Cloud Service die gute Wahl für Start-ups?

.Sicher unterwegs

swisscom

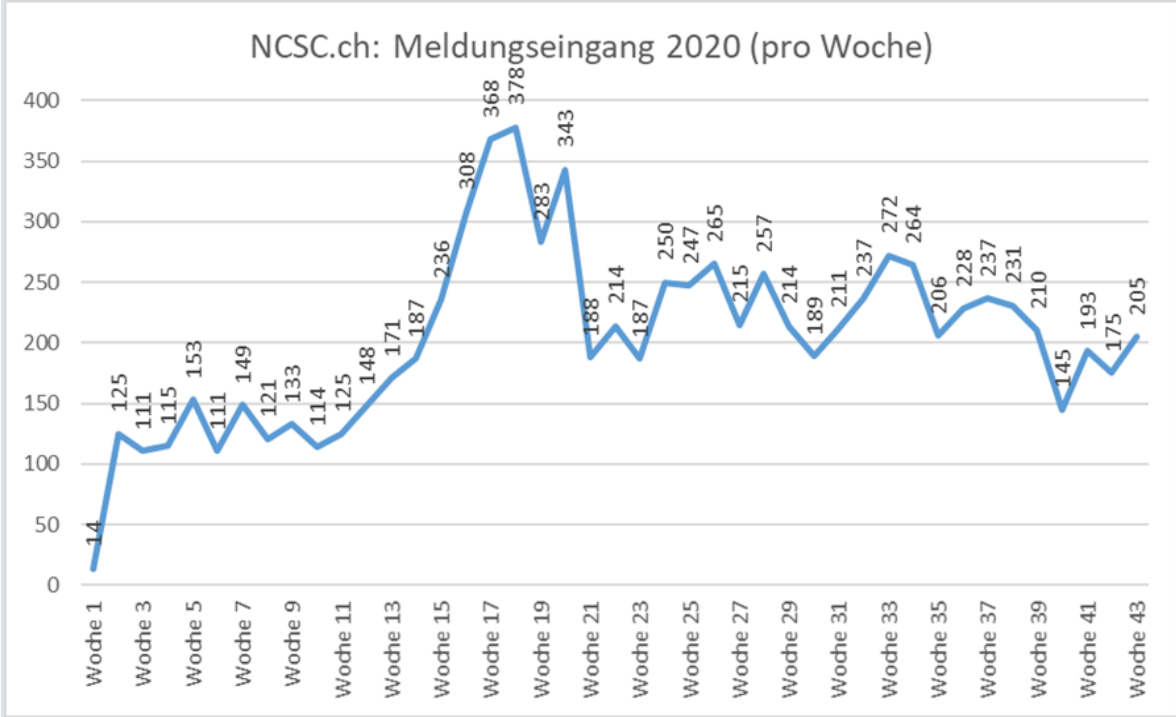
C2 Internal

Agenda

1. Beachtung schenken- Cyberkriminalität
2. Wie läuft ein Angriff ab und was heisst das für mein Start-up?
3. Wie kann ich mein Start-up schützen?
4. Fragerunde

Cybervorfälle nehmen zu. Auch in der Schweiz.

Je nach ICT Abhängigkeit kann damit die Unternehmenstätigkeit zum Stillstand gebracht werden.



Quelle: Nationales Zentrum für Cybersicherheit der Schweiz: Auswertung seit 1.1.2020 (Link)

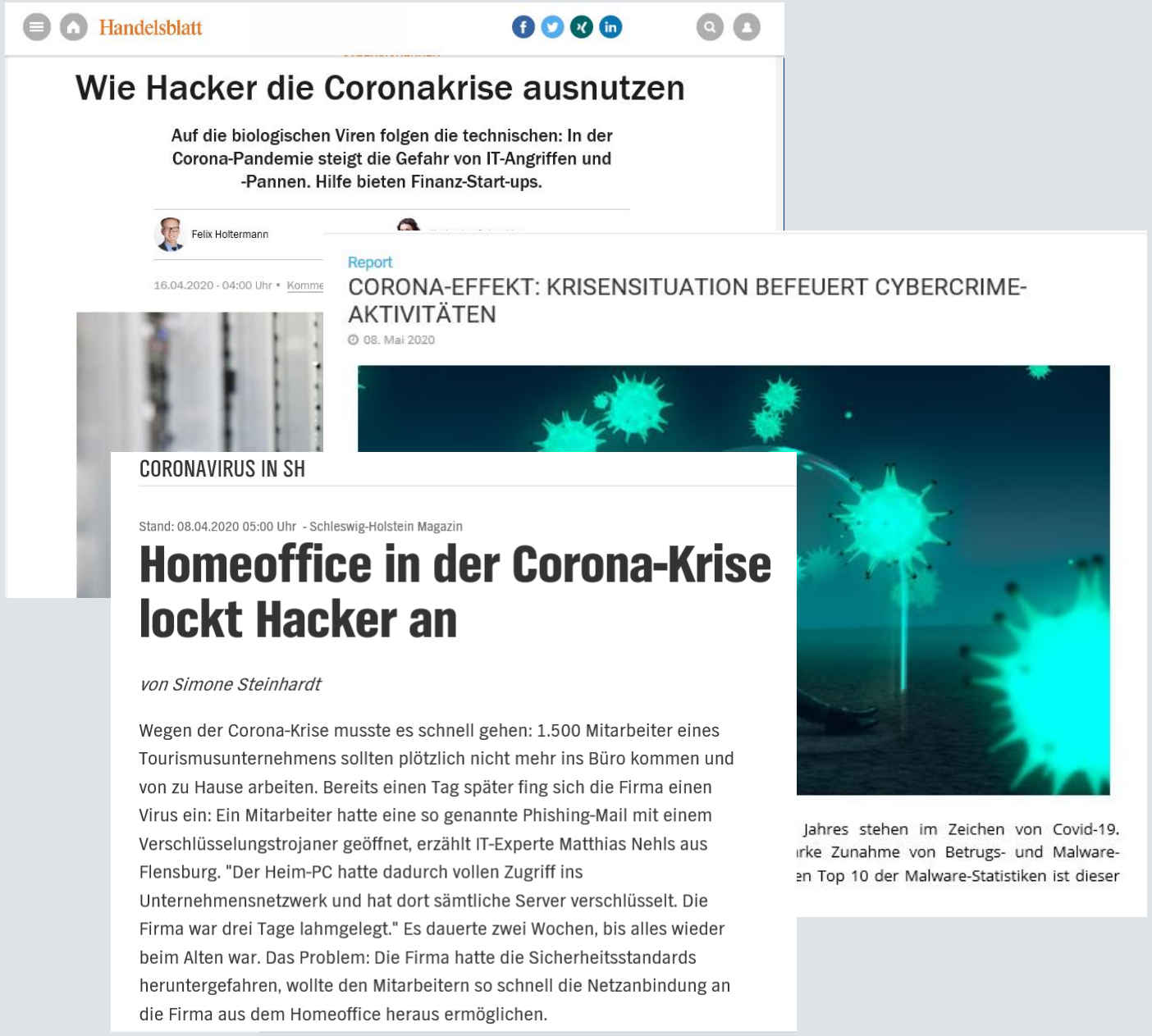
Rang		Prozent	2019 rang	Trend
1	**Cyber-Vorfälle (z.B. Cyberkriminalität, IT-Ausfall, Datenschutzverletzungen, Geldbußen und Strafen).**	**57%**	2 (48%)	▲
2	Betriebsunterbrechung (inkl. Lieferkettenunterbrechung)	**56%**	1 (58%)	▼
3	Rechtliche Veränderungen (z.B. Handelskriege und Zölle, Wirtschaftssanktionen, Protektionismus, Brexit, Zerfall der Euro-Zone)	**34%**	3 (29%)	=
4	Marktentwicklungen (z. B. Volatilität, verstärkter Wettbewerb/neue Wettbewerber, M&A, stagnierende Märkte, Marktschwankungen)	**25%**	5 (25%)	▲
5	Neue Technologien (z.B. Auswirkung der Vernetzung von Maschinen, Nanotechnologie, künstliche Intelligenz, 3D-Druck, autonome Fahrzeuge, Blockchain)	**15%**	8 (17%)	▲
6	Feuer, Explosion	**13%**	6 (19%)	=
6	Makroökonomische Entwicklungen (z.B. Sparprogramme, Anstieg der Rohstoffpreise, Deflation, Inflation)	**13%**	6 (19%)	=
8	Reputationsverlust oder Beeinträchtigung des Markenwerts	**11%**	10 (10%)	▲
8	Naturkatastrophen (z.B. Sturm, Überschwemmung, Erdbeben)	**11%**	3 (29%)	▼
8	Produktrückruf, Qualitätsmängel, Serienfehler	**11%**	**NEW**	▲

Quelle: [Allianz Global Corporate & Specialty: Die 10 wichtigsten Geschäftsrisiken in der Schweiz (2020)](#).

IT Sicherheit als Wettbewerbsvorteil

- Cyberkriminalität wird zum Geschäftsrisiko
- Abhängigkeit von funktionierender IT
- Vorbereitung auf Cyberangriff als Wettbewerbsvorteil

Cyberkriminelle passen sich an die aktuelle Situation an.



Handelsblatt

Wie Hacker die Coronakrise ausnutzen

Auf die biologischen Viren folgen die technischen: In der Corona-Pandemie steigt die Gefahr von IT-Angriffen und -Pannen. Hilfe bieten Finanz-Start-ups.

Felix Holtermann

16.04.2020 - 04:00 Uhr • Komme

Report

CORONA-EFFEKT: KRISENSITUATION BEFEUERT CYBERCRIME-AKTIVITÄTEN

08. Mai 2020

Jahres stehen im Zeichen von Covid-19.
irke Zunahme von Betrugs- und Malware-
en Top 10 der Malware-Statistiken ist dieser

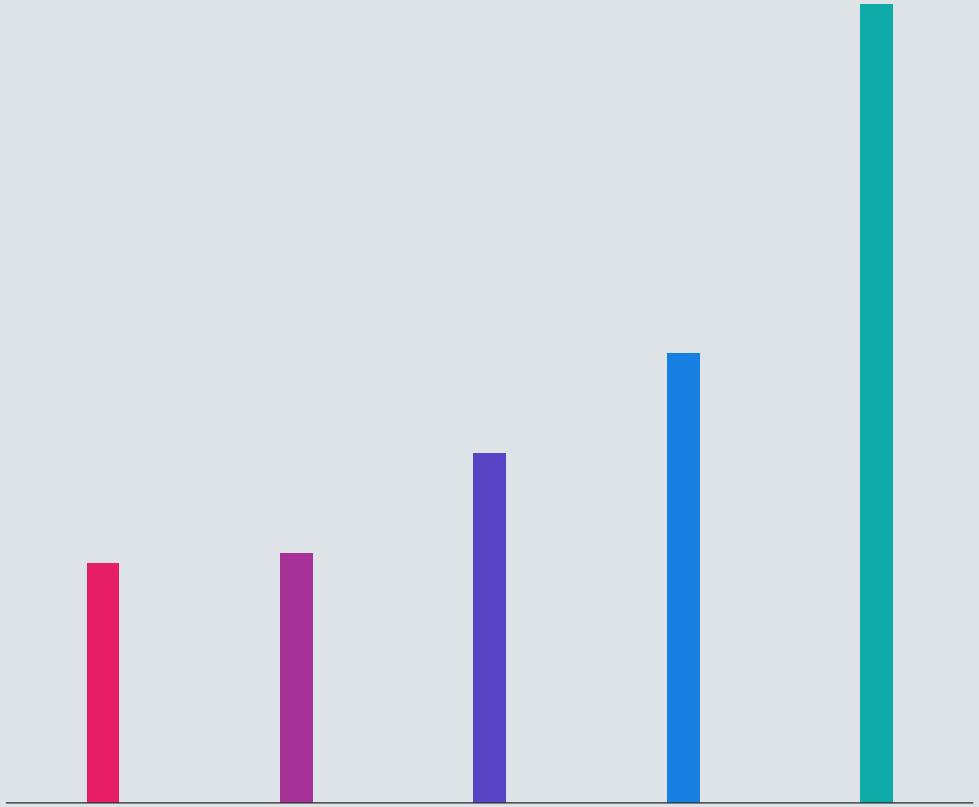
CORONAVIRUS IN SH

Stand: 08.04.2020 05:00 Uhr - Schleswig-Holstein Magazin

Homeoffice in der Corona-Krise lockt Hacker an

von Simone Steinhardt

Wegen der Corona-Krise musste es schnell gehen: 1.500 Mitarbeiter eines Tourismusunternehmens sollten plötzlich nicht mehr ins Büro kommen und von zu Hause arbeiten. Bereits einen Tag später fing sich die Firma einen Virus ein: Ein Mitarbeiter hatte eine so genannte Phishing-Mail mit einem Verschlüsselungstrojaner geöffnet, erzählt IT-Experte Matthias Nehls aus Flensburg. "Der Heim-PC hatte dadurch vollen Zugriff ins Unternehmensnetzwerk und hat dort sämtliche Server verschlüsselt. Die Firma war drei Tage lahmgelegt." Es dauerte zwei Wochen, bis alles wieder beim Alten war. Das Problem: Die Firma hatte die Sicherheitsstandards heruntergefahren, wollte den Mitarbeitern so schnell die Netzanbindung an die Firma aus dem Homeoffice heraus ermöglichen.

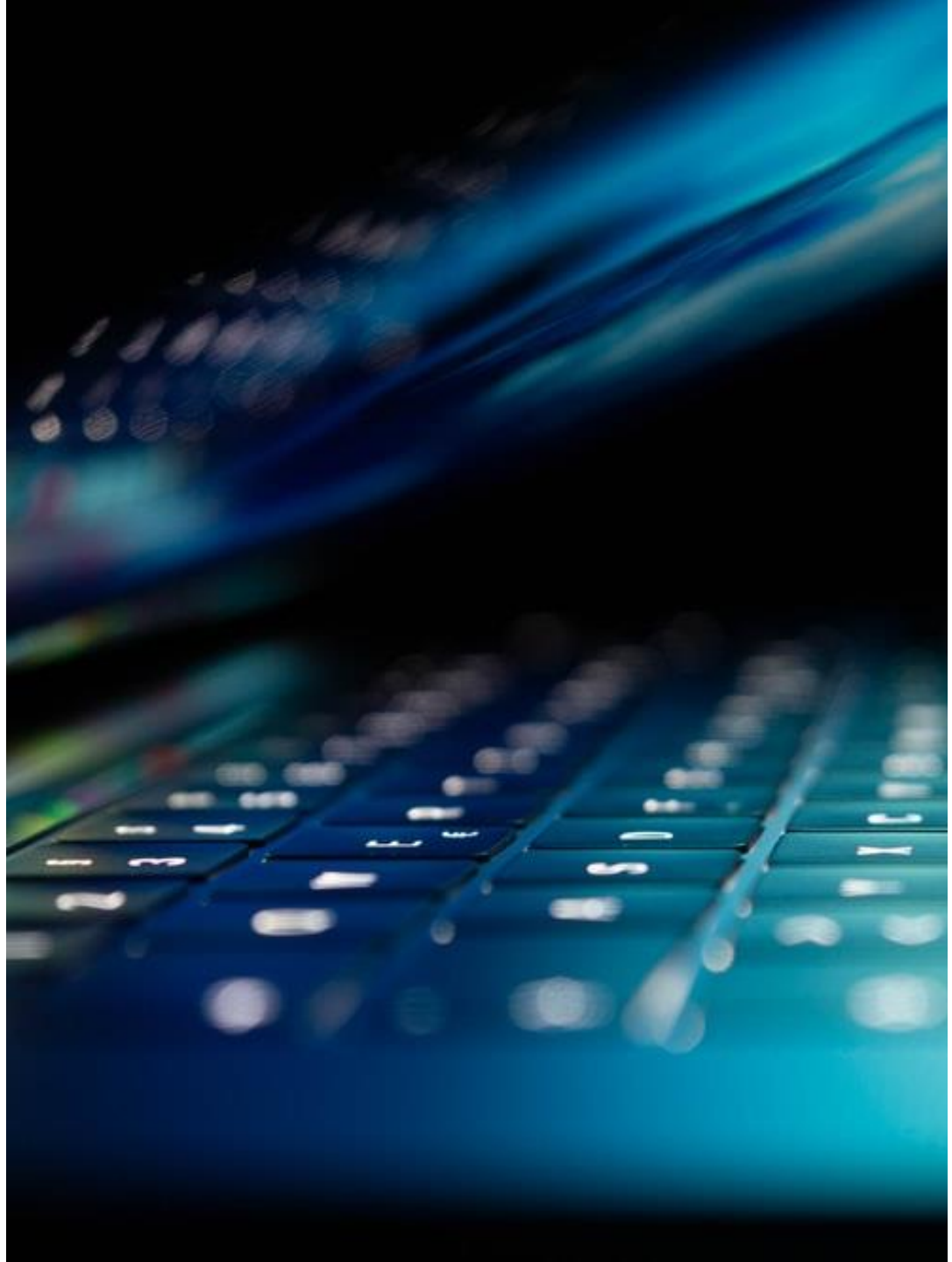


Meldungen von Ransomware Angriffen auf Unternehmen häufen sich seit 2019.

Quelle: Melani (2019)

IT Sicherheit von KMU ist oftmals lückenhaft.

Quelle: Melde und Analysestelle Informationssicherung (Melani), 19.2.2020



Was ist Ransomware?

- Bösartige Software (Trojaner)
- Verschlüsselt Daten
- Zugang zu Daten gegen Lösegeld

Wie kommt Ransomware auf den Rechner?

E-Mail Anhang (Phishing)

Nach dem Öffnen wird Schadsoftware im Hintergrund ausgeführt.

Rechner wird infiziert

Schadsoftware breitet sich im Firmennetzwerk aus.

"Drive-By-Infektion"

Beim Surfen auf einer infizierten Seite wird die Schadsoftware unbemerkt heruntergeladen.

Stadler Rail mit gestohlenen Daten erpresst

Daten konnten zwar wiederhergestellt werden aber die Firma wird dennoch mit gestohlenen Daten erpresst.

TAGBLATT

Bankrott nach gut zehn Jahren +++ Fenster zu bei Swisswindows +++ 170 Mitarbeiter auf die Strasse gestellt +++ Produktionsausfall wegen Cyberattacke

Ruinöser Preiskampf fordert Opfer: Der Mörschwiler Fensterbauer hat am Mittwoch Konkurs angemeldet. Mitarbeitende sind schockiert

Stefan Borkert
27.02.2020, 08.54 Uhr

Hören Merken Drucken Teilen

Swiss Windows nach Ransomware Angriff Konkurs

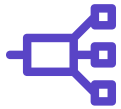
Ein Produktionsausfall von über einem Monat begleitet von massiven Folgekosten führten letztlich zum Konkurs.

Wie kann ich mein Start-up schützen

Immer aktuelles Patch Management

aktuelles Backup-Konzepte

Immer aktueller Firewall-Schutz



Netzwerk-& Nutzer-Segmentierung

Bedarfsgerechte Benutzerrechte

Fernzugriffe gut schützen (Zweiweg Authentifizierung).

Planung für einen sicheren Betrieb

Sicherheitskonzept

Netzwerk-Audit

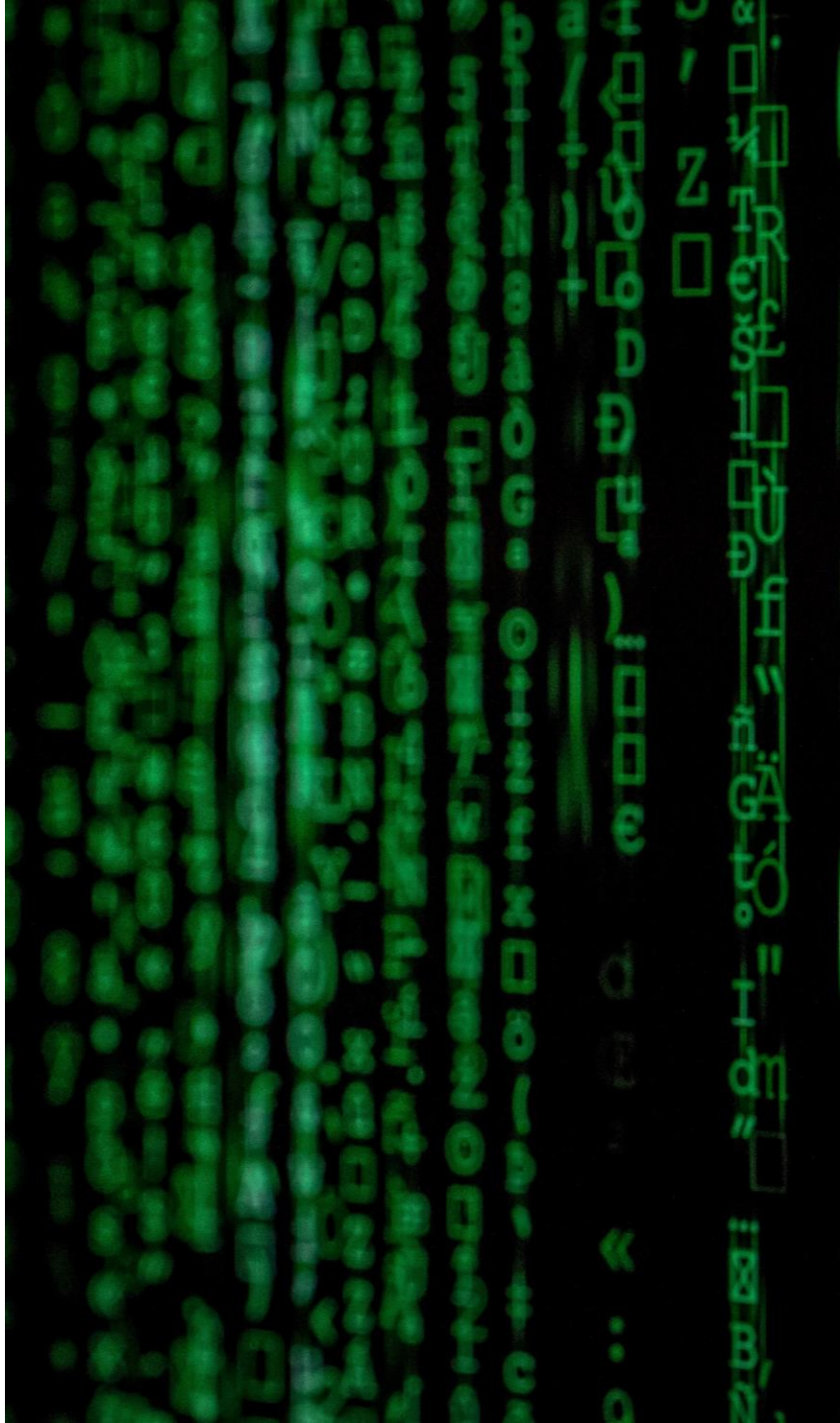
Backup-Strategie

Notfallkonzept

Mitarbeiter sensibilisieren

Wenn es doch passiert?

- Ruhe bewahren (keine Spuren vernichten)
- Verseuchte Geräte isolieren
- Unterstützung durch Experten holen
- Vorfall melden



Zahlen oder nicht?

- Lösegeldzahlung ist keine Garantie
- Empfehlung: Backup zurückspielen
- Entschlüsselung ersetzt nicht Neuaufsetzen der betroffenen Systeme

Unsere Lösungen für Ihre Sicherheit als Start Up

Sichere Datenablage

Sichere Datenablage, Backups und Web-Infrastruktur für jedes Bedürfnis und jede KMU-Grösse.

- Managed Backup
- Swisscom Cloud (DCS)
- Microsoft Azure
- Microsoft 365 (One Drive)
- Webhosting (DSGVO-ready)
- Homepagetool (DSGVO-ready)

Sichere Netzwerke

Mit unseren Services bieten wir Ihnen einen integrierten Gesamtschutz für Ihr Firmennetzwerk.

- Smart ICT
- Business Network Solutions
- Managed LAN
- Managed Security
- Internet Guard
- Internet Security
- Centro Business Router

Maximaler Service und Support

Unsere IT-Experten kümmern sich proaktiv um Betrieb und Support und gewährleisten Ihre IT-Sicherheit.

- ICT-Assessment
- KMU Helpdesk
- Vor-Ort-Support durch regionale Swisscom Partner
- KMU Sicherheitsspezialisten (z.B. Whitehat Hacker)
- 24/7 Infrastruktur Überwachung

Wir sind für Sie da!

www.swisscom.com/kmu-sicherheit

E-Learning: Security-Schulung für Ihre Mitarbeitenden

In diesem kurzen Lernspiel von 15 Minuten zeigen wir Ihnen, wie Sie sich bereits dank einfachen Verhaltensregeln und Tipps besser schützen können. Link

Leitfaden IT-Sicherheit für Verantwortliche in KMU

Dieser Leitfaden zeigt den Verantwortlichen in KMU, worauf sie ihr Augenmerk legen und welche Fragen sie ihrem IT-Dienstleister unbedingt stellen sollten. Link

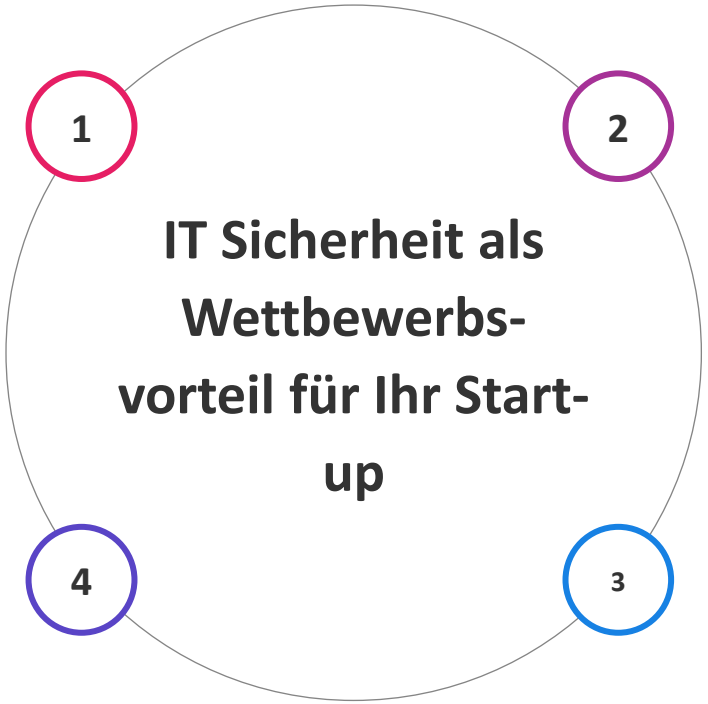
Kostenloser Security Check für Ihr KMU

Finden Sie jetzt heraus, wie gefährdet Ihr Unternehmen ist und machen Sie unseren kostenlosen Security-Check. Link

Das Wichtigste nochmal zusammengefasst

Geschäftsprozesse hängen zunehmend von IT ab

Viele KMU haben IT-Sicherheitslücken



Die Frage ist nicht ob sondern wann Ihr KMU betroffen ist

Präventive Massnahmen senken das Risiko und begrenzen den Schaden

Vielen Dank für Ihre Aufmerksamkeit