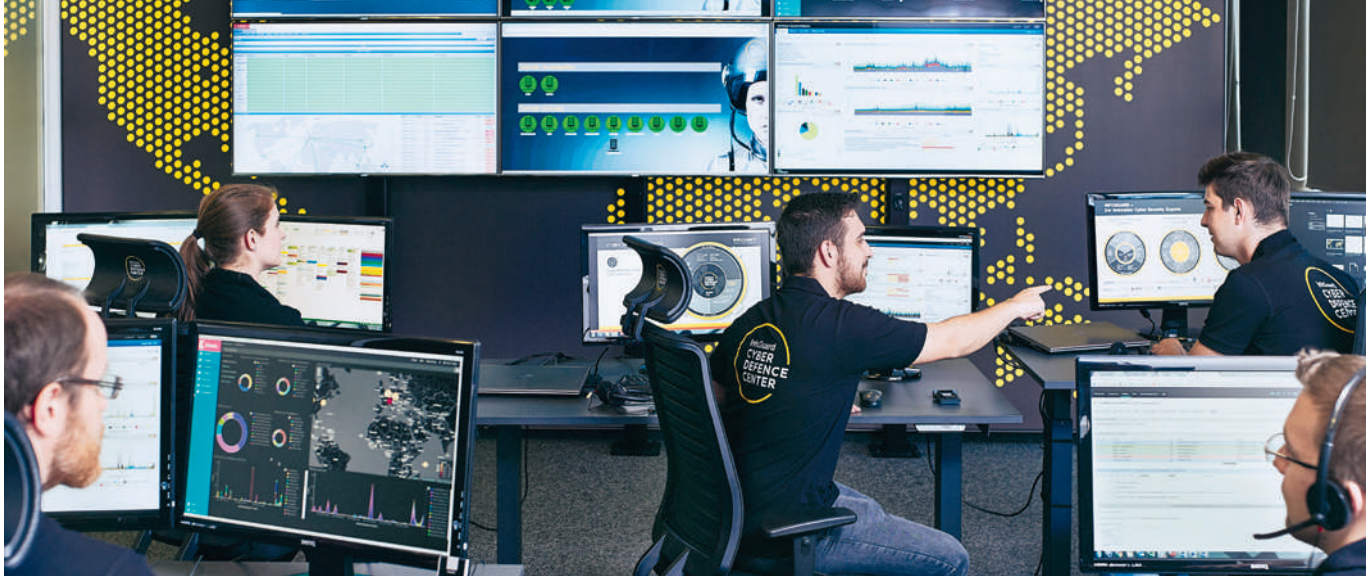

CYBER RESILIENCE STÄRKT DIE ABWEHRKRÄFTE

2017 ging als «Das Jahr der DDoS-Angriffe» in die Annalen der Cyber Security-Geschichte ein. Erst vor ein paar Tagen sorgte ein gigantischer Denial-of-Service-Angriff wieder für mächtig Gesprächsstoff. Und so müssen Behörden und Unternehmen in der Lage sein, sich mittels Cyber Resilience kontinuierlich den Herausforderungen neuer Cyberattacken zu stellen. Denn die Anzahl der Cyber-Angriffsversuche steigt täglich. Dabei gerät auch immer mehr die Schweiz in den Fokus von Angreifern.

von Franco Cerminara

Noch erinnern wir uns nur zu gut daran, wie vor knapp zwei Jahren zahlreiche Schweizer Webshops lahmgelegt wurden. Der Grund dafür war simpel, aber effektiv: Hinterhältige DDoS-Angriffe, welche die Verfügbarkeit der Online-Services stunden-, ja sogar tagelang ausfallen liessen. Wer jetzt denkt, alles sei inzwischen unter Kontrolle, der irrt sich. Erst vor ein paar Tagen sorgte ein gigantischer Denial-of-Service-Angriff wieder für mächtig Gesprächsstoff. Dies zeigt eindrücklich, dass das Internet zu einem digitalen Schlachtfeld geworden ist. Ein Schlachtfeld, auf dem immer professioneller Daten gestohlen werden. Inzwischen entstehen täglich fast 400'000 neue Schadprogramme in teilweise geringer Variation – das sind beinahe fünf pro Sekunde! Und so gilt es, die eigenen Abwehrkräfte gegen Cyberattacken gezielt zu stärken.

STÄRKEN SIE IHRE ABWEHR GEGEN CYBERATTACKEN

Cyber Resilience bedeutet aber nicht, Risiken gänzlich auszuschliessen. Das ist heute unmöglich. Auch gesundheitlich kann man nur schwer verhindern, sich keine Grippeviren einzufangen, aber man kann das Ausmass der Grippe eindämmen. So ist auch der Auf- und Ausbau zielgerichteter Massnahmen zur Stärkung der Widerstandskraft gegen Cyberattacken (Cyber Resilience) unabdingbar. Den Fokus nur auf präventive Massnahmen zu legen, wäre zu kurz gegriffen. Ein systematischer Sicherheitsansatz, der sowohl das Risikomanagement, den Schutz der Informationen, die Erkennung und Reaktion auf Sicherheitsvorkommnisse sowie die Wiederherstellung und Optimierung berücksichtigt, ist heute das A und O einer erfolgreichen Cyber Security.

Behörden und Unternehmen sind gut beraten, sich konsequent mit aktuellen und neuen Risiken auseinander zu setzen und der Informationssicherheit das nötige Gewicht beizumessen. Die Cyber Security-Strategie bildet dabei den bereichsübergreifenden, strategischen Rahmen. Internationale Standards wie ISO 27001 oder das NIST Cyber Security Framework bieten dazu ein anerkanntes Modell für die Errichtung, Umsetzung, Überprüfung und kontinuierlichen Verbesserung der eigenen Cyber Security. Gleichzeitig werden die drei Dimensionen Technologie, Prozesse und nicht zuletzt der Mensch beleuchtet. Es hat sich gezeigt, dass gerade das systematische Vorgehen einen erheblichen Mehrwert bietet. Dazu zählen u.a. ein gezieltes Risikomanagement, der Aufbau eines angemessenen Sicherheitskonzeptes und einer geeigneten Sicherheitsarchitektur. Ausserdem noch die Definition von Sicherheitsrichtlinien und -prozessen sowie der Aufbau einer Notfallplanung und die Sicherheitssensibilisierung der Mitarbeitenden.

(ICT-)SICHERHEITSMAUERN REICHEN NICHT AUS

Unternehmen können und müssen sich auf Cyberattacken vorbereiten – dies gilt aber auch für Behörden auf nationaler, kantonaler oder kommunaler Ebene. Der Schutz von Netzwerken und Unternehmenswerten wird aber immer schwieriger; insbesondere vor anspruchsvollen Attacken, die durch herkömmliche Sicherheitssysteme nicht mehr erkannt werden. Daher muss man heutzutage davon ausgehen,

dass die eigenen Systeme bereits infiltriert sind – oder dass man nächstens Opfer einer Attacke werden wird.

Es braucht ein Umdenken in der Cyber Security. Man darf sich nicht mehr nur auf (immer) höhere ICT-Sicherheitsmauern verlassen. 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 welchen die Detektion im Vordergrund steht und die Reaktion auf Angriffe ein wesentlicher Bestandteil der IT-Prozesse ist. Dazu braucht es ein Cyber Defence Center (CDC). So lässt sich die Prävention zielgerichtet und kontinuierlich verbessern.

CYBER DEFENCE CENTER ALS DREH- UND ANGELPUNKT

In einem solchen Center laufen alle Fäden zur Erkennung, Analyse und Abwehr von Cyberangriffen zusammen. Cyber Defence ist eine anspruchsvolle Arbeit – und geht weit über Netzwerk-Monitoring hinaus. Da Attacken rund um die Uhr erfolgen, muss ein CDC sieben Tage, während 24 Stunden, funktionieren. Selbstlernende Systeme und Lösungen auf Basis künstlicher Intelligenz entlasten die Spezialisten bei der Erkennung von Angriffen. Diese gilt es zu nutzen – gerade weil in diesem Bereich auch weitere Fortschritte zu erwarten sind, die ein CDC noch effizienter machen. Die Risikosituation und Bedrohungslage ändert sich aber stetig. Aus diesem Grund sind regelmässige Überprüfungen des Sicherheitsdispositivs nach neuen Bedrohungen und Schwachstellen unerlässlich. Zur Kontrolle sollten daher regelmässig System Audits, Penetration Tests und Vulnerability Scans durchgeführt werden. Nur so kann die Sicherheit an die aktuelle Risikosituation angepasst und optimiert werden.

WEITERE INFORMATIONEN

Franco Cerminara
Chief Consulting Officer
InfoGuard AG
Lindenstrasse 10
6340 Baar