Deutscher Mittelstand im Visier der Angreifer

22.06.2015 von Tim Cappelmann, Leiter Managed-Services, Air-IT-Systems

Erst im Dezember letzten Jahres erfuhr die Öffentlichkeit erneut, welchen Schaden Advanced-Persistent-Threats (APTs) anrichten können. Angreifer legten das Sony-Netzwerk mit gezielten Attacken lahm, zogen wertvolle Daten ab, veröffentlichten Interna und machten die Mitarbeiter eines Global-Players nahezu handlungsunfähig. Wer dabei an seltene Einzelfällte denkt, der irrt: Tagtäglich finden Angriffe auf deutsche Unternehmen statt. Dabei stehen nicht die großen Multis im Fokus, sondern der Know-how-starke Mittelstand.

Bildquelle: © Imillian - fotolia.com

Die Liste der internationalen APT-Opfer ist lang: Google, Adobe Systems, Yahoo, Sony. Diese Angriffe sind sehr real, dem durchschnittlichen deutschen Mittelständler gleich-zeitig aber unendlich fern. Ein gefährlicher Irrglaube, denn angesichts solch groß angelegter Angriffe auf weltbekannte Konzerne unterschätzen viele deutsche Unternehmen die Bedrohung durch APTs erheblich. Sie sehen sich selbst nicht auf der Liste attraktiver Ziele und halten ähnliche Fälle im eigenen Unternehmen für unrealistisch. Auch, dass Deutschland politisch nicht an vorderster Front für solche Angriffe steht, führen diese Skeptiker oft als Argument bei der Risikoeinschätzung an.

Spezialisierter Mittelstand attraktiv für Angreifer

Die Bedrohung durch APTs lässt sich allerdings nicht an der Größe eines Unternehmens fest machen. Fakt ist: Neben Behörden sind die Geschädigten am häufigsten produzierende und Know-how-basierte Unternehmen sowie die Dienstleistungs- und Technologiebranche. Kaum jemand weiß, dass Deutschland 2013 weltweit auf Platz 6 der durch APTs angegriffenen Länder stand – europaweit war es sogar Platz 2. Deutschland hat viele „Hidden Champions“ zu bieten. Diese Unternehmen sind durch einen Technologievorsprung Weltmarktführer, aber der Allgemeinheit weitgehend unbekannt. Das Ziel der Hacker ist eindeutig Wirtschaftsspionage. Im Gegensatz zu „klassischen“ Angriffen unterscheiden sich APTs vor allem durch die Motivationslage: Charakteristisch sind zielgerichtete Angriffe auf einzelne Unternehmen oder Behörden, die mit hohem Aufwand durchgeführt werden, um in Form von Wirtschaftsspionage über einen längeren Zeitraum auf vertrauliche Daten zuzugreifen oder kritische Infrastrukturen (im Kontext von Cyber-Warfare oder terroristischer Motivation) zu kontrollieren. Dabei kommen die gleichen Bordmittel wie bei den klassischen Angriffen zum Einsatz. Nur wesentlich effektiver, da Hacker durch das Ausspähen des jeweiligen Unternehmens gezielt den Weg des geringsten Widerstands gehen.

Durch die lange Vorbereitungszeit eines Angriffs wäre, bei entsprechendem Know-how, ein APT also frühzeitig erkennbar. In der Tat lassen sich die Spuren bekannter Fälle teils über mehrere Jahre zurückverfolgen. In der Praxis ergibt sich für Unternehmen bereits hier ein Problem: Aufgrund der Rechtslage dürfen detaillierte Daten zur Erkennung solcher Angriffe in Deutschland erst bei einem begründeten Verdacht gesammelt werden. Zusätzlich erschweren Löschfristen die

Aufklärung des Eintrittsvektors und somit die Absicherung der Lücken, die eine erneute Kompromittierung verhindern. Da die Bereinigung eines APTs sehr aufwändig sein kann und mitunter die Erneuerung ganzer Infrastruktur-bereiche erfordert, ist die Kenntnis des Eintrittsvektors unbedingt notwendig, um nicht nach der Erneuerung gleich die nächste böse Überraschung zu erleben. Den meisten mittelständischen Unternehmen fehlt es jedoch an Know-how und der passenden Technologie zur Erkennung oder Rekonstruktion solcher Angriffe

Sicherheitslücken innerhalb von Minuten ausgenutzt

Experten-Untersuchungen zufolge beträgt die durchschnittliche Zeit, in der ein Netzwerk durch einen erfolgreichen APT-Angriff kompromittiert ist, etwa ein Jahr. Aber auch deutlich längere Zeiträume sind keine Seltenheit. Währenddessen durchläuft der Angriff üblicherweise mehrere Phasen. Die erste Phase beginnt mit dem Einbruch in das Unternehmensnetzwerk. Übliche Techniken sind Spear-Phishing, Social-Engineering, das Ausnutzen bisher unbekannter Sicherheitslücken sowie die Platzierung von Schadsoftware auf Web-seiten, die Mitarbeitern wahrscheinlich aufrufen. Weitere Phasen beinhalten die Installation von Remote-Access-Tools (RATs) und das Verschaffen von Administratorrechten. Es folgt das Ausspionieren der internen Netzwerkstruktur, um weitere Systeme zu kompromittieren, Daten zu sammeln und einen dauerhafter Zugang zum Netz zu erhalten. Erst im letzten Schritt fließen die Daten, auf die es die Angreifer abgesehen haben, ab.

Dieses Phasenmodell suggeriert einen sehr langsamen Verlauf. Durch einen hohen Automatisierungsgrad der Angriffswerkzeuge ist der gesamte Angriff jedoch sehr schnell zu durchlaufen: Das Ausnutzen einer unbekannten Sicherheitslücke und anschließende Installieren eines Remote-Access-Tools inklusive Keylogger oder Password-Cracker ist problemlos über einen infizierten USB-Stick oder eine E-Mail mit Schadsoftware möglich. Damit sind die ersten drei Phasen bereits in wenigen Sekunden durchlaufen. Zudem sind die erforderlichen Werkzeuge oder die Informationsbeschaffung für gezieltes Social-Engineering heute relativ schnell über eine einfache Internetrecherche zu erhalten.

Angriffe oft zu spät entdeckt

Im Hinblick auf kritische Infrastrukturen hat die Bundesregierung mit dem KRITIS-Entwurf (IT-Sicherheitsgesetz zum Schutz kritischer Infrastrukturen) zwar reagiert – von einer „Waffengleichheit“ gegenüber ausländischen Geheimdiensten, die APT-Angriffe durchführen, zum Beispiel aus China, Russland und den USA, ist aber kaum auszugehen. Das hat vor allem zwei Gründe: Zum einen haben entsprechende Organisationen heute die technischen Möglichkeiten, Hintertüren in internationale Standards einzubauen. Zum anderen verfügen die Mitarbeiter dieser Geheimdienste über eine sehr große Know-how-Tiefe. So ist es nicht verwunderlich, dass Unternehmen von einem APT in ihrem Netzwerk oft nur durch Zufall erfahren – oder sogar erst, wenn Know-How und
Daten bereits das Unternehmen verlassen haben.

Um APTs erfolgreich abzuwenden ist im Zeitalter ganzheitlich in IT abgebildeter Geschäftsprozesse ein teilweises Umdenken erforderlich: Beispielsweise der Fall RSA, wo die Informationen zur Bildung der Einmalpasswörter in den Tokens durch einen Angriff öffentlich wurden und somit berechenbar waren. Muss man sich hier nicht fragen, warum RSA diese Information elektronisch im Netzwerk vorgehalten hat? Für welchen Geschäftsprozess sollte dies erforderlich gewesen sein?

Komplexität der IT nimmt zu

Unter diesem Aspekt bringt auch Industrie 4.0 einige Schwierigkeiten mit sich und verfolgt mit der kompletten Vernetzung aller Informationen einen gegen-
läufiger Trend zur „Inselbildung“ der IT-Security. Hier gilt es für IT-Sicherheitsverantwortliche immer auszuloten, an welcher Stelle den aktuellen Trends Folge zu leisten ist und wann es sinnvoller ist, das eigene Unternehmen abzuschotten.

Ein weiterer Ansatzpunkt zur Vermeidung von Schäden durch APTs bietet eine genaue Kenntnis der IT-Prozesse und der dazugehörigen Applikationen sowie deren Kommunikationsbeziehungen. Die detailgenaue Dokumentation der eigenen IT-Landschaft ist zwar sehr zeitaufwändig, ermöglicht aber ein Blacklisting aller nicht benötigten Applikationen und Funktionen. Im Gegensatz zum privaten Einsatz von IT-Systemen benötigen Mitarbeiter in Unternehmen je nach Einsatzgebiet nur sehr eingeschränkte Funktionalitäten. Diese rollenbasierte IT-Nutzung ist vergleichsweise einfach zu reglementieren.

Sicherheitsmaßnahmen an Bedarf anpassen

Auf technologischer Ebene halten viele Experten SIEM-Systeme für das probate Mittel gegen APTs. SIEM steht für Information-Security-and-Event-Management. SIEM-Systeme nutzen die Abermillionen Meldungen, die jede Unternehmens-IT tagtäglich produziert und setzen sie miteinander in Beziehung. Allerdings spielen auch SIEM-Systeme ihre Stärken erst dann voll aus, wenn Unternehmen definieren können, welche Art von Kommunikation im eigenen internen Netz ungewöhnlich ist. Da diese Definition in der Praxis durch unbekannte Kommunikationsbeziehungen selten mehr liefert als bekannte und offensichtliche Angriffsmuster, kann ein SIEM oft nur genau solche erkennen. Spätestens bei Einführung eines SIEM sollten Unternehmen beginnen, bekannten Netzwerkverkehr zu definieren. Nur so können sich IT-Sicherheitsexperten auf den unbekannten Verkehr konzentrieren und diesen untersuchen. Ein besonderes Augenmerk sollten Administratoren auf Verbindungen aus dem Netzwerk heraus richten und entsprechende Logfiles unbedingt in das SIEM integrieren. Auf diese Weise helfen SIEM-Systeme bei Infektionen beispielsweise, Netzwerkverkehr zu den Command-and-Control-Servern (CnC) zu entdecken.

Möchte ein Unternehmen die Unterstützung eines Dienstleisters in Anspruch nehmen, um sich vor APTs zu schützen, sollte dieser überaus große Erfahrung in verschiedenen Branchen mitbringen. Da APTs nicht nur aus technischen Angriffen bestehen, muss ein Dienstleister nicht nur die Technologie-Ebene beherrschen.
Gerade bei einem begründeten Verdacht empfiehlt sich ein Spezialist, der über Erfahrungen in der Zusammenarbeit mit dem Wirtschaftsschutz der deutschen Verfassungsorgane verfügt: Im Gegensatz zur Staatsanwaltschaft unterliegt der Wirtschaftsschutz keiner Ermittlungspflicht und ermöglicht betroffenen Unternehmen eine Kontrolle über den Involvierungsgrad.

Security erfordert technisches Know-how

Gegen APTs vorzugehen bleibt eine große Herausforderung: Durch die Ausnutzung bisher unbekannter Sicherheitslücken bieten Virenscanner allein keinen ausreichenden Schutz. Zur APT-Erkennung bleibt die Korrelation unterschiedlicher Log-Quellen und Auswertung in SIEM-Systemen wichtigstes Hilfsmittel. Darüber hinaus sollten SIEM-Systeme auch die Integrität von Dateien überwachen. Um die optimale Wirkung eines SIEMs zu erreichen, ist eine genaue Kenntnis der IT-Prozesse, sowie technisches Know-how von IT-Sicherheitsexperten erforderlich. Next-Generation-Firewalls an den Netzwerkübergängen
bieten die dafür notwendige Kenntnis der Protokolle auf Applikationsebene.

Der beste Schutz gegen APTs ist Expertise: Gerade für Mittelständische Unternehmen empfiehlt sich hier die Unterstützung durch einen erfahrenen Dienstleister. Angesichts begrenzter Ressourcen in technischer wie in personeller Hinsicht, bleibt dem Mittelstand sonst kaum eine Chance, sein geistiges Eigentum wirkungsvoll zu schützen.

Veröffentlicht in online Ausgabe der Funkschau
www.funkschau.de