Cyber Defence – wir brauchen Sicherheit, die mitdenkt

Signaturbasierte Sicherheitsverfahren stossen bei der Erkennung aktueller APT-Angriffe an ihre Grenzen. Moderne Threat-Management-Lösungen erkennen Cyber-Angriffe durch maschinelle Lernansätze in Echtzeit.

Die Anzahl gezielter Hackerangriffe steigt rasant an. Unternehmen müssen heute davon ausgehen, dass auch ihre Systeme bereits infiltriert sind. Sie dürfen sich deshalb nicht allein auf signaturbasierte und präventionszentrierte Sicherheitsmethoden am Perimeter verlassen. Gelingt es einem Angreifer, in ein Unternehmens-Netzwerk einzudringen, kann er sich unbemerkt völlig frei bewegen und unbehelligt Daten klauen. Deswegen braucht es heutzutage neue, mitdenkende Sicherheitsmodelle. Trotzdem sollte man nicht auf signaturbasierte Lösungen verzichten, immerhin erkennen sie die Anzeichen bereits zuvor identifizierter Bedrohungen.

Ein Unternehmen muss heute davon ausgehen, dass seine Systeme bereits infiltriert sind – und erfahrungsgemäss dauert es rund 225 Tage bis dies erkannt wird.

Nur wer Hacker versteht, kann sich auch richtig schützen

Professionelle und erfahrene Hacker sind darauf bedacht, ihre Attacken stets zu modifizieren, um eine Aufdeckung zu vermeiden. Deswegen lässt sich Malware einfach verändern oder verschlüsseln, um sicher zu stellen, dass sie keiner bekannten elektronischen Signatur entspricht. So sind Angreifer zwar in der Lage, die Erscheinung der Malware neu zu verpacken, nicht aber das Ziel der Angriffe: nämlich das Ausspionieren, die Verbreitung und Diebstähle in Netzwerken der Opfer. Diese Verhaltensweisen sind elementar und von grundlegender Bedeutung für eine Attacke - und sie lassen sich beobachten.

Hier schlägt die Stunde des Cyber Threat Managements. Dabei handelt es sich um ein völlig neuartiges Verteidigungssystem gegen APT-Angriffe. Diese Technologie setzt da an, wo die Perimeter-Sicherheit aufhört. Nämlich mit der Bereitstellung einer kontinuierlichen Analyse des internen und Internet-Netzwerkverkehrs, was die automatische Erkennung aller Phasen eines unbefugten Zugriffs ermöglicht. Mit Hilfe von Data Science, maschinellem Lernen und Verhaltensanalysen ist es möglich, die grundlegenden Methoden und Aktionen eines Angriffs zu erkennen, wodurch jene Bedrohungen aufgedeckt werden, die die grössten Risiken darstellen. Unternehmen sind somit schneller in der Lage, Schaden zu verhindern oder zu begrenzen.

Cyber Defence kommt aus der Schweiz

Dank dem verhaltensbasierten Cyber Threat Management in Kombination mit dem InfoGuard Cyber Defence Center Services erhalten Unternehmen nebst der APT Detection & Incident Response, der Cyber Threat Intelligence und systematischen Analyse von Bedrohungen umfassende Cybersecurity aus der Hand von Experten. Dank der fundierten Branchenkenntnis, der interdisziplinären Kompetenz zwischen offensiver und defensiver Cyber Security und der grossen Erfahrung im Bereich Penetration Testing und Ethical Hacking können sie einschätzen, welche Sicherheitsbedrohungen auf das jeweilige Unternehmen zutreffen und frühzeitig Massnahmen einleiten.

Autor: Reinhold Zurfluh
ist Head of Marketing
bei InfoGuard AG

InfoGuard AG ist spezialisiert auf umfassende Informationssicherheits- und innovative Netzwerklösungen. Zu Ihren Kompetenzen zählen massgeschneiderte Dienstleistungen nach internationalen Sicherheitsstandards sowie die Entwicklung und Implementierung technischer Sicherheits- und Netzwerklösungen. InfoGuard ist Mitglied der Schweizer «The Crypto Group».

InfoGuard ist
ISO/IEC 27001:2013 zertifiziert.

InfoGuard
and information becomes secure

www.infoguard.ch