So vermeiden Sie gängige Office 365 Sicherheitsrisiken

IST IHR LOKALES AD DAS SCHWÄCHSTE GLIED IN DER KETTE?

Leitfaden für IT-Experten

ZUM SCHUTZ DES LOKALEN ACTIVE DIRECTORY IN EINER HYBRIDUMGEBUNG.

Quest™

EINFÜHRUNG

Office 365 wird jeden Monat von über **60 MILLIONEN BENUTZERN** aktiv genutzt und erfreut sich weiterhin wachsender Beliebtheit. Aus gutem Grund. Die Lösung ermöglicht es Unternehmen, die Infrastruktur und die Kosten im Zusammenhang mit der Lizenzierung und Wartung zu reduzieren und gleichzeitig die Storage-Effizienz zu steigern. Darüber hinaus können die Mitarbeiter mit Office 365 an jedem beliebigen Ort und mit einem beliebigen System arbeiten und steigern damit die Skalierbarkeit und Business Continuity.

Der Wechsel von einem lokalen Active Directory (AD) zu einer Cloud-basierten Version wie dem Azure AD von Office 365 gibt den Entscheidungsträgern jedoch Anlass, über das Thema Sicherheit nachzudenken. Sicherheitsverletzungen haben bekanntermaßen negative Auswirkungen auf den wirtschaftlichen Erfolg und die Reputation eines Unternehmens.

Im Jahr 2016 taxierte das Ponemon Institute die durchschnittlichen Kosten eines Datendiebstahls auf 4 Millionen $ pro Vorfall.

EINFÜHRUNG (Fortsetzung)

Auf welche Punkte sollten sich Ihre Sicherheitsüberlegungen konzentrieren? Microsoft bietet für Office 365 eine Service-Level-Vereinbarung mit einer Systemverfügbarkeit von 99,9 % an. Die Änderungssteuerung, die Zugriffs-Steuerung und die allgemeine Datensicherheit bleiben jedoch in der Verantwortung der Kunden. Ebenfalls zu berücksichtigen ist der zunehmende Einsatz von Hybrid AD Lösungen. Sehen Sie sich die Zahlen an: 75 % der Office 365 Kunden mit mehr als 500 Benutzern synchronisieren ihr lokales AD mit dem Azure AD und erstellen damit eine AD Hybridumgebung.

Dieses Szenario kann zu gefährlichen Sicherheitslücken und erheblichen Ineffizienzen führen. Jede Sicherheitslücke in der Konfiguration des lokalen AD wirkt sich auch auf das Azure AD aus. Organisationen müssen sämtliche Sicherheitsbeschränkungen des nativen AD und des Azure AD berücksichtigen und damit in einem doppelt so großen Bereich dafür sorgen, dass es nicht zu potenziellem Datendiebstahl und zu Bedrohung durch Insider kommt.

EINFÜHRUNG (Fortsetzung)

Schutz der Daten

Der Schutz der in der Hybridumgebung gespeicherten Daten bedeutet, dass die notwendigen Schritte zum Schutz des lokalen AD vor und nach der Migration durchgeführt werden müssen. In diesem E-Book geht es um die richtigen Schritte für die Vorbereitung des lokalen AD auf die Synchronisierung mit dem Azure AD, um den Schutz der Daten während der Migration und um die Best Practices zum Erhalt einer sichereren Hybridumgebung.

VOR DER MIGRATION: DAS EIGENE HAUS IN ORDNUNG BRINGEN

Viele Unternehmen gehen von der Annahme aus, dass Sicherheitsverletzungen und andere Formen von Datenverlust unausweichliche Kosten ihrer Geschäftstätigkeit sind, und setzen auf Strategien zur Minimierung des Risikos. Vor der Migration müssen die im lokalen AD gespeicherten Daten gründlich geprüft und konsolidiert werden, damit veraltete und unwichtige Elemente vorab herausgefiltert werden. Bei diesem Vorgang sollten Sie drei Ziele verfolgen:

- **Verkleinerung des Zielumfangs**: Behalten Sie nur die Daten, die von den Benutzern benötigt werden. Löschen Sie alle Daten, die weder aus geschäftlichen Gründen noch aufgrund von Compliance-Anforderungen noch benötigt werden. Veraltete Daten erfüllen keinen Nutzen. Sie erhöhen lediglich das Sicherheitsrisiko und die Wahrscheinlichkeit der Nichteinhaltung gesetzlicher Vorschriften.
- **Genaue Prüfung der Benutzerkonten**: Löschen Sie doppelte IDs und inaktive Konten, gleichen Sie Benutzernamen und zur Verwendung in Office 365 geplante Domänennamen ab und nehmen Sie Zugriffsberechtigungen zurück, die temporär zum Testen der Office 365 Funktionen gewährt worden waren.
- **Sicherere Zugriffsprotokolle**: Ermitteln Sie leicht zu erratende Kennwörter und fordern Sie die Endbenutzer auf, weniger leicht zu erratende festzulegen. Passen Sie die Administratorrechte an die aktuelle Belegschaft an und bringen Sie den Benutzerdatenzugriff auf den neuesten Stand.

IT Pro Tipp

Das Microsoft Tool IDFix erkennt und beseitigt Objektfehler im lokalen Active Directory und löscht dabei doppelte Konten, bevor die Benutzer, Kontakte und Gruppen mit der Microsoft Office 365 Umgebung synchronisiert werden.

MIGRATION: DIE DATEN IM AUGE BEHALTEN

Sobald überflüssige Daten und doppelte Konten entfernt sind, Zugriffsprobleme gelöst wurden und die Anforderungen von Sicherheitsprotokollen erfüllt sind, können Sie zu Office 365 migrieren. Die Hauptarbeit ist damit schon geleistet. Dennoch muss die Aufmerksamkeit während des gesamten Migrationsprozesses hoch bleiben, damit die Daten unbeschädigt bleiben. IT-Administratoren sollten mit Überprüfung in Echtzeit und Berichten sowie Alarmmeldungen bei Änderungen dafür sorgen, dass die Daten während der Migration sicher bleiben. Auf drei Dinge muss besonders geachtet werden:

- **Zugriff**: Unternehmen nehmen bei einer Migration häufig die Hilfe von externen Beratungsunternehmen in Anspruch. Damit geht unter Umständen einher, dass Außenstehenden ein temporärer Zugriff gewährt wird.
- **Aufbewahrung aus juristischen Gründen**: Mit hoher Wahrscheinlichkeit werden übertragene Daten aus rechtlichen Gründen aufbewahrt, etwa archivierte E-Mails oder Outlook PST-Dateien. Um rechtliche Risiken und Compliance-Risiken so gering wie möglich zu halten, muss eine klare Überwachungskette festgehalten werden.
- **Probleme**: Wenn es im Zusammenhang mit den übertragenen Daten zu Abweichungen vom Normalverhalten kommt – etwa, wenn Unbefugte auf die Daten zugreifen –, muss das Problem sofort gelöst werden. Bei besonders wichtigen Daten gilt stets die Devise: Vorsicht ist besser als Nachsicht!

IT Pro Tipp

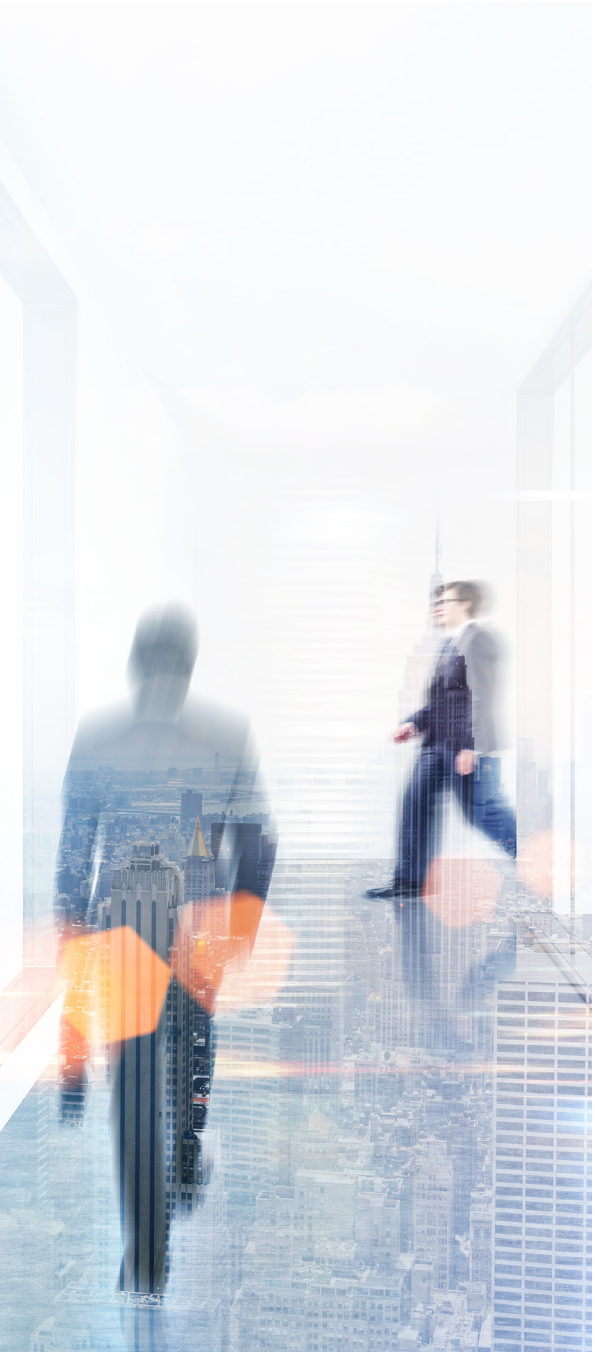
Die Migration zu Office 365 bietet die Gelegenheit, die aktuellen Lösungsanbieter unter die Lupe zu nehmen. Die einzelnen Anbieter müssen Optionen für den Umgang mit vertraulichen Daten während der Migration bieten, damit die Integrität der Daten während des gesamten Lebenszyklus gewährleistet ist. Ist das nicht der Fall, dann handeln die Anbieter nicht in Ihrem Interesse.

Nach der Migration: Dauerhafte Wahrung der Sicherheit

Die Migration zu einer AD Hybridumgebung ist eine einzigartige – wenn auch mühselige – Gelegenheit, die Risiken im Zusammenhang mit überflüssigen Daten, veralteten Berechtigungen und Zugriffsrechten sowie doppelten Benutzerkonten des lokalen AD zu reduzieren. Nachdem Sie "Ihr Haus in Ordnung gebracht haben", können Sie mit den folgenden vier Best Practices nach der Migration eine Lebenszyklusmethode zur Wahrung der neu erstellten organisierten Umgebung umsetzen:

1. Kontinuierliche Beurteilung
2. Erkennung und Benachrichtigung
3. Fehlerkorrektur und Schadensminderung
4. Untersuchung und Wiederherstellung

NACH DER MIGRATION: KONTINUIERLICHE BEURTEILUNG



1 Kontinuierliche Beurteilung

Die Überwachung Ihrer Hybridumgebung ist entscheidend für das Verständnis, wer Zugriff auf Berechtigungen, privilegierte Gruppen, sensible Geschäftsgruppen, Gruppenrichtlinienobjekte (GPO) und Daten zu jeder Zeit hat. Nach einer gründlichen Beurteilung des lokalen AD und des Azure AD müssten die folgenden Punkte einfach zu klären sein:

- Wie groß ist der angriffsgefährdete Bereich? Wie sehen Ihre Sicherheitsrisiken und Ihr Risikoprofil aus?
- Wer kann auf welche vertraulichen Daten zugreifen?
- Wie ist der Zugriff geregelt?
- Wer verfügt über umfangreichere Berechtigungen in AD sowie auf Servern und in SQL Datenbanken?
- Welche Systeme sind anfällig für Sicherheitsbedrohungen?

IT Pro Tipp

Ähnlich wie bei einer Sicherheitskamera, die "nur für den Notfall" rund um die Uhr in Betrieb ist, müssen Sie kontinuierlich prüfen, wer warum Zugriff auf Daten hat, damit vertrauliche Daten nur den Personen zur Verfügung stehen, die tatsächlich Einblick benötigen. Hierbei geht es um Bedenken in Hinblick auf Sicherheit und Compliance.

NACH DER MIGRATION: ERKENNUNG UND BENACHRICHTIGUNG

2 Erkennung und Benachrichtigung

Die Echtzeitermittlung verdächtiger Aktivitäten in der AD Hybridumgebung ist die zentrale Maßnahme zur Minimierung der Auswirkungen eines Insider-Angriffs oder eines Datendiebstahls. Durch proaktive Sicherheitsmaßnahmen müssten Sie in der Lage sein, auf verschiedenen Systemen und Geräten verteilte Daten in Relation zueinander zu setzen und Folgendes schnell zu erkennen:

- Irreguläre Benutzerberechtigungen und -aktivitäten
- Verdächtige Aktivitäten von Benutzerkonten mit zusätzlichen Berechtigungen
- Änderungen, die auf eine erhebliche Bedrohung durch Insider hindeuten
- Schnelle Erkennung von Anzeichen eines Eindringversuchs
- Erkennung eines gerade ablaufenden Brute-Force-Angriffs

Es empfiehlt sich auch, Lösungen zur Optimierung nativer Überprüfungstools in Erwägung zu ziehen. Die Überprüfungstools des nativen AD, des Azure AD und von Office 365 haben keine ausreichende Steuerungs- und Übersichtsfunktionen, wie sie für die Einhaltung der gesetzlichen Vorschriften erforderlich sind. Unter anderem gibt es die folgenden Probleme:

- Schwierigkeiten bei der Konfiguration der Überprüfung
- Posteingänge/Objekte müssen alle einzeln konfiguriert werden
- Überprüfungsrichtlinien können nicht überwacht werden, wenn sie geändert oder von anderen Administratoren deaktiviert werden
- Neue Posteingänge/Objekte können nicht automatisch mit der gewünschten Überprüfungsrichtlinie konfiguriert werden
- Es werden keine Alarmbenachrichtigungen in Echtzeit ausgegeben und die Zahl der Alarmaktionen ist begrenzt
- Die überprüften Daten werden nur für einen begrenzten Zeitraum aufbewahrt und werden danach dauerhaft gelöscht
- Schwierigkeiten bei der Interpretation von Ereignissen

NACH DER MIGRATION: FEHLERKORREKTUR UND SCHADENSMINDERUNG

3 Fehlerkorrektur und Schadensminderung

Wenn eine Sicherheitsverletzung auftritt oder ein Zugriffsfehler geschieht, müssen Sie wissen, wo es Abweichungen von der normalen Funktionsweise gibt, und sofort Korrekturen vornehmen. Falls Sie dank des Berichtsprozesses sämtliche Ereignisse während des gesamten Lebenszyklus im Detail einsehen können, sind Sie in der Lage, schnell zu handeln.

Durch eine automatisierte Sicherheitsrichtlinienerzwingung in der AD Hybridumgebung senken Sie das Risiko menschlicher Fehler und reduzieren die Wahrscheinlichkeit eines erneuten Auftretens. Der Prozess muss für Folgendes sorgen:

- Berechtigte Benutzer erhalten Zugriff; Personen von einer Blacklist erhalten keinen Zugriff.
- Den Benutzern werden nur die Rechte gewährt, die sie für ihre Aufgaben unbedingt benötigen.
- Vertrauliche Ressourcen werden geschützt.
- Eine schnelle manuelle Korrektur nicht erlaubter Änderungen ist möglich.

IT Pro Tipp

Gängige Fehler von Mitarbeitern bergen ein Risiko für die Daten. Bieten Sie umfassende Schulungen für Geschäftsanwender an, in denen die Best Practices für die Weitergabe von Daten innerhalb und außerhalb der Organisation erörtert werden. Die Schulungen müssen im jährlichen Rhythmus daraufhin überprüft werden, ob die Best Practices angesichts technischer Änderungen noch auf dem aktuellen Stand sind.

NACH DER MIGRATION: UNTERSUCHUNG UND WIEDERHERSTELLUNG

4 Untersuchung und Wiederherstellung

Falls ein Sicherheitsvorfall eintritt, müssen Sie schnell die Daten wiederherstellen, um die Ausfallzeit und den Produktivitätsverlust so gering wie möglich zu halten. Hierbei müssen Sie in der Lage sein, die grundlegenden Sicherheitsinformationen auf die Frage hin zu analysieren, wie und warum es zu dem Ereignis kommen konnte. Dieses Verfahren hilft Ihnen bei folgenden Aufgaben:

- Vermeidung einer Wiederholung des Vorfalls
- Entwicklung eines Systems zum Testen des Business Continuity-Plans ohne Wechsel in den Offline-Modus
- Bestimmung der Dauer einer manuellen Wiederherstellung nach einem AD Sicherheitsvorfall
- Festlegen der besten Methode zur Wiederinbetriebnahme des AD

WIE KANN QUEST SOFTWARE SIE UNTERSTÜTZEN?

Die Lösungen von Quest können mit einem erstklassigen Netzwerk aus Experten und Partnern dabei helfen, die Migration, die Sicherheit und die Verwaltung der Office 365, Azure AD und AD Hybridumgebung zu vereinfachen. Quest kann auf zahlreiche Migrations- und Konsolidierungsprojekte und ein umfassendes Lösungsportfolio verweisen und hilft Ihnen bei den folgenden Aufgaben:

- Modernisierung des AD im Hinblick auf die Cloud
- Beschleunigung von Migration und Bereitstellung
- Schutz vor Sicherheitsverletzungen
- Reduzierung von Compliance-Risiken
- Automatisierung von Sicherung und Wiederherstellung
- Maximierung der Investitionsrendite durch Optimierung der Lizenzkosten

Mit nahezu zwei Jahrzehnten Erfahrung bei der Migration von Microsoft Plattformen hilft Quest Organisationen dabei, auf Office 365 und Azure AD umzusteigen, ohne erhebliche Kosten, Risiken, Ängste und Ungewissheiten in Kauf nehmen zu müssen. Erfahren Sie mehr darüber, wie Quest Ihrer **Hybridumgebung zum Erfolg verhelfen kann**.

Quest

Join the Innovation.