Cyber Defence als Antwort auf Cyberangriffe

Kaum ein Tag vergeht, an dem nicht über Cyberangriffe berichtet wird. Angriffe nehmen weltweit stark zu, auch in der Schweiz und besonders auf KMU. Neue Ansätze sind gefragt, die jedoch nicht nur die Schutzmauern erhöhen, sondern Angriffe mittels Cyber Defence auch effektiv abwehren – von 24/7-Monitoring über die proaktive Suche nach Anomalien bis hin zur aktiven Bewältigung von Cyberangriffen und forensischen Analysen. Die Lösung: ein Cyber Defence Center.

Während Cyberrisiken unter anderem durch die Digitalisierung und globale Vernetzung stetig zunehmen, agieren auch Cyberkriminelle immer professioneller – nicht nur hinsichtlich Angriffsmethoden, sondern auch ihres profitablen Unternehmertums. Wenig verwunderlich reichen hohe Schutzmauern allein, sprich präventive Massnahmen, längst nicht mehr aus. Insbesondere Ransomware-Angriffe nehmen drastisch zu und zeigen, wie vulnerabel selbst eigentlich gut geschützte Unternehmen sein können. Gefragt ist ein Cyber Defence Center mit dedizierten Fachleuten, welche die Wirkungsmechanismen der Angreifer bestens kennen, die Infrastruktur rund um die Uhr überwachen und Anomalien analysieren sowie umgehend reagieren, wenn ein Angriff bemerkt wird. So wird eine 360°-Abdeckung möglich, die Angreifer in jeglichen Angriffsphasen entdeckt und aufhält.

Cyber Defence aus einer Hand

Besonders KMU haben häufig weder das Know-how noch die Ressourcen, um Cyber Defence inhouse so zu betreiben, wie es nötig wäre. Daher ist es sinnvoll, solche Dienstleistungen in Form von Cyber-Defence- und Managed-Security-Services bei einem externen Spezialisten mit eigenem Cyber Defence Center zu beziehen. Dort werden neuste Technologien genutzt, Prozesse effizient gemanagt und hoch spezialisierte Fachkräfte eingesetzt, welche für Kunden 24/7 im Einsatz sind – sei es zur Überwachung der Infrastruktur, der umgehenden Beseitigung von Schwachstellen oder der proaktiven Suche nach Anomalien.

Incident Response: Nicht immer ist es zu spät

Doch was, wenn Angreifer bereits im Netzwerk sind? Auch darauf hat ein professionelles Cyber Defence Center eine Antwort in Form von Incident-Response-Services. Dabei sind Fachleute umgehend im Einsatz, wenn Unternehmen angegriffen werden. Nebst forensischen Analysen übernehmen sie auch Verhandlungen mit den Angreifern und unterstützen bei der raschen Wiederherstellung des ordentlichen Betriebs. Eine schnelle Reaktion ist hierbei genauso wichtig wie eine erfahrene Expertise, sodass in Kombination häufig auf eine Zahlung der Lösegeldforderung bei Ransomware-Angriffen verzichtet werden kann. Nichtsdestotrotz sollte es gar nicht so weit kommen, weshalb die Sensibilisierung der Mitarbeitenden, umfassende Schutzmechanismen für alle Bestandteile des Unternehmensnetzwerkes inkl. Cloud und IoT/OT sowie eine permanente Überwachung umso wichtiger sind.

Im InfoGuard Cyber Defence Center (CDC) in Baar/Zug arbeiten über 70 hochqualifizierte Cyber Security Experts und Analysts.

Cybersecurity (er)fordert sämtliche Bereiche

Nicht vergessen werden dürfen natürlich auch die traditionellen Komponenten der Cybersecurity. Ein systematischer Sicherheitsansatz ist das A und O. Dabei müssen sowohl das Risikomanagement, der Schutz der Informationen, die Überprüfung des Sicherheitsdispositivs mittels Penetration Testing und Cyber Attack Simulations, 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 hilfreiche Modelle. Effektive Cybersecurity erfordert – oder vielmehr fordert – somit sämtliche Bereiche mitsamt Cyber Defence. Letzteres nimmt auch zukünftig an Relevanz zu, weshalb Unternehmen frühzeitig agieren und einen erfahrenen Partner beiziehen sollten. ■

InfoGuard
SWISS CYBER SECURITY

InfoGuard AG
Lindenstrasse 10, CH-6340 Baar/Zug
✆ +41 (0)41 749 19 00
info@infoguard.ch, www.infoguard.ch