Data Breach Detection

IT-Einbrüche schnellstmöglich entdecken

Illustration: © Leo_Traveling/shutterstock.com

Eine Konstante – wenn auch keine sehr angenehme – im Bereich IT-Security sind Berichte über Data Breaches, also Fälle bei denen Unternehmen Daten verlieren. Kaum ein Tag vergeht, an dem die Medien nicht über den Verlust von mehr oder weniger sensiblen Daten informieren. Hinzu kommt die Dunkelziffer, wahrscheinlich eine beachtliche Anzahl von Vorfällen, die einfach verschwiegen werden.

Zum einen steigt die absolute Zahl von Vorfällen, bei denen Unberechtigte Zugriff auf Daten erhalten weiterhin an. Zum anderen ist die Spanne hinsichtlich der Ursachen für Datenpannen recht groß und reicht von Hackern, denen es gelang, Systeme zu manipulieren und Daten zu exfiltrieren bis hin zu Insidern, die Daten aus Unternehmen entwenden. Ein oft zu wenig beachteter Punkt sind Konfigurationsfehler, die dazu führen, dass sensible Daten für Dritte leicht sichtbar und damit einer breiten Öffentlichkeit zugänglich werden. Diese große Spanne interner und externer Angriffsmöglichkeiten beziehungsweise Sicherheitspannen erschwert es Unternehmen, sich ganzheitlich zu schützen.

Zu den zentralen Zielen jeder Sicherheitsstrategie gehört es, möglichst schnell und umfassend einen Überblick über aktuelle Sicherheitsvorfälle zu erhalten. Nur dann kann man rechtzeitig die Bedrohung bewerten und Gegenmaßnahmen einleiten.

Security Policy. Auf technische Lösungsansätze kommen wir später noch zu sprechen. So viel sei aber schon verraten – diese haben sich so weiterentwickelt, dass entsprechende Technologien eine große Unterstützung hinsichtlich einer möglichst präzisen und schnellen Erkennung von Data Breaches sein können. Allerdings sollte man nicht alleine auf technische Hilfsmittel vertrauen, sondern vielmehr auch die internen Prozesse überprüfen. Viele Vorfälle sind beispielsweise darauf zurückzuführen, dass unberechtigte Personen Zugriff auf Daten haben. Hier gilt es, die Security Policy rund um Berechtigungs- und Zugangskonzepte näher zu beleuchten. In der Praxis werden Berechtigungen oftmals einmal erteilt und wandern dann mit dem Mitarbeiter innerhalb des Unternehmens von Arbeitsplatz zu Arbeitsplatz. Wir haben schon Accounts von ehemaligen Auszubildenden gesehen, die mehr Rechte hatten als so mancher Manager. Dies lag einfach daran, dass während der Ausbildung viele Abteilungen durchlaufen wurden – immer mit der entsprechenden Rechtevergabe. Allerdings erfolgte bei einem Abteilungswechsel kein Entzug der jeweiligen Rechte.

Minimale Rechtevergaben für administrative und lokale User. Gerade unstrukturierte Daten, also alle Arten von Daten und Informationen, die nicht in einer Datenbank oder einer anderen speziellen Datenstruktur abgelegt werden, enthalten häufig die wertvollsten und gleichzeitig sensibelsten Informationen. Diese unstrukturierten Daten sind zudem meistens überall im Unternehmen verteilt. Um diese Daten effektiv zu schützen, ist es erforderlich, Transparenz zu schaffen – das gilt im Übrigen nicht nur für klassische Unternehmensstrukturen, sondern auch für die Cloud. Hilfreich sind hier Sicherheitslösungen, die Nutzer mit bestimmten Privilegien auf Basis (minimaler) Rechtevergaben ausstatten. Darüber hinaus ist es ratsam, unnötige Berechtigungen beziehungsweise unberechtigte User aufzuspüren und zu eliminieren. Durch den Entzug oder die Einschränkung lokaler Administratorrechte lässt sich die Angriffsfläche deutlich verkleinern und das Risiko senken, dass Angreifer durch die Ausnutzung lokaler Admin-Rechte in die IT-Umgebungen eindringen, sich lateral bewegen und sich somit weitere Rechte verschaffen.

Zum Schutz von Domänen-Controllern und anderen wertvollen Ressourcen ist es jedoch auch sinnvoll, privilegierte Anmeldedaten zu sichern, indem das Austauschen beziehungsweise Teilen von Administrationspasswörtern und -rechten verhindert wird. Ebenfalls sollten bei beiden – administrative und lokale User – umfassende Password-Richtlinien hinsichtlich Länge, Wechselzeiträumen etc. gelten.

Monate bis zur Entdeckung. Kommen wir nun zum eigentlichen Vorfall – einem Datenverlust beziehungsweise dem unautorisierten Zugang zu Daten (Data Breach). Je nach Quelle wird davon ausgegangen, dass jedes zweite bis dritte Unternehmen gezielt angegriffen wird. Gemäß einer Studie des Ponemon Instituts benötigen Unternehmen im Schnitt 256 Tage um einen Hackerangriff zu entdecken. Ein Datenverlust durch Anwenderfehler wird im Durchschnitt nach fünf Monaten (158 Tagen) entdeckt. Durchschnittlich bedeutet, dass es Unternehmen gibt, die einen entsprechenden Datenverlust innerhalb von Minuten oder Stunden erkennen, andere benötigen jedoch viel länger als die genannten 256 Tage. Es besteht ein unmittelbarer Zusammenhang hinsichtlich der Zeit bis ein Einbruch entdeckt wird und den Kosten: Es entstehen umso höhere Kosten bei Cyberangriffen, je länger Hacker Zeit haben, Schaden anzurichten und Daten zu exfiltrieren.

Schwerwiegender als die direkten Kosten rund um den Datenverlust ist meist jedoch der immaterielle Schaden.

Wie wir alle wissen, ist es ein äußerst langwieriger und schwieriger Prozess, verlorengegangenes Vertrauen wieder aufzubauen und Kunden zurückzugewinnen.

In der Regel findet ein Hackerangriff nicht innerhalb von Minuten statt, sondern dauert Tage oder sogar Monate. Diese Vorgehensweise von Hackern hat Vor- und Nachteile: Auf der einen Seite ist sie schwerer zu erkennen, gibt Unternehmen auf der anderen Seite aber auch Zeit, den Einbruch zu entdecken – im Idealfall bevor wertvolle Daten abfließen.

Die langwierige und mehrstufige Vorgehensweise von Hackern wird durch die »Cyber Kill Chain« von Lockheed Martin sehr gut beschrieben. Normalerweise beginnt alles damit, dass ein Angreifer versucht, zunächst sein Opfer umfassend auszukundschaften und möglichst viele Informationen über sein Opfer zu sammeln. Bereits hier können Systeme Auffälligkeiten entdecken. Spätestens aber zu dem Zeitpunkt, an dem die Malware ausgeliefert werden muss, sollten moderne Systeme Malware erkennen – auch für Schadcode, für den noch keine Signatur vorliegt. Moderne Antiviren-Systeme (AV) identifizieren Malware nämlich nicht nur aufgrund einer bekannten Signatur, sondern arbeiten mit mathematischen Methoden. Ebenfalls nicht signaturgesteuert funktionieren Sandbox-Systeme, die Schadcode zunächst in einer sicheren Umgebung (Sandbox) ausführen und dort erkennen, ob ein Code bösartiges Verhalten aufweist.

Bevor wir weiter auf diese neuen Technologien eingehen, noch ein Hinweis: Es gibt eine ganze Reihe von einfachen Vorkehrungen, um zumindest das Ausmaß von Angriffen zu verringern. Beispielsweise kann das eigene Netz strategisch segmentiert werden. Es gibt keinen Grund, warum die Netze so eng miteinander verbunden sein müssen, dass sich ein Wurm oder andere Schädlinge ungehindert ausbreiten können. Eine Trennung von Office- und Produktionsnetzen oder eine Trennung von Gast-WLANs zum übrigen Netz sollen hier nur exemplarisch genannt werden. Grundsätzlich ist es ratsam, sensible Daten im Unternehmen konsequent zu verschlüsseln.

> **Normalerweise beginnt alles damit,** dass ein Angreifer versucht, zunächst sein Opfer umfassend auszukundschaften und möglichst viele Informationen zu sammeln. «

Cyber Kill Chain

Quelle: Lockheed Martin

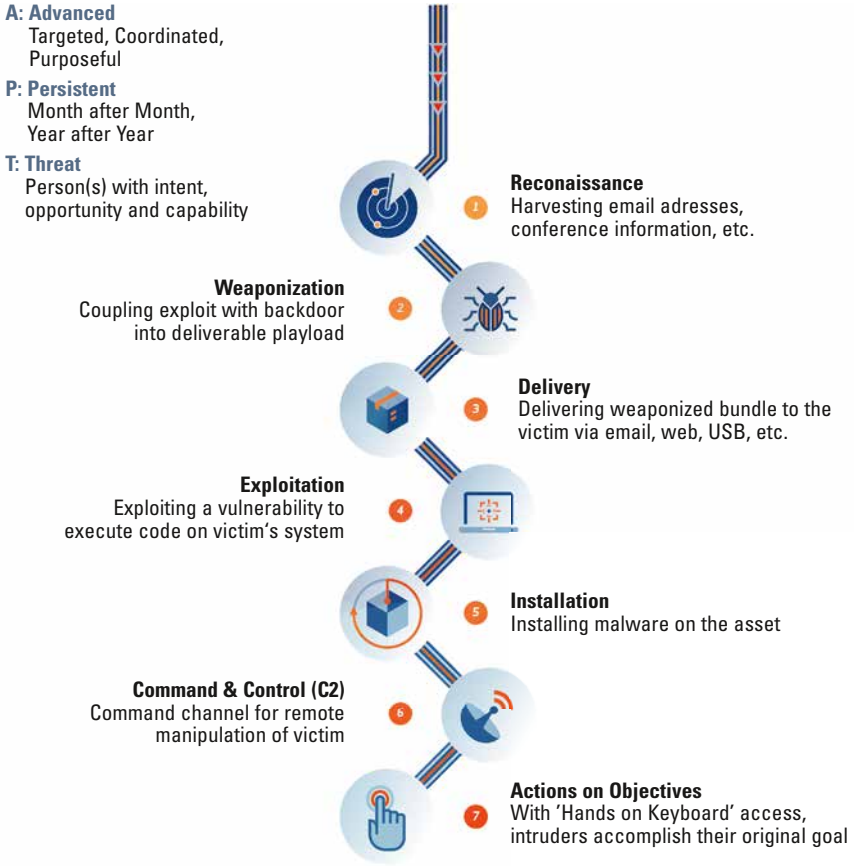

Abbildung: Die langwierige und mehrstufige Vorgehensweise von Hackern wird durch die »Cyber Kill Chain« sehr gut beschrieben.

Data-Breach-Detection-Systeme. Gelingt es einem Angreifer, bösartigen Code zu seinem Bestimmungsort zu bringen – und davon muss man leider ausgehen – sollte das Ziel darin bestehen, einen solchen Eindringling so schnell wie möglich zu erkennen und nicht erst nach den genannten 256 Tagen. Dazu ist es sinnvoll, neben den bereits etablierten Maßnahmen in Prevention (Firewall, AV, IPS etc.) auch in Data-Breach-Detection-Technologien zu investieren. Wirkungsvolle Data-Breach-Detection-Systeme arbeiten ähnlich wie die bereits beschriebenen signaturlosen Antiviren-Scanner. Auch diese beziehen ihre Intelligenz aus mathematischen Formeln und Algorithmen. So soll in der Cyber Kill Chain bereits das Erkunden von Systemen erkannt werden – spätestens beim Aufbau von Verbindungen mit einem sogenannten Command & Control Server oder beim Exfiltrieren der Daten. Ein Data-Breach-System hat also den Anspruch, bereits in einer frühen Phase der Cyber Kill Chain Einbrüche zu entdecken und nachvollziehbar zu alarmieren. Bei der Exfiltration der Daten – zum Beispiel über DNS – kann das System feststellen, ob die Pakete außerhalb der Norm üblicher DNS-Anfragen und -Antworten liegen und löst dann einen entsprechenden Alarm aus.

Fazit. Vorhandene Abwehrmechanismen sollten nicht nur um eine weitere Technologie ergänzt werden, sondern vielmehr muss die Sicherheitsarchitektur betreibbar sein. Lücken, die durch neue Angriffsvektoren entstanden sind, müssen geschlossen werden. Hierbei können neue Ansätze der KI-Technologien (Künstliche Intelligenz) helfen. Diese bieten oftmals eine bessere Erkennungsleistung und sind häufig in Lösungen für Cloud-Security, Next Generation Endpoint oder Netzwerk-Anomalie-Erkennung bereits integriert. Vor dem Einsatz von weiteren technischen Hilfsmitteln ist es auf jeden Fall sinnvoll, grundsätzlich Maßnahmen wie Zugriffs- und Rollenkonzepte oder die interne Segmentierung zu überprüfen. Kommen zusätzliche technische Komponenten zur Abwehr oder zur schnellen Entdeckung von Einbrüchen zum Einsatz, ist es wichtig, bei der Auswahl unbedingt auf Feinheiten zu achten. Controlware verfügt nicht nur über umfassendes Security-Know-how, sondern auch über langjährige Projekterfahrung. Wir unterstützen unsere Kunden von der Beratung über die Konzeption bis hin zur Realisierung anspruchsvoller IT-Security-Lösungen. Bei Bedarf übernehmen wir auch den Betrieb durch unser ISO 27001-zertifiziertes Customer Service Center.

Mario Emig

Mario Emig,
Head of Information Security Business Development bei Controlware GmbH

www.controlware.de