Zeitschrift: Schweizer Soldat : die führende Militärzeitschrift der Schweiz
Herausgeber: Verlagsgenossenschaft Schweizer Soldat
Band: 97 (2022)
Heft: 7-8

Artikel: Wirtschaftsschutz für KMU
Autor: Eckert, Chris
DOI: https://doi.org/10.5169/seals-1006055

Wirtschaftsschutz für KMU

Wirtschaftskriminalität, Cyberattacken und Industriespionage: In der Schweizer Wirtschaft werden dadurch jährlich Schäden in Milliardenhöhe verursacht. Straftaten, gezielte Spionage, Fehlverhalten oder fehlende Awareness bedrohen Unternehmen wie Organisationen zunehmend oder stürzen sie in tiefe Krisen, leider geht's oft auch ums finanzielle Überleben oder um die Reputation. Die Erkennung von Gefahren, Angriffsmethoden und der Einsatz von Gegenmassnahmen verlangt nach umfassendem Unternehmensschutz und Integraler Sicherheit.

Chris Eckert, Swiss Business Protection AG.

Autor

Chris Eckert ist Founding Partner der Swiss Business Protection AG. Er verfügt über mehr als 30 Jahre kriminalistische Erfahrung, erworben bei der Kantonspolizei Zürich sowie der Bundeskriminalpolizei. Seit über 12 Jahren ist er selbständig. Als Kriminalist, CSO / CISO a.i. in den Bereichen Informationssicherheit, Forensik und Kriminalprävention stellt er seine Erfahrung konzeptionell, strategisch und operativ zur Verfügung. Daneben ist er als Dozent in den Fachbereichen Social Engineering, Informationssicherheit und Wirtschaftsschutz tätig.

Egal in welcher Branche man tätig ist oder wie gross das Unternehmen ist: Know-how, Arbeitsplatzsicherheit, Leistungswille, Qualität, Produkte und Innovation sind Eigenschaften, die unsere Unternehmen und Institutionen auszeichnen. Bestechende Geschäftsmodelle, erprobte Prozesse, geheime Patente oder nachhaltige Technologien ziehen immer Neugier auf sich.

Leider sind nicht nur ihre Kunden die Interessierten. Profiteure, Kriminelle, Hacker und Konkurrenten im In- und Ausland sind automatisch Akteure. Keine Branche, kein Unternehmen ist gefeit vor Kriminalität, Sabotage und Spionageangriffen.

Sie finden statt u.a. mittels Cyberattacken, vorgelagert meist durch Human Hacking; und selbst durch Täter von innen, vorsätzlich oder unbewusst. Gefährdet sind Produktionsstätten, Verwaltungseinheiten, Know-how, Informationen und Mitarbeiter, ob im Büro, zu Hause oder auf Geschäftsreise.

Die Angreifer brechen kaum noch brachial durch das Kellerfenster ein. Viel erfolgversprechender und günstiger sind konventionelle und digitale Angriffe mittels Einsatzes von günstig verfügbarer Elektronik, dem Aneignen von kaum ge-

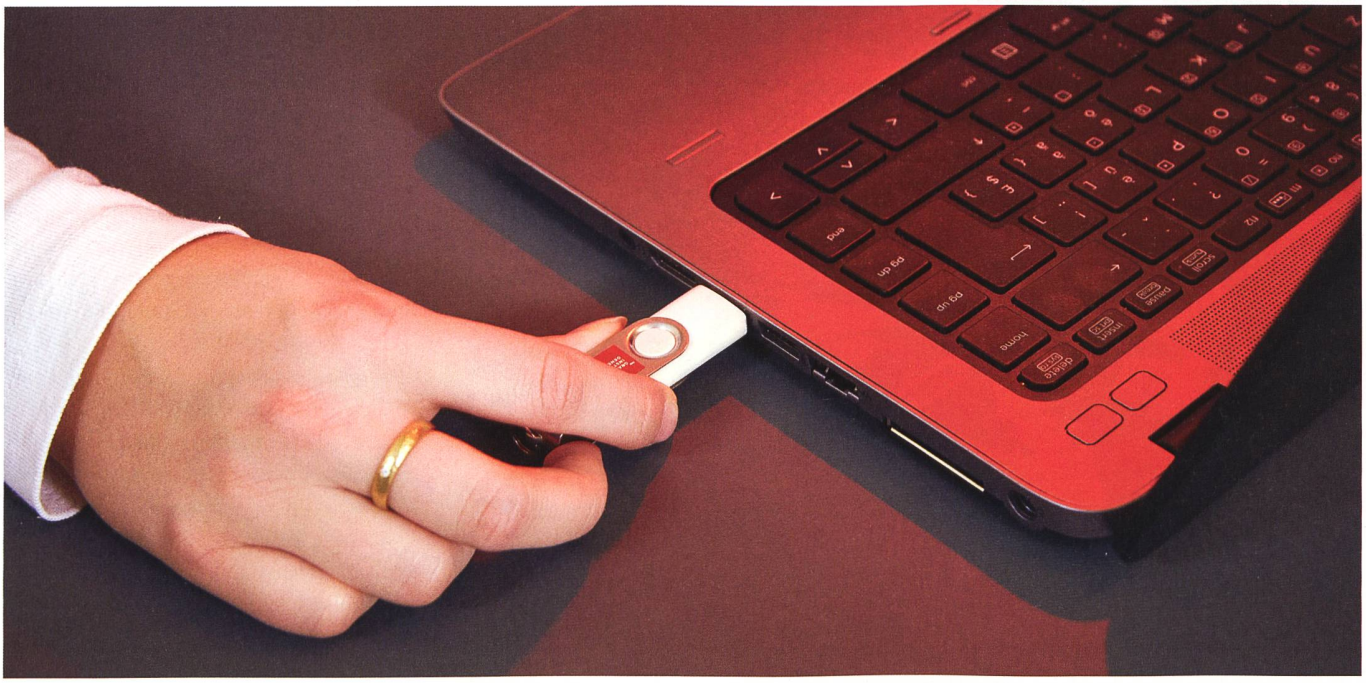

Bild: VBS

Die Angreifer brechen kaum noch brachial durch das Kellerfenster ein. Viel erfolgversprechender und günstiger sind konventionelle und digitale Angriffe mittels Einsatzes von günstig verfügbarer Elektronik.

schützten Informationen durch Social Engineering und das Eindringen in ungenügend abgesicherte IT-Infrastruktur. Die grösste Schwachstelle ist allerdings nach wie vor der Risikofaktor Mensch.

Integrale Sicherheit

Fortwährendes Ziel jeder Unternehmensführung oder Organisationsleitung sollte sein, die eigenen Mitarbeitenden zu schützen, eine reibungslose Produktion zu gewährleisten und die Verfügbarkeit von Information und Innovation zu sichern. Der Schutz der zentralen Unternehmenswerte – quasi der unternehmerischen Kronjuwelen – steht im Zentrum.

Präventiver Unternehmensschutz

Der beste und günstigste Schutz jedes Unternehmens ist gewährleistet, wenn die negativen Einwirkungen oder Angriffe verhindert werden können. Idealerweise werden mit präventiven Massnahmen Risikobeurteilungen durchgeführt, Sicherheitsstrategien entwickelt und Sensibilisierungskampagnen für alle Mitarbeitenden implementiert. Regelmässige Checks, z.B. mittels Audits oder Red-Teaming-Angriffen runden die Präventivmassnahmen ab.

Basierend auf den drei Säulen Infrastruktur, Mensch und Organisation sowie Information gilt es, präventive Überlegungen anzustellen, Früherkennung zu betreiben und gezielte Abwehr- sowie Gegenmassnahmen z.B. für folgende Themen umzusetzen:

- Standortsicherheit inkl. Lauschabwehr (Technical Surveillance Counter Measures)
- Risikofaktor Mensch
- Notfall- und Krisenmanagement
- Cyber Security und genereller Informations- und Datenschutz.

Ereignisbewältigung im Notfall

Tritt trotz Prävention ein Schadensereignis ein, steht die rasche und zielgerichtete Ereignisbewältigung im Vordergrund. Der Notfall erfordert entschlossenes und koordiniertes Handeln unterschiedlicher Spezialisten, vergleichbar wie bei der Feuerwehr. Idealerweise steht ihnen intern eine Anlaufstelle zur Verfügung. In der Praxis sind KMU im Bereich der integralen Unternehmenssicherheit noch nicht so breit aufgestellt, weshalb schweizweit das Kompetenzzentrum Wirtschaftsschutz (www.swissbp.ch) mit breiter operativer Erfahrung und interdisziplinären Kompetenzen zu Rate gezogen werden kann.

KMU's werden präventiv und im Ereignisfall rasch, unbürokratisch und wirksam unterstützt. Der Support umfasst die präventive und reaktive Abwehr aktueller und künftiger Gefahren in den Bereichen Cyber Crime, Wirtschaftskriminalität und Industriespionage.

Praxisorientierte Weiterbildung

Zugeschnitten auf den umfassenden Unternehmensschutz für KMU in der Schweiz wurde ein neuer Lehrgang erschaffen. Der CAS «Business Protection» an der Hochschule für Wirtschaft HWZ in Zürich startet am 9. März 2023 und dauert berufsbegleitend 18 Tage bis am 2. September 23.

Kolumne

Fokus CdA

Der Krieg gegen die Ukraine zeigt, dass sich auch in Europa konventionelle Kriege nicht ausschliessen lassen. Neben neuartigen Mitteln wie Cyberangriffen und Drohnen werden nach wie vor auch Kampfflugzeuge, Panzer und Artillerie eingesetzt. Bedrohungen verstehen wir als Produkte aus Potential und Absicht. Potentiale werden über Jahre hinweg aufgebaut, Absichten jedoch können sich rasch ändern.

Die Armee hat detailliert aufgezeigt, wie sie den heutigen und künftigen Bedrohungen begegnen will. Die dazugehörigen Konzepte wurden in drei Grundlagenberichten veröffentlicht: Luftverteidigung der Zukunft (2017), Zukunft der Bodentruppen (2019) und Gesamtkonzeption Cyber (2022). Aus aktuellem Anlass wurden diese in der Broschüre «Konzeption Zukunft der Armee» zusammengefasst, zu finden auf der Homepage der Gruppe Verteidigung – die Lektüre lohnt sich.

Ein detaillierter Plan für die Umsetzung dieser Konzepte und den Aufbau der Fähigkeiten über die nächsten Jahre liegt vor.

Bundesrat und Parlament haben reagiert und entschieden, dass die Armee für die Umsetzung mehr finanzielle Mittel erhalten soll. Konkret soll das Armeebudget ab 2023 bis 2030 schrittweise von heute rund 0.7 auf mindestens 1% des Bruttoinlandproduktes erhöht werden. Damit lässt sich unser Plan rascher umsetzen und die Modernisierung unserer Armee wird insgesamt beschleunigt, weil Ausrüstungslücken zügiger geschlossen sowie veraltete Systeme schneller ersetzt werden.

Damit die Schweiz auch in Zukunft auf alle Bedrohungen reagieren kann, muss sie über eine robust aufgestellte Armee verfügen. Diese muss über die gesamte Breite der Fähigkeiten verfügen. Mit den vorliegenden Konzepten sind wir auf dem richtigen Weg. Damit wir auch 2030 noch verteidigen können.

Korpskommandant
Thomas Süssli
Chef der Armee