Cyber Defence – Hohe Mauern reichen nicht mehr aus

Unternehmen müssen heutzutage davon ausgehen, dass ihre Systeme bereits infiltriert sind – oder aber, dass sie nächstens Opfer einer Attacke werden. Es ist deshalb entscheidend, Infiltrationen zu erkennen, schnell darauf zu reagieren und das Sicherheitsdispositiv entsprechend zu optimieren. Genau hierfür braucht es ein Cyber Defence Center.

«WannaCry», Hackerattacken, DDoS-Angriffe … – die aktuelle Cyber-Bedrohungslage ist riesig.

Nach wie vor sind die Nachrichten voll mit Meldungen von gezielten Hackerangriffen – und zwar im ganz grossen Stil, wie dies der Angriff anfangs Mai mit dem Verschlüsselungstrojaner «WannaCry» wieder einmal deutlich vor Augen geführt hat. Ein Blick auf die Entwicklung der Cyber-Attacken macht klar: Die Angreifer sind in der Regel keine Einzeltäter; Internetkriminalität ist inzwischen professionell organisiert. Es gibt auch dort eine Aufgabenteilung wie die Programmierung von Malware, den Versand von E-Mails, die gezielte Suche nach Sicherheitslücken (Exploits) oder die Bereitstellung von Exploit-Kits. Auch staatliche Hackgruppen greifen immer häufiger nicht nur andere staatliche Organisationen an, sondern auch private Unternehmen – und all das, unter Einsatz nahezu unbegrenzter Mittel.

Cyber Security besteht nicht nur aus (ICT-)Sicherheitsmauern

Deshalb müssen Unternehmen hinsichtlich der Cyber Security umdenken – und dürfen sich nicht nur auf (immer) höhere ICT-Sicherheitsmauern verlassen. Der Trend geht klar in Richtung einer intensiveren Überwachung von Sicherheitssystemen und Erkennung von Vorfällen, wie es auch das NIST Cyber Security Framework empfiehlt. 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.

Dies wären grundsätzlich alles Aufgaben, die ein Security Operation Center erledigt. Deshalb gilt ein SOC auch als eine entscheidende Entwicklung im Bereich der Cyber Security, um den immer komplexeren, raffinierteren Attacken zu begegnen. Jedoch gibt nur gerade jedes zweite Unternehmen an, ein SOC im Einsatz haben – und ob es sich dabei wirklich um ein SOC handelt, sei dahingestellt. Denn in vielen Unternehmen muss sich das SOC auch um operative Aufgaben im IT-Betrieb kümmern, womit die Erkennung von Angriffen, die Analyse und die Reaktion auf Vorfälle oft zu kurz kommt. Wenn also ein SOC Helpdesk-Anfragen beantworten muss, stehen die Chancen für einen erfolgreichen Cyberangriff relativ gut. Gut für den Angreifer, aber schlecht für das Unternehmen! Wie sollte somit eine effektive Cyber Defence, mit einem SOC der Zukunft aufgebaut sein?

SOC 2.0 – das Cyber Defence Center

Natürlich braucht es auch zukünftig nebst entsprechenden Werkzeugen zur Erkennung von Attacken oder Infiltrationen IT-Spezialisten; aber noch viel wichtiger sind Cyber Threat- und Intelligence-Analysten sowie Security Experten. Es muss also in einem Cyber Defence Center (CDC) eine klare Aufgabenteilung und trotzdem die eminent wichtige Teambildung geben zwischen dem Blue Team (Cyber Security- und Cyber Defence-Experten) und dem Red Team (Cyber Threat-Analysten und Penetration Tester). Denn in einem CDC lau-

SWISS CYBER DEFENCE CENTER VON INFOGUARD

InfoGuard hat Ende Mai ein neues, 250 m² grosses Cyber Defence Center eröffnet. Die Services umfassen u.a. Security Information & Event Management (SIEM), Vulnerability Management, Breach Detection sowie Cyber Threat Intelligence, 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.

fen alle Fäden zur Erkennung, Analyse und Abwehr von Cyber-Angriffen zusammen. Erforderlich sind dafür erfahrene Experten mit einem umfassenden Know-how, Security-Tools und nicht zuletzt ein physisch geschützter Operation-Raum mit den notwendigen Arbeitsplätzen für beide Teams.

Sie sehen: Cyber Defence ist eine anspruchsvolle Arbeit. Insbesondere aufgrund des Fachkräftemangels fällt es den Unternehmen immer schwerer, kompetentes Personal aus dem Informatiksektor zu finden. Da Attacken rund um die Uhr erfolgen, muss ein Cyber Defence Center natürlich auch rund um die Uhr funktionieren, was den Personalbedarf zusätzlich erhöht. Selbstlernende Systeme und Lösungen mit Künstlicher Intelligenz, die die Security-Analysten im Bereich der Breach Detection unterstützen, können bis zu einem gewissen Grad Arbeitserleichterung bringen. Diese gilt es zu nutzen, gerade weil hier sicherlich auch weitere Fortschritte zu erwarten sind, die ein CDC noch effizienter machen. Eine Vollautomatisation wird es aber nie geben. Gerade weil auch in Zukunft Security Experten benötigt werden, steigt die Nachfrage nach geeigneten, externen Spezialisten – wie beispielsweise InfoGuard, welche diese anspruchsvolle Arbeit für Unternehmen als Service übernehmen.

Autor:
Mathias Fuchs,
Head of Cyber Defence,
InfoGuard AG

Die InfoGuard AG ist spezialisiert auf umfassende Cyber Security. Zu ihren Kompetenzen zählen massgeschneiderte Dienstleistungen im Bereich der Sicherheitsberatung und Security Audits sowie in der Architektur und Integration führender Netzwerk- und Security-Lösungen. State-of-the-Art Cloud-, Managed- und SOC-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.

InfoGuard
SWISS CYBER SECURITY
www.infoguard.ch

InfoGuard ist ISO/IEC 27001:2013 zertifiziert.