SPECIAL
SWISS CYBER SECURITY DAYS

KEYSTONE/ZÜRICH/MICHAEL WOLF

Schweizer KMU Sicherheit ist zahlbar

Cyberkriminalität ist eine Gefahr für die globale und nationale Stabilität.

KLAUS RIMNOV

Technologie verändert die uns vertraute Welt in beispielloser Geschwindigkeit. Seit Jahrzehnten erleben Gesellschaften und Volkswirtschaften weltweit einen radikalen Wandel, der durch digitale Transformation angetrieben wird. Die Digitalisierung wird so zu einer immer wichtigeren Voraussetzung für den Erfolg moderner Volkswirtschaften und beeinflusst das Leben der Menschen grundlegend. Die Digitalisierung macht die Welt zum Dorf; sie verlängert und multipliziert unsere Möglichkeiten gewaltig.

Das Fundament, der Cyberraum, ist jedoch ungenügend gesichert, während es Länder, Menschen und Organisationen dieser Welt milliardenfach miteinander verbindet. Die nationale Sicherheit, die Pfeiler unserer Demokratie oder unsere eigenen vier Wände: Cyber erfasst unser ganzes Leben. Rund um die Uhr, 365 Tage im Jahr. Unser Leben digital sicher zu gestalten, ist deshalb eine der dringlichsten und komplexesten Herausforderungen unserer Zeit. Kurz: Der digitale Raum ist unlängst eine kritische Infrastruktur, welche alles verbindet und weitgehend kontrolliert.

Parallel dazu ist die internationale Grosswetterlage angespannt wie seit langem nicht mehr. Unterschiedliche Wertesysteme und geopolitische Ansprüche konkurrieren mit Vehemenz um die Deutungshoheit. Der dabei zur Verfügung stehende Instrumentenkoffer an hybriden Beeinflussungs- und Angriffsmöglichkeiten wird durch neuartige technologische Möglichkeiten stark erhöht. Sei es im Bereich der Wirtschaftskriminalität, Desinformation, Spionage oder des Terrorismus: Cyberangriffe sind heute eine der grössten und akutesten Bedrohungen für die globale Stabilität. Zu dem Schluss kommt auch der Bericht «Global Cybersecurity Outlook 2023», der auf der Weltwirtschaftsforums-Jahrestagung 2023 in Davos vorgestellt wurde.

Die Schweiz und ihre KMU sind besonders betroffen

Es vergeht kein Tag, an dem Cyberkriminalität kein Thema wäre. Ob Angriffe auf KMU, Verwaltungen, Betreiber kritischer Infrastrukturen, Forschungseinrichtungen oder Privatpersonen: Die Häufigkeit von Cyberattacken ist in den letzten Jahren explodiert; das Schadensausmass erreicht besorgniserregende Dimensionen. Allein die Zunahme der Ransomware-Attacken betrug 2020 plus 435 Prozent im Vergleich zum Vorjahr. 2022 verursachte die weltweite Cyberkriminalität rund dreissigmal höhere Schäden als alle Naturkatastrophen im selben Jahr zusammengerechnet. Datenbasierte Annahmen gehen 2027 von einem Schadensausmass von rund 24 Billionen Franken aus. Das ist mehr als das Bruttoinlandprodukt der USA.

Die Schweiz ist als innovativstes Land der Welt in erheblichem Ausmass von Cyberkriminalität und -spionage betroffen. Das ist nicht nur eine grosse Gefahr für unsere Wettbewerbsfähigkeit; Angriffe von staatlichen und nicht staatlichen Hackergruppen bedrohen die nationale Sicherheit und die Grundzüge unserer Demokratie.

Falsche Einschätzung der eigenen Verwundbarkeit

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, die 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.

Swiss Cyber Security Days (SCSD)

Die SCSD ist die führende Dialog- und Know-how-Plattform der Schweiz im Bereich Cybersicherheit. Die SCSD überbrücken die Wissenslücke zwischen Technologie, Wirtschaft und Bevölkerung und bieten Politik, Verwaltung, Fachleuten sowie Anwendern Einblicke in aktuelle und zukünftige Bedrohungen und innovative Lösungen. Im Fokus stehen Politik, Wirtschaft, Bildung und Forschung. Allen beteiligten nationalen und internationalen Akteuren steht die Plattform offen für den Informationsaustausch, Inspiration und Treffen mit Politik, Verwaltung, Wirtschaft sowie führenden Cybersicherheitsexpertinnen und -Experten.

Die fünfte Ausgabe der SCSD findet am 20. und 21. Februar 2024 in Bern auf dem Bernexpo-Gelände statt.

435
Prozent
So stark war der Anstieg von Ransomware-Attacken 2020 gegenüber dem Vorjahr.

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. 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, für Abhängigkeiten und Wechselwirkungen.

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

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.

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 und die Mitarbeitenden kontinuierlich für das Thema sensibilisiert, kann ein zuverlässiger IT-Schutz mit wenig Budget in jedem Betrieb implementiert werden.