Hohe Sicherheitsmauern reichen nicht aus

Unternehmen müssen heute davon ausgehen, dass ihre Systeme bereits infiltriert sind oder sie Opfer einer Attacke werden. Umso wichtiger ist es daher, sich nicht nur auf die präventive Sicherheit zu verlassen. Es ist entscheidend, Infiltrationen zu erkennen, schnell darauf zu reagieren und das Sicherheitsdispositiv entsprechend zu optimieren. Deshalb braucht es ein Cyber Defence Center.

Die Medien überschlagen sich derzeit mit Meldungen zu unterschiedlichsten Hackerangriffen wie Ransomware, APT-Angriffe oder DDoS-Attacken. Angriffe, die längst nicht nur auf Grossunternehmen zielen, sondern vermehrt auch auf kleine und mittlere Unternehmen. Sicherheitsvorfälle sind nicht nur ärgerlich, sondern können auch enorme Kosten und einen riesigen Imageschaden nach sich ziehen und die Bedrohung durch Cyberangriffe nimmt stetig zu.

Hackern wenig Angriffsfläche bieten

Unternehmen haben sich in der Vergangenheit darauf fokussiert, Cyber-Risiken zu identifizieren und entsprechende Sicherheitsmassnahmen zu integrieren. Aber auch das beste Sicherheitsdispositiv bringt nichts, wenn (Sicherheits-)Systeme und Applikationen verwundbar sind. Die Vergangenheit zeigt: Oftmals haben Angreifer leichtes Spiel. Viele erfolgreiche Angriffe nutzten Schwachstellen in ICT-Komponenten aus, die seit mehr als einem Jahr bekannt waren. Dies zeigt, wie wichtig – nebst geeigneten Sicherheitssystemen – ein funktionierendes Schwachstellenmanagement ist. Natürlich garantiert auch dies keinen 100-prozentigen Schutz vor Eindringlingen, jedoch werden damit die Eintrittsbarrieren erheblich erhöht.

Breach Detection und Incident Response sind entscheidend

Hohe Sicherheitsmauern und ein funktionierendes Schwachstellenmanagement reichen aber leider nicht mehr aus. Es braucht neue Sicherheitsansätze, bei welchen die Detektion im Vordergrund steht und die Reaktion auf Angriffe ein wesentlicher Bestandteil der IT-Prozesse ist. Geschickt umgesetzt kann so die Prävention zielgerichtet und kontinuierlich verbessert werden. Um bei der Cyber Defence überhaupt eine Chance zu haben, müssen sich Sicherheitsverantwortliche folgende Punkte vor Augen führen:

- Das Unternehmen wird (früher oder später) mit Sicherheit kompromittiert werden und die Angriffsfläche wird durch den Einsatz neuer Technologien wie Smart-Devices, IoT usw. immer grösser.
- Nicht alles muss gleich geschützt werden. Es gilt die eigenen Kronjuwelen und business-kritische Assets zu identifizieren und Prioritäten zu setzen.
- Die (ICT-)Schutzmauer ist oft bereits sehr hoch – aber es fehlt an geeigneten Werkzeugen zur Erkennung von Infiltrationen und zur entsprechenden Reaktion darauf.
- Und zu guter Letzt: Verhindern kann man Angriffe nicht!

Die Nadel im Heuhaufen finden

Es geht also nicht mehr nur darum, Risiken zu minimieren und sich gezielt vor Cyber-Attacken zu schützen. Vielmehr gilt es Angriffe und Anomalien zu erkennen und schnell zu reagieren, damit das Ausmass auf ein Minimum reduziert werden kann. Eine gute Möglichkeit um Angreifer nach einem erfolgreichen Angriff aufzuspüren bieten Breach-Detection-Lösungen, bei denen der Netzwerkverkehr mittels Data Science, maschinellem Lernen und Verhaltensanalysen durchsucht und ausgewertet wird. Moderne und professionelle Network-Behavior-Analysesysteme geben Sicherheitsverantwortlichen den benötigten Überblick, um schnell auf Cyberbedrohungen reagieren zu können.

Retrospektive Informationen helfen zudem, sich schnell ein Bild der im Angriff involvierten Prozesse zu machen. Nur so lässt sich die gesamte Infrastruktur im Bedarfsfall flächendeckend nach «Indicators of Compromise» (IoC) durchsuchen. Um all diese Aufgaben erfolgreich zu meistern empfiehlt es sich, ein Team von Experten und entsprechende Tools zur Breach Detection, für das Security Information & Event Management (SIEM), aber auch für den Incident Response in einem dedizierten Cyber Defence Center zu vereinen. Security Operation ist jedoch eine anspruchsvolle Arbeit und benötigt entsprechende Skills. Oftmals fehlt es Unternehmen schlicht an Ressourcen. Der Betrieb dieser Infrastruktur ist zeitintensiv und anspruchsvoll, wobei die Sicherheit folglich auf der Strecke bleibt. Abhilfe schaffen da professionelle Services von spezialisierten Anbietern wie InfoGuard. Dort setzen sich Analysten tagtäglich mit der aktuellen Bedrohungslage auseinander. So können Unternehmen von der grossen Erfahrung profitieren, ohne ein eigenes Cyber Defence Center aufbauen zu müssen.

InfoGuard baut ein 250m2 grosses Cyber Defence Center

InfoGuard baut eines der modernsten Cyber Defence Center in der Schweiz, in welchem ab Mitte Mai 2017 Sicherheitsexperten und Analysten arbeiten werden. Die Services umfassen u.a. Security Information & Event Management (SIEM), Vulnerability Management, Breach Detection, aber auch Cyber Threat Intelligence, Incident Response und Forensik. Sie basieren auf führenden Detection Technologien – auch aus dem Bereich der Artifical Intelligence und Machine Learning. Das neue Cyber Defence Center verfügt über ein mehrstufiges, physisches Sicherheitskonzept und die Sicherheitssysteme werden rund um die Uhr überwacht – und das 365 Tage im Jahr. Gleichzeitig erfüllt InfoGuard die strengen Vorgaben des Schweizer Datenschutzes und die Richtlinien für den schweizerischen Finanzsektor.

InfoGuard
SWISS CYBER SECURITY

infoGuard AG
Lindenstrasse 10
6340 Baar
041 749 19 00
www.infoguard.ch