Einbruch muss nicht Diebstahl heissen - Datensicherheit selbst im Fall eines Sicherheitsverstosses

Mit der wachsenden Zahl immer ausgefeilterer Cyberattacken stellt sich nicht mehr die Frage, ob, sondern eher wann ein Unternehmen Opfer eines Angriffs wird. Viele Organisationen konzentrieren ihre Sicherheitsbemühungen immer noch auf Techniken zur Absicherung von Perimetern und investieren grosse Summen in den Versuch, Angreifer von ihren Netzwerken, Servern und Anwendungen fernzuhalten. Doch sollte der Sicherheitsfokus heutzutage auch auf den sensiblen Unternehmensdaten liegen und nicht nur auf den immer anfälligeren Schutzmauern, die sie umgeben ? denn auf lukrative Daten haben es Angreifer zumeist abgesehen. Deshalb verlagern immer mehr Unternehmen ihre Security-Strategie hin zu einer optimierten Identifizierung, Kontrolle und Absicherung ihrer sensiblen Datenbestände. Im Folgenden vier grundlegende Schritte für einen datenzentrierten Sicherheitsansatz:

1. Schritt: Wissen, was geschützt werden muss
Für Unternehmen, die eine datenzentrierte Sicherheitsstrategie verfolgen möchten, ist der beste Ausgangspunkt eine umfassende Datentaxonomie. Schliesslich ist es unmöglich, wirksame Sicherheitsmassnahmen zu ergreifen, wenn man nicht weiss, was es zu schützen gilt. Die Klassifizierung und Strukturierung der eigenen Daten hilft Unternehmen, den vollen Umfang ihrer Sicherheitsanforderungen zu verstehen.

3. Schritt: Kontrolle, wer Zugriff auf sensible Daten hat

Sobald die Daten entsprechend klassifiziert und eingestuft sind, besteht der nächste Schritt darin, den Zugriff auf diejenigen Nutzer zu beschränken, die ihn tatsächlich benötigen. In diesem Stadium ist es wichtig, sich daran zu erinnern, dass nicht alle Datenschutzverletzungen bösartig sind. Viele sind das Ergebnis unbeabsichtigter Nachlässigkeit von Mitarbeitern wie verlorene Memory-Sticks oder Laptops. Die Einführung einer Zugangskontrolle für sensible oder vertrauliche Daten macht es nicht nur böswilligen Insidern und externen Angreifern deutlich schwieriger, Daten zu stehlen, sondern ist auch eine der schnellsten Möglichkeiten, unbeabsichtigte Sicherheitsverstösse zu verhindern. Schliesslich können Mitarbeiter nichts verlieren, was sie gar nicht haben.

Dieser Ansatz gewährleistet auch die Sicherheit der Daten, unabhängig davon, ob sie sich im Ruhezustand, in Ãœbertragung oder in Bearbeitung befinden. In Kombination mit Sicherheits-Best-Practices wie Data-Awareness-Schulungen kann dieser Ansatz weitaus mehr Sicherheit bieten, als sich allein auf Firewalls und Antivirensoftware zu verlassen.

4. Einsatz datenzentrierter Technologien zur weiteren Stärkung der Sicherheit

Als weitere Sicherheitsschicht gibt es zahlreiche datenzentrische Sicherheitstechnologien, die speziell für den Schutz sensibler Daten entwickelt wurden. Data Loss Prevention (DLP), Cloud Access Controls, Verschlüsselungs- und Datentransparenzstrategien können ein erfolgreiches Programm ergänzen und bieten noch robusteren Schutz in der heutigen anspruchsvollen Online-Umgebung.

Trotz des alarmierenden Anstiegs der Cyber-Angriffe in den letzten Jahren ist es wichtig, sich daran zu erinnern, dass ein Sicherheitsverstoss nicht automatisch zu Datenverlust führt. Die Wahl eines datenzentrierten Ansatzes, anstatt ausschliesslicher Verteidigung des Perimeters, kann im Falle eines Verstosses Datenlecks verhindern. Ein grundlegender datenzentrierter Schutz muss nicht kompliziert sein. Wenn man sich nur die Zeit nimmt, um zu ermitteln, welche sensiblen Daten im Unternehmen existieren, wo sie sich befinden und wer Zugang zu ihnen haben sollte, kann dies die Verteidigung der Unternehmen erheblich stärken.