

The logo consists of the letters 'ACP' in a white, bold, sans-serif font, positioned on a dark grey rectangular background. A thin red horizontal line is located directly beneath the grey background.

ACP

A wide-angle photograph of a grand, multi-story historical building with a white facade and a red-tiled roof. The building features a central clock tower with a dark dome and a bell. The architecture includes numerous windows with decorative elements and a central statue. The sky is blue with scattered white clouds.

**Herzlich Willkommen
zum ACP Jahresauftakt 2024**

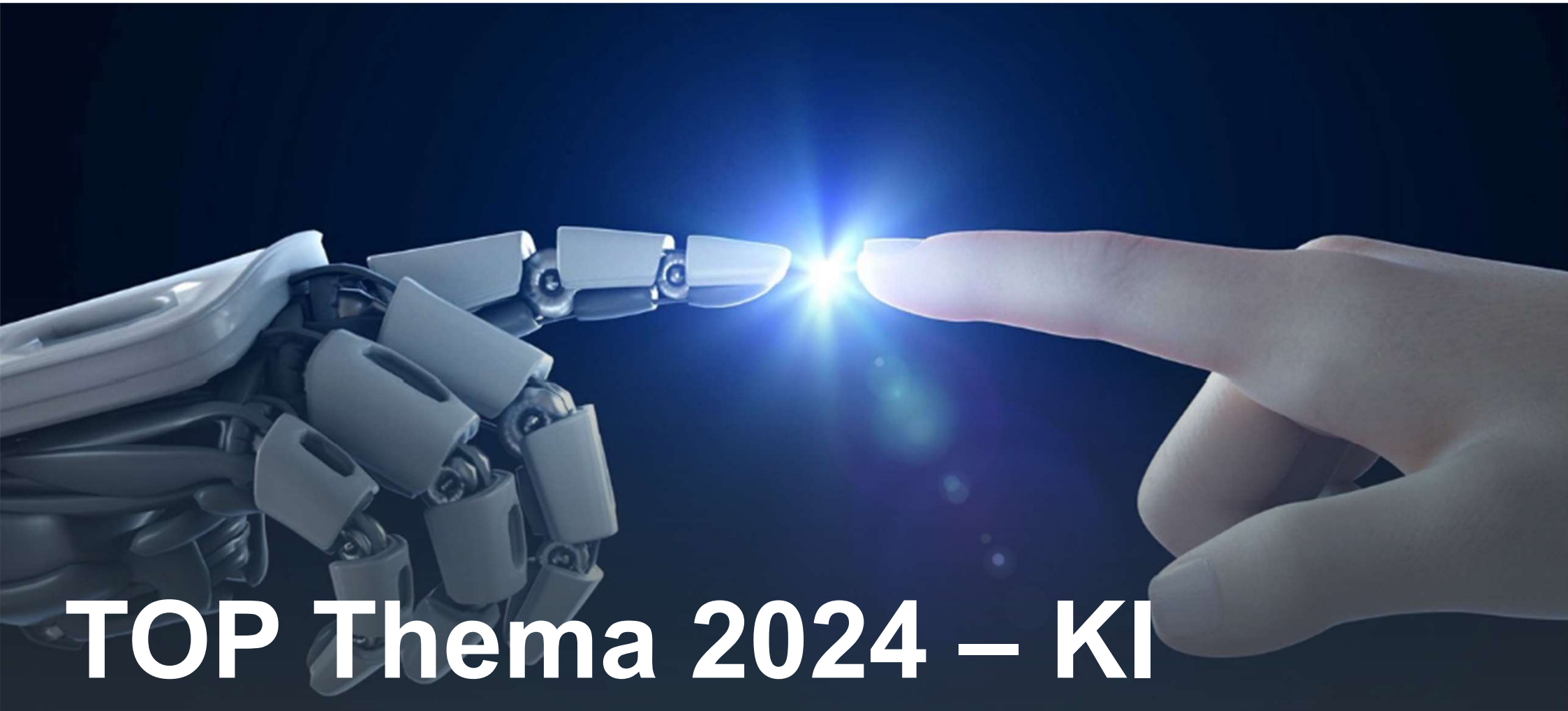
Unsere Zielsetzung für heute

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



«Das Aufk
was der M
– Stephen

«KI ist gef
– Elon Mu

«KI wird a
– Profess

**Künstliche Intelligenz
ist dann erst erreicht, wenn
der Rasenroboter genauso
wenig Lust hast, den Rasen
zu mähen, wie man selber.**

via Dorothee Bär, Digital-Ministerin

hlimmste,

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







Falsche Todesmeldung

Haaland von künstlicher Intelligenz erschossen



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





"Hurra, hurra, der Pumuckl ist da!"



KI – Stimmen, Bilder, Videos,





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.

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.



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



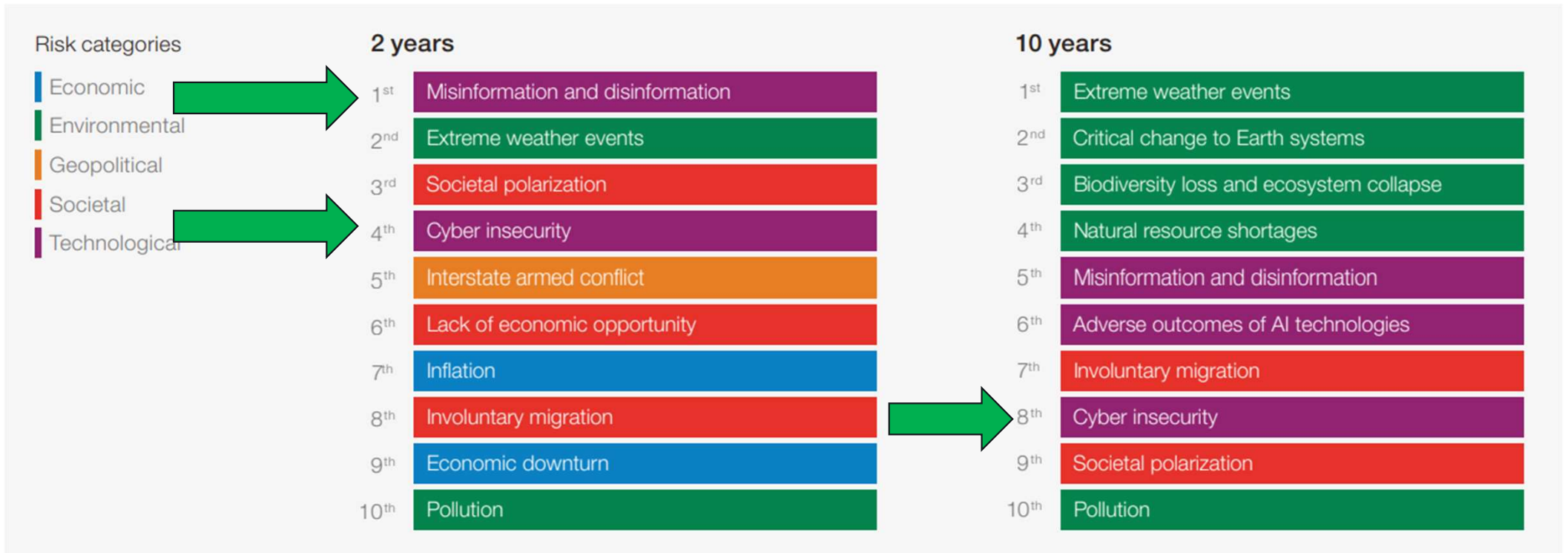


Weltrisikobericht 2024

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 – was fehlt ?



9th Economic downturn

.....auf Im

10th Pollution

ent zu erheben.

..... und den krieg in der Ukraine kann ich in 24h lösen.

Der 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](#)



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



Cisco kauft Splunk für 28 Mrd. US\$

IT-Sicherheit



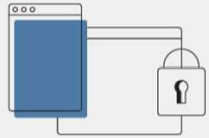
IT Sicherheitslagebericht BSI

Die Lage der IT-Sicherheit in Deutschland 2023 im Überblick

Ransomware

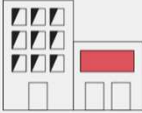
ist weiterhin die größte Bedrohung.

2 Ransomware-Angriffe auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



68 erfolgreiche Ransomware-Angriffe auf Unternehmen wurden bekannt.

15 davon richteten sich gegen IT-Dienstleister.



Mehr als **2.000** Schwachstellen in Software-Produkten (15 % davon kritisch) wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %**.



Eine Viertelmillion neue Schadprogramm-Varianten wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.




66% aller Spam-Mails im Berichtszeitraum waren Cyberangriffe: 34% Erpressungsmails, 32% Betrugsmails



84% aller betrügerischen E-Mails waren Phishing-E-Mails zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.



Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
 Identitätsdiebstahl Sextortion Phishing	 Ransomware Abhängigkeit innerhalb der IT-Supply-Chain Schwachstellen, offene oder falsch konfigurierte Online-Server	 Ransomware APT Schwachstellen, offene oder falsch konfigurierte Online-Server

Rund **21.000** infizierte Systeme wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.



Durchschnittlich rund **775** E-Mails mit Schadprogrammen wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.



370 Webseiten wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.



6.220 2022
5.100 2021

7.120
Teilnehmer hatte die Allianz für Cyber-Sicherheit im Jahr 2023.



Deutschland
Digital•Sicher•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.



Ransomware ist und bleibt die größte Bedrohung

Bei Cyberangriffen mit Ransomware beobachtet das BSI eine Verlagerung der Attacken: Nicht mehr nur große, zahlungskräftige Unternehmen stehen im Mittelpunkt, sondern zunehmend auch kleine und mittlere Organisationen sowie staatliche Institutionen und Kommunen. Insbesondere von erfolgreichen Cyberangriffen auf Kommunalverwaltungen und kommunale Betriebe sind die Bürgerinnen und Bürger unseres Landes oft auch unmittelbar betroffen: So kann es dazu kommen, dass bürgernahe Dienstleistungen eine Zeit lang nicht zur Verfügung stehen oder persönliche Daten in die Hände Krimineller gelangen.

ACP

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

Feststellung erstmaliger Zugriff auf Systeme des Kunden

Tag X-x

Ausspähen der Umgebung
Abgreifen von Daten und Zugangsdaten, Vorbereiten

Kunde kontaktiert ACP / ein Rapid Response Team

Analyse durch Response Team, um Einfallstor zu finden
Schaden ermitteln, ...

Rapid Response Team stellt Einfallstor fest
Lücken werden geschlossen

1-x Tage

Tag X+x

x Tage 24x7

Schaden

x Tage 24x7

Tag X+x

Tag X+x

Tag X

Angriff auf den Kunden durch Hacker(gruppe).
Verschlüsselung von Systemen
Zeitpunkt:
Freitag >20:00 Uhr

Wiederherstellung der Umgebung und Schadensbehebung

Alle Workloads wiederhergestellt und Online



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 (Virens scanner) (Strategie ?)*
- Fehlendes Logging/Logging-Historie
- Kein SIEM – keine Korrelation von Informationen
- Best Practice Empfehlungen werden oft ignoriert

WARE

Sofortmaßnahmen

- Kappen der Internetanbindung





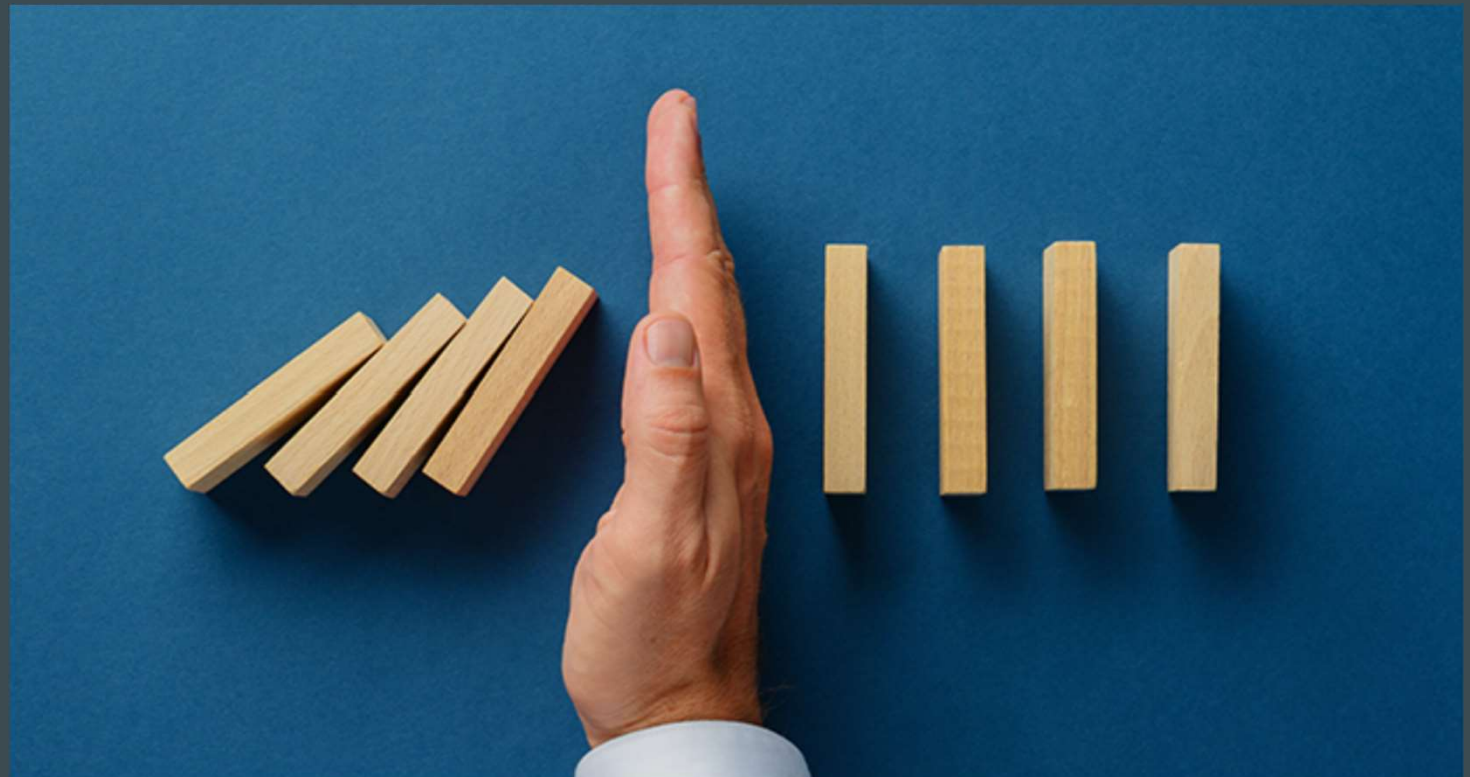
Sofortmaßnahmen

- 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 !!!

WARE

(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
- Disaster-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