Benutzer-Management

Risiko Mitarbeiter

[29.04.2019] Angriffe auf die IT von innen stellen auch in Behörden eine große Gefahr dar. Um Datenmissbrauch vorzubeugen, ist eine professionelle Benutzer-Management-Lösung notwendig, die rechtzeitig auf ein eventuelles Fehlverhalten der Mitarbeiter hinweist.

Was für Unternehmen gilt, betrifft kommunale Einrichtungen ebenso: Angriffe von eigenen Mitarbeitern können größeren Schaden verursachen als Attacken von Cyber-Kriminellen. Gerade bei Behörden, die hoheitliche Aufgaben wahrnehmen, drohen im Falle eines Datenmissbrauchs schwerwiegende Konsequenzen. Geraten beispielsweise Wählerlisten oder Steuerunterlagen in die falschen Hände, entsteht der Gesellschaft als Ganzes wie auch den betreffenden Personen erheblicher Schaden.
Während externe Angreifer aufgrund der IT-Sicherheit oft massive Hürden überwinden müssen, sind internen Mitarbeitern Tür und Tor zur IT geöffnet. Natürlich gibt es einige Maßnahmen, mit denen IT-Administratoren dafür sorgen können, dass Mitarbeiter nur auf die für sie relevanten Informationen Zugriff haben. Doch sind diese nur wirksam, wenn sie permanent richtig angewendet werden. Viele Organisationen nutzen Active Directory (AD) beziehungsweise Azure Active Directory (AAD) von Microsoft zur Identifizierung und Autorisierung von Mitarbeitern in ihren Netzen. Während Active Directory den Zugriff auf das lokale Netzwerk steuert, wird Azure Active Directory in Microsofts Cloud-Plattform Azure sowie im Cloud-Dienst Office 365 verwendet.

Datenlecks vorbeugen

Doch jedes Authentifizierungssystem ist nur so gut, wie die darin enthaltenen Informationen. Jeder Mitarbeiter erhält – neben den üblichen Anmeldeinformationen – auch eine Gruppenzugehörigkeit. Dadurch sind Daten, die beispielsweise für die Gehaltsabrechnung relevant sind, lediglich für Mitarbeiter der Personalabteilung, des Controllings oder der Buchhaltung einsehbar. Kollegen aus anderen Abteilungen bleiben diese Informationen verschlossen. Besitzt ein Mitarbeiter Zugang zu für ihn nicht relevanten Informationen, entsteht ein gefährliches Datenleck. Assistenzen, die oftmals mehrere Abteilungen durchlaufen, sind dafür ein klassisches Beispiel. Bei mangelhaftem Benutzer-Management könnte diese Rolle eine derjenigen sein, die auf die größte Menge an Daten zugreifen kann.

Was für die IT problematisch ist

In der Studie „Insider Threat 2018 Report“ hat die Online-Plattform Cybersecurity gemeinsam mit der Information Security Community auf LinkedIn und mit Unterstützung von Quest Software IT-Verantwortliche zu ihrer Einschätzung hinsichtlich der Gefahren durch Insider befragt. Das Ergebnis: Rund 90 Prozent der Befragten waren sich der Anfälligkeit ihrer Organisationen gegenüber Insider-Attacken durchaus bewusst. Für die IT als problematisch erachteten 37 Prozent der Befragten zu weit gefasste Zugriffsrechte, 36 Prozent nannten den zunehmenden Einsatz immer komplexerer Geräte und 35 Prozent eine immer komplexer werdende IT. Bei der Frage, ob Angriffe aus interner oder externer Quelle wahrscheinlicher sind, gab es eine klare Antwort: Über die Hälfte der Befragten (53 Prozent) gab an, dass die eigenen Mitarbeiter das höhere Risiko darstellen.
Doch wie begegnen IT-Verantwortliche diesen Bedrohungen? Für 64 Prozent der Studienteilnehmer war die rechtzeitige Erkennung ausschlaggebend, 58 Prozent gehen den Weg über das Management und

setzen auf Sensibilisierung und Sanktionen. Analyse und Forensik spielten für 49 Prozent der Befragten eine Rolle. Demnach folgt nur knapp die Hälfte der Befragten einem technischen Ansatz. Dabei wäre gerade eine technische Lösung ideal, um eventuelles Fehlverhalten von Mitarbeitern effizient und rechtzeitig zu erkennen. Doch über die gängigen Bordmittel gestaltet sich dies ziemlich kompliziert.

Passende Werkzeuge wählen

Das Problem bei der Verwaltung von Mitarbeiterrechten in Active Directory und Azure Active Directory: Diese bieten hierfür zwar eigene Werkzeuge an, jedoch nicht in dem Umfang, den sich Administratoren für das umfassende Benutzer-Management wünschen. Außerdem benötigen Administratoren ihrerseits auch Sicherheit. Denn wenn eine verdächtige Veränderung in den Nutzerberechtigungen oder Rollen erfolgt, sollte der IT-Sicherheitsbeauftragte der Behörde nachvollziehen können, von welchem der Administratoren die Änderung im AD oder AAD ausgeht. So entsteht kein Generalverdacht und unbescholtene Mitarbeiter bleiben von falschen Verdächtigungen verschont. Abhilfe schafft eine Lösung zur Verwaltung von AD- und AAD-Konten und -Gruppen. Mit einer Echtzeit-Log-Analyse sind Administratoren in der Lage, durchgeführte Änderungen in großer Menge zu überwachen.
Um Berechtigungen je nach Bedarf setzen und entziehen zu können, müssten Mitarbeiter-Konten rollenbasiert definiert werden können. Lösungen von Drittanbietern sind dazu in der Lage. Außerdem erkennen diese im Gegensatz zu den Bordmitteln eine missbräuchliche Nutzung der Konten und weisen Administratoren sofort darauf hin. Mittels künstlicher Intelligenz und eigens entwickelter Lerntechnologien werden Analysen des Verhaltens sowohl der Nutzer als auch der Entitäten erstellt. So können Risikofaktoren rasch aufgespürt werden. Ferner bieten sie eine IT-Sicherheitssuche mit der IT-Verantwortliche Bedrohungssituationen schnell analysieren und darauf reagieren können. Zu den Hauptfunktionen der Lösung zählen außerdem umfangreiche Auditing-Funktionen, welche sowohl Forensik als auch eine Sicherheitsüberwachung ermöglichen.

Plus an Sicherheit

Letztlich sollten IT-Entscheider an einer effizienten Nutzerverwaltung interessiert sein. Das erspart einerseits Administratoren einiges an Arbeit, sodass sie sich strategischeren Aufgaben zuwenden können. Andererseits führt es zu einem Plus an Sicherheit, denn mögliche Verstöße und riskante Situationen werden sofort erkannt. Damit kann Schaden bereits im Vorfeld abgewendet werden.

()

Dieser Beitrag ist in der Ausgabe April 2019 von Kommune21 im Schwerpunkt IT-Sicherheit erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Authentifizierung, Benutzer-Management