IT-SICHERHEIT HEISST: PROAKTIV AGIEREN

Die Gefahr durch IT-Wirtschaftskriminalität steigt kontinuierlich, die Angriffe werden immer komplexer. Heute geht es um viel mehr, als um eine rein reaktive Abwehr von Angriffen. Es braucht ein strategisches Vorgehen, das bei der Erfassung von Bedrohungen beginnt und über die Abwehr von Angriffen bis hin zur raschen Reaktion geht.

→ **VON UMBERTO ANNINO**

Gemäss verschiedenen Berichten haben die meisten gehackten Unternehmen die aktuellsten Antiviren-Updates auf ihren Rechnern und die meisten ausgenutzten Schwachstellen waren über ein Jahr alt. Es vergingen rund 243 Tage, bis ein gezielter Angriff (zumeist von Drittparteien) entdeckt wurde. Die Rede ist von APT, Advanced Persistent Threats, komplexen, zielgerichteten und effektiven Angriffen auf vertrauliche Daten von Unternehmen aller Branchen, welche aufgrund ihrer Erfolgsfaktoren potenzielle Opfer darstellen.

SCHWEIZER UNTERNEHMEN ALS LOCKENDE UND LOHNENDE BEUTE

Antriebssysteme, Kaffeemaschinen, Sensorik, Pharmaceuticals – in der Schweiz mangelt es nicht an herausragenden Unternehmen. Auch Ihre Firma hat Produkte und Dienstleistungen zu bieten, deren Daten ein lohnender Besitz sind. Dass dies auch die Gegenseite so sieht, lässt sich anhand diverser Beispiele erhärten. Da wäre die Geschichte des Freiburger Unternehmens, das im Januar mittels eines Trojaners und dem damit verbundenen Zugriff auf firmeneigene Bankkonten um eine Million Franken erleichtert wurde. Ebenso verbreitet ist Ransomware, bei der bei Betrieben sensible Informationen gestohlen und verschlüsselt werden – die Dechiffrierung erfolgt dann (wenn überhaupt) erst gegen Bezahlung von Lösegeldern.

So lohnend die Angriffe sind, so wenig wird noch dagegen unternommen. Es gibt auch Mitte 2015 noch immer drei Schwachstellen, durch die Kriminelle hauptsächlich ihren Weg in ein Unternehmensnetzwerk finden, um dort entweder wertvolle Daten zu entwenden, Geld zu erschleichen oder zu erpressen. Gefahrenherd erster Güte bleibt der Mensch. Ihm lässt sich mittels Social Engineering, Phishing und Auskundschaften auf Social Media vieles an Firmen-Interna entlocken. Ein beliebtes Leck sind private Mobilgeräte 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.

Zum Autor

Autor: Umberto Annino, Senior Security Consultant, InfoGuard AG. infoguard.ch

Die Firma:
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

NICHT OB – SONDERN WANN

Heute stellt sich jedem Unternehmen nicht mehr die Frage ob, sondern wann es gehackt wird. Ging man früher davon aus, dass ein Drittel aller Betriebe einmal Ziel einer Cyber Attacke werden, liegt diese Zahl heute bei gegen 100 %. Dabei sind die Angriffe so raffiniert, dass es die Unternehmen, wie eingangs erwähnt, aufgrund fehlender Monitoring- und Kontrollverfahren über Monate hin gar nicht bemerken. Stand bislang der reine Schutz vor Attacken im Zentrum der Bemühungen, braucht es heute ein umfassendes Cyber Threat Management: Dieses zielt darauf ab, Attacken zu erkennen, daraus die entsprechenden Lehren zu ziehen und mit den Angreifern stets Schritt zu halten.

Nur ein verantwortungsbewusster Umgang mit erkannten Risiken führt zu einer Verminderung der Aufwände. 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 ideal zu ergänzen. Zur Abwehr der Bedrohung wird ein mehrstufiges und laufend weiterentwickeltes Konzept 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.

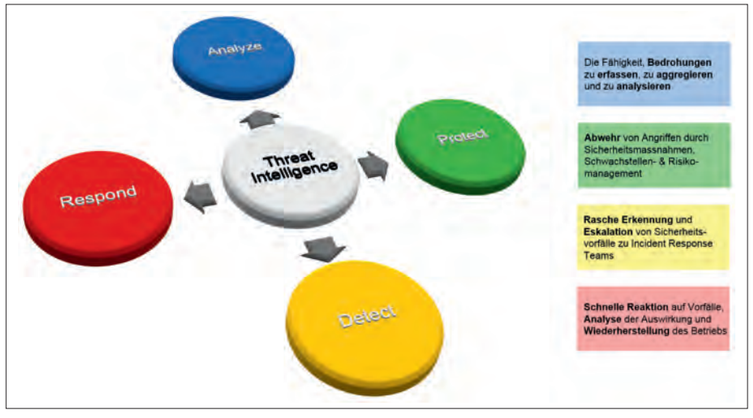
Zentral hierzu ist die lückenlose Überwachung aller Ereignisse. In den zunehmend komplexen Unternehmensnetzwerken von heute

werden täglich Tausende von Log-Files, IDS- und IPS-Reports sowie Vulnerabilty-Benachrichtigungen generiert. Angesichts der schieren Datenmenge kapitulieren viele Unternehmen und 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 Angriffe jedoch bereits während ihrer Entstehung entdeckt und im Keim erstickt werden. Hierzu braucht es ein gelebtes Security Information und Event Management (SIEM). Dieses überwacht laufend die sicherheitsrelevanten Ereignisse, erkennt Bedrohungen und informiert im Krisenfall eskalationsstufengerecht das Management. Nur so können Angriffe erkannt, ein Einblick in Abläufe gewährt und Berichte und Alarme generiert werden.

SICHERHEIT AUS DEM ISO/OEC 27001 ZERTIFIZIERTEN SOC IN DER SCHWEIZ

Die Sicherheit und Zuverlässigkeit von ICT-Systemen ist für Unternehmen unerlässlich. Die Überwachung und der Schutz der eigenen Infrastruktur werden aber immer komplexer und benötigen hochspezialisierte Fachkräfte. Aus diesem Grund hat InfoGuard in den letzten Jahren viel in ihre Managed Security- und Support-Services investiert. Zu diesem Zweck erfolgte der Aufbau des eigenen Security Operation Centers «cyberguard SOC» mit zertifizierten Sicherheits- und Netzwerkexperten und ein Ausbau des Service-Portfolios bis hin zu einem 7x24 Outsourcing der gesamten Netzwerk- und Sicherheitsinfrastruktur. Im Rahmen eines umfassenden Audits erlangte die InfoGuard im Juni 2015 die Zertifizierung nach ISO/IEC 27001:2013. Im Zentrum stand hierbei nebst dem ISMS-System auch die Überprüfung des neuen Security Operation Centers. Dieses erfüllt sämtlichen Anforderungen in punkto physischer, organisatorischer und logischer Sicherheit– und verfügt nachweislich über die optimalen Prozesse im Handling akuter Security Probleme.



Cyber Threat Management sorgt für Transparenz und Sicherheit

Mit dem SIEM-Service (Security Information und Event Management) von InfoGuard werden Schwachstellen und Angriffe auf die IT-Infrastruktur aufgedeckt, so dass diese gezielt und schnell eliminiert werden können. Um Gefahren frühzeitig zu erkennen und die richtigen Schlüsse daraus zu ziehen, setzt InfoGuard auf viele verschiedene Faktoren. So werden laufend Feeds von nationalen Computer Security Incident Response Teams (CSIRT) sowie von Partnerunternehmen überwacht und analysiert. Zudem werden alle Systeme proaktiv auf Schwachstellen und Konfigurationsfehler überprüft. Gleichzeitig erhalten die Kunden dadurch die vollständige Transparenz über den Sicherheitszustand im Netzwerk und können dadurch das Sicherheitsniveau nachhaltig erhöhen. Dank dem Outtasking des Security Information & Event Managements an das InfoGuard Security Operation Center stehen den Kunden die Schweizer Sicherheitsexperten rund um die Uhr mit ihrer langjährigen Erfahrung zur Verfügung. ←

Dieser Beitrag wurde von der Firma **InfoGuard** zur Verfügung gestellt. Computerworld übernimmt für dessen Inhalt keine Verantwortung