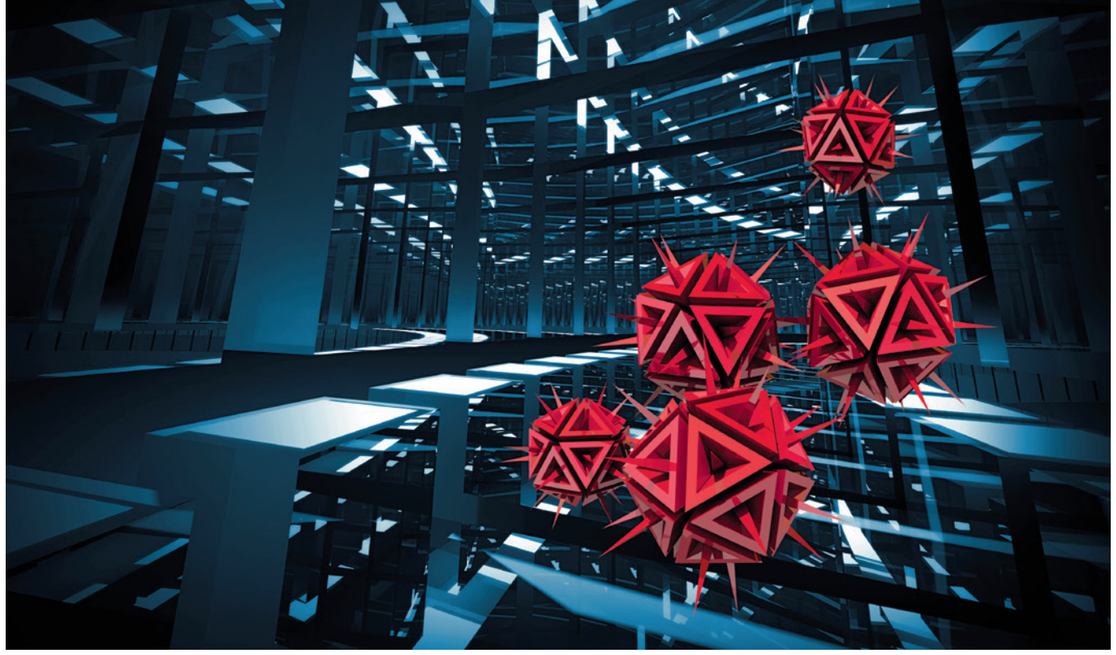


Es geht um die lückenlose Überwachung aller Ereignisse.

Cyber Threat Management

Während Sie dies lesen, werden Sie vielleicht gerade gehackt

von Umberto Annino

Ohne Internet geht gar nichts mehr in der heutigen Wirtschaftswelt. Das machen sich auch die Kriminellen zunutze. Defensive IT-Sicherheit reicht dabei nicht mehr: Heutzutage braucht es ein Cyber Security Management. Denn es geht um viel mehr als um eine reine Abwehr von Angriffen aus dem Internet. Es braucht eine eigentliche Bedrohungsaufklärung, welche bereits bei der Analyse beginnt und bei der Fähigkeit, Bedrohungen zu erfassen, zu beurteilen und rasch zu reagieren.

Vollbestand im Abwehrdispositiv der weltweiten Unternehmen: Gemäss verschiedenen Berichten hatten 100 Prozent der einmal gehackten Unternehmen die aktuellsten Antiviren-Updates auf ihren Rechnern, und 99.9 Prozent der Schwachstellen waren über ein Jahr alt. 75 Prozent der Sicherheitsexperten meinen, dass langjährige und bewährte Methoden zunehmend ineffektiv werden, 243 Tage vergingen, bis ein gezielter Angriff (zumeist von Drittparteien) entdeckt wurde. Die Rede ist von Advanced Persistent Threats (APT), komplexen, zielgerichteten und effektiven Angriffen auf kritische IT-Infrastrukturen und vertrauliche Daten von Gross- und immer mehr auch Mittelstandsunternehmen aller Branchen, welche aufgrund ihres USP potenzielle Opfer darstellen.

Lockende und lohnende Beute

KMU bilden, wie so schön gesagt wird, das Rückgrat der Schweizer Wirtschaft und machen den Grossteil der Unternehmen hierzulande aus. Und sie gelten als besonders innovativ: Antriebssysteme, Kaffeemaschinen, Sensorik, Pharmaceuticals, in der Schweiz mangelt es gewiss nicht an herausragenden Klein- und Mittelunternehmen. Auch Ihre eigene Firma hat Produkte und Dienstleistungen zu bieten, deren Daten einen lohnenden Besitz darstellen. Dass dies auch die Gegenseite so sieht, lässt sich anhand diverser Beispiele erhärten. Da wäre die Geschichte des Freiburger Unternehmens, das im Januar 2015 mittels eines eingeschleusten Trojaners und dem damit verbundenen Zugriff auf firmeneigene Bankkonten um eine Million Franken erleichtert wurde. Ebenso verbreitet ist Ransomware, bei welcher bei Betrieben sensible Informationen gestohlen und verschlüsselt werden – die Dechiffrierung erfolgt dann erst gegen Bezahlung von Lösegeldern.

So lohnend die Angriffe sind, so wenig wird auch dagegen unternommen. Es sind auch Mitte 2015 noch immer drei Schwachstellen, durch welche Kriminelle hauptsächlich ihren Weg in ein Unternehmensnetzwerk finden, um dort entweder wertvolle Daten zu entwenden oder ein Maximum an Schaden anzurichten. Gefahrenherd erster Güte bleibt der Mensch. Aus ihm lassen sich naturgemäss mittels Social Engineering, Phishing und Auskundschaften auf Social Media vieles an Firmen-Interna entlocken. Ein beliebtes Leck sind private Mobilgeräte im Unternehmen und deren externer Zugriff auf die Unternehmens-IT sowie Web-Anwendungen. So kann relativ einfach in ein System oder Netzwerk eingedrungen werden. Deutliches Verbesserungspotenzial besteht auch bei den geschäftskritischen Informationssicherheitsprozessen, dem Umgang mit Sicherheitsvorfällen, dem entsprechenden Notfallprozedere sowie der Bewertung der Gefahrenbereiche und systematische Bewirtschaftung von Risiken. Hier zeigen sich aufgrund unserer Erfahrung deutliche Schwächen.

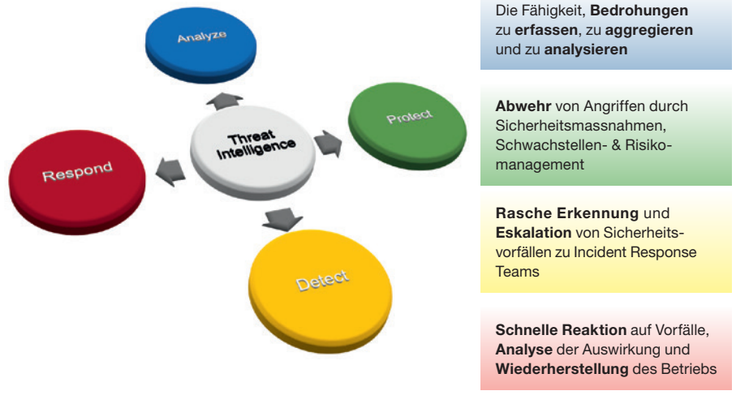
Identifikation statt Pflästerlipolitik

«Heute stellt sich jedem Unternehmen nicht mehr die Frage, ob, sondern nur noch, wann es gehackt wurde. Stand bis vor Kurzem der reine Schutz vor Cyber-Attacken im Zentrum des Interesses, braucht es heute ein umfassendes Cyber Threat Management: Dieses zielt darauf ab, Attacken zu erkennen, daraus die entsprechenden Lehren zu ziehen und somit mit den Angreifern stets Schritt zu halten», resümierte Thomas Meier, CEO von InfoGuard anlässlich der diesjährigen Security Lounge im Juni 2015. Ging man früher davon aus, dass ein Drittel aller Betriebe einmal Ziel einer Cyber-Attacke würde, liegt diese Zahl heute bei gegen 100 Prozent. Dabei sind die Angriffe so raffiniert, dass es die Unternehmen, wie eingangs erwähnt, aufgrund fehlender Monitoring- und Kontrollverfahren über Monate hin gar nicht bemerken.

Gelegenheit macht Diebe: Letztere wird es immer geben, darum müssen die Gelegenheiten ausgemerzt werden. Denn die betroffenen Anwender und ihre für die Informationssicherheit zuständigen Personen stehen in der Verantwortung gegenüber ihren Anspruchsgruppen wie den Aktionären, Kunden, Gläubigern und den Mitarbeitern. Nur ein verantwortungsbewusster Umgang mit erkannten Risiken führt zu einer Verminderung der Aufwände durch Vermeidung materieller und immaterieller Schäden und Verluste. Wie aber kann mit nicht erkannten Risiken umgegangen werden? Der Fokus bewegt sich zunehmend auf die Erkennung von (bisher unbekannten) Angriffen und Mustern, um die defensiven Sicherheitsmassnahmen – die insbesondere auf identifizierte Risiken reagieren – ideal zu ergänzen.

Vier Pfeiler

Zur Abwehr der Bedrohung wird ein mehrstufiges und laufend weiterentwickeltes Konzept zur Abwehr krimineller Eindringversuche mit periodischer Wirksamkeitsprüfung benötigt sowie ein eingespieltes Krisenmanagement nach Feststellung eines erfolgten Angriffs. Cyber Threat Management umfasst demzufolge nicht nur die Reaktion auf Vorfälle. Die Bedrohungsaufklärung besteht aus vier Pfeilern, der Analyse von Bedrohungen, der Abwehr von Angriffen durch Sicherheitsmassnahmen, der raschen Erkennung und Eskalation von Sicherheitsvorfällen sowie einer schnellen Reaktion auf Vorfälle und Verdachtsmeldungen, Analyse der Auswirkungen und einer zeitnahen Wiederherstellung des Betriebs.



Cyber Threat Management sorgt für Transparenz und Sicherheit.

Zentral hierzu ist die lückenlose Überwachung aller Ereignisse. In den zunehmend komplexen Unternehmensnetzwerken von heute werden täglich Tausende von Log-Files, IDS- und IPS-Reports sowie Vulnerabilty-Benachrichtigungen generiert. Angesichts der schieren Datenmenge kapitulieren viele Unternehmen, und sie werten die Daten weder systematisch aus, noch werden sie analysiert, sie werden lediglich gespeichert und dann überschrieben.

Um dem immer professionelleren Vorgehen der Angreifer mit geeigneten Sicherheitsmassnahmen Herr zu werden, müssen diese Vorfälle jedoch bereits während ihrer Entstehung entdeckt und im Keim erstickt werden. Hierzu braucht es ein Security Information & Event Management (SIEM).

Dieses überwacht laufend die sicherheitsrelevanten Ereignisse, erkennt Bedrohungen und informiert im Krisenfall eskalationsstufengerecht das Management. Es ist ein wichtiges Glied einer jeden Security-Strategie im Unternehmen und fungiert als Überwachungssystem innerhalb des gesamten Unternehmensnetzwerks. So können Angriffe erkannt, ein Einblick in Abläufe gewährt und Berichte und Alarme generiert werden.

Schweizer Informationssicherheit aus der Cloud

Der SIEM-Service der InfoGuard deckt Schwachstellen und Angriffe auf die IT-Infrastruktur auf, sodass diese gezielt und schnell eliminiert werden können. Gleichzeitig erhalten die Kunden dadurch die vollständige Transparenz über den Sicherheitszustand im Netzwerk und können dadurch das Sicherheitsniveau nachhaltig erhöhen. Dank des Outtasking des Security Information & Event Management an das InfoGuard Security Operation Center stehen den Kunden die Schweizer Sicherheitsexperten rund um die Uhr mit ihrer langjährigen Erfahrung in der Informationssicherheit zur Verfügung. ■

Umberto Annino

ist Senior Security Consultant der InfoGuard AG.

www.infoguard.ch