IT-Sicherheit

Cyberangriffe bedrohen den Wirtschaftsstandort Schweiz

Cyberkriminalität gehört mittlerweile zum Alltag in der Schweiz, und sie nimmt rasant zu. 2021 war mindestens jedes dritte Schweizer Unternehmen Opfer von Cyberkriminalität. Es ist ratsam, ein eigenes IT-Sicherheitskonzept zu erstellen, das die notwendigen Massnahmen zum Erreichen und Aufrechterhalten des gewünschten Sicherheitsniveaus beschreibt.

› Nicolas Mayencourt

«Unsere gesamte Produktion kam auf einen Schlag zum Erliegen», sagt Adrienne Seiler, CEO des Basler Pharma-Unternehmens «Health Science». «Sämtliche Bildschirme schwarz, Lieferaufträge waren keine mehr ersichtlich. Unsere Kunden konnten wir darüber nicht informieren, da wir auch keinen Zugang zu unseren Kundendaten hatten.» Die vollständig automatisierten und computergesteuerten Produktionsanlagen des Basler KMU standen wochenlang komplett still. Daraufhin wurde «Health Science» infolge der Produktionsausfälle mit Konventionalstrafen eingedeckt und ging Konkurs.

Immense Schadenssummen

Der Grund? Ransomware. Oder anders formuliert: Es hat nicht mehr gebraucht, als ein doppelter Mausklick auf den Anhang einer E-Mail, um ein prosperierendes Unternehmen in den wirtschaftlichen Ruin zu treiben. Zugegeben, das Schicksal der «Health Science» aus Basel ist rein fiktiv. Grund zum Jubeln gibt es dennoch wenig; solche Vorfälle von Cyberkriminalität sind unlängst Alltag in der Schweiz. Tendenz stark steigend.

Cyberattacken haben sowohl global als auch national seit der Pandemie drastisch zugenommen. Sicherheitsforscher von Check Point Research (CPR) registrierten 2021 weltweit einen Anstieg von über 50 Prozent auf Unternehmensnetze. In der Schweiz betrug die Zunahme 65 Prozent.

Die Angriffe aus dem Cyberraum werden immer professioneller und hochgradig automatisiert ausgeführt. Waren es 2015 noch rund 450 Milliarden Schweizer Franken, beliefen sich die globalen Schäden durch Cyberangriffe 2021 auf etwa fünf Billionen Schweizer Franken. Experten gehen davon aus, dass die globalen durch Cyberkriminalität verursachten Schäden 2025 bei über zehn Billionen Schweizer Franken liegen. Weitere Experten gehen von rund 23 Billionen Schweizer Franken bis 2027 aus.

Im Vergleich: Die globale Schadenssumme aller Naturkatastrophen betrug 2022 bislang circa 115 Milliarden Schweizer Franken. Organisierte Cyberkriminalität verursacht heute Schäden, welche die weltweiten Schadenssummen von Naturkatastrophen um mehr als das Fünfzigfache übersteigen.

kurz & bündig

- Waren es 2015 noch rund 450 Milliarden Schweizer Franken, beliefen sich die globalen Schäden durch Cyberangriffe 2021 auf etwa fünf Billionen Schweizer Franken.
- KMU sehen sich denselben professionellen und orchestrierten Angriffen aus dem Cyberbereich ausgesetzt wie Grosskonzerne.
- Ein Schutz vor Cyberangriffen ist auch mit wenig Ressourcen möglich. Beispielsweise, indem KMU eigene IT-Sicherheitskonzepte erstellen.

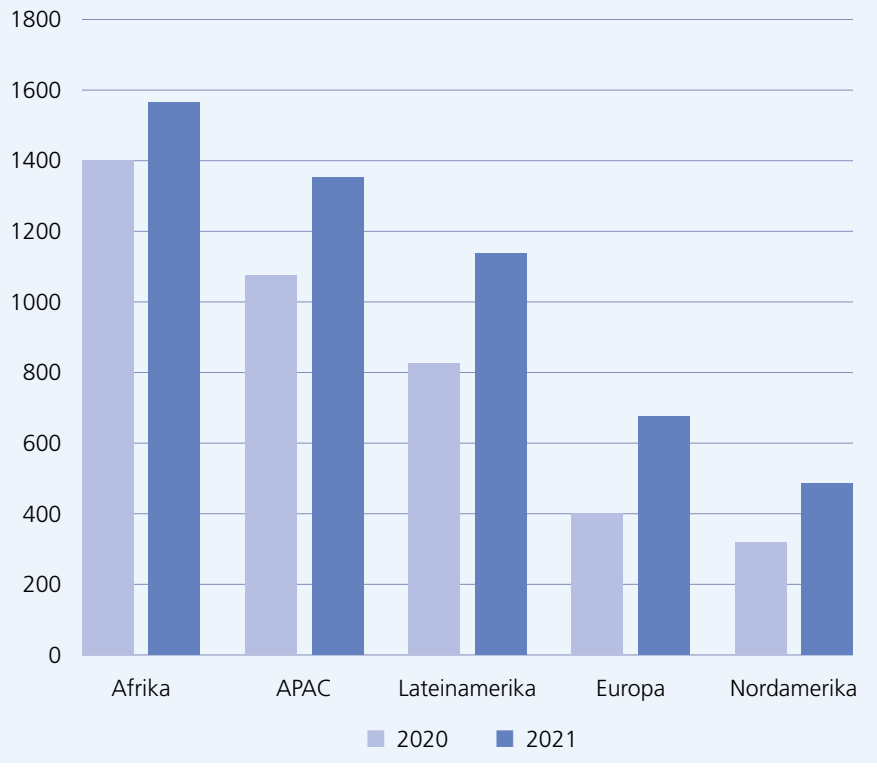
KMU besonders gefährdet

Der starke Anstieg von Cyberangriffen macht sich in der Schweiz deutlich bemerkbar. 2021 war mindestens jedes dritte Schweizer Unternehmen Opfer von Cyberkriminalität. Einzelne Firmen wurden in einem Jahr mehr als 20-Mal ange-

griffen. Das ist eine Verdoppelung zu 2020. Dabei muss beachtet werden, dass bereits 2020 ein weiteres negatives Rekordjahr für die Schweiz war, was die Summe der Angriffe aus dem Cyberraum anbelangt. Da nur rund ein Viertel aller Fälle gemeldet werden, handelt es sich bei den publizierten Zahlen lediglich um die Spitze des Eisberges.

Der durchschnittliche Schaden durch einen Cyberangriff für ein KMU beläuft sich auf mehrere hunderttausend Schweizer Franken. Schwere Angriffe wie auf die eingangs erwähnte «Health Science» liegen im hohen zweistelligen Millionenbereich. Was für die betroffenen Unternehmen mühsam bis existenzbedrohend ist, hat auch negative Auswirkungen auf den Wirtschaftsstandort Schweiz und gefährdet unsere gesamte Wettbewerbsfähigkeit. Das hängt mit der besonderen Bedeutung der KMU für die Schweiz zusammen.

Abb. 1: Rasante Zunahme von Cyberattacken



Bezahlen keine Option

Die rund 580 000 kleinen und mittleren Unternehmen bilden das Rückgrat der Schweizer Wirtschaft. Sie machen mehr als 99 Prozent aller Unternehmen aus, stellen über zwei Drittel aller Arbeitsplätze zur Verfügung und steuern über 50 Prozent der totalen Bruttowertschöpfung der Schweiz bei.

KMU haben im Vergleich zu Grosskonzernen weniger Ressourcen zur Verfügung, welche sie in ihre Cyber-Security-Infrastruktur investieren können. Eine unglückliche Konstellation, denn die KMU sehen sich denselben professionellen und orchestrierten Angriffen aus dem Cyberbereich ausgesetzt wie Grosskonzerne.

Mit dieser Dynamik hält das Verhalten der Unternehmen in der Schweiz nicht Schritt. Kommt es dann zum Schaden, sind die angegriffenen KMU oft bereit zu zahlen, denn ohne professionelle Vorbereitung wird die Schadensbehebung ein Vielfaches teurer und dauert zu lange. Da erscheint Zahlen als die beste Option unter allen schlechten. Aber genau das sollte nie der Fall sein. Geht nämlich ein kompromittiertes KMU auf die Forderungen der Kriminellen ein, erhält es das Label «Good Customer» und wird für Angreifer erst recht attraktiv. Durch Bezahlen unterstützen betroffene KMU ausserdem kriminelle Organisationen, die auch vor Terror nicht zurückschrecken.

Sinnliche Wahrnehmung fehlt

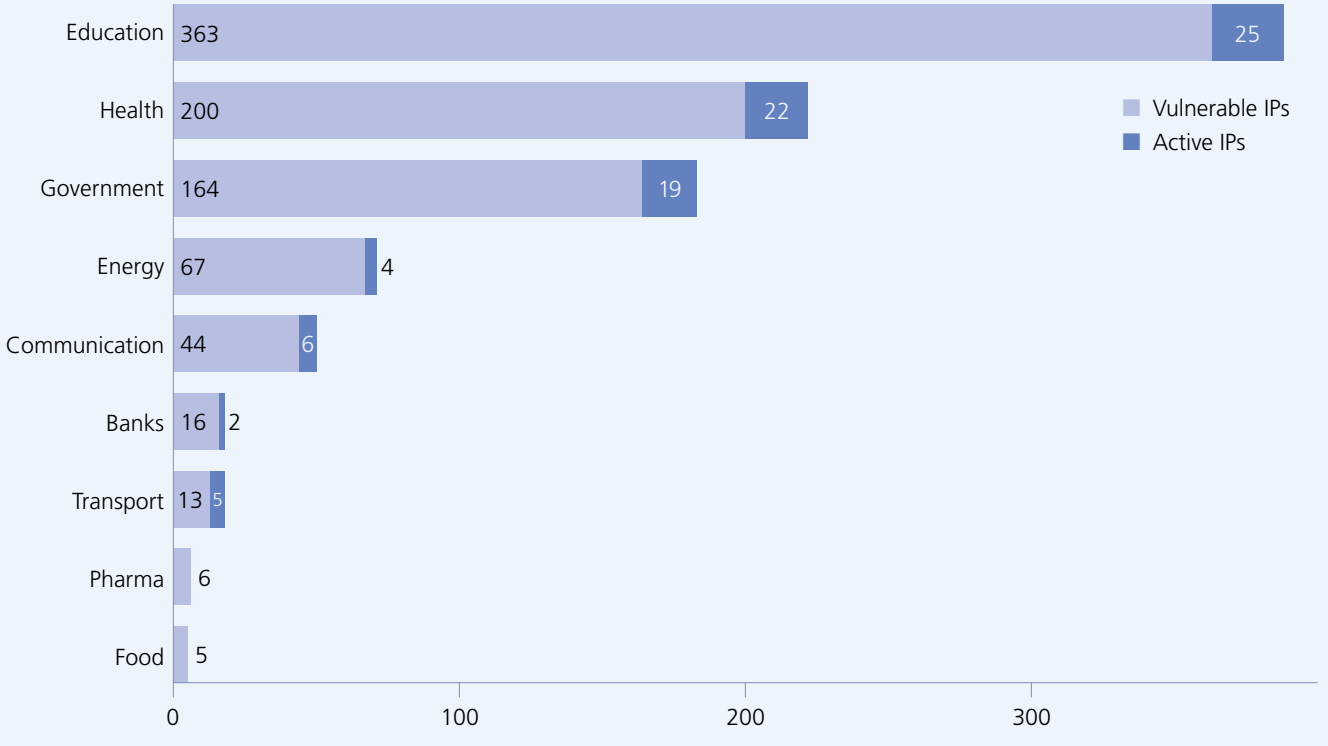
Viele KMU sehen sich nicht als potenzielle Ziele von Cyberangriffen oder verstehen das Schadensausmass nicht. Eine mögliche Erklärung für diese gefährliche Haltung ist die Tatsache, dass der Mensch keine sinnliche Wahrnehmung für den abstrakten Cyberraum hat.

Cyberraum und -kriminalität sind abstrakte, physisch nicht wahrnehmbare Gebilde und Ereignisse. Das hat zur Folge, dass die Gefahr und das Schadensausmass falsch eingeschätzt werden. Luft, Wasser, Erde und Weltall sind die uns umgebenden vier sinnlich wahrnehmbaren Dimensionen. Der Cyberraum ist die erste von Menschenhand geschaffene Dimension. Sie durchdringt alle anderen vier Dimensionen, bleibt aber ein abstraktes technologisches Konstrukt, welches der Mensch sinnlich nicht wahrnehmen kann.

Hinzu kommt, dass die digitale Vernetzung und Komplexität unserer globalisierten Welt ein gigantisches, nicht überschaubares Ausmass angenommen haben. Uns fehlt es an Verständnis für die technologische Hypervernetzung, Abhängigkeiten und Wechselwirkungen.

Auf den Punkt: Da wir den Cyberraum sinnlich nicht wahrnehmen können, wird die Tragweite des Schadensausmasses sehr oft falsch eingeschätzt, die eigene Verwundbarkeit unterschätzt und notwendige Abwehr-Massnahmen werden nicht umgesetzt.

Abb. 2: Anzahl Schweizer IPs und Domains mit bekannten, kritischen Verwundbarkeiten



Quelle: CyObs-Scan März 2022

Guter Schutz ist einfach

Die gute Nachricht ist: Ein Schutz vor Cyberangriffen ist auch mit wenig Ressourcen möglich. Beispielsweise, indem KMU eigene IT-Sicherheitskonzepte erstellen. Dieses beschreibt die notwendigen Massnahmen zum Erreichen und Aufrechterhalten des gewünschten Sicherheitsniveaus. Ausgangspunkt eines jeden IT-Sicherheitskonzepts sind Fragen nach dem Schutzbedürfnis. Was genau will das KMU schützen? Die Analyse des Risikos gibt Antwort auf die Frage, gegen welche Risiken das KMU geschützt werden soll.

Weiter muss geklärt werden, mit welchen Massnahmen der gewünschte Schutz erreicht werden kann. Am Schluss muss definiert werden, wie viel die Massnahmen kosten dürfen, respektive wie hoch der Schaden bei einem Angriff sein könnte. Massnahmen sollten prioritär dort umgesetzt werden, wo das Schadensausmass am grössten ist.

Fazit

Es gilt, sich mit seiner IT-Sicherheitsinfrastruktur auseinanderzusetzen. Angriffsflächen im Cyberraum können bereits mit wenig finanziellen Mitteln deutlich reduziert werden. Werden Software und Firewalls stets aktualisiert sowie konfiguriert, die Mitarbeitenden für das Thema sensibilisiert, kann ein zuverlässiger IT-Schutz mit wenig Budget in jedem Betrieb implementiert werden. «

Porträt

Nicolas Mayencourt
Founder and Global CEO, Dreamlab Technologies AG

Kontakt

nicolas.mayencourt@dreamlab.net
www.dreamlab.net