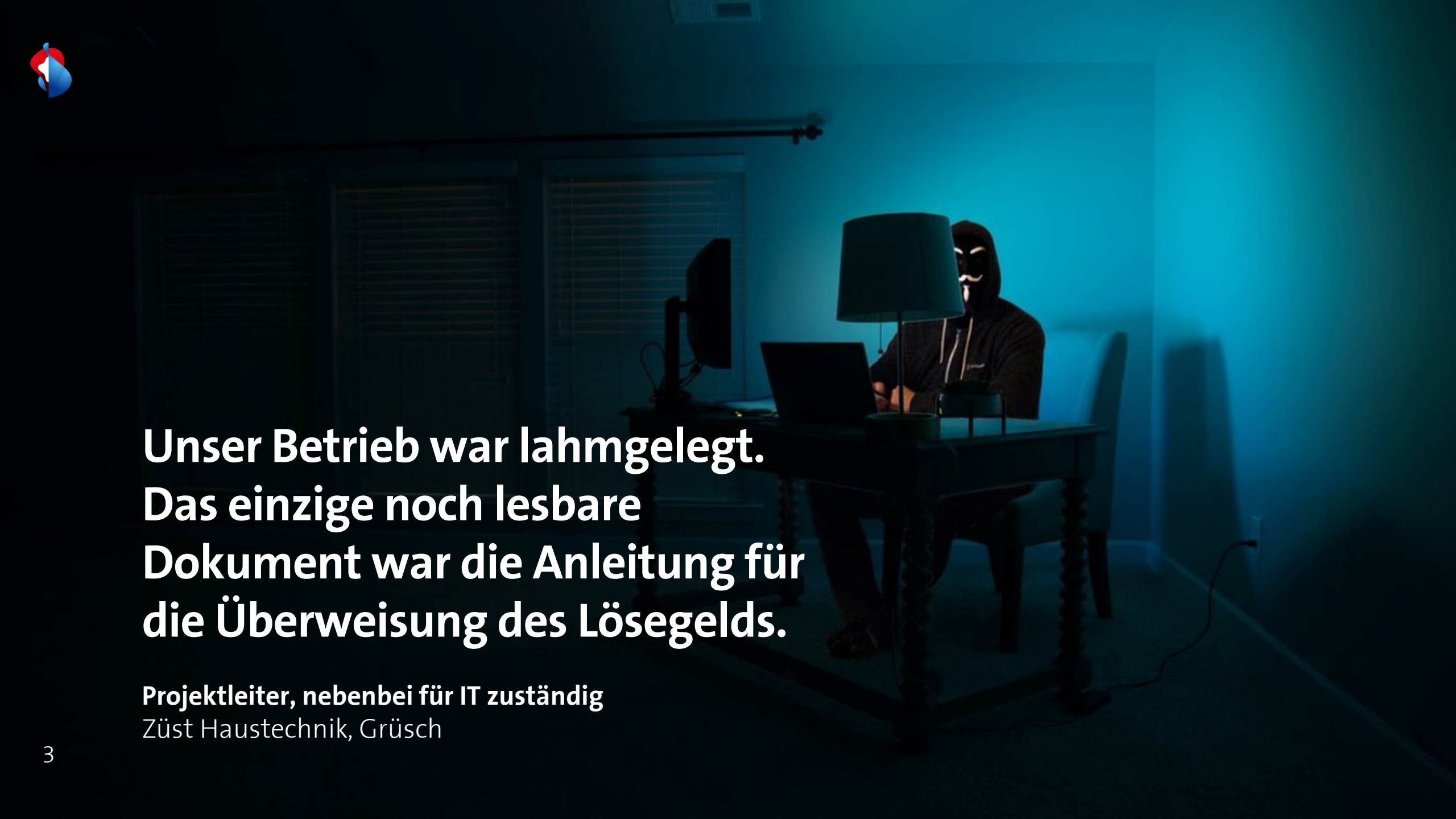
Cybersecurity im Treuhand- und Wirtschaftsprüfungssektor

Mit fortschreitender Digitalisierung werden Daten zentraler Bestandteil der Wertschöpfung. Umso wichtiger ist es, dass Unternehmen Strategien entwickeln und Maßnahmen ergreifen, um ihre Organisation nachhaltig vor Cyberangriffen zu schützen und jeden Mitarbeiter sensibilisiert und entsprechend ausbildet.

15. November 2022

C1 External

swisscom



Unser Betrieb war lahmgelegt. Das einzige noch lesbare Dokument war die Anleitung für die Überweisung des Lösegelds.

Projektleiter, nebenbei für IT zuständig
Züst Haustechnik, Grüsch

Swiss Windows nach Ransomware-Angriff Konkurs

2694

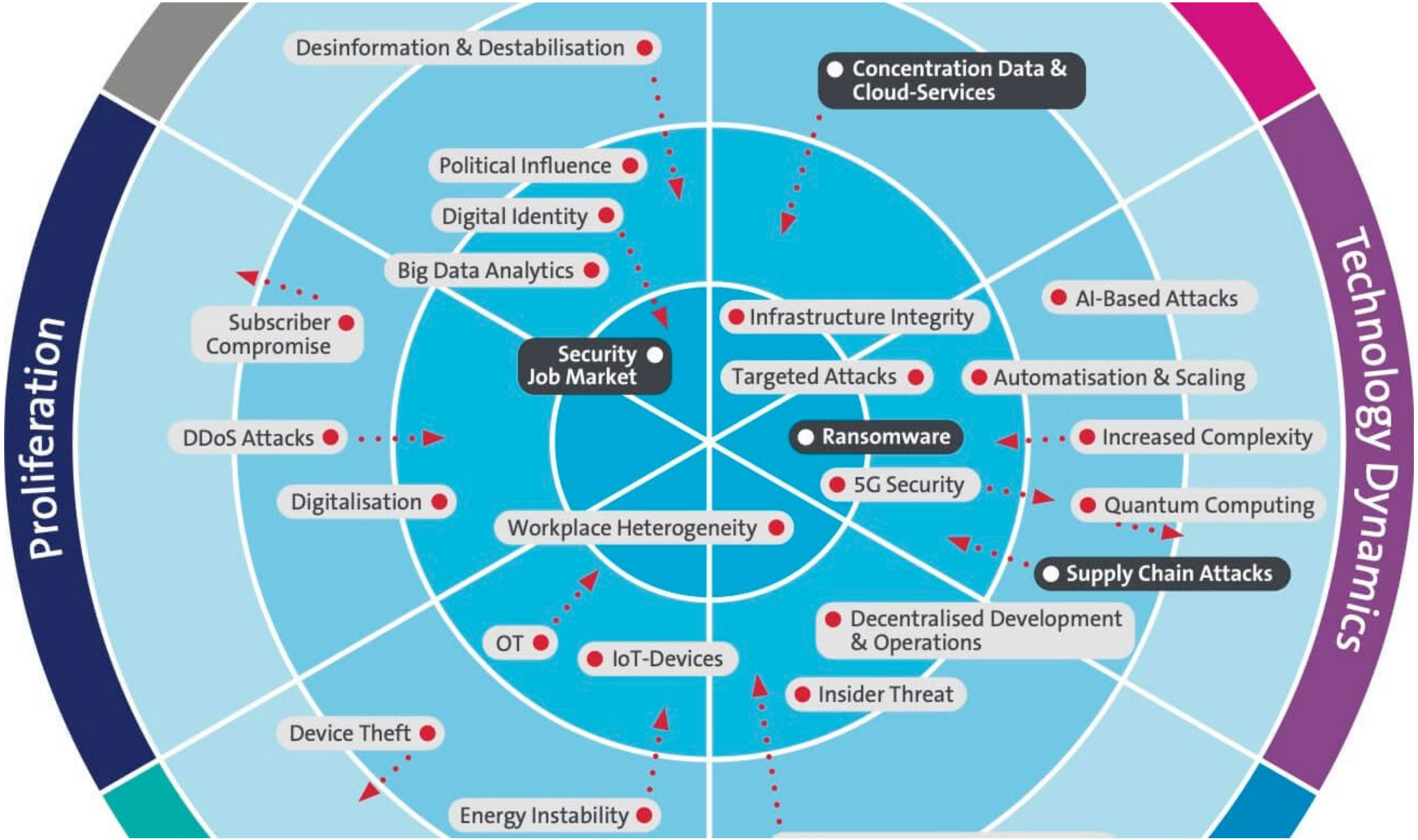
Daten von Schweizer Unternehmen im Darknet veröffentlicht[1].

(August 2020-August 2021)

43%

aller Cyberangriffe weltweit richten sich gegen KMU[2].

1)Quelle: 2019 Data Breach Investigations Report (Verizon)
2)Quelle: 2020 Analyse Beobachter (Recorded Future)


Proliferation
Technology Dynamics
Desinformation & Destabilisation
Political Influence
Digital Identity
Big Data Analytics
Subscriber Compromise
Security Job Market
DDoS Attacks
Digitalisation
Workplace Heterogeneity
OT
IoT-Devices
Device Theft
Energy Instability
Concentration Data & Cloud-Services
AI-Based Attacks
Infrastructure Integrity
Targeted Attacks
Automatisation & Scaling
Ransomware
Increased Complexity
5G Security
Quantum Computing
Supply Chain Attacks
Decentralised Development & Operations
Insider Threat

Die Bedrohung ist real

Jeden Monat ungefähr...

20

Sicherheitszwischenfälle, die von Swisscom CSIRT bekämpft wurden

5'500'000

Angriffsversuche gegen die Swisscom Infrastruktur blockiert

4'700

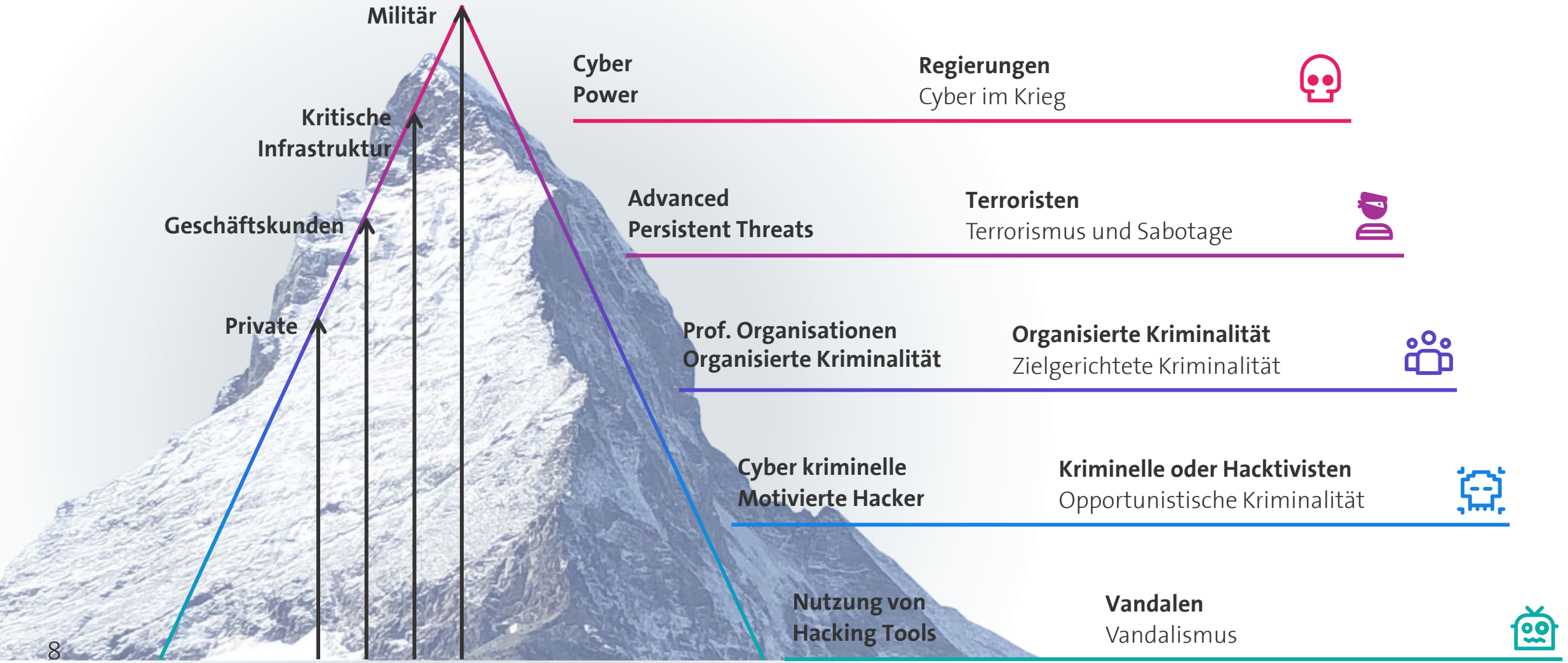
Kontaktierte Privatkunden wegen gehackter Kunden-Accounts

2'200

Erkannte und blockierte Phishing-Attacken

Es gibt keine einzelne Quelle der Bedrohung

Mit wem haben wir es zu tun?



Die grössten Sicherheitsrisiken für KMU sind …

Phishing

Ransomware
Malware
Viren
Trojaner

Fehlende Security-Awareness bei Mitarbeitenden

Quelle: Nationales Zentrum für Cybersicherheit NCSC (Schweiz); X-Force Threat Intellligence Index von IBM (2020); Verizon Data Breach Investigations Report (2020); FHNW (2020): Digitalisierung, Home-Office und Cyber-Sicherheit in KMU (Befragung von 503 Schweizer KMU)

Die Wiederherstellung der IT-Systeme kann dauern

35%

der Betroffenen konnten die Systeme **am ersten Tag** wiederherstellen

42%

brauchten **bis zu drei Tage**

22%

der Betroffenen benötigten **mehr als drei Tage**

Zwei Drittel sind tagelang offline

Quelle: GDV, Repräsentative Forsa-Befragung von 300 Entscheidern in kleinen und mittleren Unternehmen (April 2020)

76%

aller Schweizer KMU sehen Mitarbeitende als grösste Sicherheitslücke.

11%

der befragten Schweizer KMU* denken nicht, dass ihre Mitarbeitenden einen Phishing-Angriff erkennen würden.

* Quelle: MSM Research (2021), ICT-Security in kleineren und mittleren Unternehmen (bis 99 MA)

Ransomware

Unter Ransomware versteht man einen getarnter Angriff mit dem Ziel, Lösegeld zu erlangen. Hierbei wird eine angeblich harmlose Datei mit einem schädlichen Programm versehen, die den Zugriff auf Geräte sperrt oder darauf erhaltene Dateien verschlüsselt.

Opfert erhält eine manipulierte Datei, Link oder Applikation

Beim Öffnen wird der Rechner mit Ransomware infiziert

Der Zugriff auf einzelne Ordner / Festplatte wird gesperrt

Opfer wird aufgefordert Lösegeld zu bezahlen

Zahlung erfolgt → Zugriff wird wiederhergestellt

Zahlung erfolgt nicht → Zugriff bleibt weiterhin gesperrt

Es gibt keine Garantie dafür, dass nach Zahlung die betroffenen Geräte/Daten wieder entsperrt werden

Die meisten Cyberangriffe beginnen mit einer Phishing-Mail

So machen sich Cyberkriminelle die Leichtgläubigkeit der Benutzer zunutze

Der Nutzer erhält eine angeblich glaubwürdige Mail (Phishing-Mail).

Die Mail fordert das Öffnen eines Links und gegebenenfalls die Eingabe von Daten.

Der Benutzer glaubt dem Inhalt und öffnet den Link.

Die Kopie einer täuschend echt aussehenden Website fragt nach Daten (meist Anmeldedaten).

Der Nutzer gibt die geforderten Daten ein.

Die Täter besitzen die Daten vom Nutzer und können diese auf der Originalseite verwenden.

Wie sensibilisiere ich meine Mitarbeiter

- Simulation von Phishing Angriffen
- Online Schulungsplattform für Mitarbeitende
- Messung des Erfolgs der Massnahmen
- Professionelle Planung & Durchführung

1.

Sicherheitslücken identifizieren

Wir geben Ihnen ein objektives Bild der Ausgangslage Ihrer IT-Sicherheit.

2.

IT, Netzwerk & Daten schützen

Mit unseren Services bieten wir Ihnen einen integrierten Gesamt-schutz für Ihre IT.

3.

Daten und IT im Krisenfall wiederherstellen.

Im Angriffsfall sind Sie mit unseren Services in der Lage, Ihre Daten und Systeme rasch wiederherzustellen.

Sicherheitslücken identifizieren

Die Analyse der Ausgangssituation der IT-Sicherheit Ihrer Firma bildet eine solide Grundlage für die Erstellung und Überarbeitung eines IT-Sicherheitskonzepts.

Analyse der IT-Organisation und Geschäftsprozesse

Analyse der Gegebenheiten: IT-Organisation, Governance, Zugriffs- und Datenschutz, Business Continuity etc.

Durchleuchten der IT-Infrastruktur

Identifikation von technischen Schwachstellen und Fehl-konfigurationen (Vulnerability-Scan)

Risikofaktoren identifizieren

Massnahmen ableiten

IT, Netzwerk und Daten schützen

Schutz des Netzwerks gegen Eindringen von Schadsoftware

Schutz von Cloudanwendungen/-speicher gegen Angriffe und unberechtigte Zugriffe

Sicherer Netzwerkzugriff im Homeoffice/unterwegs

E-Mail-Kommunikation und Internet-Kommunikation sichern

Identity- und Access-Management

Sichere Standortvernetzung

Zonierung des Netzwerks

Schutz der Arbeitsplätze und Hardware

Daten und IT im Krisenfall wieder-herstellen

Daten, Programme, IT-Infrastruktur stehen auf Grund von Hacker-Attacken, Serverfehler, Stromausfall, Bugs oder Viren (u. v. m.) nicht mehr zur Verfügung.

Daten-Backup

Regelmässige Sicherung der Daten in der Cloud

Disaster Recovery

Permanente Spiegelung der lokalen IT-Infrastruktur in der Cloud

Wiederherstellung einleiten

- Daten können wieder-hergestellt werden
- IT muss ggf. neu aufgesetzt werden
- Ausfall: bis zu mehrere Tage oder Wochen

- Betrieb kann aufrecht erhalten werden
- IT-Infrastruktur steht in der Cloud zur Verfügung
- Ausfall: Firma kann innert kürzester Zeit weiterarbeiten

Rettungskette bei einem Cyberangriff

Ruhe bewahren und keine vorschnellen Handlungen vornehmen.

Helfen lassen – Spezialisten wie das Swisscom Rapid Response Team beiziehen.

Kommunizieren – Krisenkommunikation aktivieren basierend auf dem Krisenkommunikationshandbuch

Technik – **Systeme wieder herstellen** / Backup Restore

Melden – NCSC und Polizei über den Vorfall informieren und Strafanzeige erstatten

Prävention – Massnahmen ergreifen um eine Wiederholung zu vermeiden

Die Key Take-Aways

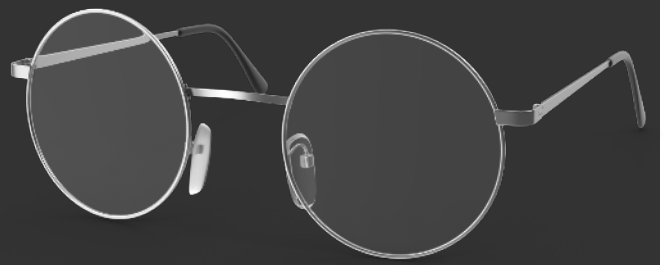
1

Security ist Chef Sache und sollte bei jedem Unternehmen egal welcher Grösse Thema sein.

2

Kriminelle Akteure konzentrieren sich aktuell immer mehr auch auf KMU's.

Vor Daten-räubern Schützen



3

Ein effektiver Grundschutz ist Key für einen sicheren Betrieb.

4

Der Mitarbeiter ist einer der wichtigsten Elemente im Rahmen der Security.

Live: Ihr KMU wurde gehackt – was nun?

Das erwartet Sie

- Die wichtigsten Sofortmassnahmen für den Ernstfall
- Vorgehen für Anzeige und Meldung einer Cyberattacke
- Woran Sie denken sollten und wer Ihnen helfen kann

Link zum Webinar

Live am 08 Dezember, ab 11:00 Uhr

«Die Frage ist nicht, ob man von Cybercrime betroffen ist, sondern wann.»

Bernhard Droz

Dienstchef IT-Forensik und Cybercrime, Kantonspolizei Aargau

Fragen & Antworten

Soforthilfe bei Cyber- und Hackerangriffen auf Ihr KMU

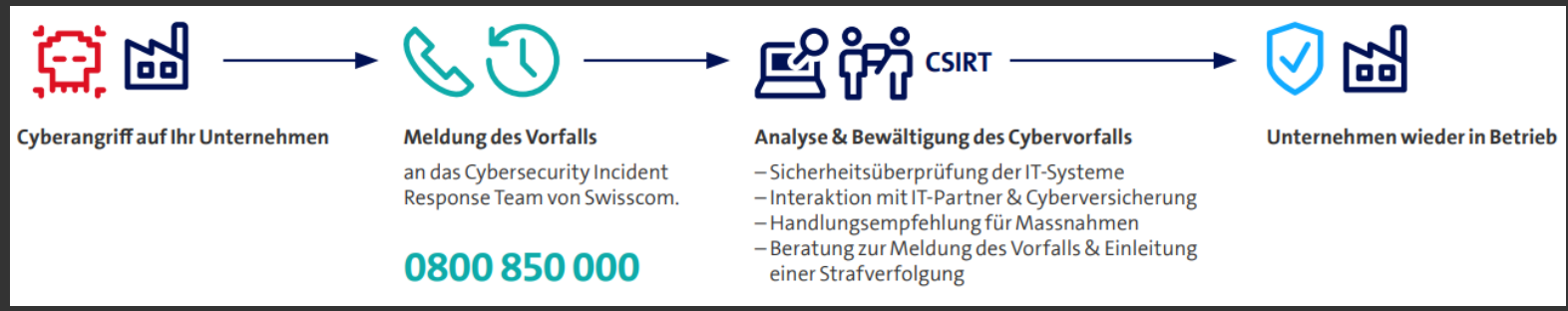
Soforthilfe bei einem Cyberangriff: 0800 850 000. Das CSIRT von Swisscom ist 24/7 für Sie da.

Der Service

•Ein bestens ausgebildetes Cybersecurity-Team mit breiter Erfahrung steht Ihnen 24/7 zur Verfügung.

Wann ist unsere Soforthilfe die richtige Lösung?

Wie aus dem Nichts sind IT und Tagesbetrieb Ihres KMU lahmgelegt. Ihr Webshop ist nicht mehr erreichbar, der Datenzugriff funktioniert nicht mehr. Das einzige lesbare Dokument ist eine Anleitung, wohin Sie das Lösegeld überweisen sollen, um diesem Horrorszenario zu entkommen. Genau für solche Cyberangriffe auf KMU steht unser erfahrenes Expertenteam für Sie bereit. Dieses analysiert die Situation schnellstmöglich und liefert Ihnen eine solide Grundlage, damit Sie fundiert entscheiden und adäquate Massnahmen einleiten können.



Swiss Cyber Defence DNA **6 Key Massnahmen**

Massnahme Nr. 1

Aktuelle unveränderbare Datensicherung / schreibgeschütztes Backup

Massnahme Nr. 2

Umfassender und aktueller Schutz vor Schadsoftware

Massnahme Nr. 3

Netzwerke und Fernzugriffe absichern

Massnahme Nr. 4

Hardware und Software aktuell halten

Massnahme Nr. 5

Mitarbeiter und deren Rollen

Massnahme Nr. 6

Notfallprozesse definieren

Gewusst wo nachschauen...

Swiss Cyber Defence DNA Massnahmen

https://scd-dna.ch/massnahmen/

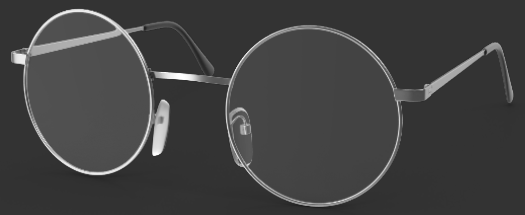
Plattform für Internetsicherheit

https://www.ibarry.ch/de/

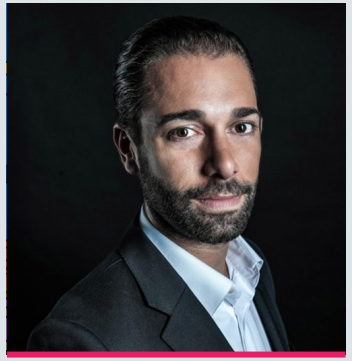
Swisscom KMU Security Check

https://www.swisscom.ch/de/business/kmu/it-cloud/security-check.html#/start

Bett-lektüre



Ihre Kontaktpersonen



Raphaël Boullet
Head Security SOHO & Midmarket
Swisscom Schweiz AG
raphael.boullet@swisscom.com