Cyber Threat Intelligence –

zu Besuch bei Hackern und Cyber-Kriminellen

Um Cyber-Angriffe besser abwehren zu können, muss man wie ein Angreifer denken. Cyber-Kriminalität ist ein gewinnorientiertes Unternehmen. Nur wer weiss, warum und was Cyber-Kriminelle vorhaben, mit welchen Bedrohungen in Zukunft zu rechnen ist, kann frühzeitig agieren. Aber genau diese Informationen findet man nicht auf der Strasse, im öffentlichen Internet. Sondern im Darknet. Cyber Threat Intelligence liefert hierzu die optimale Grundlage für den proaktiven Schutz von Informationen und Intellectual Property.

Cyber-Kriminalität ist gut organisiert

Den klassischen Cyber-Angreifer gibt es nicht. Wenn man versucht, sich einen Cyber-Kriminellen vorzustellen, kommen unweigerlich Bilder aus Kino und Fernsehen in den Kopf: Im düsteren Raum, der nur von einigen Computer-Bildschirmen erleuchtet wird, sitzt ein Junk-Food knabbernder Freak. Er schaut gebannt auf eines der Displays und hackt auf seiner Tastatur herum. Plötzlich reisst er eine Faust in die Luft: Geschafft, er ist drin. Diese Vorstellung ist problematisch: Betrachtet man alleine die Top-15-Cyber-Bedrohungen der ENISA (EU-Agentur für Netz- und Informationssicherheit), findet man Ausprägungen wie Malware-Attacken, Phishing, Bot-Netze, Insider-Attacken, Cyber-Spionage, Identitätsdiebstahl, DDoS-Attacken, Spam, Gerätediebstahl und Online-Erpressung (Ransomware). Diese Angriffsmethoden deuten auf eine gezielte Vorgehensweise und hohe Professionalität sowie eine langfristige und sorgfältige Planung der Cyber-Kriminellen hin.

Die dunkle Seite im Netz

All diese Angriffsarten lassen eine fortschreitende Professionalisierung der Angriffsmittel und –methoden erkennen. Woher kommt das? Ein Grund liegt im verborgenen (sprich von den Suchmaschinen nicht indexierten) Netz – dem Darknet. Zugang

zum Darknet verschafft man sich über entsprechende Anonymisierungs-Software. Populär sind Tor-Browser. Laut aktueller Hochrechnung von Tor gibt's zum Darknet bis zu drei Millionen Nutzer täglich – darunter auch viele Schweizer. Erste Anlaufstelle ist The Hidden Wiki: ein ellenlanges Link-Verzeichnis, das auf die unterschiedlichsten Darknet-Seiten und Angebote verweist. Die «Vorzüge» des verborgenen Schattennetzwerks haben leider auch Kriminelle für Ihre Zwecke erkannt. Zu finden gibt es einiges, von Drogen und Waffen, über gefälschten Pässe bis hin zu Auftragsmördern, vertraulichen Informationen oder Hackern. Diese nutzen das Darknet um mit Zero-Day Vulnerabilities, Ransomware und gestohlenen Informationen zu handeln. So findet man beispielsweise Angebote wie «Crime as a Service» oder «Malware as a Service» – bezahlt wird in bedingt verfolgbaren Bitcoin. Die Schattenwirtschaft der Cyber-Kriminalität im Darknet ist sehr gut organisiert und findet teilweise auf dedizierten Plattformen statt. Immer wieder werden aktuelle Zugangsdaten zum Kauf angeboten, wie beispielsweise kürzlich von LinkedIn, MySpace oder Tumblr.

Setzen Sie auf präventive Sicherheit

Der Schutz von Netzwerken und Unternehmenswerten wird dadurch immer schwieriger – insbesondere vor anspruchsvollen Attacken, die durch herkömmliche Sicherheitssysteme nicht mehr erkannt werden. Traditionelle Sicherheitssysteme wie Intrusion-Detection und Anti-Virus-Lösungen haben den Fokus auf der Erkennung von Angriffen, wenn bereits erste Barrieren überwunden oder Muster bekannt sind. Eine kontinuierliche Professionalisierung der Angreifer und Weiterentwicklung von Einbrüchen und Verschleierungstaktiken definiert diese Sicherheitsansätze alleine als nicht mehr ausreichend. Sicherheitsverantwortliche benötigen zur Optimierung der bestehenden präventiven Abwehr-Mechanismen detaillierte und zuverlässige Informationen über die sich ständig wandelnden Angriffsmethoden. Eine präventive Cyber Security beinhaltet heutzutage eine Threat Intelligence. Bei dieser Art des Schutzes werden Angriffe frühzeitig entdeckt, wodurch weiterführende Stufen des Angriffs abgewehrt werden können. Egal ob es sich um «opportunistische» Cyberkriminalität handelt oder um einen gezielten, komplexen Angriff (Advanced Persistent Threat, APT). Dabei werden systematisch Daten über aufkeimende Bedrohungen und Trends gesammelt, gefiltert, analysiert und korreliert, um daraus nützliche Informationen abzuleiten und mit den Angreifern stets Schritt zu halten. Denn nur wer seine Gegner im Detail kennt, kann aus einer fundierten Informationsposition heraus agieren (und muss nicht kurzfristig oder überhastet reagieren). Wenn also Unternehmen über die relevanten (teilweise gar personalisierten) Threats so zeitnahe wie möglich im Bilde sind, dann können sie auch rechtzeitig Massnahmen initiieren und das Schliessen von Sicherheitslücken einleiten, um das Risiko zu mindern oder gar zu verhindern.

360°-Sicht auf die konkrete Bedrohungslage aus der Schweiz

Cyber Threat Intelligence ist eine anspruchsvolle Arbeit – und bleibt leider bei vielen Unternehmen durch den Businessalltag auf der Strecke. Abhilfe schaffen da professionelle Services wie beispielsweise vom Schweizer Cyber Security Experten InfoGuard. Dort setzen sich die Cyber Threat Analysten im Cyber Defence Center tagtäglich mit der aktuellen Bedrohungslage auseinander und analysieren Informationen aus dem Darknet, von Threat Intelligence Feeds und vielen weiteren Quellen. Zudem wird gezielt nach digitalen Spuren, Benutzernamen und Passwörter, Applikationen, vertraulichen Dokumenten, Kreditkartendaten und weiteren Angriffsvektoren zum entsprechenden Unternehmen gesucht. Dank der grossen Erfahrung der Cyber Analysten erhalten Unternehmen eine umfassende Rundum-Sicht auf die aktuelle Bedrohungslage und können anhand der aufgezeigten Sicherheitsmassnahmen zeitnah den Schutz gezielt erhöhen.

Die Cyber Security Experten von InfoGuard setzen sich im Cyber Defence Center tagtäglich mit der aktuellen Bedrohungslage auseinander.

Autor: Markus Limacher
Senior Security Consultant,
InfoGuard AG

Über InfoGuard

Die InfoGuard AG ist spezialisiert auf umfassende Informationssicherheits- und innovative Netzwerklösungen. Zu ihren Kompetenzen zählen massgeschneiderte Dienstleistungen nach internationalen Sicherheitsstandards, die Entwicklung und Implementierung technischer Sicherheits- und Netzwerklösungen sowie umfassende Supportleistungen, bis zu Managed Security und SOC-Services aus dem ISO/IEC 27001 zertifizierten InfoGuard Cyber Defence Center. InfoGuard hat ihren Hauptsitz in Zug und eine Niederlassung in Bern.

InfoGuard ist ISO/IEC 27001:2013 zertifiziert.

InfoGuard
and information becomes secure

www.infoguard.ch