Quest

90%

der Unternehmen fühlen sich verwundbar gegenüber internen Bedrohungen.[1]

Interne Angriffe erkennen, abwehren und alles wiederherstellen

Sie haben eine beeindruckende Außenverteidigung aufgebaut – aber sind Sie auf die Bedrohungen vorbereitet, die sich bereits in Ihrem Netzwerk befinden?

DIE HERAUSFORDERUNG

Offenbar landet jede Woche ein neuer Datensicherheitsverstoß in den Schlagzeilen. Alle machen sich Sorgen über Hackerangriffe, daher investieren Unternehmen meist in eine starke Außenabwehr. Doch in Wahrheit passiert etwa die Hälfte aller Sicherheitsverletzungen innerhalb des Netzwerks,[2] z. B. ein Mitarbeiter, der eine IP stiehlt und zu seinem neuen Job mitnimmt, oder ein ungeschickter Admin, der fatale Konfigurationsfehler einbaut. Häufig ist es ein externer Angreifer, der ein legitimes Konto besetzt hat – Microsoft meldet, dass täglich 95 Mio. AD-Konten das Ziel von Cyberangriffen sind[3] und dass 10 Mio. Azure AD-Anmeldeversuche tatsächlich Cyberangriffe sind.[4]

Aus diesem Grund empfehlen Sicherheitsexperten, immer von Sicherheitsverstößen auszugehen: Stellen Sie sich darauf ein, dass früher oder später jemand in Ihrem Netzwerk herumschnüffelt, um Schaden anzurichten oder wichtige Daten zu stehlen. Selbst die beste Außenabwehr kann nichts tun, um dies zu verhindern, daher ist es wichtig, ein starkes Konzept für die Active Directory-Sicherheit und -Kontrolle zu haben.

AUSWIRKUNGEN AUF IHR UNTERNEHMEN

So können Sie interne Bedrohungen effektiv bekämpfen:

- **Unterstützen Sie die Unternehmensanforderungen durch Implementieren neuer Technologien – aber auf sichere Weise.** Schnellere Verlagerung in die Cloud oder die Ausweitung von BYOD kann zwar die Unternehmensziele unterstützen, aber Sie müssen die Sicherheitsrisiken minimieren.
- **Schützen Sie alle Ihre sensiblen Daten.** Das Datenwachstum ist in den letzten Jahren rasant angestiegen, und vieles davon sind unstrukturierte Daten in Cloud-Repositorys wie SharePoint Online und OneDrive, anstatt weniger Datenbanken in einem gesicherten Rechenzentrum innerhalb eines Gebäudes. Aus diesem Grund ist es sehr viel schwerer zu wissen, was Sie haben und wie Sie es sichern sollen.
- **Halten Sie die zunehmende Anzahl immer strengerer Datenschutzrichtlinien ein.** Vor nicht allzu langer Zeit waren bestimmte Branchen streng reguliert, und eine ISO-Zertifizierung reichte aus. Doch heute reichen Richtlinien wie PCI, GDPR und CCPA in jede Branche hinein. Sie müssen die Compliance nicht nur einführen, sondern auch beibehalten, wenn sich die Vorschriften ändern und weiterentwickeln.
- **Bestehen Sie Audits und vermeiden Sie rufschädigende Schlagzeilen.** Ein Datensicherheitsverstoß kann kostspielig sein – durchschnittlich 3,86 Millionen Dollar.[5] Nicht bestandene Audits ziehen empfindliche Geldstrafen nach sich und können bis zur Geschäftsaufgabe führen. Es liegt an Ihnen, Ihr Unternehmen zu schützen.

Um diese Ziele zu erreichen, müssen Sie die Benutzerberechtigungen unter Kontrolle bringen und ein Auge darauf haben, was jeder tut. Doch systemeigene Tools machen das nicht gerade einfacher – 62 Prozent der Benutzer geben an, dass sie mehr Zugriff haben, als sie benötigen.[6] SIEM bietet Einblicke in Benutzeraktivitäten, ist aber teuer bei der Lizenzierung und schwierig bei derKonfiguration und Anwendung. Außerdem funktioniert dies nur so gut wie die Daten, die Sie einspeisen – und systemeigene Protokolle haben große Lücken und unzureichende Zuverlässigkeit in kritischen Bereichen. Kein Wunder, dass Angreifer bis zu 101 Tage Zeit haben, Schaden anzurichten, bevor sie entdeckt werden.[7]

1 Cybersecurity Insiders, „Insider Threat 2018 Report“ (Bericht zu internen Bedrohungen).

2 ebd.

3 ZDNet, "Active Directory czar rallies industry for better security, identity" (Active Directory Experte fordert Branche zu mehr Sicherheit/Identität auf), 9. Juni 2015.

4 Softpedia News, „Microsoft Sees Over 10 Million Cyberattacks per Day on Its Online Infrastructure“ (Microsoft registriert täglich über 10 Millionen Cyberangriffe auf seine Online-Infrastruktur), 6. Mai 2016.

5 Ponemon Institute: „2018 Cost of Data Breach Study“ (Studie zu den Kosten von Datenpannen).

6 Ponemon Institute, „Closing Security Gaps to Protect Corporate Data: A Study of US and European Organizations“ (Sicherheitslücken schließen, um Unternehmensdaten zu schützen).

7 FireEye, „M-Trends 2018 Report“ (Bericht zu M-Trends 2018).

„Zuvor hatte ich keine Kontrolle über Änderungen an den administrativen Gruppen. Durch Change Auditor kann ich diese kritischen Änderungen ganz leicht überwachen, indem ich einfach in den E-Mail-Ordner schaue.

– Dennis Persson, IT-Systemtechniker, Region Halland

Ihre empfohlene Sicherheits- und Compliance-Lösung

EINE BESSERE METHODE

Was wäre, wenn Sie den Schaden begrenzen können, den ein Benutzer – oder jemand, der dessen Anmeldedaten stiehlt – anrichtet, indem Sie sicherstellen, dass jeder nur die Zugriffsrechte erhält, die er für seine Tätigkeit benötigt? Was, wenn Sie sofort benachrichtigt werden, sobald jemand etwas Riskantes ausführt? Was wäre, wenn Sie eine Ausgangsbasis des regulären Verhaltens für jeden Mitarbeiter erstellen könnten und Abweichungen sofort erkennen? Und was, wenn Sie Bedrohungen sofort erkennen und untersuchen könnten?

DAS GEHT NUR MIT QUEST

Quest ist der empfohlene Anbieter für Sicherheits- und Compliance-Lösungen für alle lokalen oder hybriden Microsoft-Umgebungen. Wir bieten eine vollständige Lösungs-Suite, mit der Sie Ihre interne Umgebung so engmaschig wie Ihre Außengrenze schützen können und kontinuierliche Einhaltung von Vorschriften gewährleisten.

Fehlerkorrektur und Schadensminderung

Verteidigung gegen interne Bedrohungen beginnt mit richtiger Kontrolle. Quest® Lösungen automatisieren Verwaltungsaufgaben, darunter Provisionierung und Deprovisionierung von Benutzern, um Sicherheitslücken zu schließen und die Risiken zu reduzieren. Genehmigungsbasierte Workflows sorgen für zusätzliche Führung und Kontrolle.

Schwachstellen proaktiv identifizieren

IT-Umgebungen sind dynamisch, daher müssen Sie sie regelmäßig auf Schwachstellen überprüfen. Lösungen von Quest bieten automatisierte, konsolidierte Berichterstellung für lokale, hybride und Cloud-basierte Umgebungen, sodass Sie ganz einfach bestimmen können, wer worauf Zugriff hat und wie er an diesen Zugriff gelangt ist. Außerdem können Sie entsprechende Berechtigungen direkt aus den Berichten erstellen. Sie können auch erkennen, wo sich Ihre vertraulichsten Daten befinden und diese schützen, Ihre GPOs überprüfen und sogar verhindern, dass kritische Objekte geändert werden.

Erkennen und über verdächtige Aktivitäten benachrichtigen

Lösungen von Quest ermöglichen Ihnen außerdem, bei aktiven Bedrohungen schneller Alarm zu schlagen, durch Echtzeit-Audits von Benutzer- und Admin-Aktivitäten und Alarme zu Berechtigungseskalationen, unberechtigten Änderungen und anderen verdächtigen Aktivitäten. Erweiterte Benutzerverhaltensanalysen modellieren individuelle Benutzerverhaltensmuster und erkennen ungewöhnliche Aktivitäten. Sie können sogar die Reaktionen automatisieren, wie Blockieren der Aktivität, Deaktivieren des Benutzers oder Umkehren der Änderung.

Schnelle Untersuchung und Wiederherstellung nach Angriffen

Es kostet Unternehmen durchschnittlich 69 Tage, einen Datensicherheitsverstoß aufzuhalten.[8] Quest ermöglicht Ihnen, Sicherheitsverletzungen schnell und einfach auf den Grund zu gehen, durch zentralisierte Datenerfassung und eine Google-artige Such- und Ermittlungs-Engine. Außerdem können Sie eine virtuelle Testumgebung für die DR-Planung erstellen, und den langwierigen systemeigenen AD Strukturwiederherstellungs-Prozess auf einen einfachen GUI-gesteuerten Prozess reduzieren.

Einhaltung von Vorschriften nachweisen und beibehalten

In Kombination ermöglichen diese Funktionen Ihnen, die Compliance mit verschiedenen Vorschriften einzuführen, beizubehalten und nachzuweisen. Darüber hinaus bieten Lösungen von Quest intelligente, skalierbare Protokollkomprimierung, sodass Sie Ihre Audit-Daten kostengünstig über Jahre hinweg speichern können und gleichzeitig sicherstellen , dass sie für Sicherheitsuntersuchungen und Audits zur Verfügung stehen.

8 Ponemon Institute: „2018 Cost of Data Breach Study“ (Studie zu den Kosten von Datenpannen).

Quest
quest.com/de
Sie finden Informationen zu lokalen Niederlassungen auf (quest.com/de-de/locations)

SolutionBrief-MPM_SecurityCompliance-US-DE-WL-38251