Schutz vor hinterlistigen Cyberangriffen

Von Advanced Persistent Threats (APT) spricht man, wenn Kriminelle gezielt und organisiert Unternehmen und Behörden ausspionieren. Herkömmliche Security-Produkte bieten keinen ausreichenden Schutz, weshalb Cloud-basierte Lösungen an Bedeutung gewinnen.

BILD: ISTOCKPHOTO.COM/WEERAPATKIATDUMRONG

→ **VON GIUSEPPE MAZZA**

Tat: Spionage. Tathergang: hochprofessionell und von langer Hand geplant. Tatort: das Internet. Motiv: Geld. So in etwa könnte der unmittelbare Bericht zum Cyberangriff lauten, der sich Anfang 2014 zutrug und von der Fachwelt als «Energy Watering Hole Attack» bezeichnet wurde. Kriminelle kompromittierten die Website einer renommierten Kanzlei, indem sie ein iFrame manipulierten. Die Kanzlei war jedoch nicht das eigentliche Angriffsziel, sondern Energieunternehmen, die Kunden der Kanzlei waren. Der Webauftritt der Kanzlei ist eine wichtige Anlaufstelle für die Klienten, weshalb Angestellte der Energieunternehmen auf der Seite surften. Sie konnten nicht ahnen, wie ihre Systeme dabei automatisch nach Schwachstellen wie veraltete Browser oder Plug-Ins abgesucht wurden. Wo eine Lücke erkannt war, wurde ein Exploit Kit installiert. Ab diesem Zeitpunkt waren die Computer der Mitarbeitenden infiziert und agierten als Spionagegeräte innerhalb der jeweiligen Unternehmen, indem sie Daten an die kriminelle Organisation lieferten. Dieser konkrete Fall ging noch glimpflich aus. Denn Security-Spezialisten erkannten den Angriff frühzeitig und vereitelten das Schlimmste.

«Eine Security-Lösung muss sowohl Zero-Day- und APT-Attacken abwehren als auch mobile Geräte ausserhalb des Firmenperimeters schützen»
Giuseppe Mazza

GEFÄHRLICHE BEDROHUNGEN

Das Beispiel zeigt, wie Cyberattacken heutzutage ablaufen. Die Komplexität der Angriffe hat in den letzten Jahren zugenommen, auch das Motiv der Kriminellen hat sich geändert. Kriminelle Organisationen sind hinter vertrauenswürdigen Daten her und suchen sich ihre Opfer gezielt aus. Längst vorbei die Zeiten, als allein agierende Hacker darauf erpicht waren, mit aufregenden Attacken Berühmtheit zu erlangen und gar nicht versuchten, die Spuren zu verwischen.

Der neue Typ von Bedrohung wird als Advanced Persistent Threat (APT) bezeichnet. Wie der Name andeutet, werden dabei fortgeschrittene Angriffsmethoden eingesetzt, um Unternehmen oder ganze Branchen gezielt und über längere Zeit unbemerkt zu attackieren. Die Cyberkriminellen sind gut organisiert, verfügen über beachtliche Kenntnisse sowie technische Ressourcen und verfolgen finanzielle oder politische Ziele. Keine Firma, keine Behörde und keine Branche bleibt immun gegen solche Attacken. APT richten sich in der Regel auf finanziell lohnenswerte Opfer, um maximalen Profit zu ziehen. Damit die Attacke höhere Erfolgschancen hat, werden vorgängig Informationen über das Angriffsziel gesammelt. Dazu nutzen die Angreifer alle zur Verfügung stehenden Kanäle wie soziale Plattformen (öffentliche Profile sind wahre Goldgruben), die gehackte IT-Infrastruktur und sogar physische Kontakte in Firmen. So verschaffen sie sich einen Überblick über Personal, Rollen, Beziehungsnetze und eingesetzte Informationstechnologien und eruieren vorhandene Schwachstellen. Diese machen sie sich dann zu Nutze.

Zur Initialattacke verwenden die Angreifer Social Engineering oder setzen auf Watering-Hole-Attacken. Social Engineering ist nichts anderes als die Vertuschung der eigenen Identität. Die Angreifer täuschen vor, eine vertrauenswürdige Person oder Organisation zu sein und verleiten gutgläubige Angestellte in ausgewählten Organisationen dazu, beispielsweise ein PDF-Dokument aus einer E-Mail zu öffnen. Bei Watering-Hole-Attacken werden Webseiten kompromittiert, von denen man weiss, dass Mitarbeitende der anvisierten Firma diese besuchen. Deren Computer sollen mit Malware infiziert werden, womit die eigentliche Bedrohung für die Firma erst beginnt. Die Hacker kontrollieren nun das Gerät und können von diesem aus wichtige Komponenten der ICT-Infrastruktur wie lokale Netze oder Server erreichen. Einmal im Firmennetz drin, können sie selbst Aussenstandorte oder Partnerfirmen infiltrieren. Ab diesem Zeitpunkt übermitteln die infizierten Systeme meist über einen längeren Zeitraum (Monate oder Jahre) sensible Daten an externe Systeme, ohne dass die betroffene Firma davon etwas merkt. Die gestohlenen Informationen werden danach verkauft.

ÜBLICHE MASSNAHMEN REICHEN NICHT

Die Security-Infrastruktur einer Firma besteht heute typischerweise aus mehreren Elementen wie Firewalls, Intrusion-Detection-Systemen, AV-Filtern und Proxys. Diese Lösungen befinden sich normalerweise an den Firmenstandorten zum Schutz des dedizierten Firmenperimeters. Endgeräte (PCs und Notebooks) werden zusätzlich mit lokaler Antiviren-Software geschützt.

Letztere haben einen erheblichen Nachteil: Sie erkennen Cyberattacken mittels Signatur, sprich, es werden nur bereits bekannte Angriffe von bekannten Systemen identifiziert. Dies genügt zwar, um einen Basisschutz sicherzustellen, allerdings nicht, um sich gegen APT und Zero-Day-Attacken (nie zuvor gesehene Angriffsmuster) zu wehren. Zudem werden Tablets und Smartphones oft nicht im Security-Konzept der Firma berücksichtigt und sind daher nicht speziell geschützt. Solche Endgeräte sind besonders exponiert, weshalb APT diese Schwachstellen ausnutzen. Erschwerend kommt hinzu, dass mobile Geräte auch ausserhalb des geschützten Firmenperimeters über öffentliche Netze mit dem Internet verbunden sind. Für Kriminelle öffnet sich dadurch oft ein Hintertürchen ins Unternehmen.

SCHUTZ AUS DER WOLKE

Eine frühe Erkennung von APT ist von zentraler Bedeutung, um sich wirksam schützen zu können. Technische Massnahmen alleine reichen nicht aus; Unternehmen müssen auch das Personal schulen. Denn der Faktor Mensch ist eine Schwachstelle, die APT bewusst missbrauchen. Umso wichtiger, Mitarbeitende bezüglich des korrekten Umgangs auf sozialen Plattformen oder mit Phishingmails zu sensibilisieren.

Auf der technischen Seite ist eine Security-Lösung nötig, die in der Lage ist, sowohl Zero-Day- und APT-Attacken zu identifizieren und abzuwehren als auch mobile Geräte ausserhalb des Firmenperimeters zu schützen. Dabei sollte man auf Mechanismen setzen, die suspektes Verhalten von Webseiten und Dateien sowie anormale Muster von ein- und ausgehendem Internetverkehr erkennen (z. B. Logdaten-Analyse, Sandboxing oder Verhaltensanalysen). Besonders dafür geeignet sind Cloud-basierte Security-Lösungen. Dabei wird der gesamte Internetverkehr jedes Nutzers über einen Security Gateway in der Cloud geleitet, wo verschiedene Prüfungen in Echtzeit ausgeführt und bei Gefahr der Verkehr blockiert wird.

Die Vorteile einer Cloud-basierten Lösung sind zum einen die schier unbegrenzte Rechenleistung. Dank dieser können sämtliche ein- und ausgehenden Datenpakete analysiert werden, ohne dass für den Benutzer eine spürbare Verzögerung entsteht. Neue Angriffsmuster werden somit zuverlässiger identifiziert und Abwehrmechanismen ausgelöst. Zum anderen ermöglichen Cloud-Lösungen standortunabhängige Verfügbarkeit. So wird der Schutzschirm auch über mobilen Geräten ausgebreitet, die ausserhalb des Firmennetzes auf das Internet zugreifen. Damit wird eine Sicherheitslücke geschlossen, die heute noch von vielen Unternehmen unterschätzt wird.

Weil sich immer mehr Unternehmen für den Einsatz von Cloud-basierten Sicherheitslösungen entscheiden, hat das Angebot in den letzten Jahren deutlich zugenommen. Mittelfristig wird somit auch die Security den allgemeinen Trend der Auslagerung in die Cloud mitmachen. Der Krieg gegen Cyberkriminalität wird zwar auch damit nicht beendet sein. Allerdings gewinnen Unternehmen und Behörden mit Cloud-basierter Security ein starkes Werkzeug, um sich effektiv gegen Bedrohungen wie APT zu schützen. ←

Giuseppe Mazza ist Produktmanager Managed Security Services bei Swisscom → **www.swisscom.ch**