Insider-Bedrohungen durch ausscheidende Mitarbeiter

Viele Unternehmen sind so sehr damit beschäftigt, externe Angreifer aus ihren sensiblen Netzwerken fernzuhalten, dass sie eine andere, möglicherweise noch größere Gefahr vergessen – die Bedrohung durch Insider. Insider-Bedrohungen sind laut Verizon inzwischen für 34 Prozent aller Datenverstöße verantwortlich und können von unachtsamen Angestellten bis hin zu verärgerten Dienstleistern reichen. Das vielleicht stärkste Risiko geht jedoch von einer bestimmten Untergruppe aus – den ausscheidenden Mitarbeitern.

Sicherheitsrisiken durch ausscheidende Mitarbeiter

Für Unternehmen aller Größenordnungen haben ausscheidende Mitarbeiter schon immer ein Problem dargestellt. Denn sie verfügen nicht nur über den notwendigen Zugriff und das Wissen, wo sich sensible Daten befinden, sondern haben in der Regel auch ein Motiv. In einigen Fällen kann es einfach der Wunsch sein, Kopien der eigenen Arbeit für zukünftige Referenzen mitzunehmen. In anderen Fällen allerdings sollen sensible Daten an ein Konkurrenzunternehmen verkauft oder Insider-Wissen den Medien zugespielt werden. Hohe finanzielle Verluste und Reputationsschäden können die Folge sein. Aufgrund der unbekannten Variablen sind Unternehmen im Nachteil, wenn sie sich dieser Art von Bedrohung stellen müssen. Deshalb ist es wichtig, auf verdächtige Aktivitäten und Verhaltensweisen zu achten, die auf eine potenzielle Insider-Bedrohung hinweisen.

Transparenz der Datenbewegungen zum Schutz vor Datendiebstahl

Um sich vor Datendiebstahl durch Insider zu schützen, ist in erster Linie eine Datensichtbarkeit an den Endpunkten erforderlich, aber auch dort, wo Daten das Unternehmen verlassen oder intern übertragen werden. Zumindest sollten Organisationen in der Lage sein, alle Arten von Dateibewegungen und Datenaustritten zu verfolgen und einen Audit-Trail darüber zu erstellen, was jeder Mitarbeiter vor seinem Ausscheiden aus dem Unternehmen gemacht hat. Auf diese Weise kann das Verhalten eines Mitarbeiters zwischen dem Zeitpunkt seiner Kündigung und seinem Ausscheiden genau überwacht und ihm, falls erforderlich, sogar beim Abschlussgespräch zur Klärung vorgelegt werden.

Warnzeichen für Insider-Bedrohungen durch ausscheidende Mitarbeiter

Zu den häufigsten Warnzeichen, die einen ausscheidenden Mitarbeiter als Insider-Bedrohung entlarven können, zählen Spitzen im Datenbewegungsvolumen, das heißt große Datenmengen, die auf USB-Geräte oder Cloud-Speicherorte wie Dropbox oder Google Drive gelangen. Wenn ein Unternehmen über eine Data Loss Prevention (DLP)-Lösung verfügt, ist es möglich, Dateien nach dem Grad ihrer Sensibilität zu kennzeichnen, sodass leichter zu erkennen ist, wie vertraulich die exfiltrierten Daten sind. Werden beispielsweise vertrauliche Dateien an E-Mails angehängt und entgegen den Unternehmensrichtlinien an eine private Domain wie Gmail oder Hotmail gesendet, würde die DLP-Lösung dies melden. Ein Sicherheitsanalytiker kann daraufhin den Vorfall untersuchen, um die Absicht der Person festzustellen, die die Datei versendet hat, und prüfen, wie sensibel ihr Inhalt war.

Maschinelles Lernen zur Verhaltensanalyse

In jüngerer Zeit haben Sicherheitsanbieter begonnen, maschinelles Lernen in ihren Lösungen einzusetzen, um Analysten zu entlasten, die in der Vergangenheit jeden Alarm manuell untersuchen mussten. Machine Learning bietet zudem die Fähigkeit, im Laufe der Zeit ein Standardverhaltensprofil für eine Person oder Maschine zu erzeugen. Einmal erstellt, wird alles, was außerhalb des Normalverhaltens liegt, automatisch für die weitere Analyse markiert, sodass die Sicherheitsteams verdächtige Aktivitäten viel schneller ausmachen können.

Natürlich ist die Bewegung großer Datenmengen nicht immer Grund zur Beunruhigung. Oftmals kann dies einfach das Ergebnis von Datensicherungen in Unternehmen sein. Andererseits können viele sensible Geschäftsgeheimnisse in nur einer einzigen Datei gestohlen werden. Deshalb ist es wichtig, genau zu wissen, welche Personen oder Applikationen auf sensible Informationen zugreifen, und sicherzustellen, dass die Daten angemessen geschützt sind.

Glücklicherweise haben sich die Vorgehensweisen ausscheidender Mitarbeiter in den letzten 15 Jahren nicht dramatisch geändert. Zwar mag es gelegentlich einen Mitarbeiter geben, der über das technische Know-how verfügt, gestohlene Daten in einer Bilddatei zu verstecken und mithilfe von Steganografie hinauszuschmuggeln, doch solche Fälle sind extrem selten. Mit den richtigen Sicherheitsvorkehrungen zur Überwachung auf verdächtiges Verhalten können Unternehmen Insider-Bedrohungen durch ausscheidende Mitarbeiter erheblich minimieren.