CYBER RESILIENCE – STÄRKEN SIE IHRE ABWEHRKRÄFTE

Leider sind immer mehr Schweizer Unternehmen im Fokus von gezielten Cyberattacken. Deshalb ist es wichtig, die Cyber Resilience auf allen Unternehmensebenen zu stärken und sich nicht nur auf immer höhere Sicherheitsmauern zu verlassen.

→ VON FRANCO CERMINARA

Was für die Grippeprävention gilt, gilt erst recht für die Cyber Security: Die Widerstandsfähigkeit – oder besser Cyber Resilience – gegen Viren und Co. muss gestärkt werden. Denn mit der rasant steigenden Digitalisierung, wächst auch das Risiko von Cyberattacken. Bedrohlicher als die schiere Menge der Angriffe ist ihre zunehmende Qualität, Effizienz und Professionalität. Die Cyberattacken im vergangenen Jahr auf diverse Schweizer Unternehmen sind beste Beispiele dafür.

Gleichzeitig dauert es nicht selten Wochen, Monate oder gar Jahre, bis ein erfolgreicher Angriff erkannt wird. Cyber Security ist deshalb ein enorm wichtiges Thema für den Geschäftserfolg eines Unternehmens. Neue Technologien wie die Cloud, die zunehmende Mobilität, die Virtualisierung, das «Internet der Dinge», Blockchain etc. sorgen aber für immer neue Herausforderungen und Bedrohungen im Security-Ökosystem. Darüber hinaus gilt es, zahlreiche regulatorische Vorgaben zu erfüllen.

Vor diesem Hintergrund ist es unerlässlich, mehr Ressourcen in die Erkennung, Reaktion und Wiederherstellbarkeit zu investieren.

Konventionelle Abwehrmassnahmen bleiben natürlich ein unerlässlicher Bestandteil der modernen Cyber Security. Sie sind aber keine hinreichenden Massnahmen, um die Cyber Resilience allein sicherzustellen. Dazu ist der Auf- und Ausbau zielgerichteter Massnahmen zur Stärkung der Widerstandskraft gegen Cyberattacken unerlässlich. Und: Die Verantwortung dabei obliegt dem Management.

RISIKOMANAGEMENT GEHÖRT IN DIE CHEFETAGE

Cyberrisiken haben sich in den letzten Jahren zu den grössten operativen Risiken für Unternehmen entwickelt. Obwohl das Risikomanagement nicht explizit als Aufgabe des Verwaltungsrates im OR genannt wird, ist dieser aufgrund der nicht delegierbaren gesetzlichen Aufgaben wie Rechnungslegung, Finanzkontrolle, Überwachung etc. verantwortlich. Seit der Aktienrechtsrevision trägt der Verwaltungsrat zudem die Verantwortung, dass ein internes Kontrollsystem existiert. Die Empfehlungen des Swiss Code gehen mit der weiter gefassten Definition des IKS noch stärker in Richtung umfassendes Risikomanagement. Es betrachtet sowohl finanzielle und operative (beispielsweise Cyberrisiken) als auch strategische und marktspezifische Risiken.

ABWEHRKRAFT IN NEUN SCHRITTEN STÄRKEN

Es gilt somit, die unternehmenskritischen Elemente der IT-Infrastruktur vor Ausfall, Fehlfunktionalität oder Manipulation zu schützen. Klassische IT-Sicherheit ist dabei aber nur ein Teil und umfasst lediglich den Schutz der Systeme. Dieser ist zweifelsohne notwendig, aber heutzutage nicht mehr ausreichend. Entscheidend ist die Widerstandsfähigkeit des gesamten Unternehmens mitsamt Prozessen, Mitarbeitenden und IT-Infrastruktur, um auf interne und externe Risiken vorbereitet zu sein und im Ereignisfall schnell reagieren zu können. Nachfolgend die wichtigsten Grundsätze:

- Cyber Resilience muss auf oberster Unternehmensebene wahrgenommen werden.
- Verantwortlichkeiten und Zuständigkeiten müssen klar und schriftlich geregelt sein.
- Die Kompetenz und das Verständnis für Cyber Resilience muss im ganzen Unternehmen aufgebaut werden.
- Cyber Resilience muss in die unternehmensweite Risikobetrachtung einbezogen werden.
- Die Risikostrategie (Risikoappetit) muss für das Unternehmen verbindlich festgelegt werden.
- Die Risiken müssen nachvollziehbar bewertet und dokumentiert werden.
- Es gilt, geeignete Cyber-Resilience-Massnahmen aufzubauen und die Umsetzung zu kontrollieren.
- Drittparteien müssen in die Risikobetrachtung einbezogen werden, Stichwort «Supply Chain Risk Management».

Zum Autor

Franco Cerminara:
Chief Consulting Officer

Zum Unternehmen:
Die InfoGuard AG ist spezialisiert auf umfassende Cyber Security. Zu den Kompetenzen zählen massgeschneiderte Dienstleistungen im Bereich der Sicherheitsberatung und Security Audits sowie in der Architektur und Integration führender Netzwerk- und Security-Lösungen. Cloud-, Managed- und Cyber-Defence-Services erbringt der Schweizer Cyber-Security-Experte aus dem ISO-27001-zertifizierten InfoGuard Cyber Defence Center in der Schweiz. InfoGuard hat ihren Hauptsitz in Baar/Zug und eine Niederlassung in Bern. Ihre über 150 Sicherheitsexperten sorgen tagtäglich für die Cyber Security bei über 300 Kunden in der Schweiz.

Mehr Informationen:
www.infoguard.ch

InfoGuard
SWISS CYBER SECURITY

Bild: 123RF.com /Sergey Nivens

Cyber Resilience braucht mehr als hohe Sicherheitsmauern

- Die Cyber Resilience muss regelmässig überprüft werden.

SICHERHEITSMAUERN ALLEIN REICHEN NICHT AUS

Unternehmen sind also gut beraten, sich konsequent mit aktuellen und neuen Risiken auseinanderzusetzen und der Informationssicherheit das nötige Gewicht beizumessen. Die Geschäftsleitung steuert dabei die Umsetzung von Massnahmen zur Verbesserung der Cyber Resilience und sorgt dafür, dass diese im gesamten Unternehmen aufeinander abgestimmt sind. Die Cyber-Security-Strategie bildet dabei den bereichsübergreifenden, strategischen Rahmen. Ein systematischer Sicherheitsansatz ist das A und O erfolgreicher Cyber Security. Dabei müssen sowohl das Risikomanagement, der Schutz der Informationen, die Erkennung und Reaktion auf Sicherheitsvorkommnisse als auch die Wiederherstellung und Optimierung berücksichtigt werden. Internationale Standards wie ISO 27001 oder das NIST Cyber Security Framework bieten dazu anerkannte Modelle für die Errichtung, Umsetzung, Überprüfung und kontinuierliche Verbesserung der eigenen Cyber Resilience.

Cyber Resilience ist weit mehr als eine hohe Sicherheitsmauer. Der Architektur des Unternehmensnetzwerks kommt dabei eine enorme Bedeutung zu. Einer der wichtigsten Aspekte neben der System-Redundanz stellt dabei die optimale Segmentierung der Netzwerke, Betriebsfunktionen, Einzelelemente und Überwachung der so geschaffenen Zonenübergänge dar, welche die Business-Prozesse optimal abdeckt und unterstützt. Zudem geht der Trend klar in Richtung einer intensiveren Überwachung von Sicherheitssystemen und der Erkennung von Vorfällen, wie es auch das NIST Cyber Security Framework empfiehlt. Ein simulierter Cyberangriff kann dabei wertvolle Erkenntnisse liefern. Es braucht aber auch neue Sicherheitsansätze, bei denen die Detektion im Vordergrund steht und die Reaktion auf Angriffe ein wesentlicher Bestandteil der IT-Prozesse ist.

Um eine systemische Cyber Resilience zu gewährleisten, müssen auch Drittparteien in die Cyberrisikobetrachtung einbezogen werden, soweit dies relevant und angemessen ist. Das Drittparteienmanagement ist dabei ein wichtiger Schritt und befasst sich mit der Identifizierung sowie der Verwaltung von Cyberrisiken zu externen Drittparteien (d. h. Partnern, Dienstleistern, Lieferanten von Hard- sowie Software, Outsourcing-Anbietern und Cloud-Service-Anbietern etc.).

CYBER RESILIENCE IST EIN KONTINUIERLICHER PROZESS

Da sich die Risikosituation stetig ändert, ist Cyber Resilience keine einmalige Angelegenheit. Unternehmen müssen die aktuelle Bedrohungslage beobachten und ihr Sicherheitsdispositiv optimieren sowie kontinuierlich verbessern. Wichtige Elemente einer Security Governance beinhalten deshalb Risk Assessments, organisatorische Audits, System Security Testing, Penetration Tests und Vulnerability Scans. Unternehmen sollten zudem jederzeit in der Lage sein, Sicherheitsvorkommnisse zu erkennen, schnell darauf zu reagieren und die Auswirkungen auf ein Minimum zu reduzieren. Dies hilft schlussendlich, die Cyber Resilience zu stärken sowie den Schutz der Unternehmenswerte – auch im Zeitalter der zunehmenden Digitalisierung – zielgerichtet und nachhaltig zu verbessern. ←

Dieser Beitrag wurde von der **InfoGuard AG** zur Verfügung gestellt und stellt die Sicht des Unternehmens dar. Computerworld übernimmt für dessen Inhalt keine Verantwortung.