

Cybersecurity – Reflections & Musings

Patrick Comboeuf



Cybersecurity für Verwaltungsräte

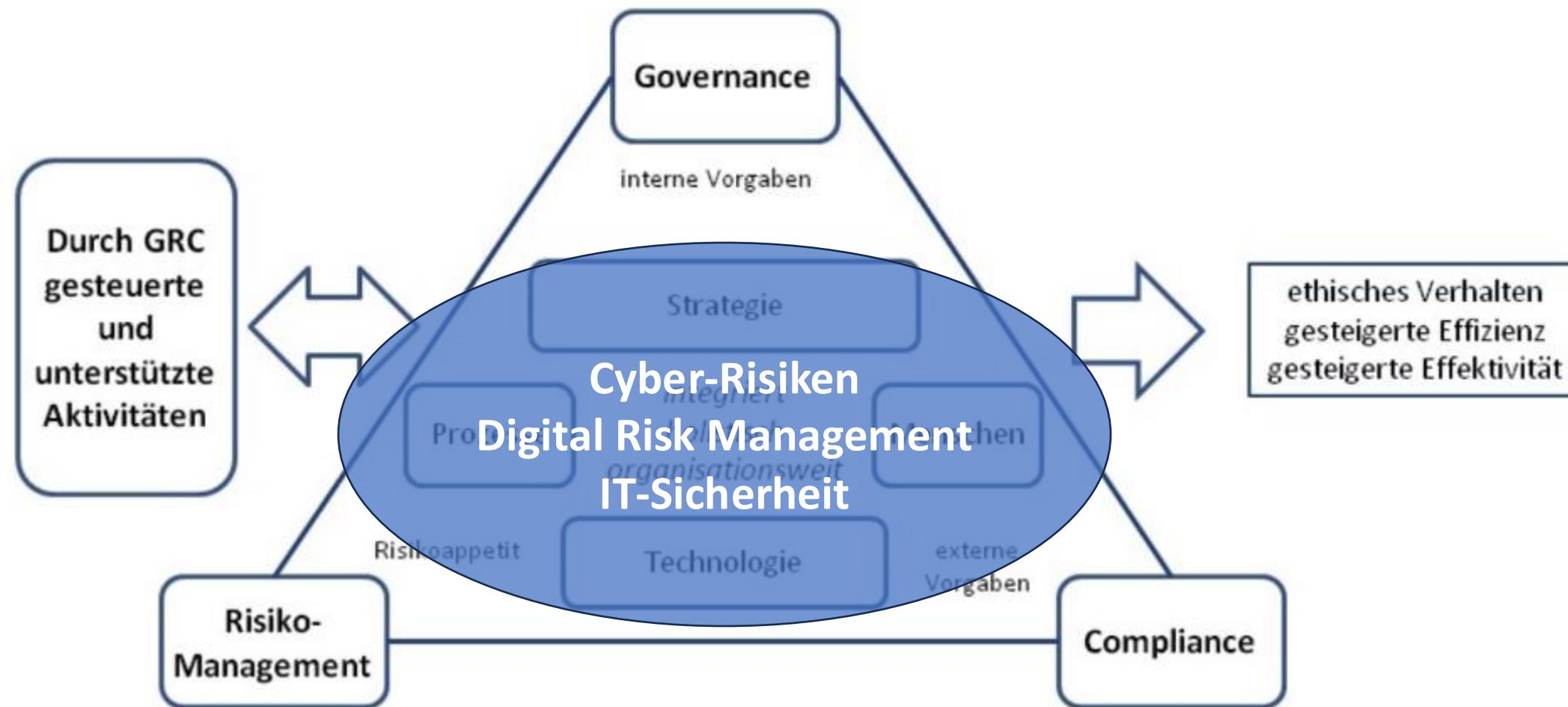
Strategische Verantwortung in der digitalen Ära



**There are two types of
companies: those who have
been hacked, and those who
don't know they've been hacked.**

John Chambers, former Cisco CEO

Kontext: Governance, Risk & Compliance (GRG)

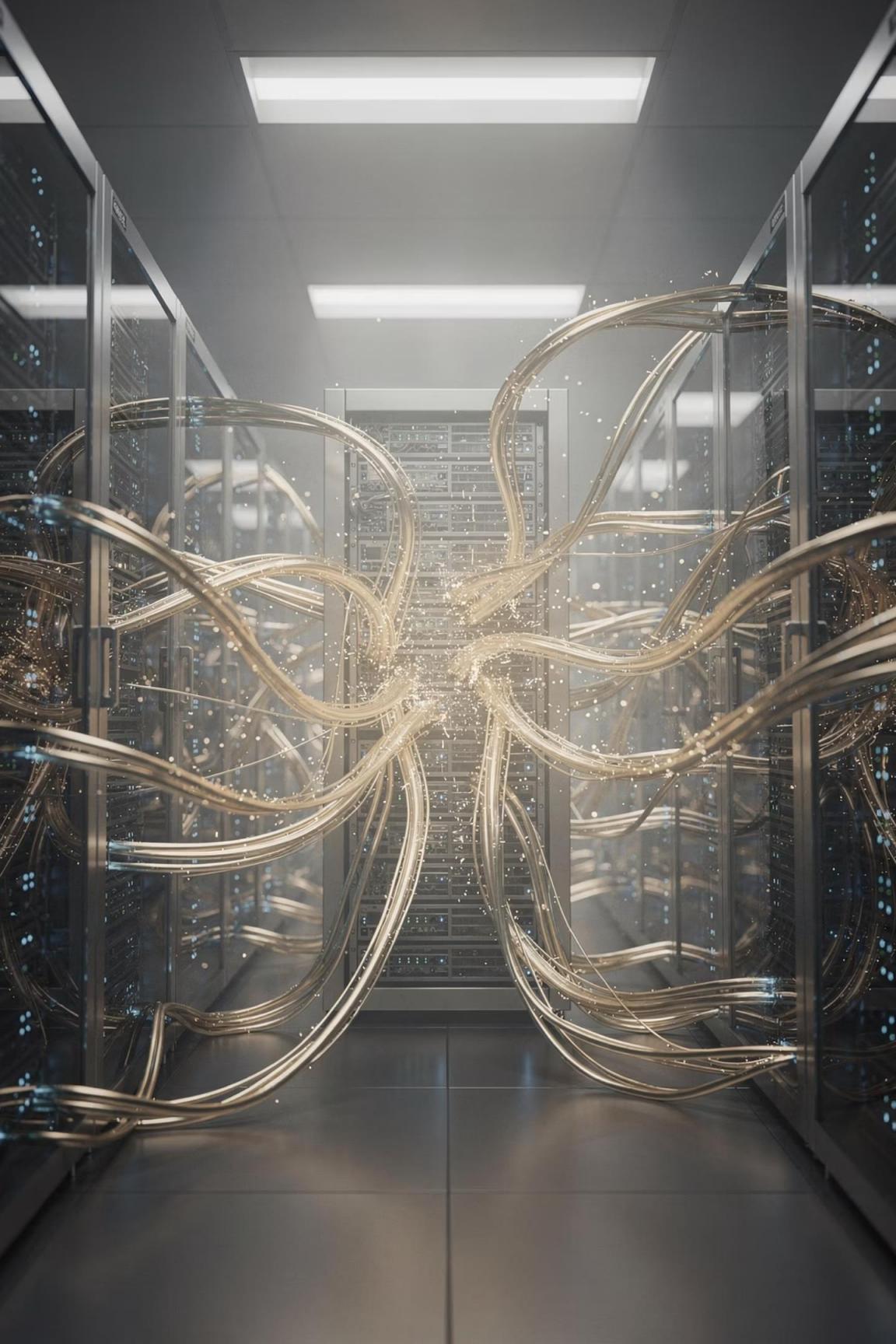


Cyberrisiken = Geschäftsrisiken

Cyberrisiken sind keine isolierten IT-Probleme mehr. Sie manifestieren sich direkt als finanzielle Verluste, operationelle Betriebsunterbrüche und nachhaltige Reputationsschäden. Der Verwaltungsrat trägt die strategische Verantwortung für das Management dieser Risiken.

Die Zeiten, in denen Cybersecurity ausschliesslich dem IT-Bereich zugeordnet wurde, sind vorbei. Heute gehört sie ins Zentrum der Unternehmensstrategie.





Technologie-Sicherheit: Warum es den Verwaltungsrat betrifft

Strategische Priorität

Sicherheitsvorfälle kosten bis zu 30% der Marktkapitalisierung.

Rechtliche Verantwortung

Verwaltungsräte haften bei Sicherheitsvorfällen (Delaware Courts, SEC, SOX).

Permanente Bedrohung

Über 2'000 Angriffe pro Tag, meist durch Social Engineering.

CHF 3.5 Mio 207 +15%

Breach-Kosten

Pro Vorfall weltweit

Erkennungszeit

Tage (Median)

Klagen gegen Boards

Jährliches Wachstum

CHF 3.5 Mio

Durchschnittliche Kosten eines Data Breach

- ☐ **Fiduciary Duty:** Der Verwaltungsrat trägt die treuhänderische Sorgfaltspflicht. Ein Data Breach kann nicht nur finanzielle Verluste verursachen, sondern auch rechtliche Konsequenzen und persönliche Haftung nach sich ziehen.



Werte werden durch Handlungen sichtbar

Ein Verwaltungsrat kann Werte und ethische Grundsätze formulieren, aber sie werden erst dann real, wenn sie im täglichen Umgang mit Daten, Kundeninformationen & Sicherheitsvorfällen konsequent gelebt werden.

Eine starke Unternehmenskultur ist die beste Verteidigungsline gegen Cyberrisiken. Sie beginnt mit klaren Erwartungen von der Führungsspitze.



Der Security-Balanceakt



Business Value

- Geschwindigkeit
- Einfaches Onboarding
- Benutzerfreundlichkeit
- Wettbewerbsfähigkeit



Security

- Datenschutz
- Compliance-Anforderungen
- Zugangskontrolle
- Investitionskosten

Der Verwaltungsrat definiert den Risk Appetite: Wo liegt die optimale Balance zwischen geschäftlicher Agilität und angemessen er Absicherung? Diese strategische Entscheidung bestimmt die Risikobereitschaft des Unternehmens.

Best of Digital Risk Management





Die Angriffsfläche: Wo Verwundbarkeit entsteht



Externe Angreifer

Nation-States, Kriminelle, Wettbewerber nutzen ausgefeilte Methoden.



Insider-Bedrohungen

Menschliche Fehler, Sabotage oder Erpressung durch Mitarbeitende.



Lieferkette

Schwachstelle durch Drittanbieter; 45% der Angriffe nutzen sie.



Legacy-Systeme

Veraltete, ungepatchte Systeme sind leichte Angriffsziele.

«Sie sind nur so sicher wie Ihr unsicherster Vendor.»

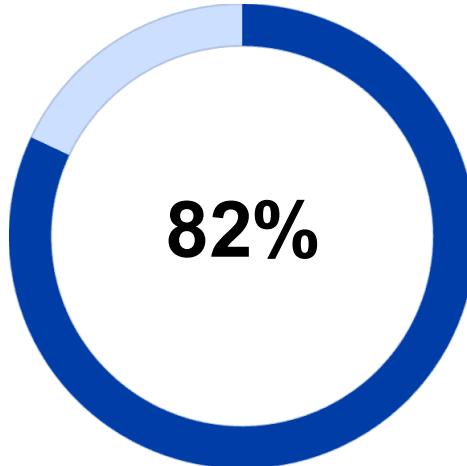


**Amateurs hack systems.
Professionals hack people.**



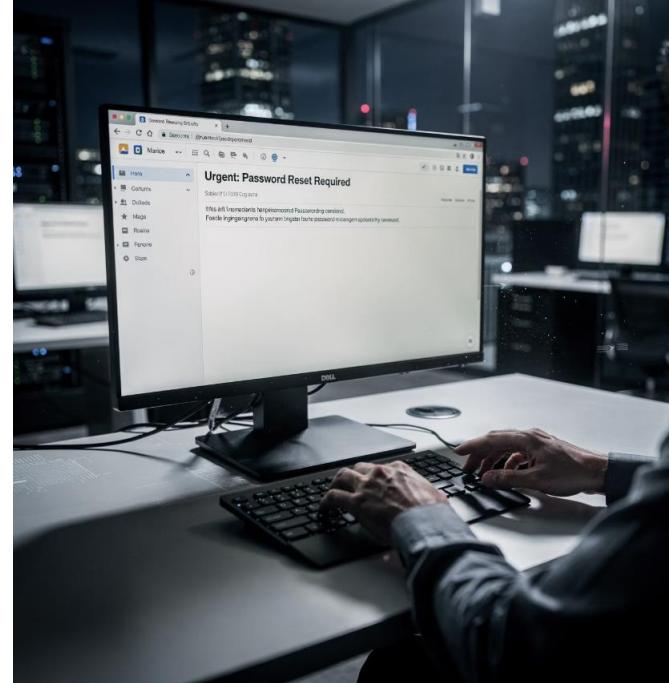
Bruce Schneier, Cybersecurity Icon

Social Engineering: Das schwächste Glied



Menschliches Versagen

Anteil aller Breaches



Häufigste Angriffsvektoren

- **Phishing:** Schädliche Links via E-Mail.
- **Pretexting:** Manipulation zur Datengewinnung.
- **Passwort-Reuse:** Wiederverwendung gestohlener Anmelddaten.

Die unbequeme Realität

Das schwächste Glied ist der Mensch. Technologie ist nur so sicher wie ihre Nutzer.

Digitale Identität als Fundament



Mitarbeiter-Zugänge

Verwaltung von Berechtigungen und
Authentifizierung



Kunden-Identitäten

Sichere Logins und Datenschutz



Partner-Accounts

Kontrollierter Zugriff auf gemeinsame
Ressourcen

«Digital Identity ist das Fundament für Business.» Der Schutz digitaler Identitäten ist heute ebenso kritisch wie der Schutz physischer Vermögenswerte. Ohne vertrauenswürdige digitale Identitäten ist kein sicheres Geschäft möglich.

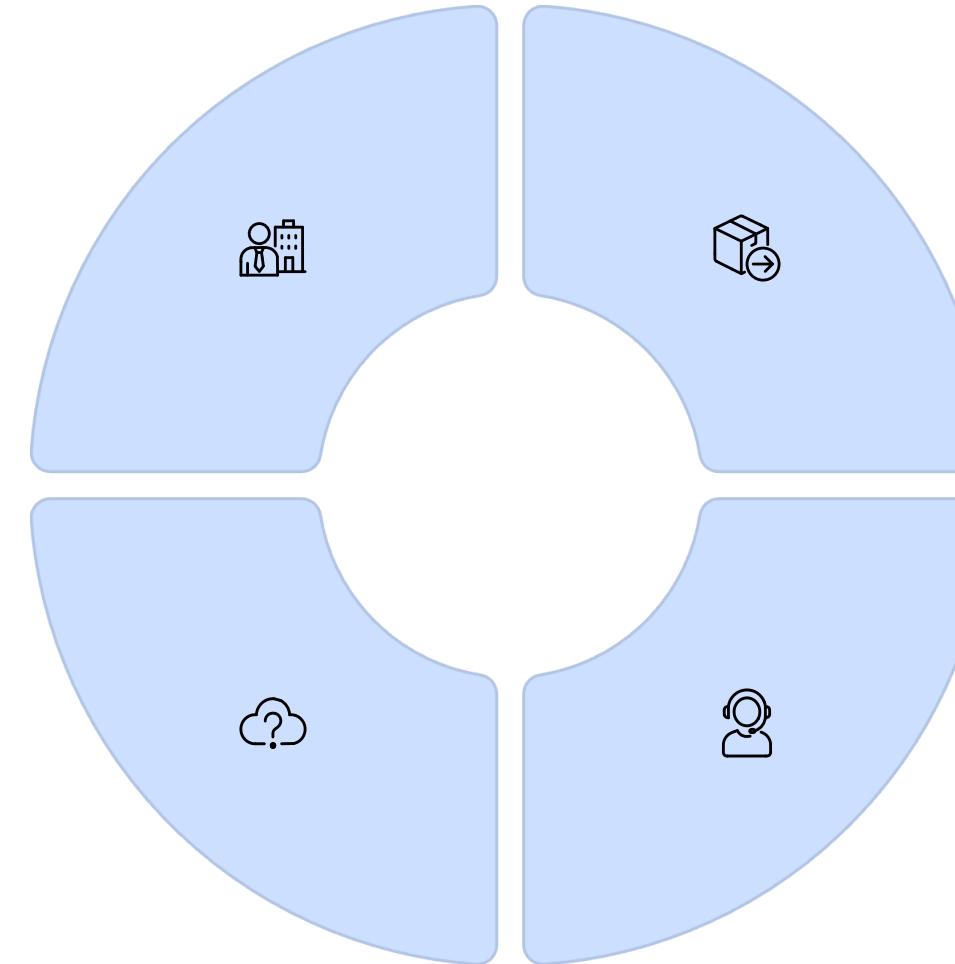
Risiken in der Lieferkette

HR-Services

Externe Personaldienstleister mit Zugriff auf Mitarbeiterdaten

Cloud-Provider

Hosting kritischer Geschäftsapplikationen



Lieferanten

Zugang zu Produktions- und Logistiksystemen

Kunden

Direkte Schnittstellen zu Geschäftssystemen

Angriffe erfolgen zunehmend über die schwächsten Glieder in der Lieferkette. Ein kompromittierter Dienstleister öffnet die Tür zu Ihrem Unternehmen.

High Impact Cybersecurity Vorfälle



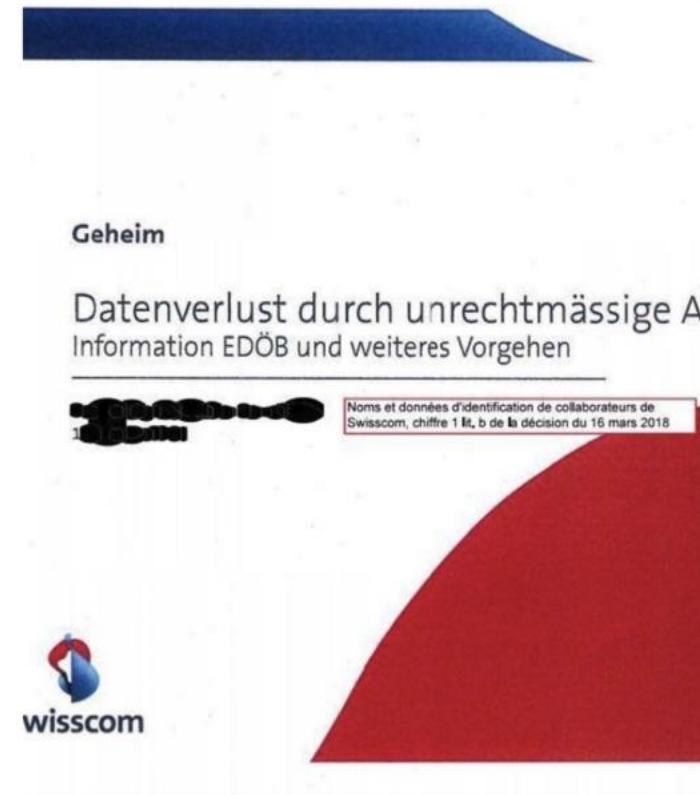
Financials

- 13% share price drop of Equifax in early trading
- FedEx suspended trading of TNT for a whole day (Petya/NotPetya)
- Maersk indicated USD 250-300m impact on results (Petya/NotPetya)
- Dropped acquisition price by 7.2% (USD 350m) for YAHOO! by Verizon

Wider Disruption

- Maersk reinstalled large amounts of their IT environment (Petya/NotPetya)
- Several C-Level step downs (CEO, CIO, CISO of Equifax)
- Several lawsuits (Equifax)

Ransomware-Angriff / Swisscom Hack in Tunesien



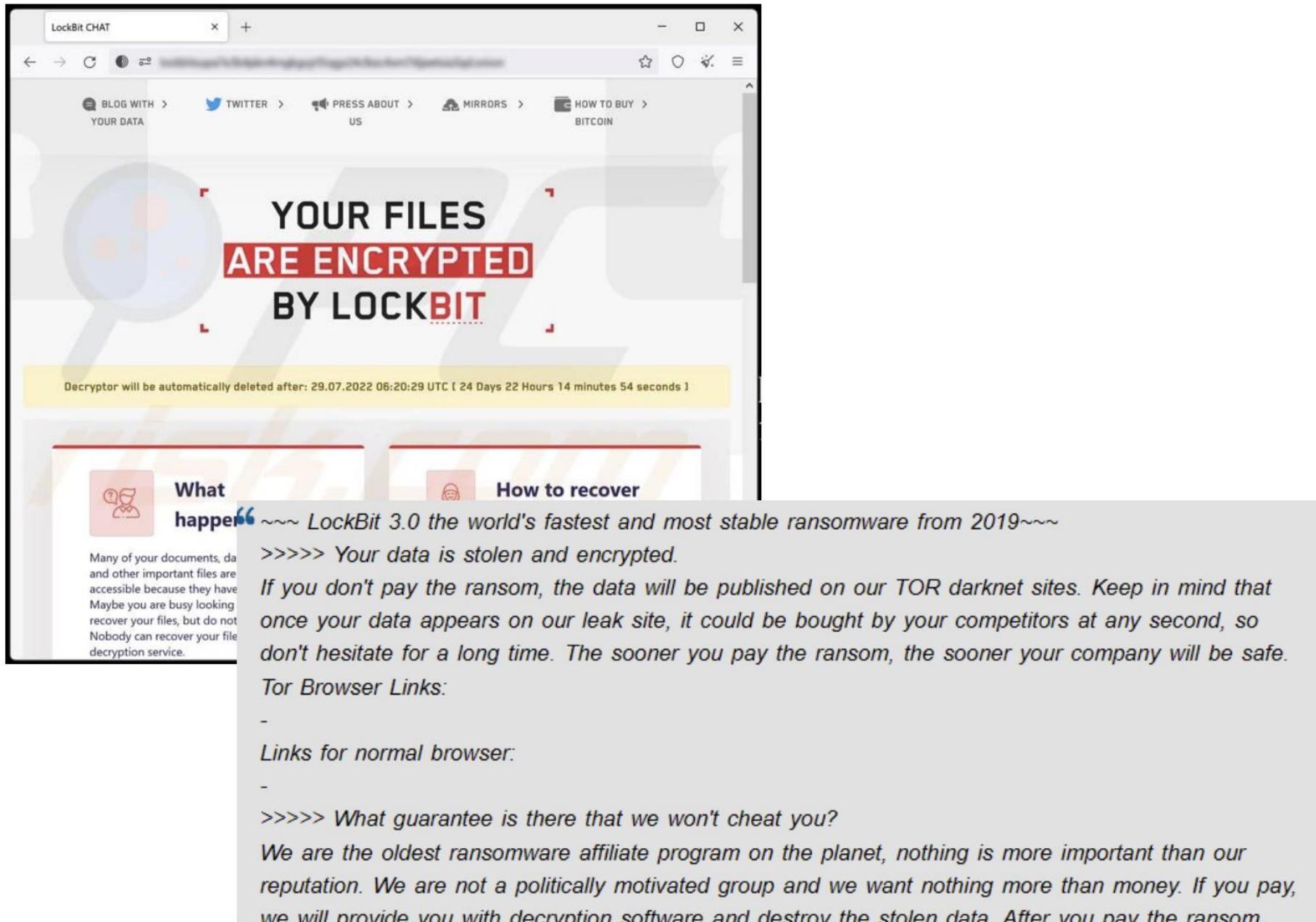
Description

Ursprünglich wollte die Swisscom den Datenklau vom Herbst 2017 geheim halten. Nun zeigen Recherchen, dass eine Marketingfirma in Tunesien Zugang zu den Schweizer Kundendaten hatte. Die Swisscom bestreitet, davon gewusst zu haben.

Link

<https://www.20min.ch/story/daten-von-800000-swisscom-kunden-wurden-in-tunesien-geklaut-552320307120>

Let's talk about 'Ransomware'



<https://www.pcrisk.de/ratgeber-zum-entfernen/11502-lockbit-3-0-ransomware>



Sicherheits-Budget & ROI

Investition

10-15% des IT-Budgets
strategisch für Security
einplanen.

ROI

\$1 Prävention = \$10
Recovery. Proaktiv spart
Kosten.

Strategie

Security ist **Versicherung**,
schützt Reputation &
Geschäft.

Investitionen in Sicherheit verhindern katastrophale Verluste.

Cybersecurity Risk Management Prozess



Step	Example and Activities
Identify Risks	<ul style="list-style-type: none">• Szenario: Externer Angriff gegen eigene IT Systeme• Trigger: Web-Applikationen sind nicht adequate geschützt• KRI: % Web-Applikationen, welche die Firewall vor DDoS Attacke schützt• KRI: % DDos Schutzsättigung (ç%)
Risk Assessment	<ul style="list-style-type: none">• Publikation / Erläuterung der KRIs• Sig-off der Assessments
Risk Response	<ul style="list-style-type: none">• Enwurf von Wiederherstellungsplänen• Zentrale Ansicht von Wiederherstellungsplänen nach 1. & 2. Verteidigungslinie• Veto oder Akzeptanz des Risikos falls Eindruck ungenügender Mitigation herrscht
Monitor Risks	<ul style="list-style-type: none">• Festlegung von Massnahmen zur Risikominimierung in den CxO / VR-Zielen• Überwachung und Reporting über Fortschritt der Abwehrmassnahmen• VR & GL-Reporting

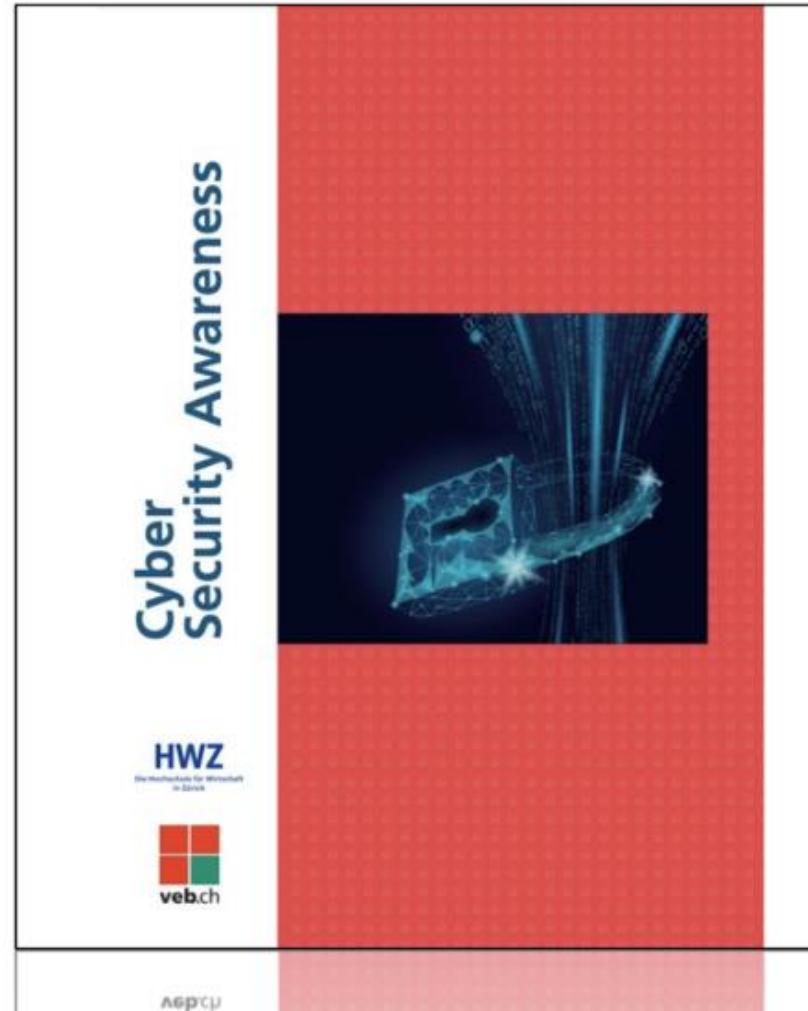
ONE

MORE

THING



Cybersecurity Whitepaper HWZ / Swissaccounting



Description

Die Checkliste ist Bestandteil der neuen Broschüre «Cyber Security Awareness», ein gemeinsames Projekt der HWZ und von veb.ch.

Das Whitepaper liefert einen Überblick über:

- Die allgemeine Lage der Informationssicherheit
- Die häufigsten Angriffsarten und die Anatomie eines Hacks am Beispiel eines CEO Fraud Angriffs
- Ein Modell für kontinuierliche Mitarbeiterschulung
- Eine Checkliste mit Empfehlungen wie man sich und sein Unternehmen mittels Sensibilisierung davor schützen kann.

<https://swissaccounting.org/blog/cyber-security-awareness>

Teil 2: Governance