CYBER RESILIENCE STÄRKT DIE ABWEHRKRÄFTE

So wie sich unser Immunsystem alle Jahre wieder gegen die Grippeviren zur Wehr setzt, so müssen auch Energiedienstleister und Betreiber kritischer Infrastrukturen in der Lage sein, sich mittels Cyber Resilience kontinuierlich den Herausforderungen neuer Cyberattacken zu stellen. Denn die Anzahl der Cyber-Angriffsversuche wie «Shadow Brokers», «Petya / NotPetya / Nyetya / Goldeneye», «WannaCry», «Cloudbleed» sowie Hacker- und DDoS-Attacken steigt täglich. Dabei geraten auch immer mehr Schweizer Unternehmen in den Fokus von Angreifern.

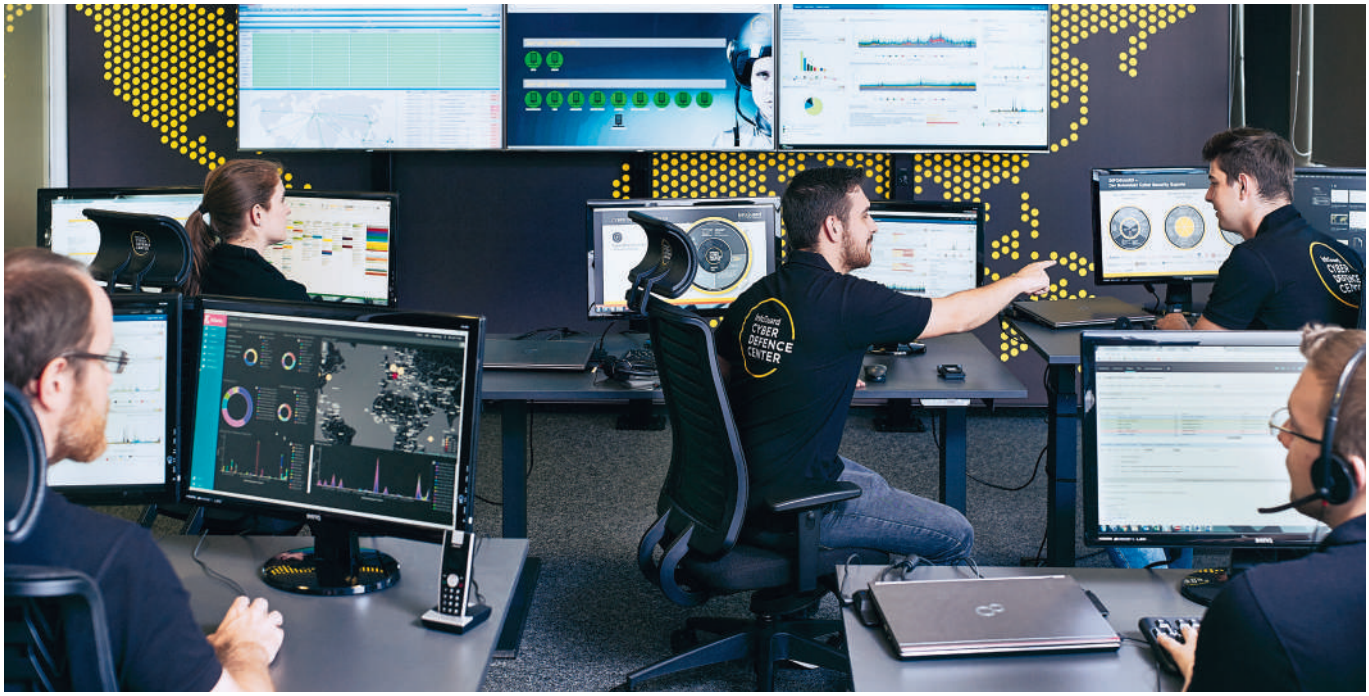
von Markus Limacher, Principal Cyber Security Consultant

Cyber Resilience bedeutet nicht, Risiken für das Unternehmen 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.

NUR DIE SPITZE DES EISBERGS

Gerade Betreiber von kritischen Infrastrukturen, egal ob in den Bereichen Energie, Wasser oder Verkehr, sind auf funktionierende Systeme der IT und der OT angewiesen. Dabei darf man sich aber nicht nur auf die traditionelle IT-Landschaft konzentrieren. Denn gerade ICS- und SCADA-Systeme benötigen durch die Zunahme der Cyberbedrohungen und Vernetzung in der Wertschöpfungskette einen umfassenden Schutz. Hackerangriffe sind nicht nur ärgerlich, sondern können auch enorme Kosten und einen riesigen Imageschaden verursachen.

Aktuelle Daten belegen, dass immer mehr Schweizer Unternehmen ins Visier der vermutlich russischen APT-Gruppe Energetic Bear (aka. Dragonfly) geraten. Diese Gruppe greift seit 2010 vornehmlich Industrieunternehmen und (Energie-)Versorger an. Die zwei bekanntesten Angriffe, welche dieser Gruppe zugeschrieben werden, führten 2015 und 2016 zu einem grossräumigen Ausfall der Energieversorgung in der Ukraine. Die Angreifer verwendeten dabei komplexe Malware, die gezielt für Angriffe auf OPC Server und dahinterliegende SCADA-Netze entwickelt wurde. Darüber hinaus wurden auch gezielt vertrauliche Dokumente und E-Mails gesammelt. Die Ex-Filtration der Daten erfolgte gut getarnt über Plattformen wie Dropbox oder z. B. DNS. Das Internet ist ein digitales Schlachtfeld. Ein Schlachtfeld, auf dem immer professioneller politische und wirtschaftliche Schlachten ausgetragen und Daten ge-



stohlen werden. Inzwischen entstehen täglich fast 400'000 neue Schadprogramme – in teilweise geringer Variation – das sind beinahe fünf pro Sekunde!

CYBER SECURITY BRAUCHT SYSTEM

Diese Entwicklung macht klar: Betreiber kritischer Infrastrukturen 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, 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 insbesondere auch für Betreiber kritischer Infrastrukturen. Der Schutz von Netzwerken und Unternehmenswerten wird aber immer schwieriger; insbesondere vor anspruchsvollen Attacken, die durch herkömmliche Sicherheitssysteme oft nicht mehr erkannt werden. Daher müssen Unternehmen heutzutage davon ausgehen, dass ihre Systeme bereits infiltriert sind – oder dass sie nächstens Opfer einer Attacke werden.

Unternehmen müssen hinsichtlich ihrer Cyber Security umdenken und dürfen sich nicht nur auf (immer) höhere ICT-Sicherheitsmauern verlassen. Der Architektur von ICS- und SCADA-Systemen innerhalb 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.

CYBER DEFENCE AUS DER SCHWEIZ

Das Schweizer Unternehmen InfoGuard mit Sitz in Zug und Bern hat sich auf Cyber Security und Cyber Defence spezialisiert. Im Mai hat InfoGuard ein neues, 250m² grosses Cyber Defence Center eröffnet. Die Services umfassen u. a. Security Information & Event Management (SIEM), Vulnerability Management, Breach Detection sowie Cyber Threat Intelligence, APT Hunting, Incident Response und Forensik. Das neue CDC verfügt über ein mehrstufiges, physisches Sicherheitskonzept, wobei die Sicherheitssysteme rund um die Uhr, während 365 Tagen im Jahr, überwacht werden.

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. Und 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. Es empfiehlt sich bewährte Best-Practice-Ansätze der Cyber Security auch auf die ICS- und SCADA-Netze zu adaptieren.

WEITERE INFORMATIONEN

Markus Limacher
Principal Cyber Security Consultant
InfoGuard AG
Lindenstrasse 10
6340 Baar