

# Der Wolf im Schafpelz – wie Cyberkriminelle vorgehen



(und wie Sie sich dagegen schützen können)



- Wer kennt jemanden, dessen Unternehmen von einem Cyberangriff betroffen war?
- Welche Art von Cyberangriff fürchten Sie (am meisten)?
- Wie groß – glauben Sie – ist das Problem (in Euro ausgedrückt)?



- Aktuelle Bedrohungsszenarien und deren Folgen
- Bedrohungswahrscheinlichkeiten
- Möglichkeiten zum Schutz



- Datensicherheit (security)
- Betriebssicherheit (safety)
- Datenschutz (i.d.R. personenbezogener Daten)

# Das klassische Bild des Hackers



- Zugriff auf (ungeschützte) Geräte
  - <http://insecam.org/en/view/936242/>
  - <http://insecam.org/en/view/1010813/>
  - <http://insecam.org/en/view/196414/>
- Zugriff auf Geräte mit ‚Werkseinstellungen‘
- Zugriff auf Geräte mit trivialen Zugangsdaten
- Zugriff auf Geräte mit veralteten Softwareständen (und bekannten Sicherheitslücken)
- Zugriff auf Daten über Schwächen von Websites (SQL-Injection)
- ...





- Moderne Hackergruppen funktionieren nicht mehr wie lose Communities, sondern wie international operierende Unternehmen:



- Arbeitsteilung & Abteilungen
- Prozesse & KPIs
- Globale Lieferkette:



Von Malware-Entwicklern über Access-Broker bis hin zu Verhandlungsteams ist die gesamte Wertschöpfungskette abgedeckt.

Fazit: Cybercrime ist heute ein industrielles Ökosystem – mit Spezialisierung und Skalierung wie bei Tech-Konzernen.

# Welche Angriffsmethoden sind ,aktuell'?



- Zero-Day-Exploits – unbekannte Schwachstellen
- Ransomware 2.0 – zielgerichtete Erpressung, Datenexfiltration
- Supply-Chain-Angriffe – Risiko durch Drittanbieter und Partner
- Social Engineering – menschlicher Faktor als größtes Risiko
- KI-gestützte Angriffe – Deepfakes, automatisierte Attacken



- Unbekannte Schwachstellen: Angreifer nutzen Fehler, von denen die Hersteller noch nichts wissen, sodass es keine Abwehrmaßnahmen gibt.
- Hohe Erfolgswahrscheinlichkeit: Da es keine Gegenmittel gibt, sind diese Angriffe oft sehr effektiv (aber verhältnismäßig ,teuer').
- Lange Lebensdauer: Viele Exploits bleiben Jahre unentdeckt, wie die Forschung zeigt.
- Wahrscheinlichkeit, dass ,nur für Sie' ein Zero Day Exploit geschrieben wird, ist gering.





- Industrialisierte Attacken sind allgegenwärtig
- Hacker setzen auf Geschwindigkeit & Automatisierung:
  - Skalierte Angriffe durch automatisierte Reconnaissance, bis zu 36.000 Scans pro Sekunde.
  - Spezialisierte „Cybercrime-as-a-Service“-Module für jede Phase: initial access, lateral movement, exfiltration.
- Im Fall des Bekanntwerdens von Sicherheitslücken geht es um Geschwindigkeit.

# RaaS – das „Amazon“ des Cybercrime



RaaS steht für Ransomware-as-a-Service

- Der größte Strukturwandel der letzten Jahre ist das Franchise-Modell:
  - Ransomware wird als Produkt vermietet, inklusive Updates, Tools und Support.
  - Affiliates führen Angriffe durch und teilen die Gewinne (typisch 70/30 o.ä.) mit den Betreibern.
  - Professionelle Marketingmaßnahmen, Rabatte und Dokumentationen sind üblich.

Folge: Fast jeder mit Basiswissen kann heute einen hochprofessionellen Angriff starten

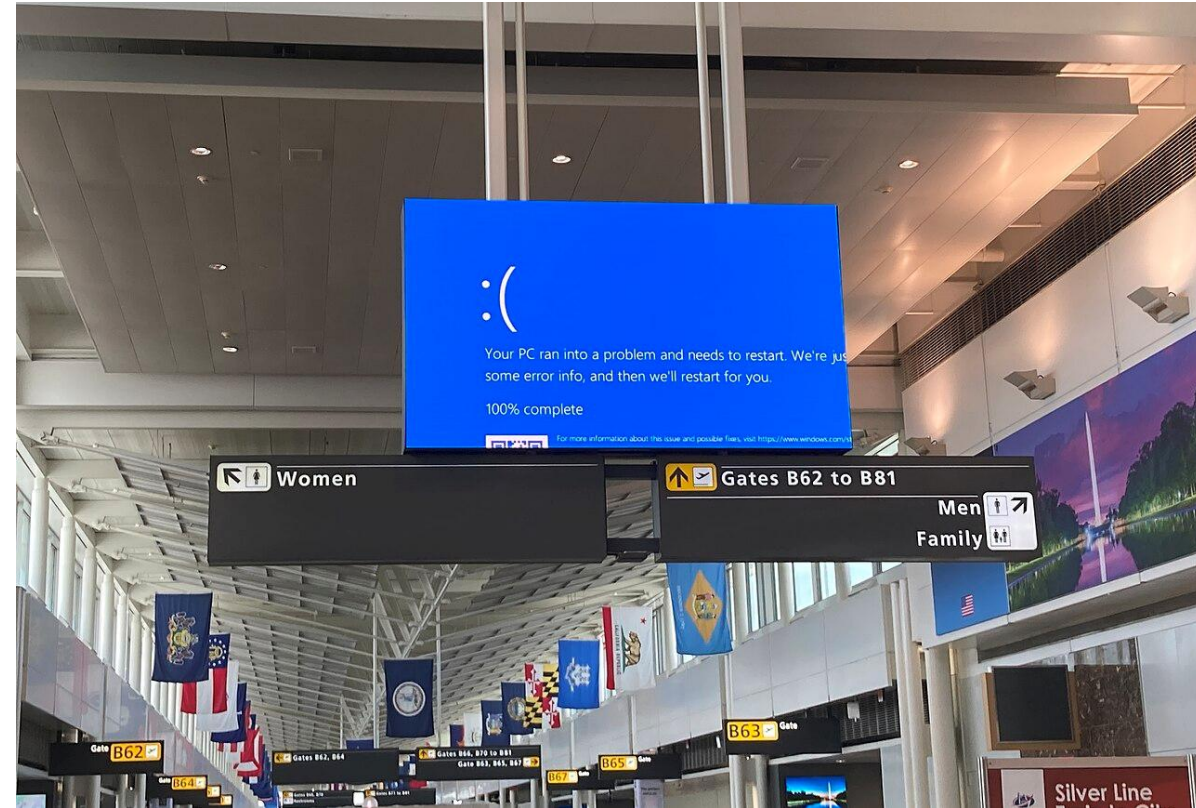




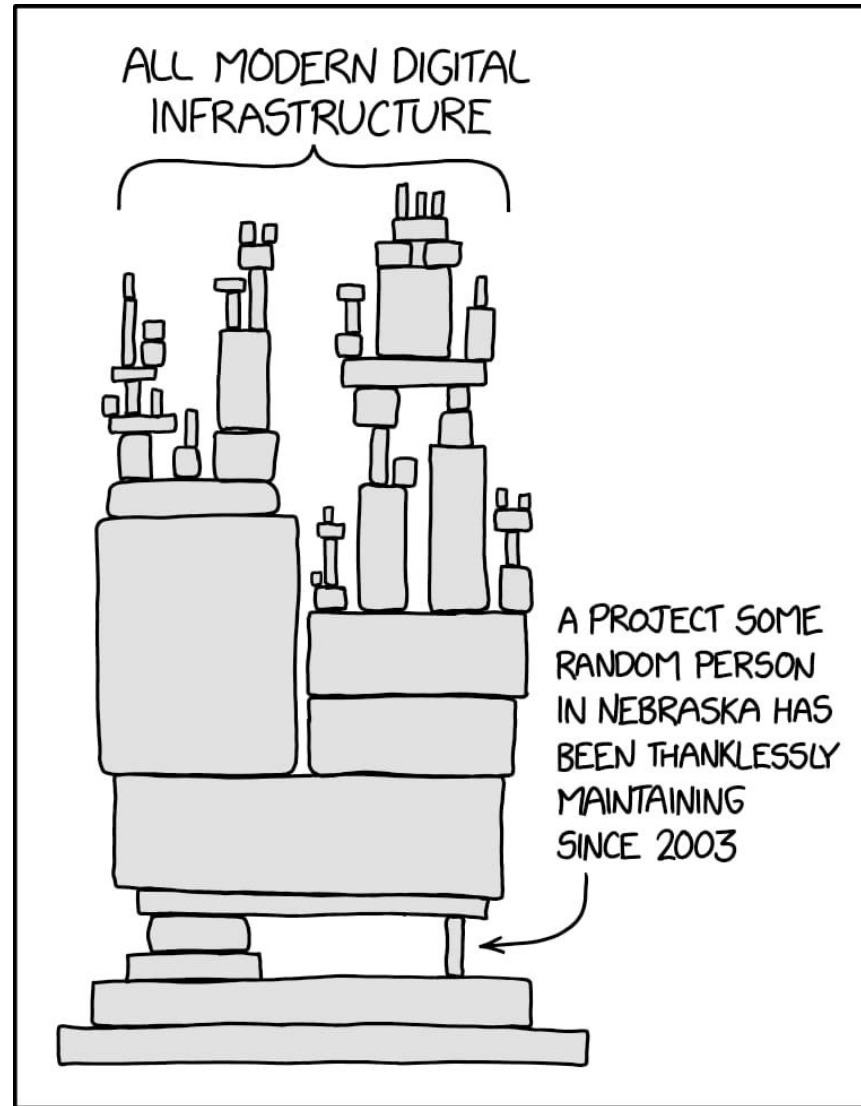
- Ziel sind Zulieferer, Partner oder Software/Hardware-Lieferanten, um über diese vertrauenswürdigen Wege böartigen Code einzuschleusen, sensible Daten zu stehlen oder das System zu kompromittieren
  - Software-Updates: Schadcode wird in legitime Updates von Drittanbietern integriert, die dann von Kunden unbewusst installiert werden
  - Hardware-Manipulation: Manipulation von Mikrochips oder anderen Komponenten, die in die Lieferkette eingeschleust werden.
  - Browser-basiert: Einschleusung von böartigem JavaScript, um Informationen aus Browsern zu stehlen (z. B. Magecart-Angriffe).
  - Open-Source-Angriffe: Ausnutzung von Schwachstellen in frei verfügbaren Code-Bibliotheken.



- CrowdStrike ist einer der weltweit größten Cybersicherheitsdienstleister. Es hat zehntausende Firmenkunden in 170 Ländern
- 2024 löste eine fehlgeschlagene Softwareaktualisierung des Cybersicherheitsanbieters CrowdStrike für sein Produkt Falcon einen beispiellosen weltweiten Ausfall aus
- Insgesamt wurden schätzungsweise 8,5 Millionen Windows-Geräte lahmgelegt



# Log4j – warum OpenSource nicht identisch mit ‚sicher‘ ist





Hacker „brechen nicht mehr ein — sie loggen sich ein“:

- Missbrauch realer Mitarbeiter über vishing, smishing, MFA-Reset-Manipulation
- Post-Compromise-Social-Engineering mithilfe KI-gestützter Mail-Analyse.
- **75 % der erfolgreichen Intrusionen basieren auf kompromittierten Identitäten statt Malware**





## Phishing:

- Täuschung: Angreifer verschicken Nachrichten (E-Mail, SMS, Social Media), die echt aussehen, oft mit Logos und Layouts bekannter Firmen.
- Aufforderung: Der Empfänger wird aufgefordert, auf einen Link zu klicken, der zu einer gefälschten Webseite führt.
- Datenabfrage: Auf der gefälschten Seite werden die Opfer gebeten, ihre Daten in ein Formular einzugeben, welche dann direkt an die Betrüger gesendet werden.

## Vishing:

- Medium: Telefonanrufe, oft über VoIP (Voice over IP).
- Methode: Social Engineering: Der Täter nutzt Vertrauen, Autorität oder Angst, um das Opfer zu manipulieren.
- Rollen: Betrüger geben sich als Bankmitarbeiter, IT-Support, Polizei, etc. aus
- Ziele: Zugangsdaten, Kreditkartennummern, persönliche Daten



MFA ist eine zusätzliche Sicherheitsebene beim Login, die neben dem Passwort mindestens einen weiteren Beweis Ihrer Identität verlangt, wie einen Code aus einer App, eine SMS, einen Fingerabdruck oder einen USB-Schlüssel, um Konten vor Hackerangriffen zu schützen, selbst wenn Ihr Passwort bekannt ist.

Angriffsmethoden:

- MFA-Anfragen-Bombardierung
- Social Engineering Angriffe auf den Service Desk
- Adversary-in-the-Middle (AITM)-Angriffe





## 2026 ist der Einsatz von KI ein massiver Gamechanger:

- Hyper-personalisierte Phishing-Mails ohne Rechtschreibfehler, perfekt auf Zielpersonen zugeschnitten.
- 703 % Anstieg bei Credential-Phishing, getrieben durch KI-unterstützte Tools.
- Deepfakes für CEO-Fraud, vishing und Identitätsmissbrauch.
- Automatisierte Angriffsketten, gesteuert durch agentische KI.



**Liebe Lena Müller,  
bitte sehen Sie sich die  
angehängte Rechnung  
von letztem Monat an.**

# Das eigentliche Ziel von Cyberangriffen



- Datendiebstahl
  - Datenexfiltration
  - Verkauf der Daten
  - Erlangung von Geschäftsinformationen (F&E)
  - Basis für weitere Angriffe
- Erpressung
  - Verschlüsselung (Ransomware)
  - Drohung der Veröffentlichung (Doxing)
  - DDoS-Angriffe zur zusätzlichen Einschüchterung
- Erlangung von Zahlungen



# Wenn Sie nur scheinbar mit dem Kunden sprechen...



From: Emma Young (emma@matteel.co.uk)  
Sent: Monday, 14. August 2023 09:42  
To: Constanze Schuster (Constanze.schuster@matteel.co.uk)  
Subject: AW: 19430/170533

From: Constanze Schuster (Constanze.schuster@matteel.co.uk)  
Sent: Tuesday, August 22, 2023 1:47 PM  
To: Emma Young (emma@matteel.co.uk)  
Subject: AW: 19430/170533

From: Emma Young (emma@matteel.co.uk)  
Sent: Tuesday, August 22, 2023 1:04 PM  
To: Constanze Schuster (Constanze.schuster@matteel.co.uk)  
Subject: AW: 19430/170533

From: Emma Young (emma@matteel.co.uk)  
Sent: Tuesday, August 22, 2023 1:31 PM  
To: Constanze Schuster (Constanze.schuster@matteel.co.uk)  
Subject: AW: 19430/170533

From: Constanze Schuster (Constanze.schuster@matteel.co.uk)  
Sent: Tuesday, August 22, 2023 1:31 PM  
To: Emma Young (emma@matteel.co.uk)  
Subject: AW: 19430/170533

From: Constanze Schuster (Constanze.schuster@matteel.co.uk)  
Sent: Tuesday, August 22, 2023 8:54 AM  
To: emma@matteel.co.uk; emma@matteel.co.uk  
Subject: 19430/170533

Ab hier findet die Kommunikation nicht mehr zwischen ECS und dem Kunden statt.

From: Emma Young (emma@matteel.co.uk)  
Sent: Monday, August 24, 2023 1:42 PM  
To: Constanze Schuster (Constanze.schuster@matteel.co.uk)  
Subject: AW: 19430/170533

From: Constanze Schuster (Constanze.schuster@matteel.co.uk)  
Sent: Monday, August 24, 2023 12:34 PM  
To: Emma Young (emma@matteel.co.uk)  
Subject: AW: 19430/170533

Ab 14.08

Freight	Packing	Net Amount	VAT	VAT Amount	Total Amount
0,00 €	0,00 €	[REDACTED]	+ 0.00% Tax	0,00 €	[REDACTED] €



Geschäftsführung: [REDACTED]  
Amtsgericht Stendal | [REDACTED]  
Commerzbank AG | [REDACTED]

Bei der Kundin ist aber folgendes angekommen:

Freight	Packing	Net Amount	VAT	VAT Amount	Total Amount
0,00 €	0,00 €	[REDACTED]	+ 0.00% Tax	0,00 €	[REDACTED] €



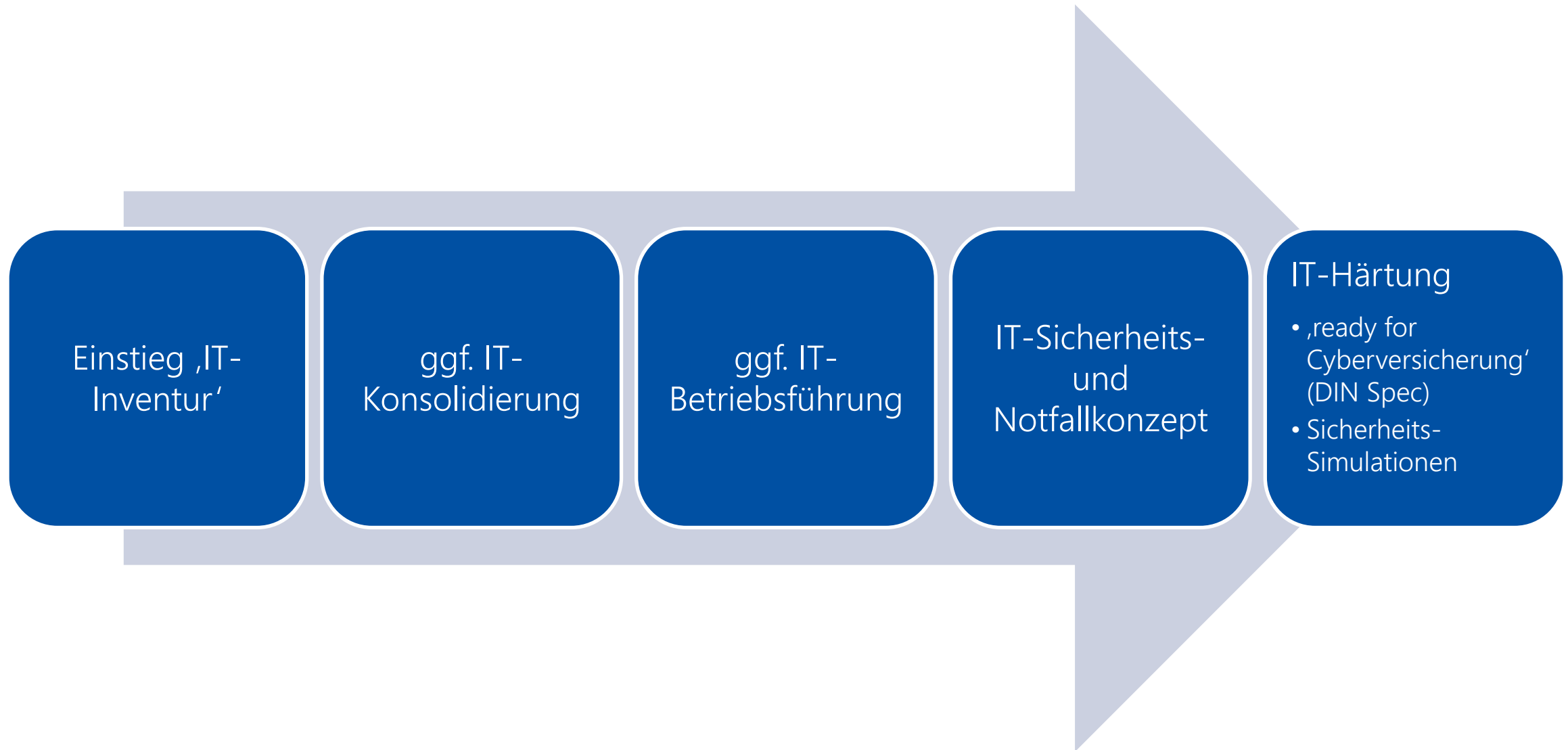
Geschäftsführung: [REDACTED]  
Amtsgericht Stendal | [REDACTED]  
Wise Bank | IBAN [REDACTED]



- DSGVO-Meldepflicht (bei personenbezogenen Daten)
- Komplette Nicht-Nutzbarkeit der IT mit allen Folgen
  - Einstellung der Kunden- und Lieferantenkommunikation
  - Ggf. Einstellung der Produktion
  - Ggf. Einstellung des Geschäftsbetriebes
  - Kosten und Zeit für Neubeschaffung von IT-Infrastruktur
  - Zeit für ggf. mögliche Daten-Wiederherstellung
  - Kosten und Zeit für Wieder-Ingangsetzung der IT
- Abfließen von Geschäftsinformationen
- Verlust von Kunden- und Lieferantenvertrauen



- IT-Infrastrukturen auf dem Stand der Technik aufbauen und pflegen
- IT-Personal auf dem Stand der Technik halten oder DL nutzen
- Schnelle Reaktion auf Sicherheitswarnungen sichern
- Risiken kennen, erträglich halten bzw. minimieren
- Notfallplan haben und verifizieren!
- Sicherheits-Policies ‚von oben nach unten‘ vorgeben und umsetzen
- Permanente Überprüfung der Sensibilität – z.B. automatisierte Phishing Simulationen





- Simulation verschiedener Szenarien
  - Internet-Ausfall
  - Ausfall der Versorgung mit Elektroenergie – Stromausfall
  - Feuer / Havarie / Zerstörung durch Diebstahl bzw. Vandalismus
  - Vorsätzliche Dienstbeeinträchtigung – extern – DDoS-Angriff
  - Vorsätzliche Datenmanipulation – extern – Ransomware-Angriff
  - Datenabfluss – extern/intern – Doxing bzw. Identitäts-Missbrauch
  - Vorsätzliche Datenmanipulation / -löschung – intern – Mailing / File-Struktur
- Beurteilung von
  - Recovery-Zeit, Kosten und Aufwände zur Herstellung der Betriebsfähigkeit
  - Materielle und ggf. ideelle Schäden
  - Mögliche Maßnahmen zur präventiven Eingrenzung von Schäden



Maßnahme	wirkt gegen						
	Internet-Ausfall	Stromausfall	Havarie Diebstahl Zerstörung	DDOS- Attacken	Ransomware- Angriff	Doxing und Identitäts- missbrauch	interne Daten- manipulation
Realisierung einer knoten- und kantendisjunkten redundanten Internetanbindung	x						
Implementierung einer redundanten Firewall	x						
Nutzung eines cloud-basierten Betriebsansatzes	x	x	x				
Notfall-Energieversorgungskonzept		x					
Vorhalten von Notfall-Geräten und Nutzung mobiler Hardware			x		x		
Implementieren eines Cloudbackups			x		x		x
Schulung der Mitarbeiter zu IT-Sicherheit					x	x	
Durchführen von Phishing-Simulationen					x		
erzwungene Password-Policy					x	x	
Aktive Überwachung				x	x	x	
Härtung der ITK-Infrastruktur (BSI-Empfehlungen)					x	x	





über 25 Jahre Erfahrungen im IT- und Telekommunikationsmarkt



3.100 Kunden, mehr als 1 Mio Gespräche pro Monat, 1.900 Vorgänge parallel in Bearbeitung



Internet und Telefonie, Anbindung und Unternehmensvernetzung, Sicherheit und Cloud, M365 Lösungsbaukasten, Digitale Räume und Lösungen, Industriekommunikation und 5G, Smart City und IoT



ITK-Analyse und Digitalisierungskonzepte, Konsolidierung, Projektierung, Betreuung und Betriebsführung



„Vernetzte digitale Infrastrukturen für Unternehmen, Verwaltungen und Organisationen“



Vielen Dank für Ihre Aufmerksamkeit!  
Welche Fragen haben Sie?

[go.TELEPORT.de](https://go.teleport.de)