

Digital Risk Management für KMU «Home Office» Fluch oder Segen?

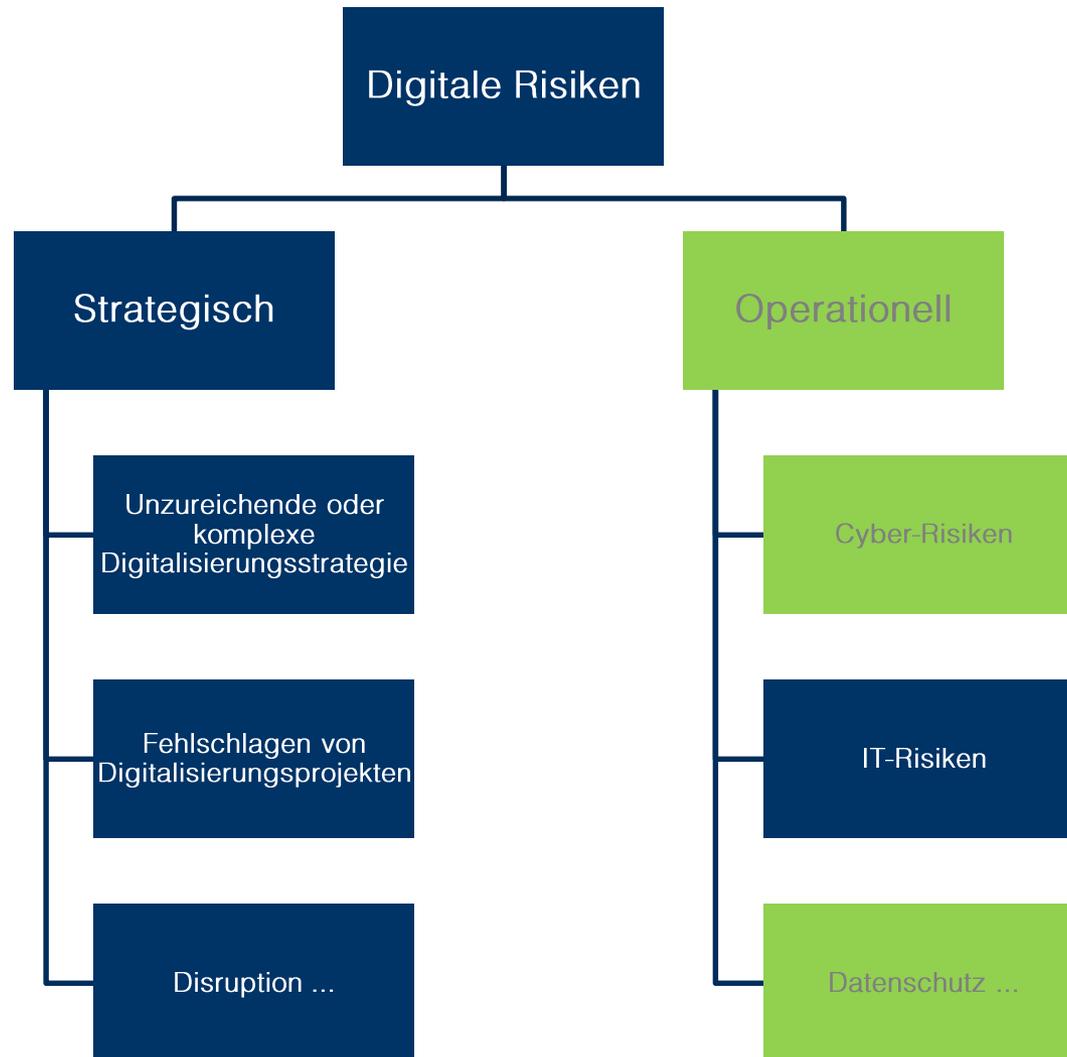
Max Keller - Lead Funk RiskLab - Funk Gruppe



Wo alles beginnt



Digitale Risiken



Risikoexponierung der KMU

Unzureichende
personelle Ressourcen

Kommunikationslücken

Schwachstellen



Fehlende
Risikotransparenz

Unzureichendes
Cyber-Security-Budget

Wissenslücken

Kommunikationslücken

Do you speak IT?



<https://www.youtube.com/watch?v=nNledu2FG7A>

Unzureichende personelle Ressourcen

Wer managed was?

Self Managed Services

- On-Premise
- Betrieb der IT-Systeme durch eine eigene IT-Abt.

Partly Managed Services

- On-Premise
- Betrieb der IT-Systeme durch einen Dienstleister

Managed Services

- Cloud
- Betrieb der IT-Systeme durch einen MSP

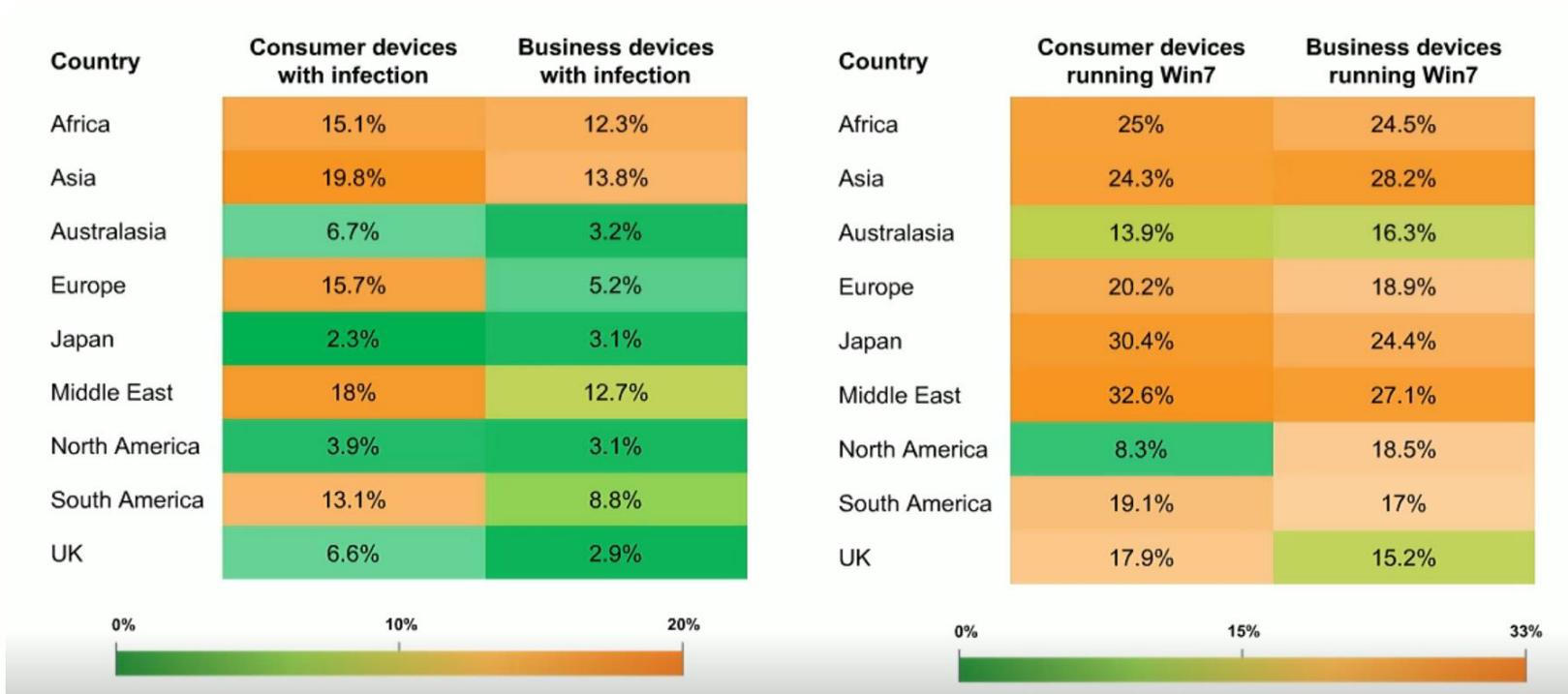


Goodbye Windows 7?

Der Support für Windows 7 endet am 14. Januar 2020.

Gilt für: Windows 7

Microsoft hat sich verpflichtet, 10 Jahre Produktsupport für Windows 7 bereitzustellen, das am 22. Oktober 2009 veröffentlicht wurde. Diese 10-Jahres-Periode ist nun beendet, und Microsoft hat die Unterstützung von Windows 7 eingestellt, so dass wir unsere Investitionen auf die Unterstützung neuerer Technologien und Anwendungen konzentrieren können. Das Datum für den Ablauf des Supports für Windows 7 war der 14. Januar 2020. Technische Unterstützung und Software-Updates von Windows Update, die zum Schutz Ihres PCs beitragen, sind für das Produkt nicht mehr verfügbar. Microsoft empfiehlt dringend, auf Windows 10 umzusteigen, um zu vermeiden, dass Sie einen Service oder Support benötigen, der nicht mehr verfügbar ist.



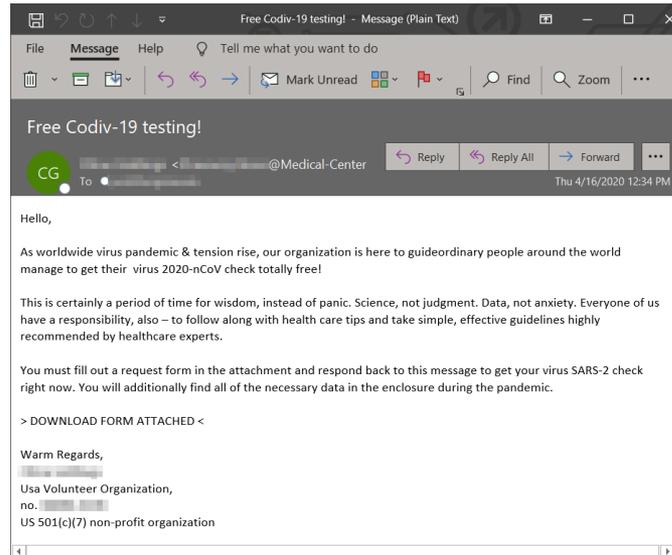
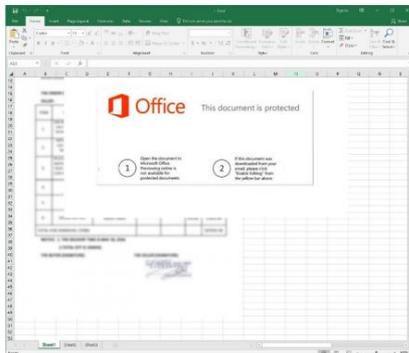
Quelle: Webroot – Threat Report 2020

Schwachstellen

Wem vertrauen?

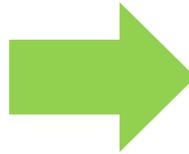
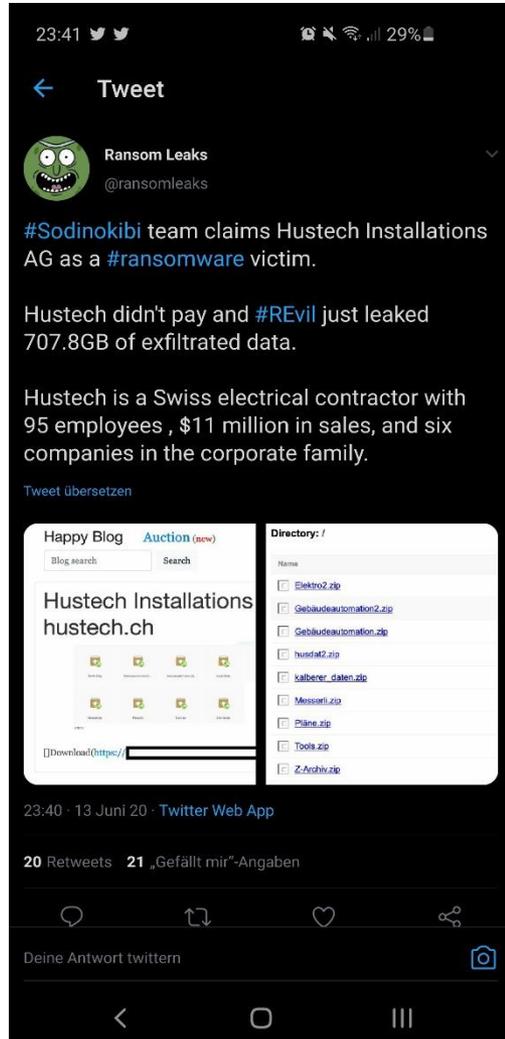


Bild eines geöffneten Anhangs:



Fehlende Risikotransparenz

Was sind unsere Kronjuwelen?



Erweiterung NEST / Anbindung Unit UMAR

Steuerung / Regelung der HLKS-Anlage der neuen Unit UMAR (urban Mining and Recycling) mit OPC – UA Anbindung an NEST-Leitsystem

MEHR INFO



Neubau Logistikgebäude, Belimo Hinwil

Neubau Logistikgebäude sowie vollautomatisiertes Hochregal- und Kleinteillager

MEHR INFO



WLAN-Schülernetz, Schule Rüti

Ausbau Schülernetz mit WLAN-Sendern sowie Racks in den Schulzimmern

MEHR INFO



Verwaltungsgebäude Letzipark Zürich

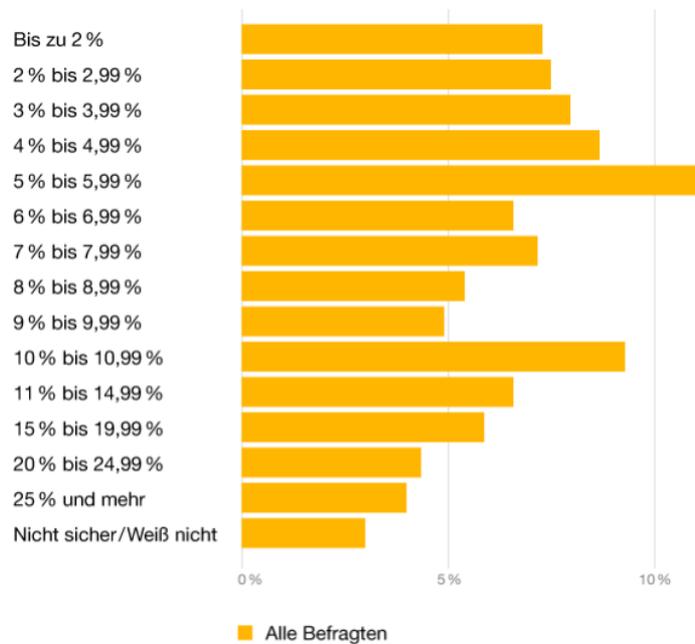
Gesamtsanierung mit Steuerung und Regulierung der Haustechnikanlagen sowie Einzelraumregulierungen für Mieterausbau Betty Bossi

MEHR INFO

Unzureichendes Cyber-Security-Budget

Investieren wir genug?

Wie viel Prozent des gesamten IT-Budgets werden Sie im Jahr 2020 für Informationssicherheit ausgeben?

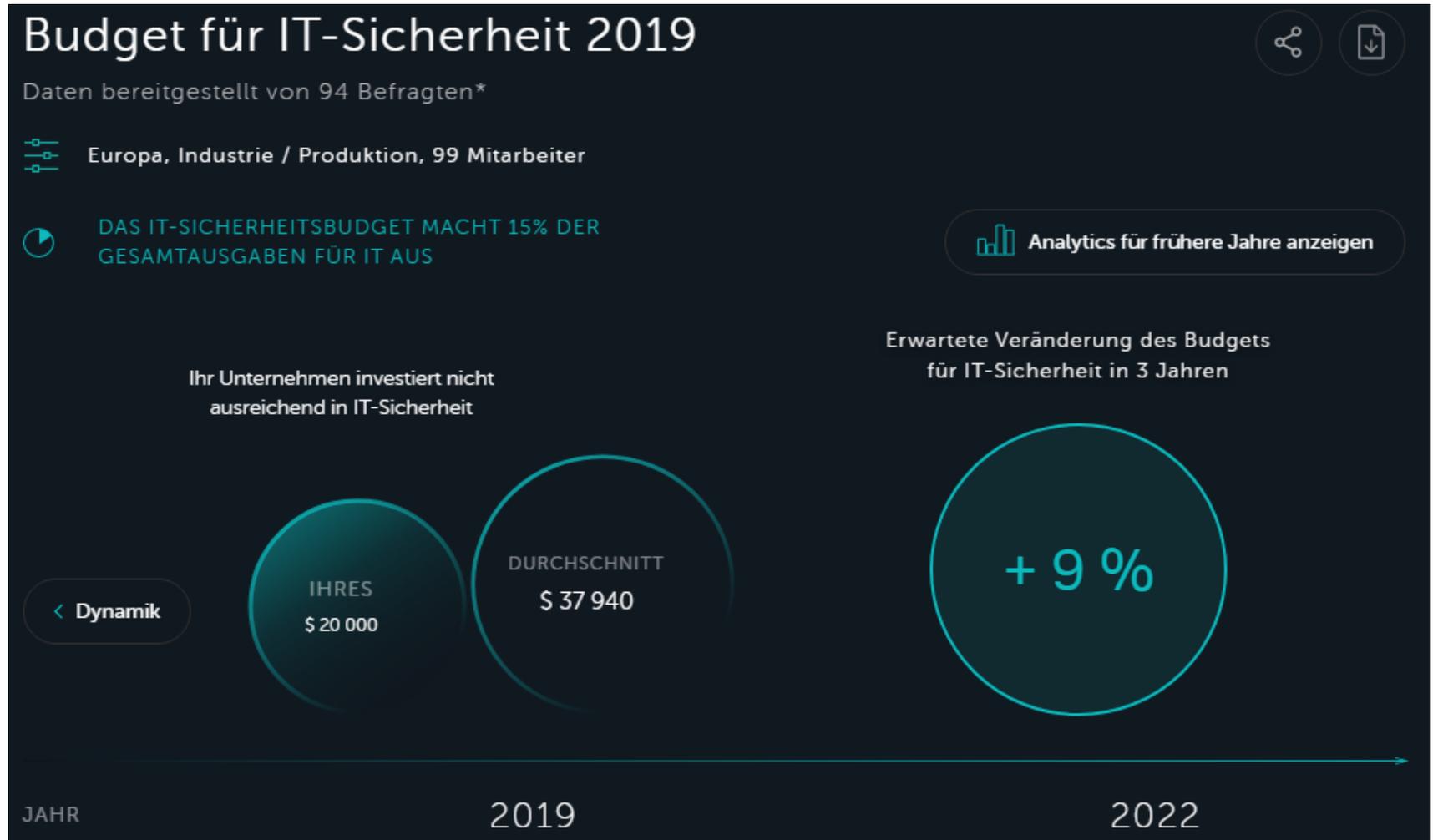


Quelle: PwC - Digital Trust Insights 2019



Unzureichendes Cyber-Security-Budget

Investieren wir genug?



Quelle: Kaspersky IT Security Calculator

Wie gehen die Angreifer am ehesten vor (TTPs)?

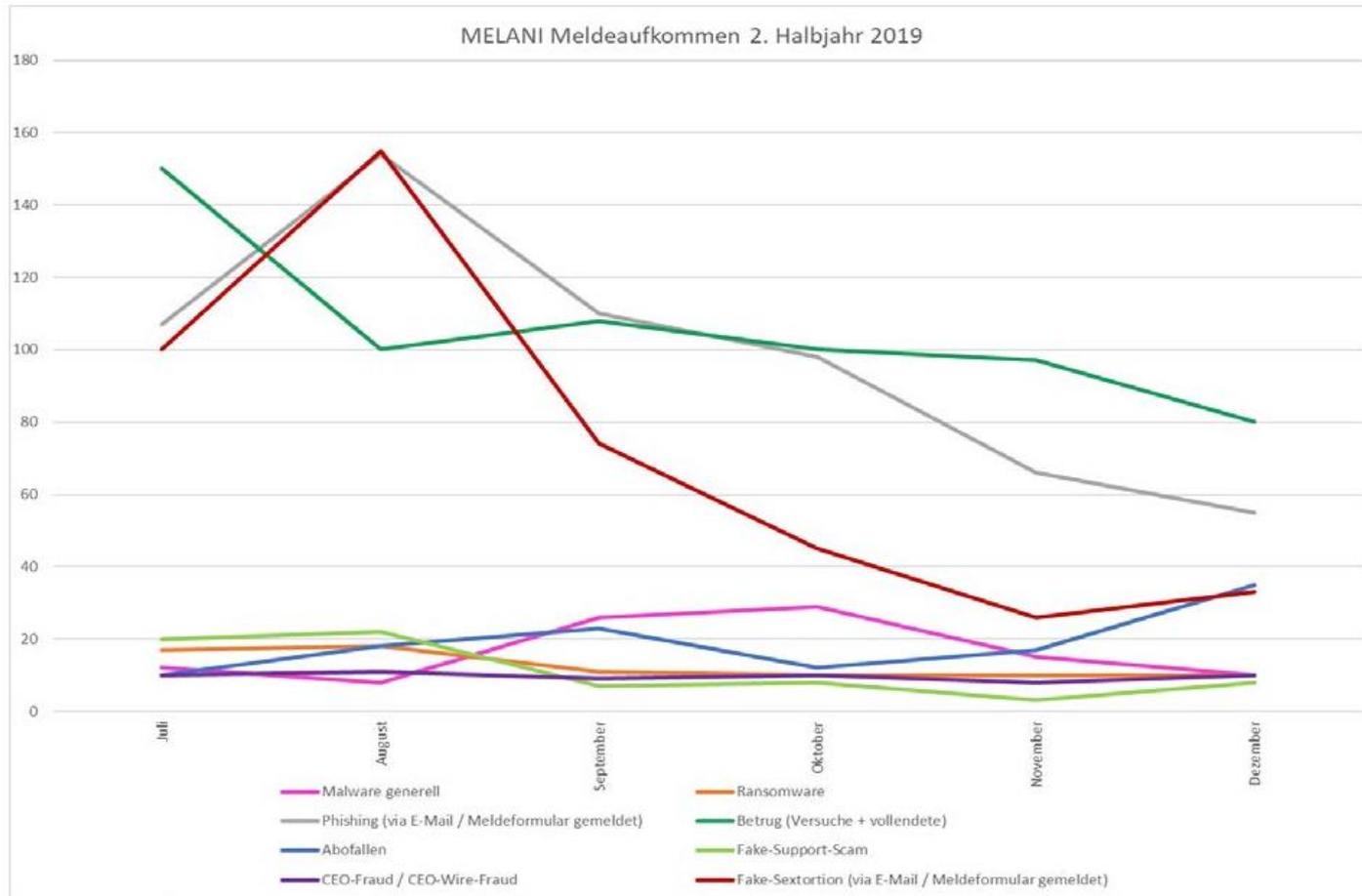
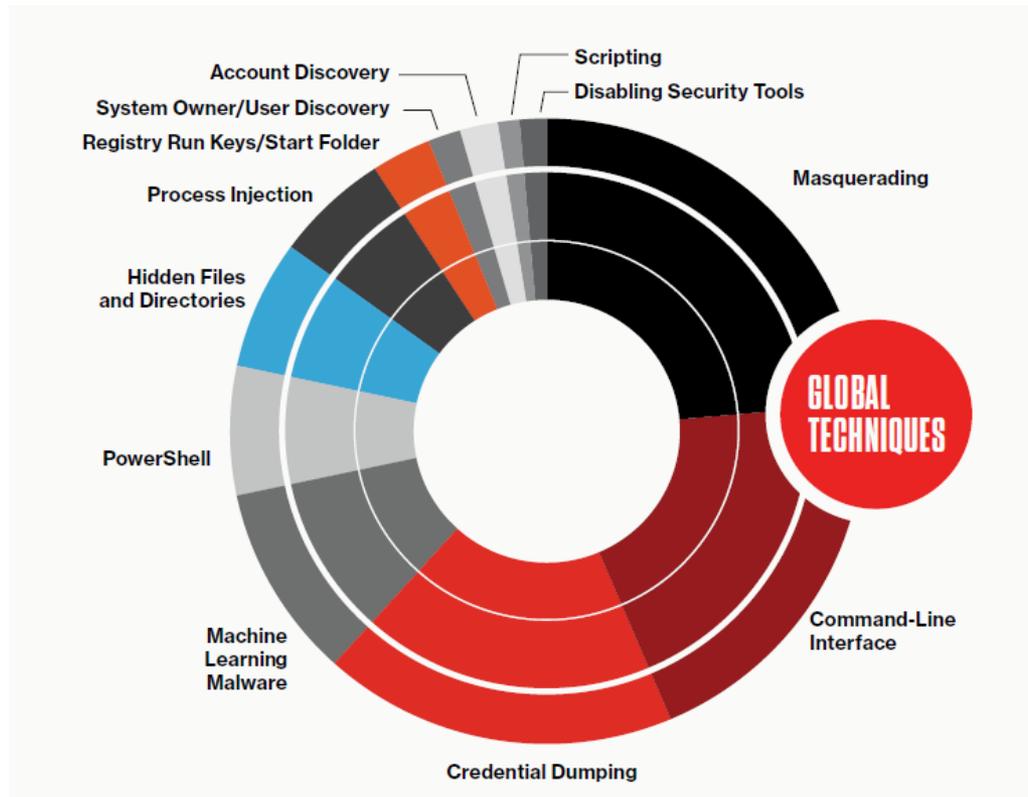


Abb. 2: Via Online-Meldeformular eingegangene Meldungen. Nicht enthalten sind Meldungen über andere Kanäle.

Quelle: MELANI – Halbjahresbericht 2019/2

Wie gehen die Angreifer am ehesten vor (TTPs)?



Quelle: CrowdStrike – 2020 Global Threat Report

Transparenz über CyberRisiken schaffen

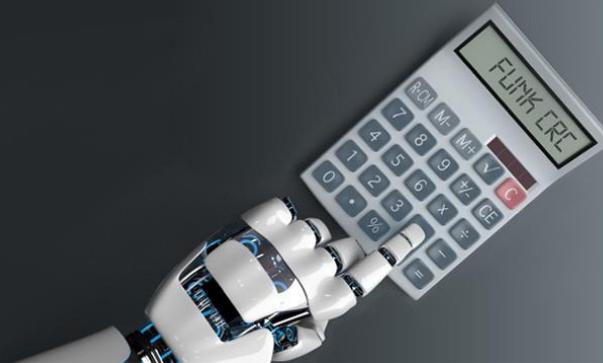


Eintrittswahrscheinlichkeiten

1. Betrieb eines Webshops oder eines eCommerce-Businesses → Kreditkartendaten etc.
2. Verarbeitung (besonders) schützenswerter Personendaten → Patientendaten, Finanzdaten etc.
3. Verarbeitung vorbörslicher Finanzinformationen → Insidertrading
4. Verarbeitung politischer Informationen → politische Spionage
5. Verarbeitung von Daten der nationalen Sicherheit → militärische Spionage
6. Technologie- oder Innovationsführerschaft → Intellectual Property, Wirtschaftsspionage
7. Internationale Ausrichtung, Geschäftspartner in mehreren Ländern → Spionage durch verfeindete Staaten/Länder
8. (Neue) Tochtergesellschaften im Ausland → Tochtergesellschaft mit geringen Maturität in der Cyber-Security (Einfallstor zur Muttergesellschaft)
9. Vertrauensvolle Geschäftsbeziehungen zu exponierten Unternehmen → über die gesamte Supply-Chain
10. Hohe Abhängigkeit der Leistungserbringung von der IT → erhöhte Erpressbarkeit

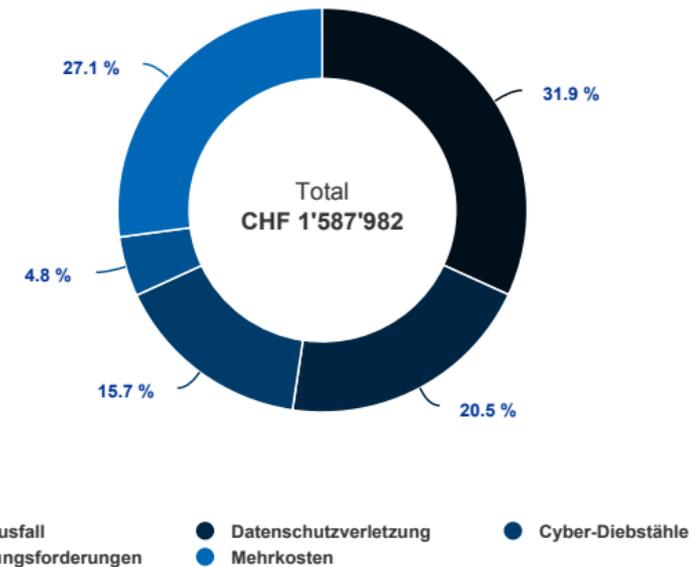
Digital Risk Management für KMU

Schadensausmass



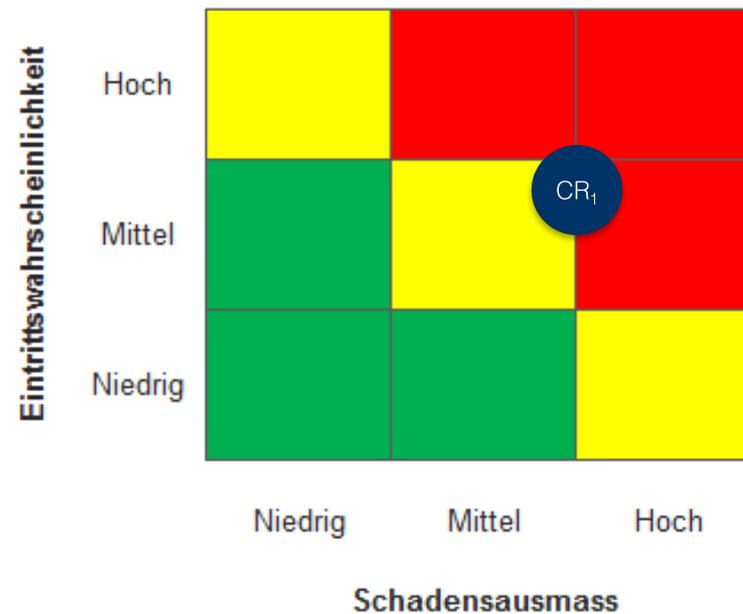
Berechnung von Cyber-Restrisiken (Schadenspotenzialen)

Cyber-Restrisiken (Schadenspotenziale)	CHF 1'587'982
IT Systemausfälle	CHF 506'062
Ertragsausfall	CHF 383'562
Mehrkosten Betriebsunterbrechung	CHF 87'500
Vertragsstrafen	CHF 35'000
Datenschutzverletzung	CHF 325'200
Benachrichtigungskosten (nur Postversand)	CHF 100'000
Bussgelder und Strafen	CHF 0
Haftpflichtansprüche Dritter Datenschutz	CHF 225'200
Kreditkarten (Neue Karten)	CHF 0
PCI DSS Non compliance fees	CHF 0
Cyber-Diebstähle	CHF 250'000
Verlust von Geldern, Wertpapieren und Waren	CHF 250'000
Erpressungsforderungen	CHF 76'000
Lösegelder	CHF 76'000
Mehrkosten	CHF 430'720
Call Center	CHF 30'720
Forensische Untersuchungen (Ursache / Sicherheitsverbesserung)	CHF 144'000
Krisenkommunikationsberater	CHF 56'000
Rechtskosten	CHF 50'000
Wiederherstellungskosten von Daten und IT-Systemen	CHF 150'000



Transparenz über Risiken schaffen

$$CR_1 = 0.2 * 1'600'000$$



Vielen Dank



Max Keller

Lead Funk RiskLab
Mitglied des Kaders
MAS Digital Business

T +41 58 311 05 51
max.keller@funk-gruppe.ch

Zugabe



<https://www.youtube.com/watch?v=nPR131wMKEo>