Nur wer die Welt der Hacker versteht, kann effektiven Schutz bieten

Bei Hackerangriffen handelt es sich längst nicht mehr um Einzelfälle, die von Individuen verübt werden. Vielmehr agieren Cyberkriminelle heute organisiert und professionell. Die Fachleute der Infoguard AG kennen sich mit den Wirkmechanismen der Angreifer bestens aus – und sind dank langjährigem Sicherheits-Know-how sowie modernster Technik in der Lage, Firmenkunden effizient zu schützen – vor, während und nach einem Angriff.

Interview mit CEO Thomas Meier und Mathias Fuchs, Vice President Investigation & Intelligence, Infoguard AG

Thomas Meier
CEO

Mathias Fuchs
Vice President Investigation & Intelligence

Thomas Meier, Mathias Fuchs, wie schätzen Sie die aktuelle Bedrohungslage für Unternehmen ein?
Mathias Fuchs: Interessanterweise war es in diesem Sommer überraschend ruhig an der Cyberfront. Während man beim Ausbruch des Kriegs in der Ukraine noch davon ausging, dass die Anzahl der Attacken aus dem Netz zunehmen würde, war eher das Gegenteil der Fall. Ransomware-Angriffe, sprich die Verschlüsselung von Unternehmensdaten und -systemen, nahmen über den Sommer hinweg ab. Allerdings ist diese ruhige Phase nun vorbei: Am vergangenen Wochenende haben wir gleich mehrere Cases registriert. Diese Ab- und Zunahme eröffnet uns spannende Einblicke in die Ökonomie der Cyberangreifer: Diese funktioniert ähnlich saisonal wie die «normale» Wirtschaft.

Warum nahm die Anzahl der Attacken gerade zum Ukraine-Krieg hin ab?
Mathias Fuchs: Wir beschäftigen uns sehr ausgiebig mit dem Thema Cyberkriminalität und sind entsprechend nahe am Geschehen. Wir wissen daher, dass viele der Teams, die Ransomware-Angriffe durchführen, sich sowohl aus ukrainischen als auch aus russischen Leuten zusammensetzen. Der Krieg stellte auch für sie einen Konfliktgrund dar und führte teilweise gar dazu, dass sie sich zersplitterten und gegenseitig unterminierten.

Thomas Meier: Wenn wir uns aber jetzt das aktuelle Volumen an Angriffen betrachten, stellen wir ein extrem hohes Wachstum fest. Während wir vor einigen Jahren vielleicht 40 Fälle von Ransomware-Attacken pro Jahr betreuten, hat sich deren Anzahl per 2021 mit 125 Cases mehr als verdreifacht.

Wo stehen wir aktuell in diesem Jahr?
Thomas Meier: Bisher haben wir 110 Cases verzeichnet. Allerdings muss man diese Zahlen ein Stück weit relativieren: Infoguard ist mittlerweile in der gesamten DACH-Region tätig, wodurch wir es natürlich mit mehr Vorfällen zu tun bekommen, als wenn wir weiterhin primär in der Schweiz operierten. Als kompetente Anlaufstelle für Incident-Response konnten wir uns dank unserer weitreichenden Erfahrung sowie ausgewiesenen Expertise sehr gut etablieren und positionieren. Das ist wichtig, da sowohl die schiere Anzahl als auch die Aggressivität der Ransomware-Attacken zunimmt und die Gefährder zunehmend professioneller agieren.

Welche präventiven Massnahmen kann man Unternehmen empfehlen?
Mathias Fuchs: Die Gefahrenquelle Nummer eins für Unternehmen stellt nach wie vor das Handling von externen Zugriffsmöglichkeiten dar. Jedes Mal, wenn ich einer Person oder Organisation Zugang zu meinem System erlaube, kann dies zu einer potenziellen Sicherheitslücke werden. Aus diesem Grund ist es essenziell, eine echte Multifaktor-Autorisierung zu aktivieren. Dies muss heute in jedem Betrieb zum Pflichtprogramm gehören.

Thomas Meier: Dann gibt es leider immer wieder Computersoftware-Schwachstellen, welche von extern angreifbar sind. Um solche Schwachstellen zu schliessen, ist das regelmässige Durchführen von Updates enorm wichtig. Zudem gibt es noch sogenannte «Zero-Days». Dabei handelt es sich um Schwachstellen, die sowohl den Userinnen und Usern als auch den Anbietenden unbekannt sind und von Angreifern gezielt ausgenutzt werden können. Des Weiteren lohnt es sich, wenn wir von präventiven Massnahmen sprechen, frühzeitig auch die Partnerschaft mit einem Unternehmen zu etablieren, das auf das Handling von Sicherheits-Incidents spezialisiert ist. Wir von Infoguard überprüfen zum Beispiel die getroffenen Schutzmassnahmen unserer Kundenfirmen und führen entsprechende Audits sowie gezielte Penetrationstests durch. Bei der «Attack-Simulation» agiert ein Angriffsteam von uns wie eine Hacker-Organisation und führt Cyberangriffe in der vollen Bandbreite durch – natürlich ohne die Systeme zu schädigen. Basierend auf den Erkenntnissen der verschiedenen Massnahmen erstellen wir dann eine ausführliche Roadmap zur weiteren Verbesserung der Cybersicherheit.

Wenn es zu einem Incident gekommen ist – wie geht man vor und wie kann Infoguard seine Kundschaft unterstützen?
Thomas Meier: Unser Unternehmen besteht seit mehr als 20 Jahren und von Anfang an war «Security» unsere DNA. Dementsprechend haben wir Cyber Security umfassend aufgebaut. Einen Teil davon bildet der Bereich «Prevention», der die bereits umrissenen Schutzmassnahmen umfasst. Zudem haben wir sehr früh Detect- und Response-Infrastrukturen sowie die entsprechenden Prozesse und das Expertenteam aufgebaut. Heute kommt man nicht mehr darum herum, sich für einen konkreten Schadensfall zu wappnen. Und gerade, wenn es um das Reagieren und das richtige Vorgehen bei sicherheitsrelevanten Incidents geht, sind wir bei Infoguard führend. Unsere Klientel setzt sich daher aus eher grösseren Unternehmen zusammen, die in sämtlichen Branchen tätig sind. Die Bandbreite reicht von Banken und Versicherungen über Industrieunternehmen aller Art. Auch Energieunternehmen, Spitäler sowie die Chemie- und Pharmabranche decken wir ab, ebenso Dienste der Öffentlichen Hand.

Was kann man sich unter dem Cyber Defence Center von Infoguard vorstellen?
Thomas Meier: Dabei handelt es sich um eine zentrale Plattform, über die wir sämtliche SOC-Dienstleistungen (Security Operation Center) für unsere Kundschaft verfügbar machen. Dadurch können sich unsere Cyber-Defence-Expert:innen 24 Stunden am Tag sowie sieben Tage die Woche der Sicherheit unserer Kundschaft widmen. Rund 200 Fachleute sind hierfür im Einsatz, um eine 360-Grad-Abdeckung bezüglich Cybersicherheit bieten zu können. Und wir gehen noch einen Schritt weiter: Kürzlich bauten wir ein brandneues SOC, welches mehr als 550 Quadratmeter umfasst. In diesen Räumlichkeiten arbeiten Analyst:innen Hand in Hand mit unseren Incident-Response-Teams und Plattformentwickler:innen zusammen. Auf diese Weise bündeln und konzentrieren wir unser Sicherheits-Know-how zusätzlich. Und davon profitieren natürlich unsere Kundenunternehmen.

Mathias Fuchs: Typischerweise begleiten wir unsere Kundschaft hinsichtlich Cyber Security von A bis Z. Im Angriffsfall unterstützen wir also den Krisenstab und führen schnellstmöglich forensische Arbeiten durch. Auf diese Weise eruieren wir unter anderem, wie die Angreifer ins System gelangt sind und wie sie sich darin konkret bewegen. Zudem prüfen wir, welche Daten exfiltriert wurden. Ferner können wir jederzeit spezialisierte Anwältinnen und Anwälte hinzuziehen, um potenzielle juristische Folgen ebenfalls direkt zu adressieren. Das entspricht unserem Anspruch, alles sicherheitsrelevanten Dienstleistungen aus einer Hand erbringen zu können.

Mathias Fuchs: Im Gegensatz zu vielen anderen Sicherheitsdienstleistern besteht unser wesentlicher Fokus darin, den finanziellen Schaden eines Cyberangriffs möglichst gering zu halten. Wir möchten also den Cashflow einer Firma aufrechterhalten und entlang der unternehmerischen Wertschöpfungskette des Kunden retten, was noch zu retten ist. Zu diesem Zweck ist eine schnelle Reaktion unumgänglich, weswegen das Cyber Defence Center eine so zentrale Rolle spielt.

Und was geschieht, wenn nichts oder kaum noch etwas zu retten ist?
Mathias Fuchs: Wir verfügen über ausreichend Erfahrung, um die meisten Unternehmen zu befähigen, einen sicheren Minimalbetrieb aufzunehmen. Dadurch können sie ihrer Geschäftstätigkeit partiell nachkommen und dann auch zeitnah wieder voll produktiv werden. Im Übrigen gehört auch die Verhandlung mit den Angreifern zu unserer Dienstleistung, etwa bei Ransomware-Attacken, die stets mit einer Lösegeldforderung einhergehen. Dieser Dialog dient dazu, uns sowie dem Kundenunternehmen Zeit zu verschaffen, die Arbeitsweise der Cyberkriminellen besser zu verstehen – und im Idealfall Zwietracht zwischen den gegnerischen Akteuren zu säen. Die Kombination aus Expertise sowie schneller Reaktion führt dazu, dass unsere Kundschaft in den allerseltensten Fällen die Erpresser bezahlen muss.

Wie wird sich die Bedrohungslage aus dem Netz Ihrer Meinung nach künftig verändern?
Thomas Meier: Das Verbrechen ist immer da, wo auch das Geld ist. Die Motivation der Angreifer wird sich also nicht grundlegend verändern in Zukunft. Die Frage ist, wie bald die IT-Infrastruktur einen so hohen Sicherheitsstandard erreicht, dass sie die Gefährder dazu zwingt, aufzustocken und noch professioneller zu agieren. Denn obschon sich bereits eine regelrechte «Hacker-Ökonomie» gebildet hat, gibt es noch Potenzial nach oben. Dessen muss man sich bewusst sein – und sich entsprechend vorbereiten.

Mathias Fuchs: Wir werden einen Sprung in der Qualifikation der Angreifenden sehen. Das ist insofern kritisch, als dass die Angriffsfläche nicht kleiner wird, sondern sich vielmehr vergrössert: Das Internet der Dinge sowie der vermehrte Sicherheitsbedarf bei OT (Betriebstechnologie kritischer Infrastrukturen) werden unseren Alltag immer stärker durchdringen. Wir bereiten uns darauf vor, indem wir uns heute schon auf Technologien fokussieren, die noch nicht breit eingesetzt werden. Das wird sich in Zukunft ändern – und dafür wollen wir bereit sein.

Über die Infoguard AG

Die Infoguard AG ist spezialisiert auf umfassende Cyber Security. Ihre rund 200 Sicherheitsexpert:innen sorgen tagtäglich für die Cyber Security bei über 400 Kunden in der Schweiz, Deutschland und Österreich. Zu den Kompetenzen zählen massgeschneiderte Dienstleistungen im Bereich der Sicherheitsberatung und Security Audits sowie in der Architektur und Integration führender Netzwerk- und Security-Lösungen. Cloud-, Managed- und Cyber Defence Services erbringt der Schweizer Cyber-Security-Experte aus dem ISO 27001 zertifizierten Infoguard Cyber Defence Center in der Schweiz, welches im September 2022 auf die doppelte Fläche vergrössert und personell ausgebaut wurde. Infoguard hat ihren Hauptsitz in Baar/Zug sowie eine Niederlassung in Bern. Zudem ist Infoguard ISO/IEC 27001:2013 zertifiziert und Mitglied bei FIRST (Global Forum of Incident Response and Security Teams).

Weitere Informationen unter
www.infoguard.ch

InfoGuard
SWISS CYBER SECURITY