Grüsse aus dem Darknet von «Petya», «WannaCry» und Co.

Die Anzahl der Cyber-Angriffsversuche wie «Petya/NotPetya», «WannaCry», Hacker- und DDoS-Attacken steigt täglich an – mit kaum noch beziffer-baren Schäden für die betroffenen Unternehmen.

Heutzutage müssen Unternehmen 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.

Die Nachrichten sind voll mit Meldungen von Hackerangriffen. Betrachtet man rein die Top 15 Cyber-Bedrohungen der ENISA, findet man Ausprägungen wie Malware-Angriffe, Phishing, Bot-Netze, Cyber-Spionage, Identitätsdiebstahl, DDoS- und Insider-Attacken sowie Spam, Gerätediebstahl und Online-Erpressung (Ransomware), beispielsweise «Petya», resp. «NotPetya», und «WannaCry». Dies bestätigt auch der kürzlich veröffentlichte Post-Intrusion-Report von Vectra Networks. Dieser liefert einen einzigartigen Einblick in reale Angriffe gegen existierende Unternehmensnetzwerke. Innerhalb der ersten drei Monaten 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.

Das Tor ins Darknet

Die zunehmende Digitalisierung und die immer dichtere Vernetzung durch das Internet der Dinge bieten Hackern laufend neue Angriffsflächen. Inzwischen poppen täglich fast 400 000 neue Schadprogramme auf – das sind beinahe fünf pro Sekunde! Diese Entwicklung macht klar: Die Angreifer sind in der Regel keine Einzeltäter; Internetkriminalität ist inzwischen professionell organisiert. Das Internet ist zu einem digitalen Schlachtfeld geworden. Ein Schlachtfeld, auf dem immer professioneller Daten gestohlen werden. Dazu trägt auch massgeblich das Darknet bei. Und dort gibt es einiges zu finden: von Drogen und Waffen, über gefälschte Pässe bis hin zu Auftragsmördern, vertraulichen Informationen oder Hackern. Diese nutzen das Darknet, um mit Exploit-Kits, Ransomware und gestohlenen Informationen zu handeln. Aber auch staatliche Hackergruppen greifen immer häufiger nicht nur andere staatliche Organisationen an, sondern auch private Unternehmen – und all das, unter Einsatz nahezu unbegrenzter Mittel.

Um ins Darknet zu gelangen, benötigt man einen speziellen, aber für jedermann downloadbaren Tor-Browser, welcher als eine Art digitales Schutzschild dient und die Pfade verschlüsselt. Grundsätzlich kann man damit jedoch genau gleich surfen wie mit den gängigen Browsern. Der Unterschied: Man kann so auf Seiten zugreifen, auf denen illegal gehandelt wird oder auf spezielle Foren, ohne Spuren zu hinterlassen. Für den anonymen Zugriff auf Darknet-Dienste werden meistens Zugangsinformationen wie Login und Passwort benötigt und man muss zudem Aufgaben lösen oder ein Rätsel entschlüsseln. Das Darknet-Pendant zu Google heisst «Grams». Mit dieser Suchmaschine und der entsprechenden Software kann mit dem Hidden Service im Darknet «googelt» werden. Allerdings sollte man auf jeden Fall den Tor-Browser verwenden, damit die Privatsphäre gewahrt wird.

Exploits verkaufen ist nicht illegal, aber lukrativ

Kriminelle nutzen bei den meisten Cyberangriffen Sicherheitsschwachstellen aus, beispielsweise veraltete Browser Plugins (Flash, Java, Silverlight) oder alte Browserversionen. Die Angriffe sind sehr hinterlistig, perfide und können so selbst besonders achtsame Benutzer hinters Licht führen. Unter der Bezeichnung Exploit versteht man die Ausnutzung eines Software-Bugs, um eine oder mehrere vorhandene Sicherheitsbarrieren zu umgehen. Von Zero-Day-Exploits spricht man, wenn Hacker eine noch weitgehend unbekannte Schwachstelle ausnutzen, für die noch kein Patch

verfügbar ist. Für die Verbreitung von Malware nutzen Cyber-Kriminelle sogenannte Exploit-Kits. Dies sind vorverpackte Toolkits mit Schadwebseiten oder -software, die Kriminelle kaufen, lizenzieren oder leasen können, um Malware in Umlauf zu bringen. Anstatt selbst herauszufinden, wie man eine Webseite präparieren muss um Besucher zu infizieren, verlassen sich die Angreifer auf einen vorgefertigten Angriffscode im Exploit-Kit. Dieser testet eine Reihe bekannter Sicherheitslücken in der Hoffnung, dass eine funktioniert. Neben Exploit-Kits, die als Übertragungsweg das Internet nutzen, existieren auch eine Reihe ähnlicher Exploit-Kits für E-Mail- und Phishing-Kampagnen. Bei diesen versendet der Angreifer einen Dateianhang an nichts ahnende Nutzer, die diesen im Optimalfall öffnen und dadurch die Malware installieren.

(ICT-)Sicherheitsmauern reichen nicht aus

Der Schutz von Netzwerken und Unternehmenswerten wird dadurch immer schwieriger, insbesondere vor anspruchsvollen Attacken, die durch herkömmliche Sicherheitssysteme nicht mehr erkannt werden. Daher müssen Unternehmen heutzutage davon ausgehen, dass ihre Systeme bereits infiltriert sind – oder aber, 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 Trend geht klar in Richtung einer intensiveren Überwachung von Sicherheitssystemen und der 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 hier liegt das nächste Problem: Der globale Mangel an gut ausgebildeten Cyber Security-Fachleuten.

Sorgt für Sicherheit Made in Switzerland – das Cyber Defence Center von InfoGuard in Baar/Zug.

Cyber Defence ist eine anspruchsvolle Arbeit – und geht weit über ICT-Sicherheitsmassnahmen hinaus. Und da Attacken rund um die Uhr erfolgen, muss ein CDC natürlich auch 7 Tage, während 24 Stunden funktionieren. Dies erhöht den Personalbedarf zusätzlich. Selbstlernende Systeme und Lösungen auf Basis Künstlicher Intelligenz können hier bis zu einem gewissen Grad Abhilfe schaffen. 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 ihren Kompetenzen. Im Mai hat InfoGuard zudem ein neues, 250 m² grosses Cyber Defence Center in Baar/Zug 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.

Autor:
Reinhold Zurfluh,
Head Marketing
InfoGuard AG, Lindenstrasse 10,
6340 Baar

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 ist ISO/IEC 27001:2013 zertifiziert.

InfoGuard
SWISS CYBER SECURITY
www.infoguard.ch