Schutz vor «Petya», «WannaCry» und Co.

«Petya/NotPetya», «WannaCry», Hackerattacken, DDoS-Angriffe – die aktuelle Cyber-Bedrohungslage ist riesig. Es ist deshalb entscheidend, Infiltrationen zu erkennen und schnell darauf zu reagieren.

Die Nachrichten sind voll mit Meldungen von gezielten Hackerangriffen – und zwar im ganz grossen Stil, wie die Angriffe mit den Verschlüsselungstrojanern «Petya, resp. NotPetya» und «WannaCry» deutlich vor Augen führte. Dies bestätigt auch der kürzlich veröffentlichte Post-Intrusion-Report von Vectra Networks. Er liefert einen einzigartigen Einblick in echte Angriffe gegen real existierende Unternehmensnetzwerke. Innerhalb der ersten drei Monate des Jahres wurde dabei eine starke Zunahme von Ransomware-Attacken, Sicherheitslücken (Exploits) von Web-Applikationen mit dem Ziel, Gigabytes an Daten aus den Unternehmen herauszuschmuggeln, und ein auffälliger Anstieg bei IoT-Botnets verzeichnet. Diese Entwicklung der Cyberattacken macht klar: Die Angreifer sind in der Regel keine Einzeltäter; Internetkriminalität ist inzwischen professionell organisiert und spielt sich im Darknet ab. Zu finden gibt es dort einiges: von Drogen und Waffen über gefälschte Pässe bis hin zu Auftragsmördern, vertraulichen Informationen oder Hackern. Letztere nutzen das Darknet, um mit Exploit-Kits, Ransomware und gestohlenen Informationen zu handeln. Aber 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 Defence Center der InfoGuard auf über 250 Quadratmeter

(ICT-)Sicherheitsmauern reichen nicht aus

Unternehmen müssen heutzutage davon ausgehen, dass ihre Systeme bereits infiltriert sind – oder aber, dass sie als nächstes Opfer einer Attacke werden. 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. Dazu braucht es ein Cyber Defence Center (CDC). So lässt sich die Prävention zielgerichtet und kontinuierlich verbessern. In einem CDC laufen alle Fäden zur Erkennung, Analyse und Abwehr von Cyberangriffen zusammen. Erforderlich sind dafür erfahrene Experten mit einem umfassenden Know-how, Security-Tools und nicht zuletzt ein physisch geschützter Operationsraum mit den notwendigen Arbeitsplätzen. Zur Erkennung von Attacken oder Infiltrationen braucht es entsprechende Werkzeuge und IT-Spezialisten. Aber noch viel wichtiger sind Cyber Threat- und Intelligence-Analysten sowie Security Experten. Aber genau dies ist das nächste Problem: Der globale Mangel an gut ausgebildeten Cyber Security-Fachleuten. Cyber Defence ist eine anspruchsvolle Arbeit und geht weit über ICT-Sicherheitsmassnahmen hinaus. Und da Attacken rund um die Uhr erfolgen können, muss ein CDC natürlich auch 24 Stunden am Tag und sieben Tage in der Woche funktionieren, was den Personalbedarf zusätzlich erhöht. Selbstlernende Systeme und Lösungen auf der Basis Künstlicher Intelligenz können bis zu einem gewissen Grad Arbeitserleichterung bringen. Diese gilt es zu nutzen, gerade weil hier auch weitere Fortschritte zu erwarten sind, die ein CDC noch effizienter machen.

Cyber Defence aus der Schweiz

Das Schweizer Unternehmen InfoGuard mit Sitz in Zug und Bern hat sich auf Cyber Security und Cyber Defence spezialisiert. So zählen nebst massgeschneiderten Dienstleistungen im Bereich der Sicherheitsberatung und Security Audits sowie in der Architektur und Integration führender Netzwerk- und Security-Lösungen zu seinen Kompetenzen. Im Mai hat InfoGuard zudem ein 250 Quadratmeter grosses Cyber Defence Center in Baar / Zug eröffnet. Die Services umfassen unter anderem 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, an 365 Tagen im Jahr, überwacht werden.

InfoGuard
SWISS CYBER SECURITY

KONTAKT

Mathias Fuchs
Head Cyber Defence

InfoGuard AG
+41 (0)41 749 19 00

www.infoguard.ch