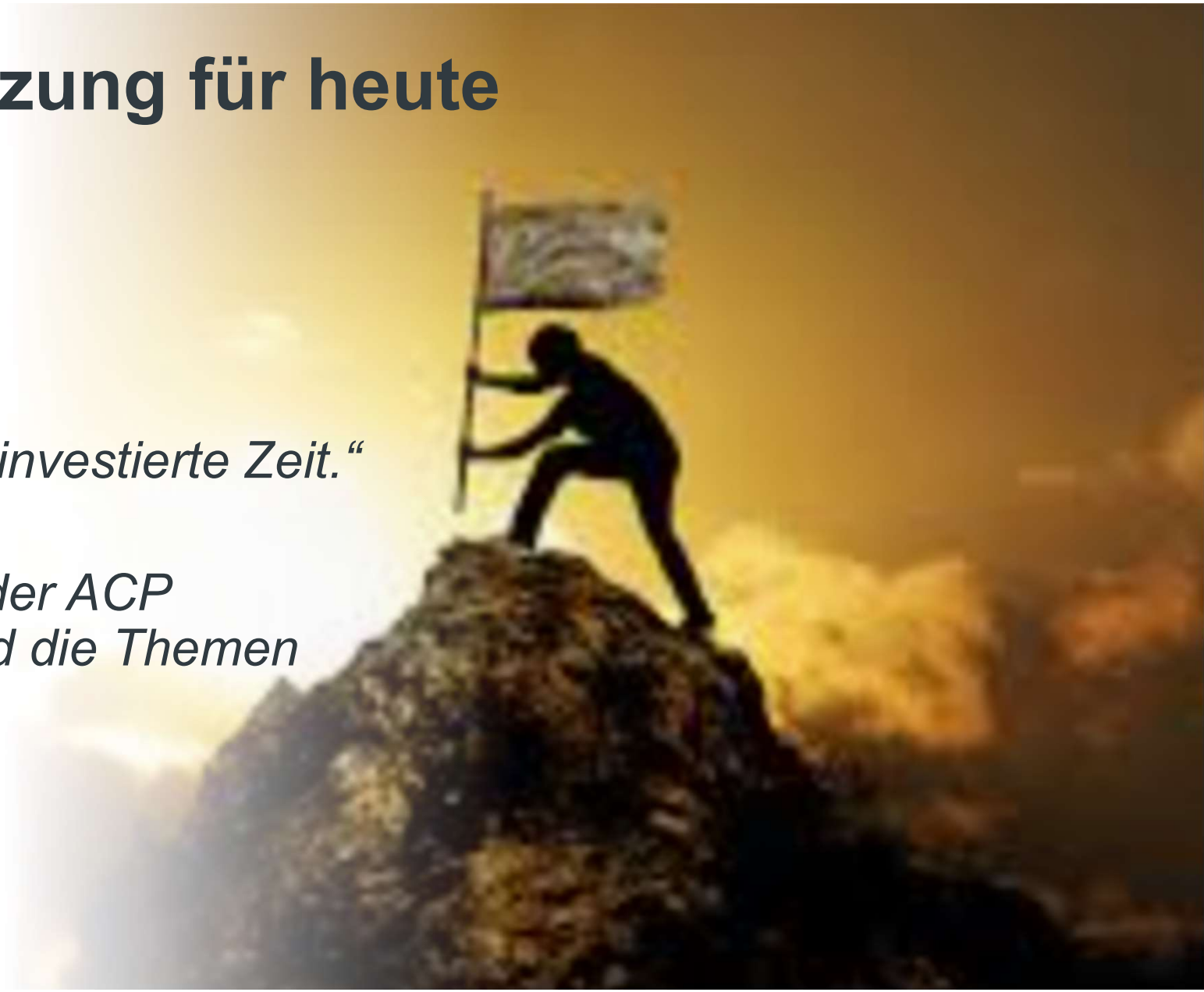
zum ACP Jahresauftakt 2024

Unsere Zielsetzung für heute

dass Sie sagen:

„Der Tag war wertvoll investierte Zeit.“

„Wir müssen uns mit der ACP zusammen setzen und die Themen diskutieren.“



TOP Thema 2024 – KI

KI – Zitate/Einschätzungen

«Das Aufk *hlimmste, was der M*
– Stepher

«KI ist gef
– Elon Mu

«KI wird a
– Professo

"KI wird echte Schäden anrichten", glaubt ein Microsoft-Topmanager – und warnt trotzdem vor Begrenzungen

KI – Chancen und Risiken

KI – Chancen und Risiken

Bild

Falsche Todesmeldung

Haaland von künstlicher Intelligenz erschossen

KI – Chancen und Risiken

Air Canada

Chatbot verspricht Fluggast irrtümlich Rückerstattung – Airline muss zahlen

Er gewährte einen Rabatt, den es gar nicht gab: Weil ein Chatbot gegen die eigenen Richtlinien verstieß, wollte Air Canada einen Kunden auf dessen Kosten sitzen lassen. Nun entschied ein Gericht gegen das Unternehmen.

19. Februar 2024, 21.22 Uhr • 1 Min

KI – Stimmen, Bilder, Videos, ……

"Hurra, hurra, der Pumuckl ist da!"

KI – Stimmen, Bilder, Videos, ……

KI – Stimmen, Bilder, Videos, ……

KI – Stimmen, Bilder, Videos, ……

tagesschau Sendung verpasst?

KI im US-Wahlkampf

Falscher Biden fordert zum Zuhausebleiben auf

Stand: 23.01.2024 10:17 Uhr

Das Telefon klingelt - und der US-Präsident ist am Apparat. So ging es Wählern im US-Bundesstaat New Hampshire. Die Überraschung war sicher groß, doch die Stimme war gefälscht. Der Generalstaatsanwalt hat eine Untersuchung angekündigt.

Kurz vor den ersten Vorwahlen der US-Demokraten in New Hampshire hat es offenbar einen Versuch der Wahlbeeinflussung gegeben.

KI – Chancen und Risiken

Das BSI Themen IT-Sicherheitsvorfall Karriere Service

Generative KI sorgt für neue Risiken, aber auch für neue Chancen

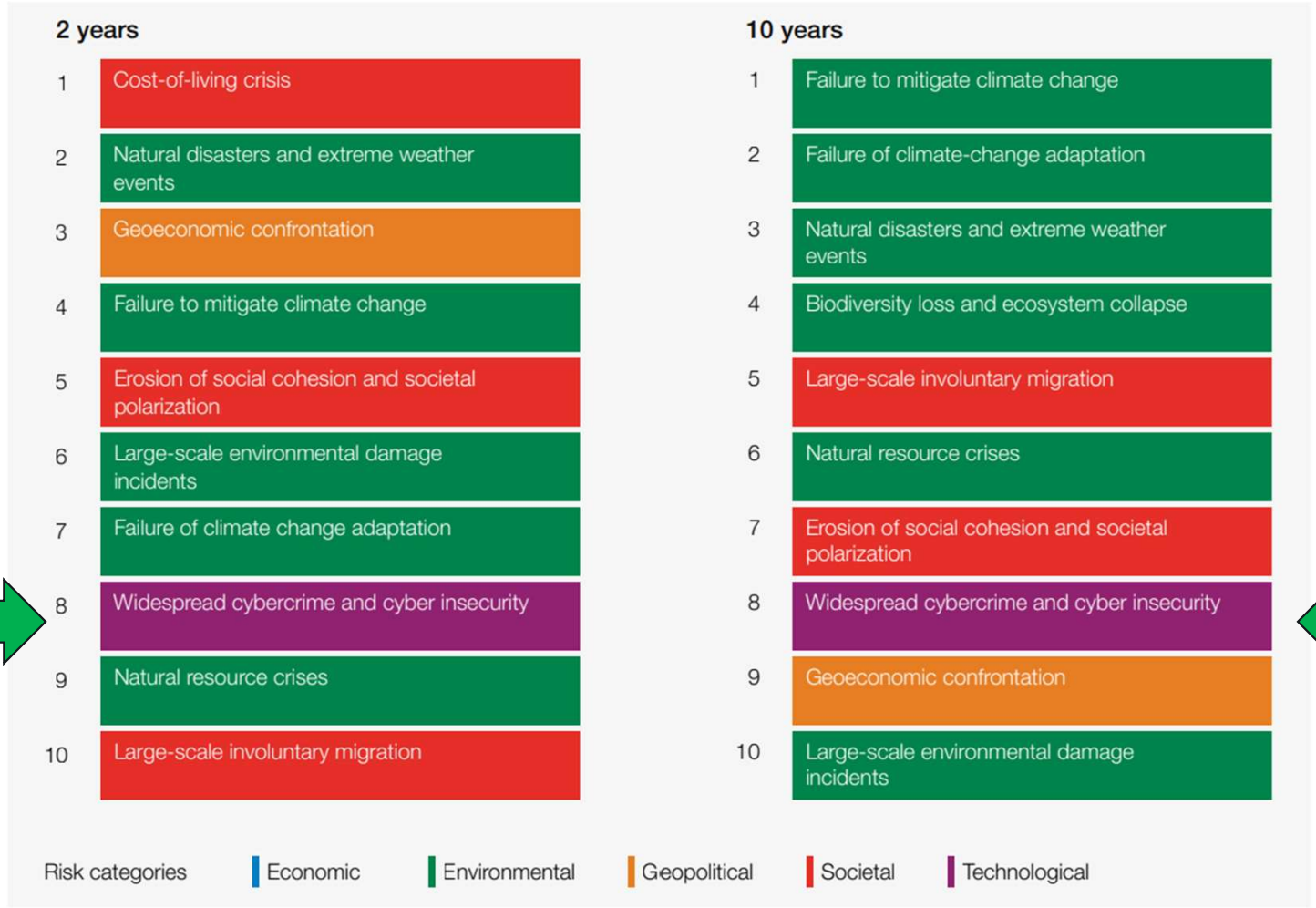
Mit ChatGPT, Bard und LlaMa sowie einer Vielzahl weiterer Tools ist Künstliche Intelligenz in einer breiten, auch wenig technikaffinen Öffentlichkeit angekommen. Diese Tools sind einfach zu bedienen und liefern eine hohe Qualität. Dabei können sie auch für kriminelle Zwecke missbraucht werden. So können sie dafür sorgen, dass sogenannte Deepfakes – manipulierte Bilder, Videos und Stimmen - immer authentischer werden und dadurch immer schwerer zu entlarven sind. Auch kann KI Phishing-Mails glaubwürdiger machen, im Social Web zu Desinformationskampagnen beitragen oder selbst Schadcode generieren – und das wesentlich schneller und zum Teil wesentlich besser als menschliche Cyberkriminelle. KI kann auch selbst zur Schwachstelle werden. Sie kann gehackt und missbräuchlich eingesetzt werden. Das stellt das Schwachstellenmanagement in Unternehmen und Behörden vor noch nie dagewesene Herausforderungen.

Risiken

Weltrisikobericht

Der "Global Risks Report" ist ein Bericht, den die Schweizer Stiftung Weltwirtschaftsforum (abgekürzt WEF nach dem englischen Namen World Economic Forum) jährlich herausgibt.

Weltrisikobericht 2023



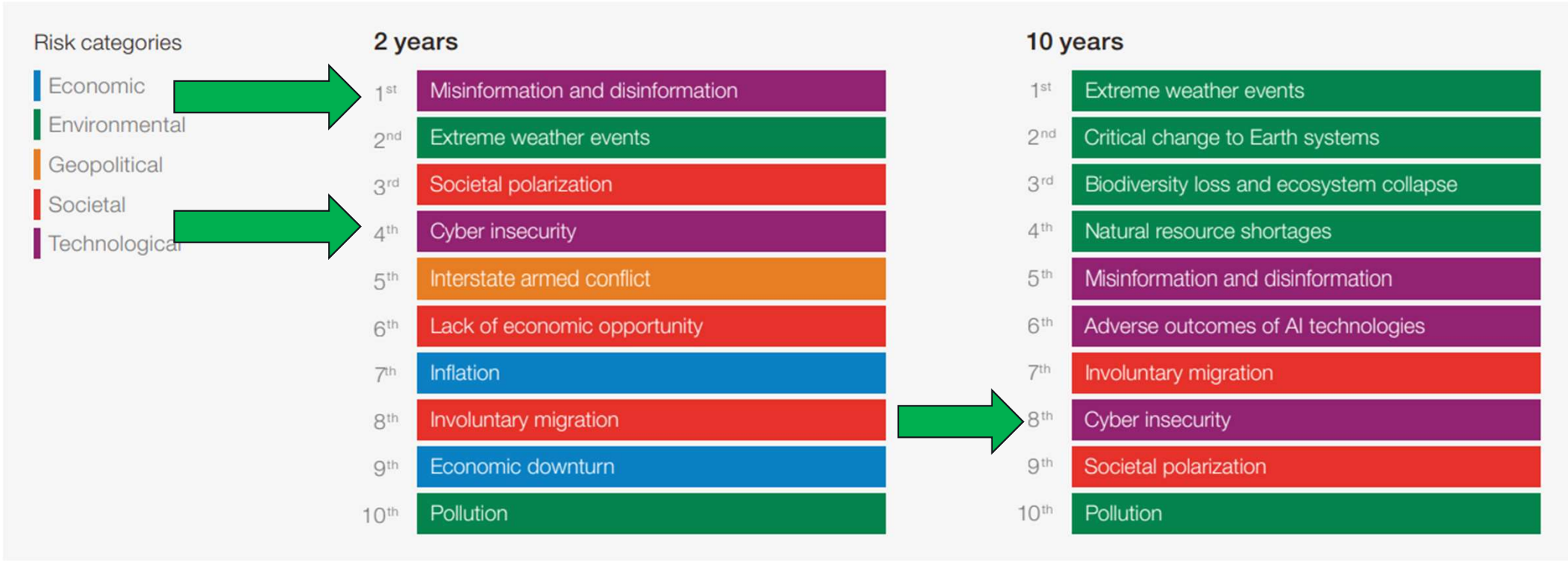
Weltrisikobericht 2024

Weltrisikobericht

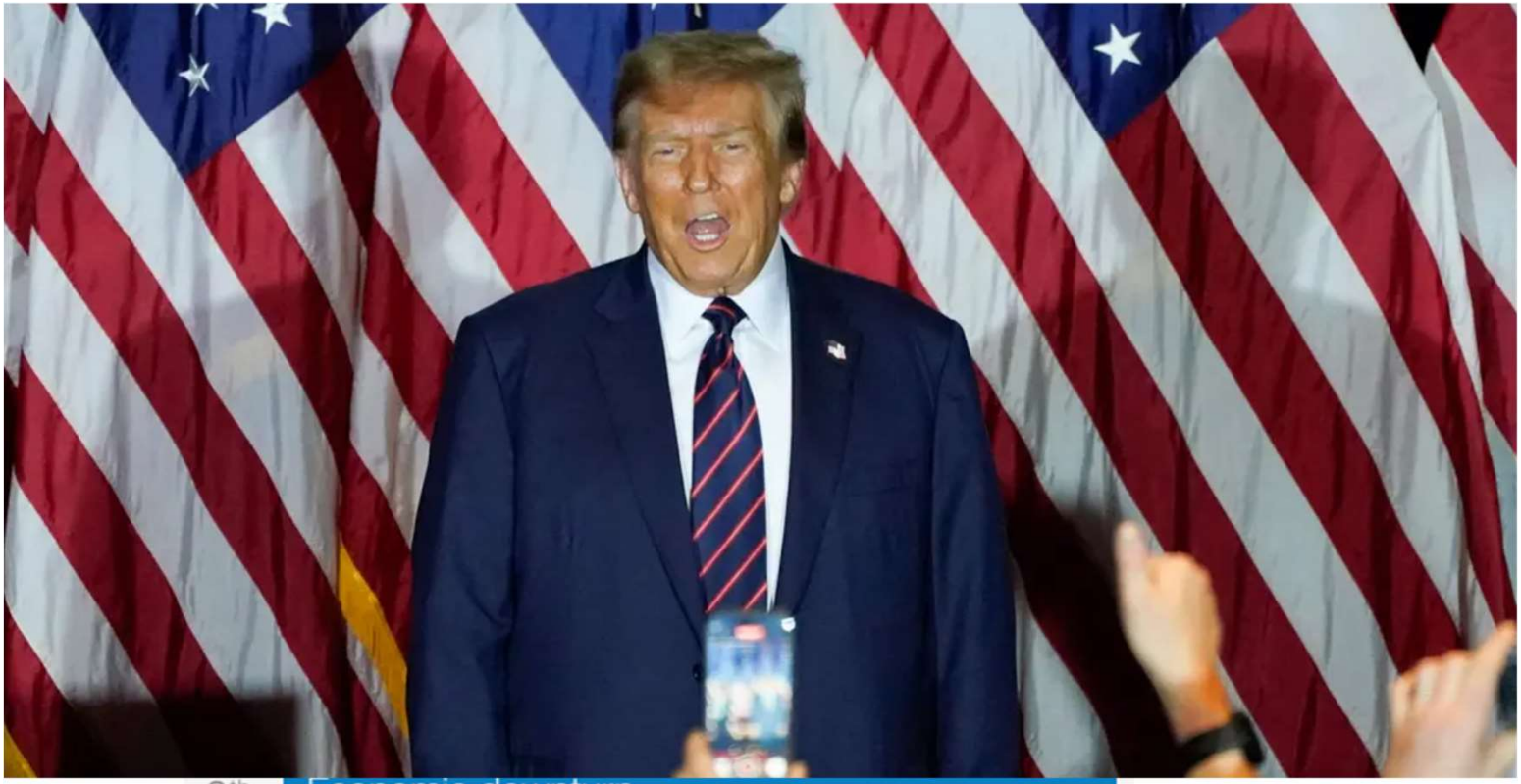
Der "Global Risks Report" ist ein Bericht, den die Schweizer Stiftung Weltwirtschaftsforum (abgekürzt WEF nach dem englischen Namen World Economic Forum) jährlich herausgibt.

"**Als größtes Risiko für die kommenden zwei Jahre nennt der Bericht Falsch- und Desinformation**, gefolgt von Extremwetter-Ereignissen, gesellschaftlicher Polarisierung und bewaffneten Konflikten", sagt Saadia Zahidi, Geschäftsführerin des Weltwirtschaftsforums

Weltrisikobericht 2024



Weltrisikobericht 2024 – was fehlt ?



9th Economic downturn

10th Pollution

…..auf Imp…ent zu erheben.

……. und den Krieg in der Ukraine kann ich in 24h lösen.

Der IT-Markt ……..

IT for innovators.

IT Markt

IT Markt

ChannelPartner

Daily mittags

27. Februar 2024

Folgen Sie uns auf

KKR greift für rund 4 Milliarden Dollar zu

Broadcom verkauft VMwares EUC-Sparte an Investor

Die beürchtete Filetierung von VMware nach der Übernahme von Broadcom beginnt: Für rund 4 Milliarden Dollar will Investor KKR jetzt die EUC-Sparte als eigenes Unternehmen an den Markt bringen. Weiterlesen

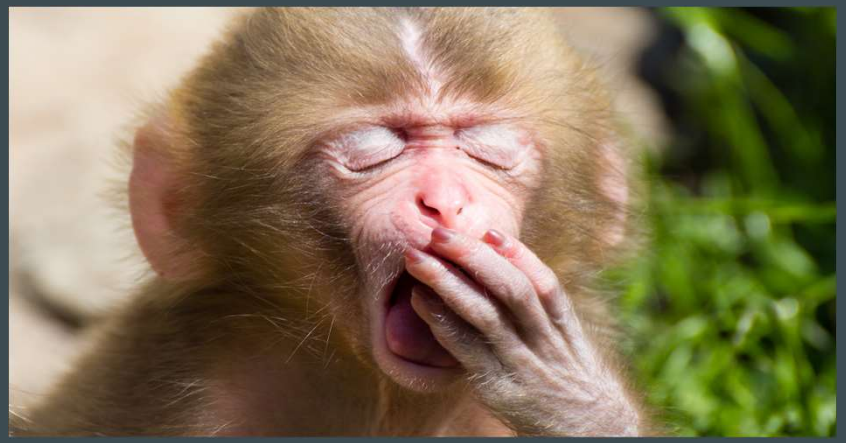
IT Markt

HPE kauft Juniper Networks für 14 Mrd. US$
Was bedeutet das für das jeweilige Portfolio ?

IT Markt

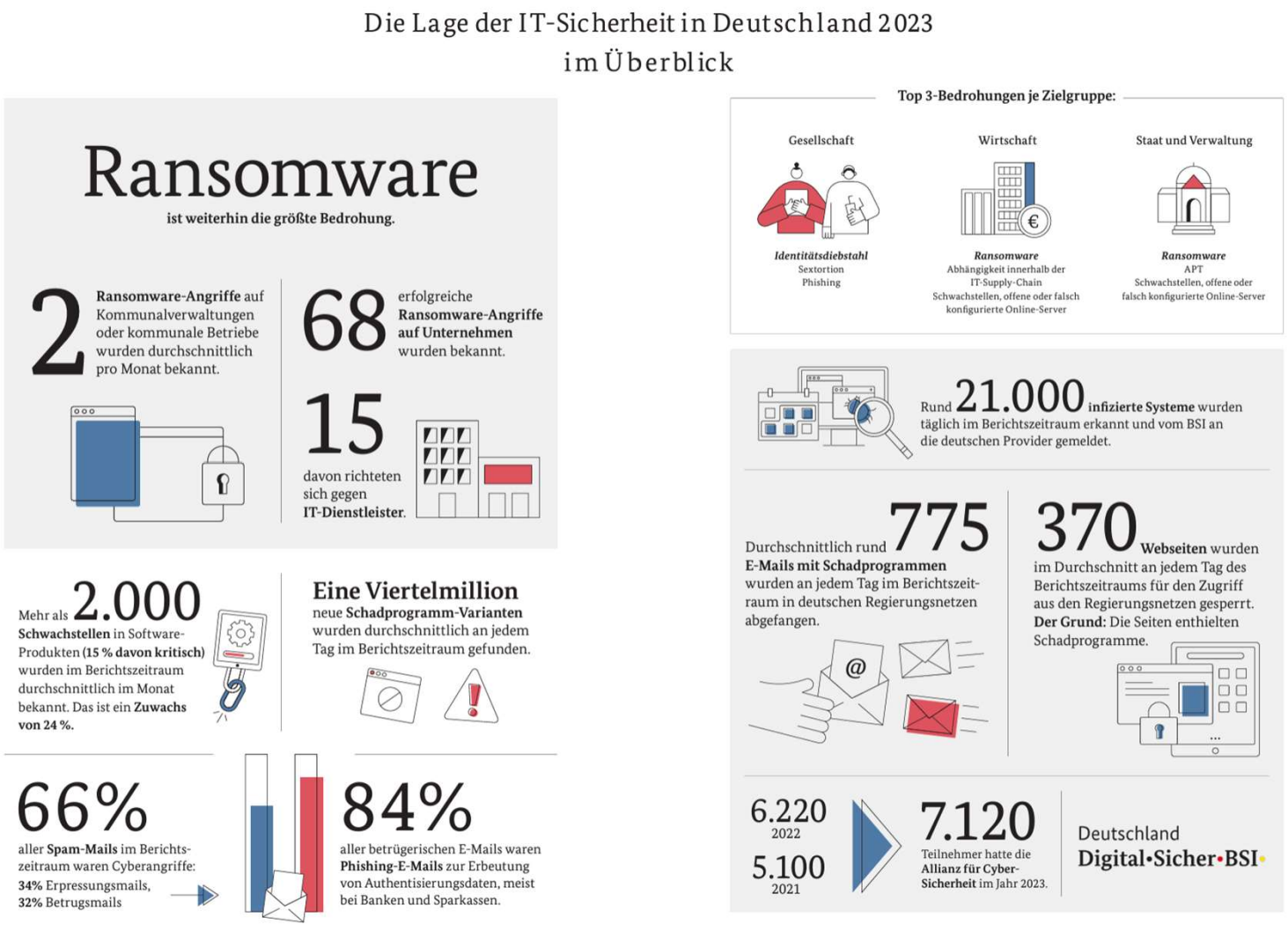
Cisco kauft Splunk für 28 Mrd. US$

IT-Sicherheit



IT for innovators.

IT Sicherheitslagebericht BSI



IT Sicherheit - Schwachstellenmanagement

Schwachstellen bei Software auf besorgniserregendem Niveau

Das BSI registriert immer mehr Schwachstellen in Software. Diese Schwachstellen sind oft das Einfallstor für Cyberkriminelle auf ihrem Weg zu einer Kompromittierung von Systemen und Netzwerken. Das BSI hat mit durchschnittlich knapp 70 neuen Schwachstellen in Software-Produkten pro Tag nicht nur rund ein Viertel mehr registriert als im Berichtszeitraum davor. Mit der Anzahl stieg auch ihre potenzielle Schadwirkung: Immer mehr Lücken (etwa jede sechste) werden als kritisch eingestuft.

Quelle: BSI

1. Cybercrime

Rückgang der erfassten Cyberstraftaten um 6,5% (Inlands-PKS). Auslandstaten steigen an.

Die Aufklärungsquote für Cybercrime bewegt sich mit ca. 29% auf dem Niveau des Vorjahres.

Der russische Angriffskrieg auf die Ukraine birgt auch im Cyberraum massives Eskalationspotential.

Ransomware bleibt primäre Bedrohung für Unternehmen und öffentliche Einrichtungen.

Phishing ist Haupteintrittsvektor für Schadsoftware und passt sich aktuellen gesellschaftlich relevanten Themen an.

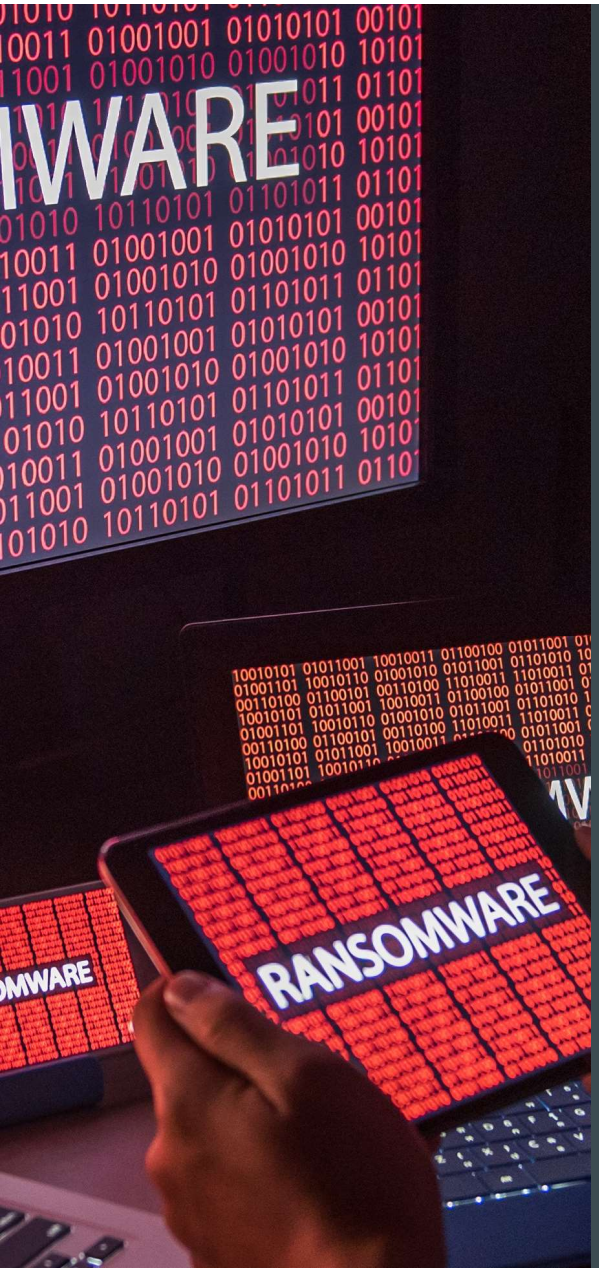
Quelle: CybercrimeBundeslagebericht 2022

Bedrohungslage

Cyberangriff -
alles verschlüsselt !
was nun?

Security (Vor)Fälle aus der Region
ein Erfahrungsbericht

IT for innovators.

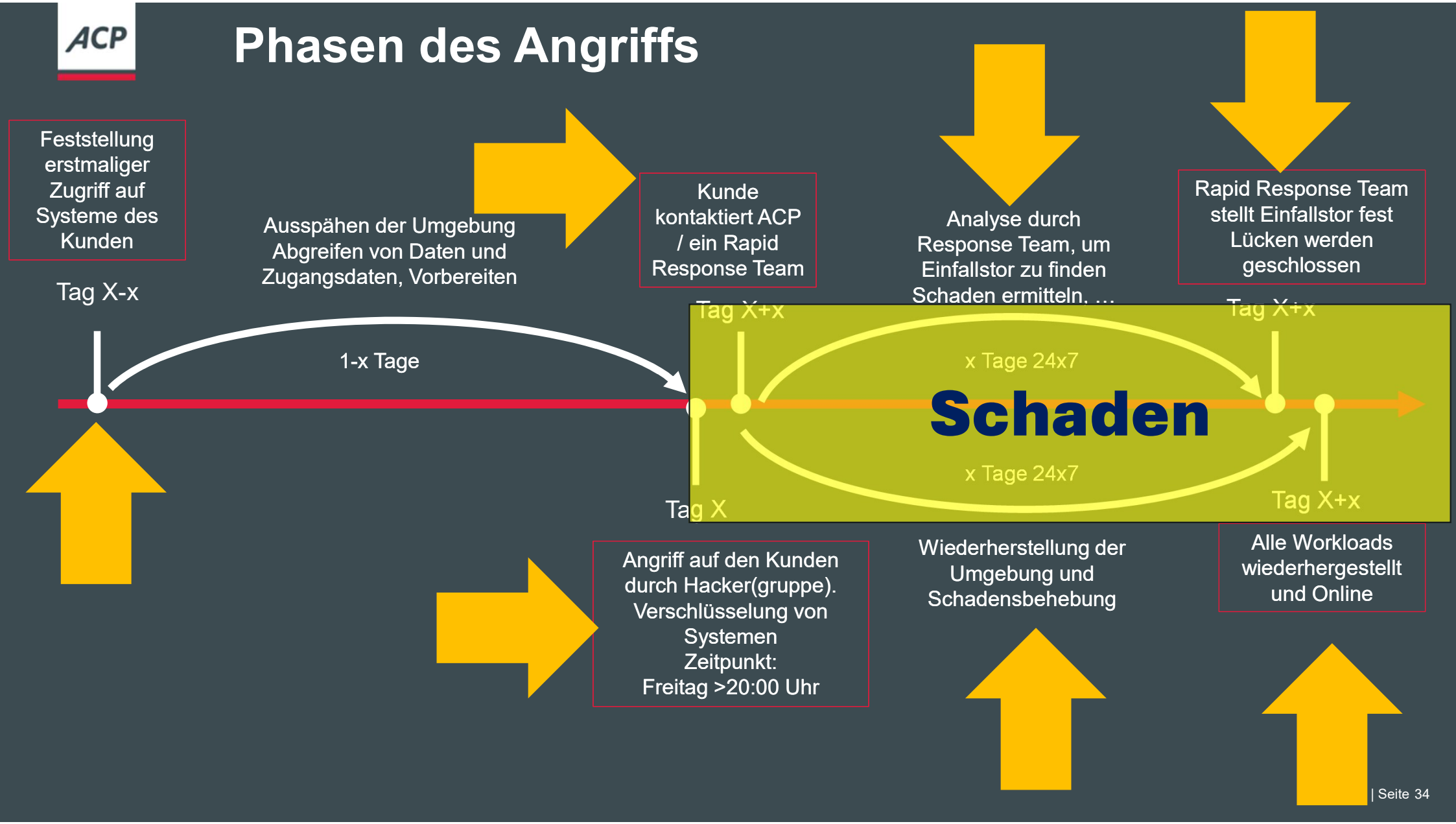


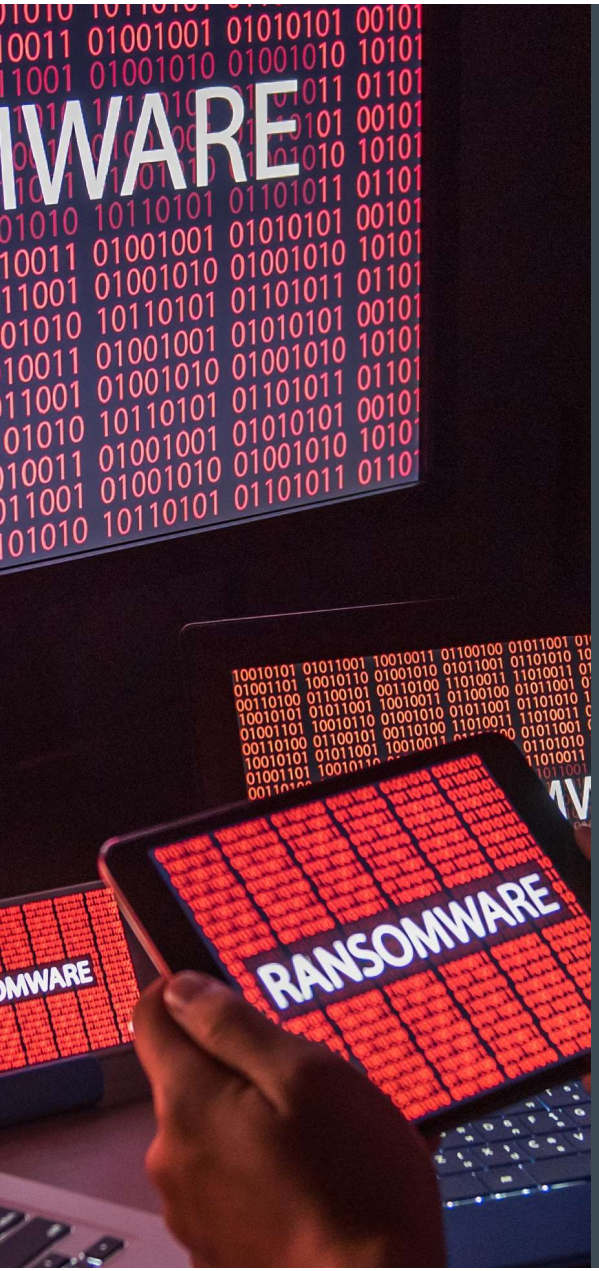
Ransomware = Erpressung

- verschlüsselte Daten oder „wir haben ihre Daten“
- meist organisierte Kriminalität
- oder staatlich organisiert (Datenklau)
- Es geht um Summen 1-XX Millionen
- Es trifft (mittlerweile) auch „kleine“ Firmen

…

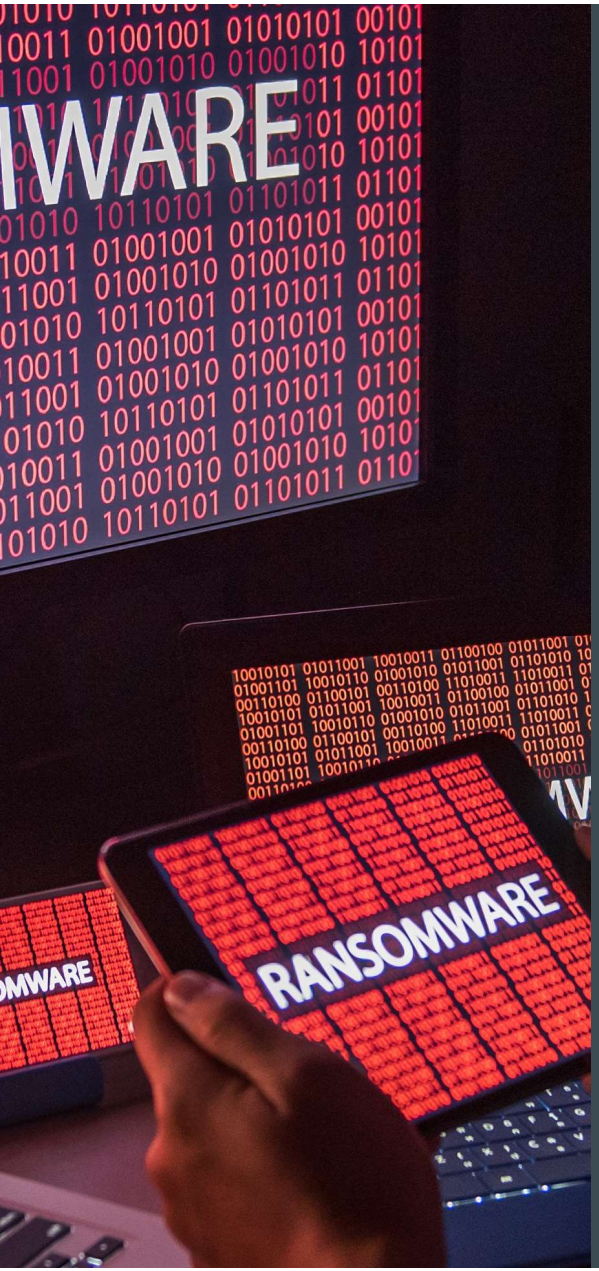
Phasen des Angriffs





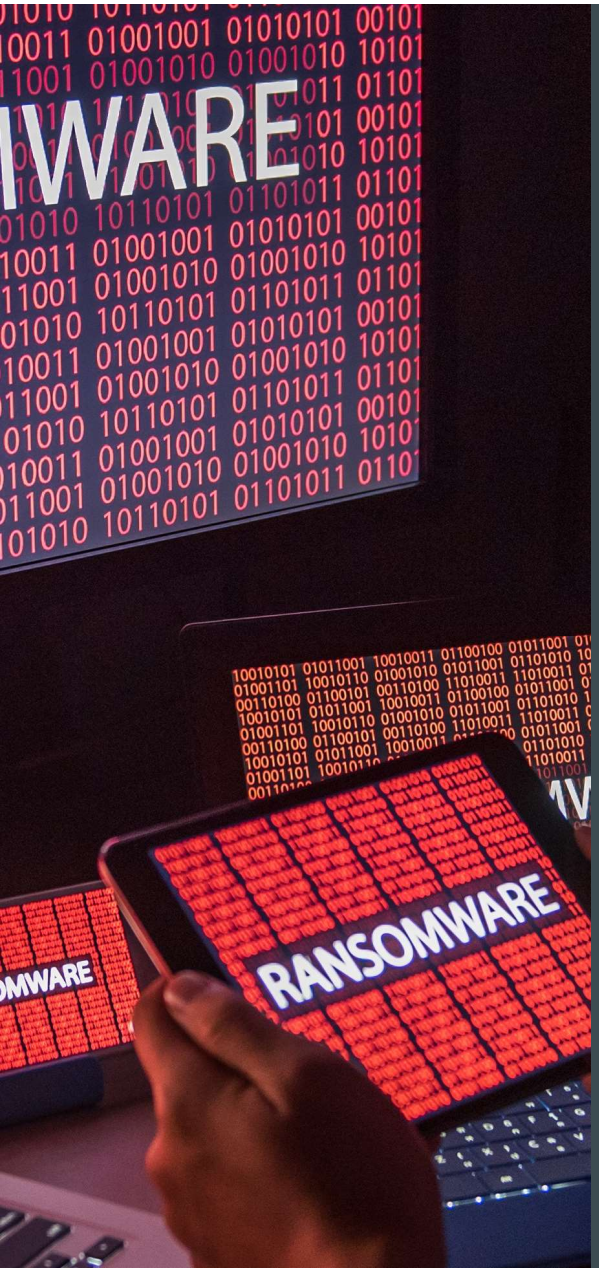
Angriffsvektoren und Angriffsmuster I

- Externer Zugriff mit User/Passwort
  ohne Multifaktor-Authentication
- Ausnutzen von bekannten Schwachstellen
  Keine aktuellen Sicherheitspatches installiert
- Keine oder unzureichende Netzwerksegmentierung
- Zentrale Systeme unzureichend abgesichert
  - Backupserver im selben Netz und im Active Directory
  - Backupserver für alle erreichbar
  - Backup Device(s) für alle erreichbar
  - Admin Accounts in use für…….



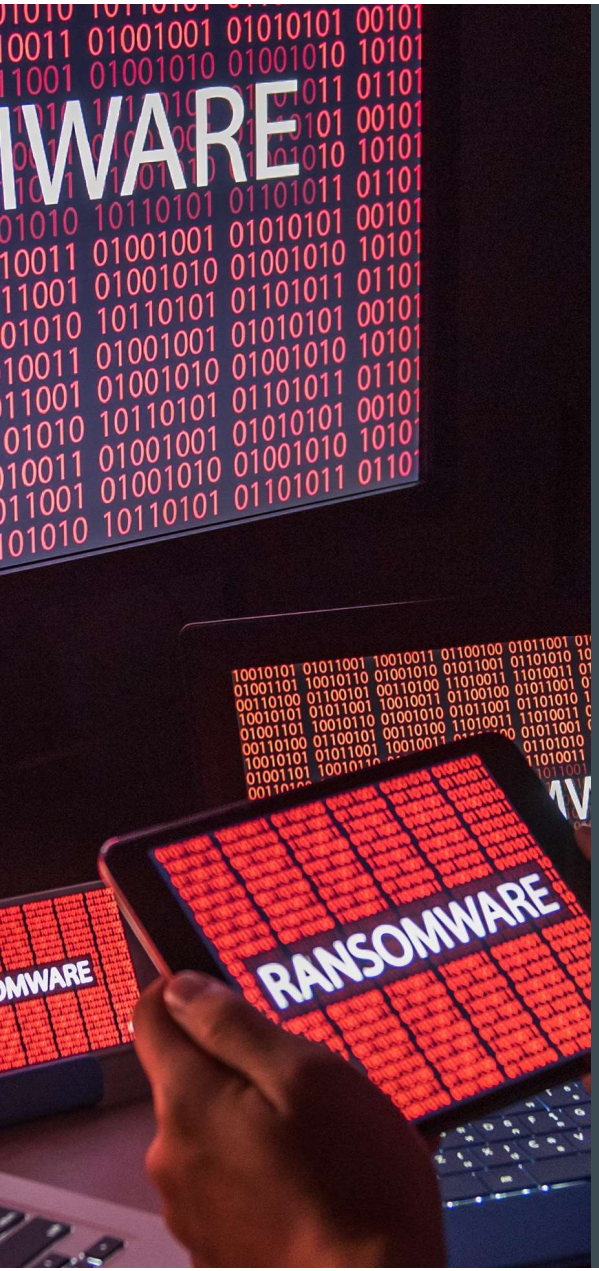
Angriffsvektoren und Angriffsmuster II

- Keine Kennwortrichtlinien
  - „altbekannte Kennwörter“ auf vielen Systemen
  - Ein Standardpasswort für viele Geräte
  - keine Sperren nach X Versuchen
  - Admin Accounts in use – schlechte Passwörter
- „Suboptimales“ Firewall-Regelwerk
- *EndPoint Protection (Virenscanner) (Strategie ?)*
- Fehlendes Logging/Logging-Historie
- Kein SIEM – keine Korrelation von Informationen
- Best Practice Empfehlungen werden oft ignoriert



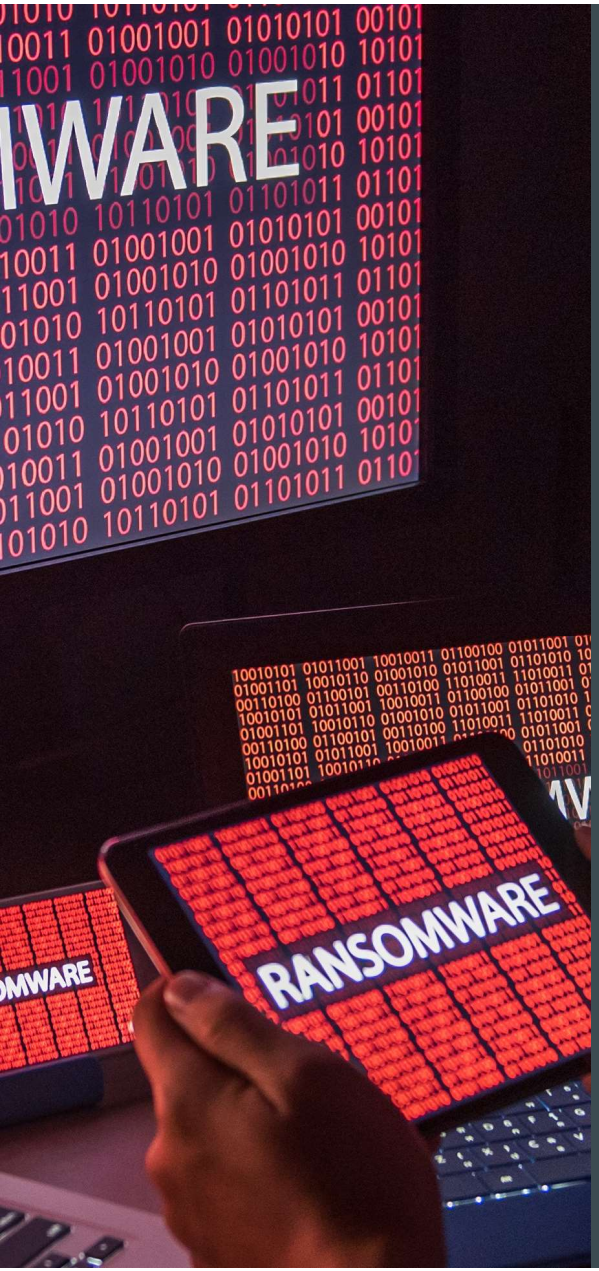
Sofortmaßnahmen

- Kappen der Internetanbindung



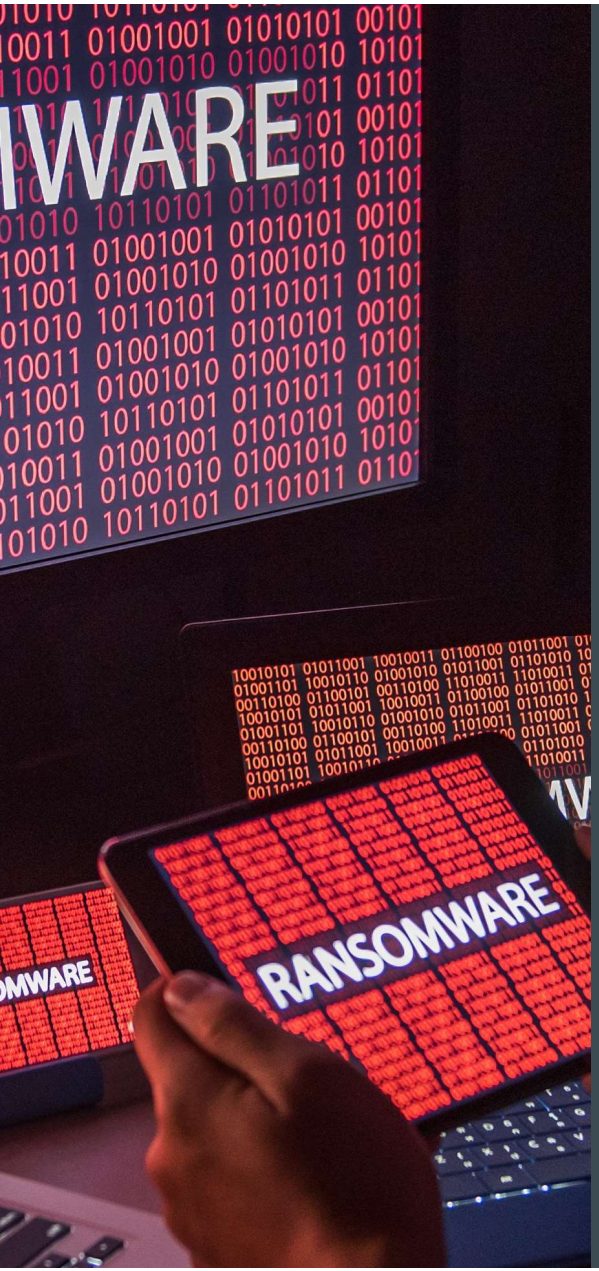
Sofortmaßnahmen

- Systeme ausschalten J/N



Sofortmaßnahmen

- Abschotten der internen Systeme

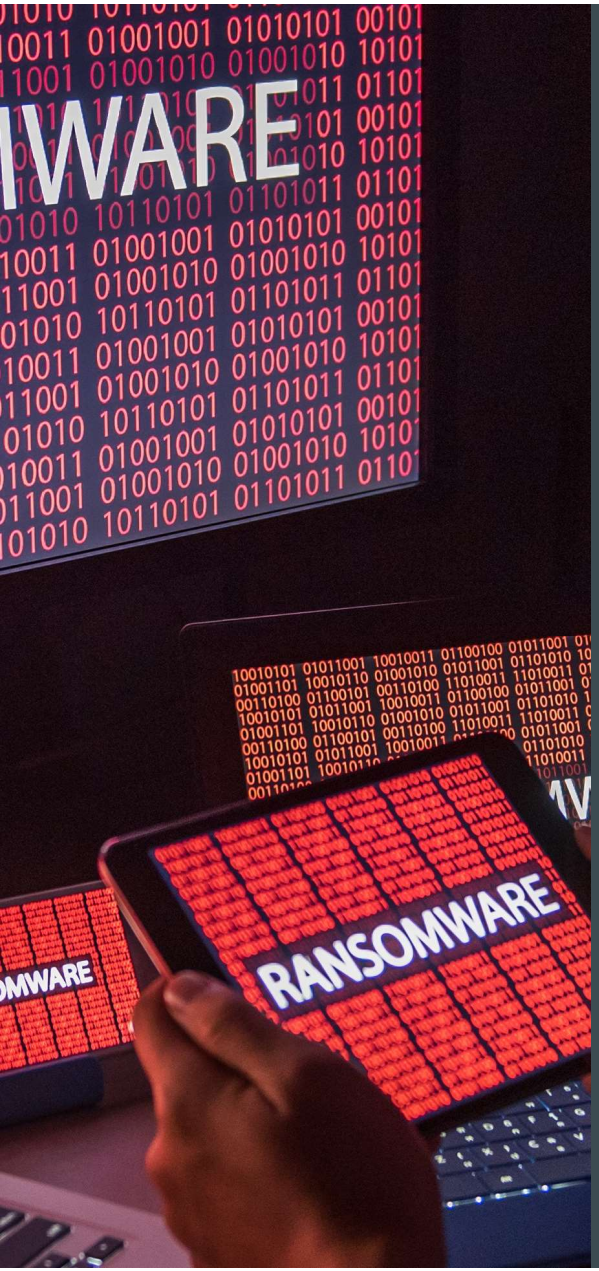


(Sofort)maßnahmen

- Notfallhandbuch raus holen
- Dienstleister + Response Team hinzuziehen
- Analyse durch Response Team
  - Betroffene Systeme finden
  - Angreifer identifizieren
  - Ausmaß und Zeitrahmen erkennen
  - Betroffene Systeme wiederherstellen,prüfen/bereinigen
  - Einfallstore lokalisieren
  - ….

WICHTIG:

Response Teams machen in der Regel Forensik und keine Restoreaktivitäten !!!



(Sofort)maßnahmen

- Ihre Systeme sind in der Regel nicht nutzbar !
  - da kompromittiert / verschlüsselt
  - diese für Forensik gebraucht werden
  - ggbf. Beweissicherung betrieben werden soll/muss
  - ……

Sie haben erstmal kein einsatzfähiges IT-System

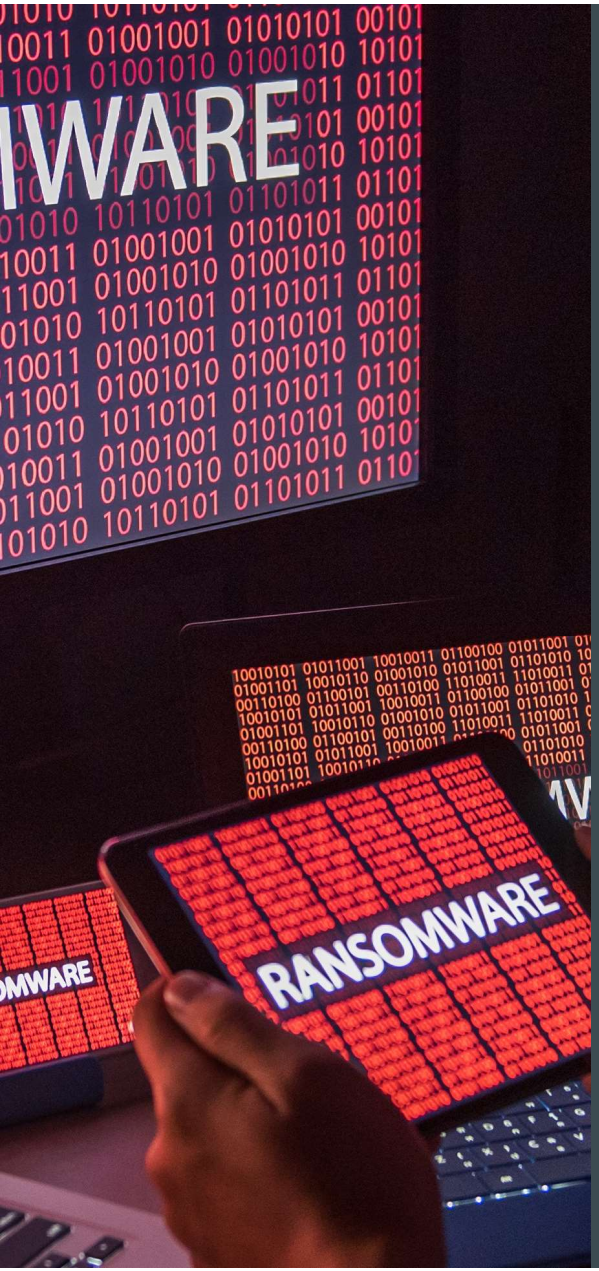
Sie brauchen ~~Starthilfe~~ ein Leihauto !

Ein ACP “Leihauto” ?

- Erkenntnisse aus vielen Einsätzen
- Was beschleunigt den Wiederanlauf ?
- Welche Dienste werden gebraucht ?
- Was können wir dafür (im Vorfeld) vorbereiten ?
- Wie unterstützen wir Response Teams ?
- ….

ACP „Cyber Rescue Service“

- Mobiles unabhängiges „Datacenter“
  - Mit **kundenspezifischer Betankung** in wenigen Stunden verfügbar
  - Für Kooperation mit Response Teams vorbereitet
- Isoliertes System das gekoppelt werden kann
- Virtuelle Umgebung mit zentraler Storage
- Unabhängiger physischer Backupserver
- Eigenes Routing, eigene IP Services
- Dedizierte Firewall mit eigenem WAN-Uplink
- Ein erfahrenes Spezialisten-Team mit Tools
- Wir bringen ein kundenspezifisch vorbereitetes System zum Einsatz.

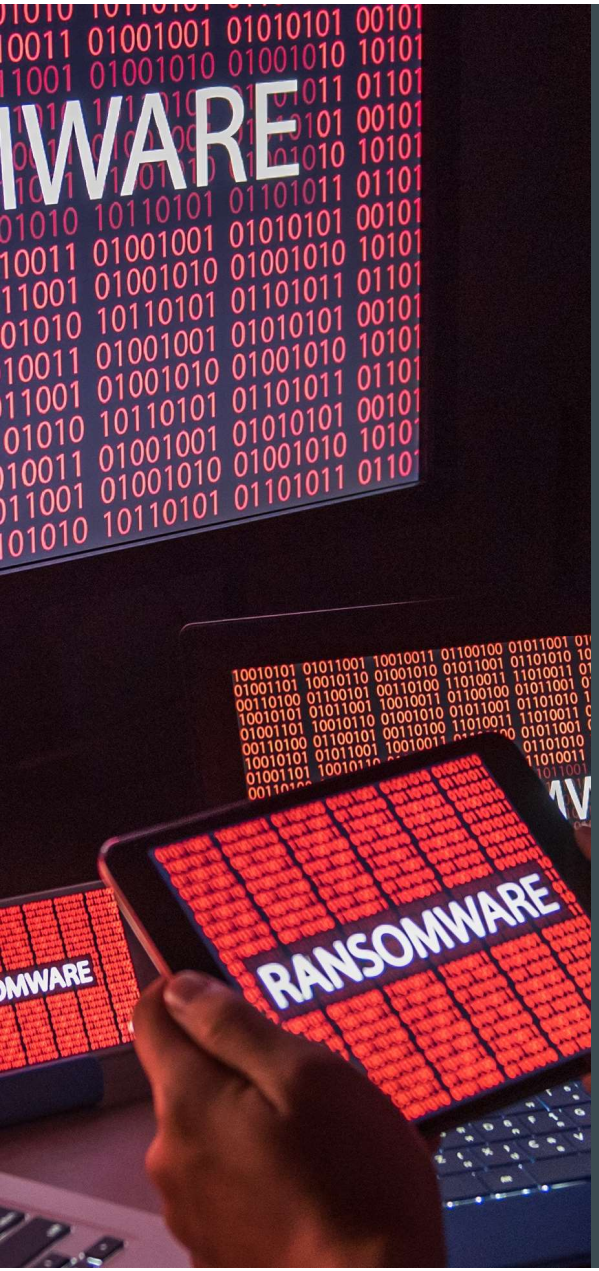


Security (Gesamt) Strategie

- Systembetrachtung
- Operative und organisatorische Security Strategie
- Gesamtkonzept - compliance konform

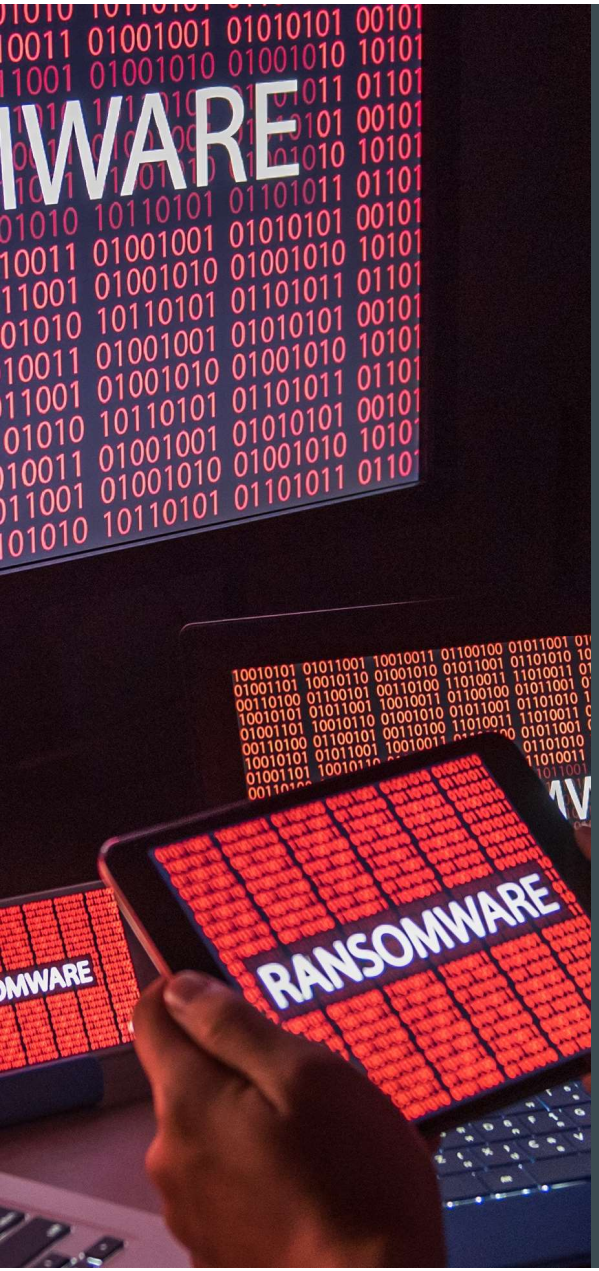
- K-Fall Vorbereitung
- Backup als fester Bestandteil der SEC Strategie
- Desaster-Recovery Plan / Wiederanlaufplan

- Vorbereitetes Cyber Rescue System verkürzt die Wiederanlaufzeiten deutlich (4 - >10 Tage)



Notfallhandbuch – DR-Fahrplan

- Prioritätenliste, Strukturierung der Workloads
  - Kritikalität
  - Abhängigkeiten
- Kommunikationsmatrix
  - Lieferanten
  - Kunden
  - Interne Kommunikation, Außenstellen
  - Ansprechpartner Software interne+externe Dienstleister
- Offiziell geltende Meldepflichten
  - Pressemeldung
  - (welche Stellen sollen/müssen informiert werden?)
  - NIS2 bringt neue Meldepflichten

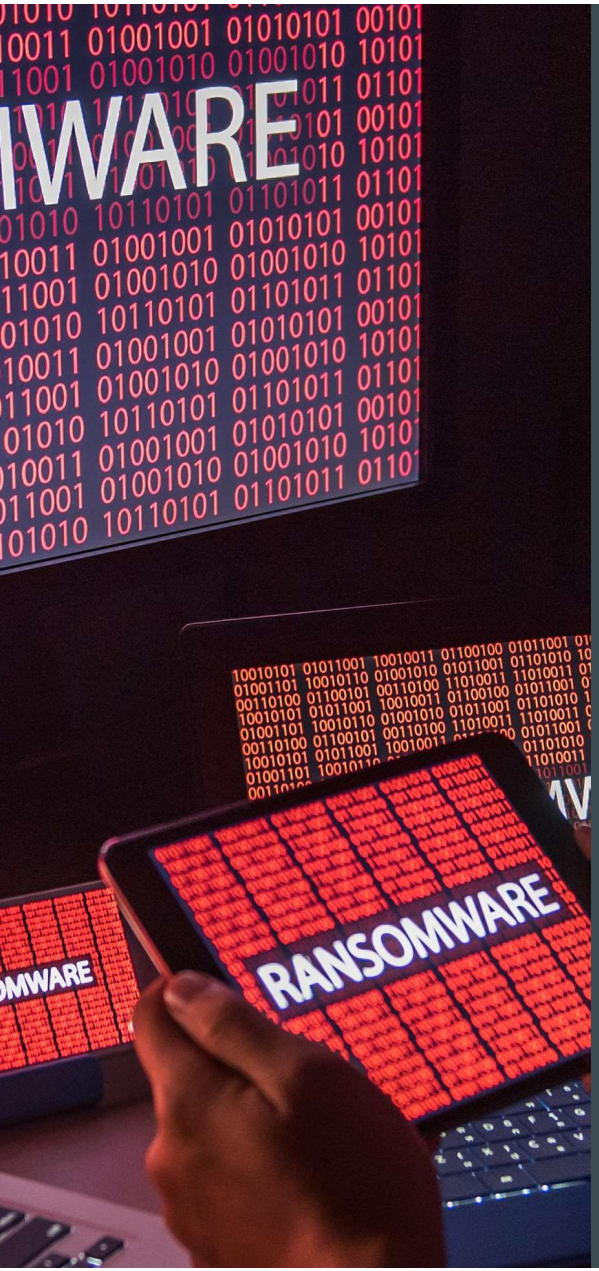


Zahlen – Ja oder Nein ?

- Keine Zusammenarbeit mit Hackergruppen
  - Kosten meist in Millionenhöhe
  - Einfallstor bleibt offen
  - Zerstörte Daten sind nicht wiederherstellbar
  - Gestohlene Daten bleiben in Händen der Angreifer
  - Unterstützung der kriminellen Tätigkeiten

„Die Entscheidung, keine Zusammenarbeit mit Hackern bei Verschlüsselungsangriffen einzugehen, ist nicht nur eine Frage der Rechtmäßigkeit, sondern auch eine Frage der Integrität und des Vertrauens. Unternehmen sollten sich bewusst sein, dass ethisches Handeln in der Cyberwelt genauso wichtig ist, wie in der physischen Welt.“

- Chat GPT



Zahlen - Ja oder Nein ?

Weil der Druck zur Schadensbegrenzung der Betroffenen nach einem Ransomware-Angriff enorm hoch ist, zahlen viele Opfer das geforderte Lösegeld in der Hoffnung, schnell wieder arbeitsfähig zu sein.

Es gibt jedoch keine Garantie dafür, dass die Cybererpresser die verschlüsselten Daten tatsächlich wieder freigeben oder die gestohlenen Daten tatsächlich löschen.

Auch besteht die Möglichkeit, dass das vom Angreifer zur Verfügung gestellte Entschlüsselungstool fehlerhaft ist.

Das BSI rät darum ausdrücklich von der Zahlung eines Lösegelds ab.

Zudem müssen einmal ausgeleitete Daten grundsätzlich als kompromittiert betrachtet werden

Quelle: Sicherheitsjahresbericht 2023

Unsere Zielsetzung für heute

dass Sie sagen:

„Der Tag war wertvoll investierte Zeit.“

„Wir müssen uns mit der ACP zusammen setzen und die Themen diskutieren.“

Vielen Dank für Ihre Aufmerksamkeit

IT for innovators.