DIE 10 WICHTIGSTEN IN AZURE AD UND OFFICE 365 ZU ÜBERWACHENDEN SICHERHEITSEREIGNISSE

Erkennen Sie, wo native Überwachungstools Schwächen haben und was Sie dagegen tun können

Quest

Ist Ihr Unternehmen jetzt, da Sie Anwendungen in der Cloud ausführen, wirklich sicherer?

Effizienter wahrscheinlich. Aber sicherer?

Benutzer können auch in der Cloud weiterhin hochriskante Aktionen ausführen und Anmeldeinformationen können weiterhin kompromittiert werden. Microsoft warnt Admins seit Jahren, dass jeden Tag zig Millionen AD-Konten das Ziel von Cyberangriffen werden.[1] Außerdem ist bei 34 Prozent aller Datenverstöße jemand im Spiel, der sich bereits innerhalb des Netzwerks befindet.[2]

Leider lassen die nativen Überwachungstools von Office 365 und Azure AD hinsichtlich der Überwachung von Rollen, Gruppen, Anwendungen, Freigaben und Postfächern eine Menge zu wünschen übrig. Ihre Suchfunktionen sind eingeschränkt und Überwachungsereignisse werden nur für eine begrenzte Zeit in Protokollen festgehalten.

Office 365 und Azure AD bieten nur eingeschränkte Suchmöglichkeiten und bewahren Überwachungsergebnisse nur für einen begrenzten Zeitraum auf.

Dieses E-Book stellt zehn Sicherheitsereignisse heraus, auf die Administratoren ein strenges Augenmerk haben, um die Sicherheit ihrer Azure AD- und Office 365-Umgebungen zu gewährleisten. Es untersucht, welche Überwachungsinformationen ihnen von nativen Tools und Konsolen bereitgestellt werden, und nennt die häufigsten Fallstricke bei nativen Überwachungsberichten. Schließlich stellt es eine Lösung vor, mit denen sich einige dieser Einschränkungen der nativen Überwachung umgehen lassen.

1 Fontana, John, "Active Directory czar rallies industry for better security, identity" (Active Directory-Experte fordert Branche zu mehr Sicherheit/Identität auf), ZDNet, Juni 2015, https://www.zdnet.com/article/active-directory-czar-rallies-industry-for-better-security-identity/

2 "2019 Data Breach Investigations Report" (Untersuchungsbericht zu Datenverstößen 2019), Verizon, Mai 2019, https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/

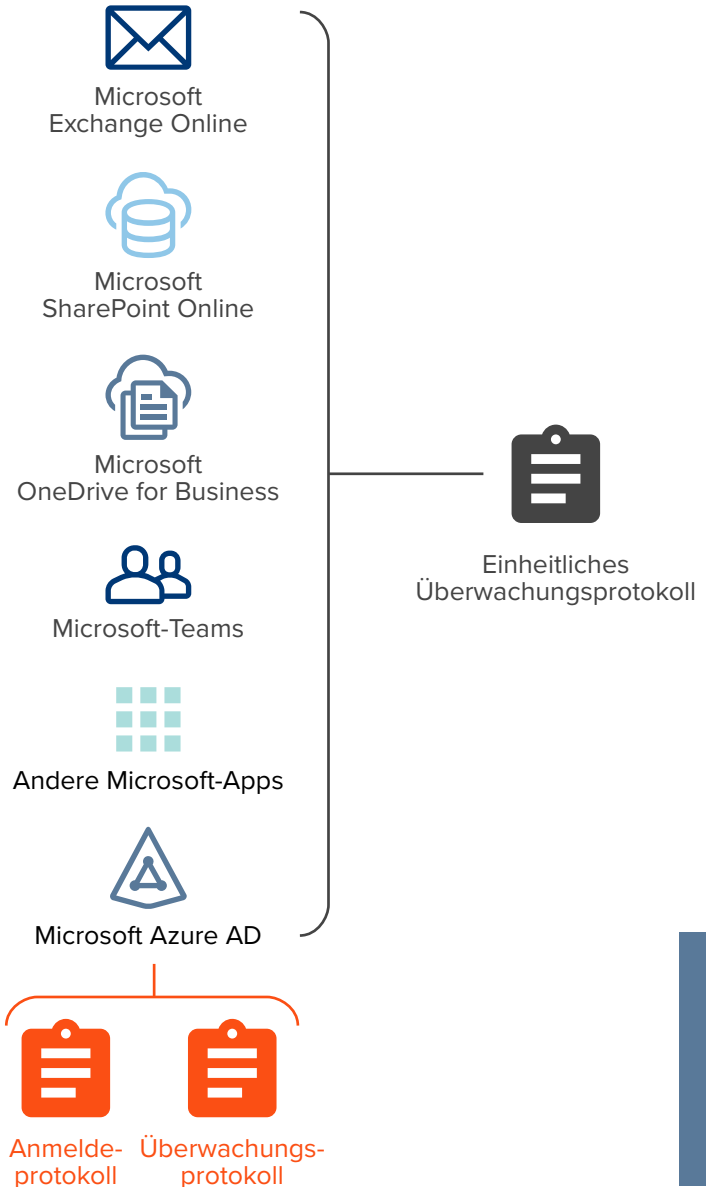


Abbildung 1: Einheitliches Überwachungsprotokoll (für Suchen im Überwachungsprotokoll von Office 365)

Wie funktioniert die Überwachung in Azure und Office 365?

Die Verwaltung und Absicherung einer Cloud-Umgebung beginnt mit der Möglichkeit, die An- und Abmeldeereignisse eines Benutzers verfolgen zu können.

Um diese Informationen vor Ort zu erhalten, müssen Systemadministratoren, die Benutzerverläufe nachverfolgen wollen, verschiedene Protokolle auf den einzelnen Windows Domänencontrollern prüfen und Überwachungsereignisse in den Protokollen verschiedener Server abgleichen.

In der Cloud müssen Administratoren auf ähnliche Weise Abgleiche zwischen zwei Protokollen in Azure AD vornehmen: dem Überwachungsprotokoll mit allen Änderungsereignissen und dem Anmeldeprotokoll mit allen Authentifizierungsereignissen (siehe Abbildung 1). Der Zugriff auf die Protokolle erfolgt entweder über das Azure Portal oder über PowerShell.

Bei Office 365 schreibt jede Anwendung – Exchange Online, SharePoint Online, OneDrive for Business, usw. – in das künftig so bezeichnete einheitliche Überwachungsprotokoll von Office 365, das alle Ereignisse auf Administrator- und Benutzerebene enthält. Das einheitliche Überwachungsprotokoll enthält auch Ereignisse aus dem Überwachungsprotokoll und dem Anmeldeprotokoll von Azure.

Administratoren wissen, welche Arten von Daten in den Protokollen stehen. Doch diese Daten zu extrahieren und sie für die Verwaltung und Absicherung der jeweiligen Umgebung zu verwenden ist eine andere Sache.

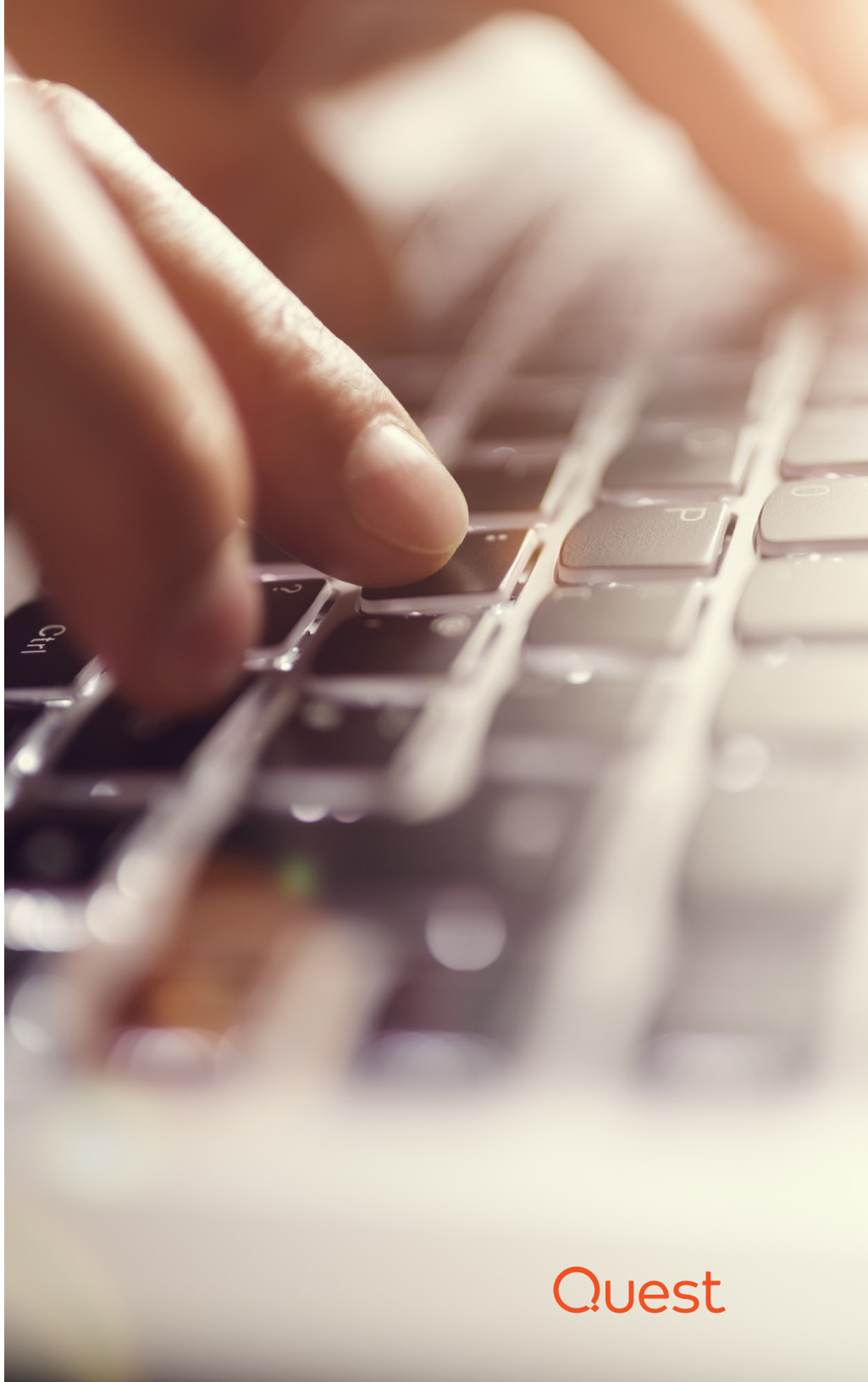
Quest

Die Administratoren wissen, wo sich diese Protokolle befinden, und sie wissen, welche Arten von Daten in diesen Protokollen erfasst werden. Doch diese Daten zu extrahieren und sie für die Verwaltung und Absicherung der jeweiligen Umgebung zu verwenden ist eine andere Sache.

DIE ÜBERWACHUNGSLÜCKEN NATIVER TOOLS

Die Überwachung in Azure und Office 365 unterliegt einer Reihe von Einschränkungen.

- Für Organisationen mit hybriden Umgebungen ist das Durchsuchen von Überwachungsaktivitäten in sowohl lokalen als auch Cloud-Workloads in einer einzigen Ansicht nicht möglich.
- Ebenso müssen die Überwachungsrichtlinien für lokale Workloads getrennt von denen für Cloud-Workloads konfiguriert werden. Außerdem können Überwachungsrichtlinien nicht mehr überwacht werden, wenn sie sich ändern oder von anderen Administratoren deaktiviert werden.
- Bei manchen Einträgen ins Überwachungsprotokoll können 24 oder mehr Stunden vergehen, bis sie ins einheitliche Überwachungsprotokoll aufgenommen werden.
- Der Aufbewahrungszeitraum von Protokollen in Azure ist unterschiedlich, abhängig vom Workload- und Abonnement-Typ. Dies kann eine Einschränkung darstellen, wenn von der IT Vorfälle untersucht werden. Es kann außerdem für manche gesetzliche bzw. behördliche Vorgaben eine zu große Unbekannte sein.
- Je nach Art des Ereignisses und danach, ob es sich vor Ort oder in der Cloud ereignet hat, haben Ereignisse unterschiedliche Formate. Ohne ein standardisiertes Format sind die über native Konsolen sichtbaren Protokolle schwierig zu interpretieren.
- Auf die Überwachungsergebnisse für Azure und Office 365 kann über PowerShell zugegriffen werden. Außerdem bieten sowohl Azure als auch Office 365 ein Web-Portal für den Zugriff auf Überwachungsereignisse. Doch das Portal zeigt nur 15 Ereignisse auf einmal an und die Verarbeitungsverzögerung bedeutet, dass nicht unbedingt alle relevanten Überwachungsereignisse auf einmal da sind.



1. Änderungen – wichtiger Rollen

In einer lokalen Infrastruktur gelten mehrere Gruppen in AD, zum Beispiel Domänenadministratoren, Kontenoperatoren und Serveradministratoren, wegen ihrer erweiterten Rechte als wichtig. In der Cloud gilt dies auch für Rollen im Azure-Mandanten.

Das Problem ist, dass im Laufe der Zeit Benutzer wie Administratoren, Operatoren, Manager und Helpdesk-Techniker allmählich mehr Rechte erwerben als sie eigentlich haben sollten. Daher gehört zu einer sorgfältigen Verwaltung auch die Möglichkeit, Änderungen innerhalb dieser Gruppen und Rollen zu melden und entsprechende Warnungen abzugeben.

Das Problem ist, dass im Laufe der Zeit Benutzer wie Administratoren, Operatoren, Manager und Helpdesk-Techniker allmählich mehr Rechte erwerben als sie eigentlich haben sollten.

ROLLEN IM AZURE-AUDITPROTOKOLL FINDEN

In der Cloud besteht der erste Schritt darin, wichtige Rollen im Azure-Portal zu bestimmen. Im Abschnitt **Überwachungsprotokolle** unter Azure Active Directory gibt eine Suche im Dienst **Kernverzeichnis** und in der Kategorie **RoleManagement** (Rollenverwaltung) alle Rollenänderungen im Mandanten zurück – siehe Abbildung 2. Leider ist dabei eine direkte Suche nach nur den als wichtig geltenden Rollen nicht möglich. Administratoren müssen jedes Überwachungsereignis einzeln prüfen, um zu sehen, welche Rolle geändert wurde.

Quest

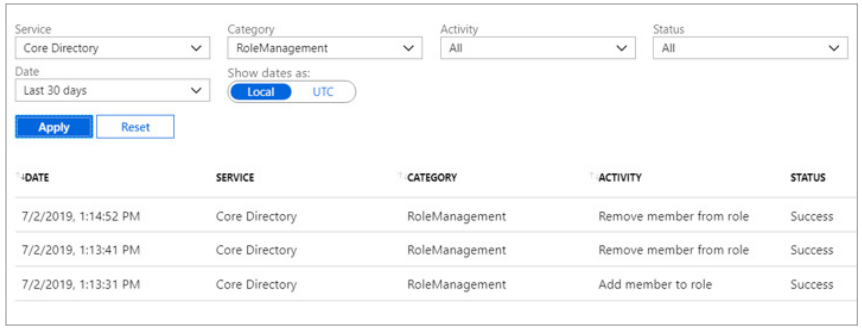


Abbildung 2: Suche nach Rollen im Azure-Portal

Eine weitere Möglichkeit ist der Export der Ergebnisse als Microsoft Excel-Arbeitsblatt zur anschließenden Analyse. Dies erfordert ein Abonnement nicht nur von Office 365, sondern auch von Azure.

ROLLEN IM EINHEITLICHEN AUDITPROTOKOLL FINDEN

Sie können diese Informationen auch über eine Suche im Überwachungsprotokoll über das Office 365 Security & Compliance Center erhalten. (Diese Suchen werden in den Protokollen von Azure AD und in den Protokollen aller Tools von Office 365 vorgenommen, wie oben beschrieben. Sie dauern eventuell länger als eine Suche lediglich im Überwachungsprotokoll von Azure.)

Bei den Suchen werden alle einzelnen Aktivitäten in Verbindung mit der Rollenverwaltung innerhalb eines bestimmten Datumsbereiches zurückgegeben (siehe Abbildung 3), was einen Vorteil gegenüber der Suche im Überwachungsprotokoll von Azure darstellt.

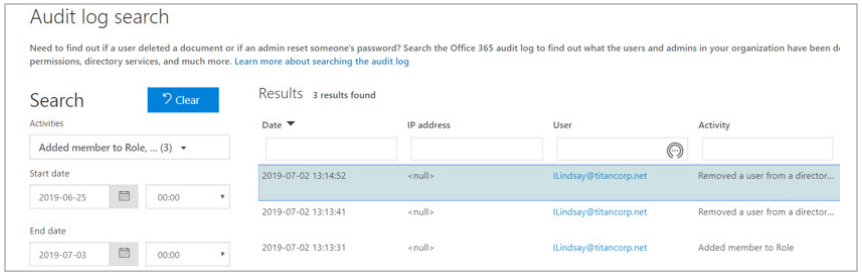


Abbildung 3: Suche im einheitlichen Überwachungsprotokoll

Hier befinden sich jedoch alle Überwachungsdetails in einer einzigen eingebetteten JSON, weshalb alle Details durchsucht werden müssen, wenn man feststellen will, welche Rolle geändert wurde. Die Daten können in ein Tool wie etwa Excel exportiert werden, doch wie in der Spalte AuditData (Überwachungsdaten) in Abbildung 4 erkennbar, erschwert die JSON das Filtern nach den geänderten Rollen.

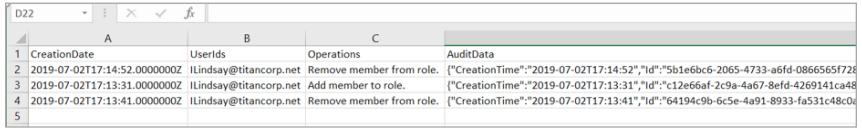


Abbildung 4: Darstellung von Suchergebnissen in Microsoft Excel

2. Änderungen – von Gruppen

Gruppen spielen in AD seit langem die Schlüsselrolle beim Gewähren von Zugriff auf Ressourcen. Das gilt auch in der Cloud, wobei noch einige Komplikationen hinzukommen.

- Azure erlaubt mehr Gruppentypen. Zum Beispiel können Benutzer anhand von Anwendungen wie Outlook oder Teams Gruppen erstellen.
- Office 365-Gruppen, wie etwa die per Teams erstellten, generieren andere Azure-Ressourcen zur Unterstützung der Anwendung.[3]
- Azure AD B2B vereinfacht das Erstellen von Gruppen für die Zusammenarbeit mit Kunden und Lieferanten. Dies birgt aber auch das Risiko, dass ein Benutzer einem Dritten einen nicht gewollten Zugang ermöglicht.

Azure AD B2B vereinfacht das Erstellen von Gruppen für die Zusammenarbeit mit Kunden und Lieferanten. Dies birgt aber auch das Risiko, dass ein Benutzer einem Dritten einen nicht gewollten Zugang ermöglicht.

3 Weitere Informationen hierzu finden Sie im E-Book "Frequently Asked Questions: Office 365 Groups" (Häufige gestellte Fragen: Office 365-Gruppen) https://www.quest.com/whitepaper/frequently-asked-questions-office-365-groups8134485/.

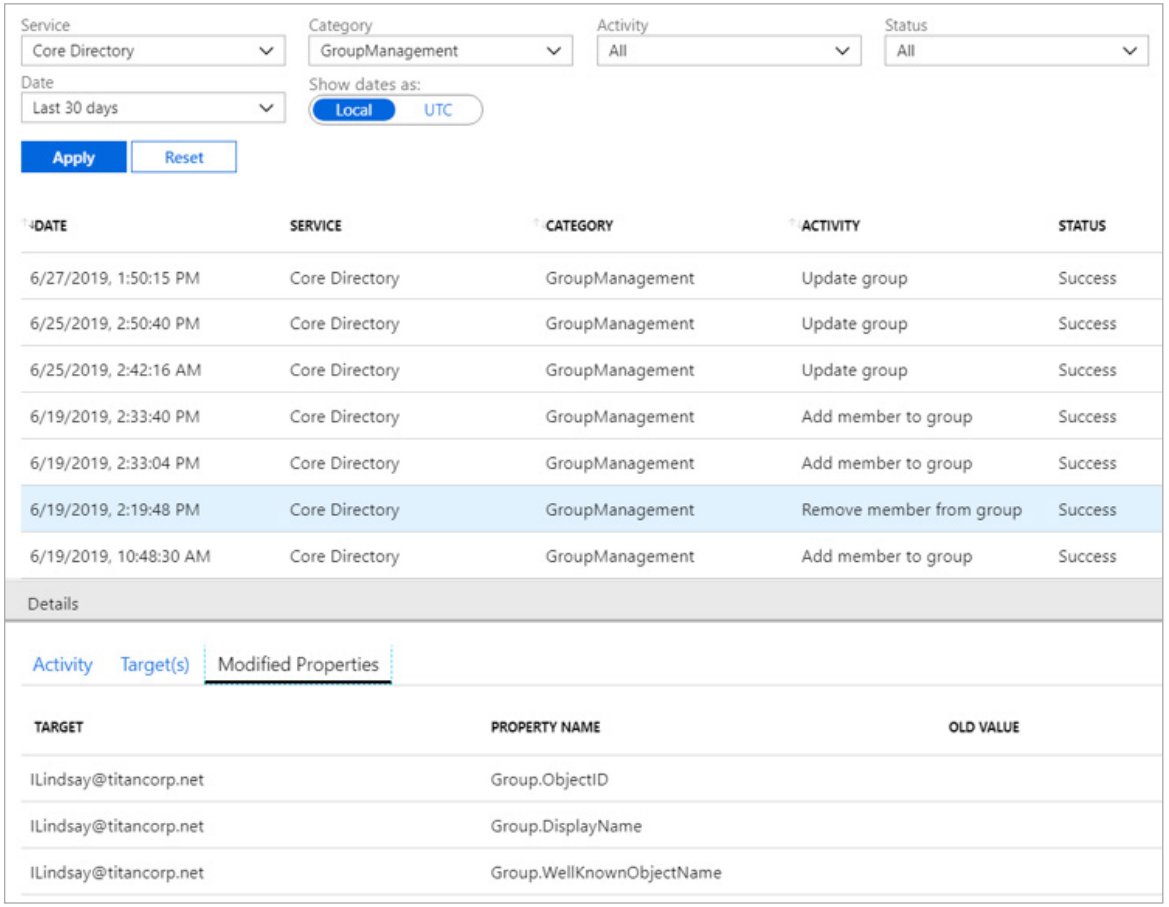


Abbildung 4: Suche nach Gruppen im Azure-Portal

GRUPPEN IM AZURE-AUDITPROTOKOLL FINDEN

Wie bei Rollenänderungen ist das Azure-Portal der logische erste Schritt bei der Kontrolle von Gruppen. Im Abschnitt **Überwachungsprotokolle** unter Azure Active Directory gibt eine Suche im Dienst **Kernverzeichnis** und in der Kategorie **GroupManagement** (Gruppenverwaltung) alle Gruppenänderungen im Mandanten zurück – oben in Abbildung 4). Wiederum ist dabei eine direkte Suche nach nur den für wichtig geltenden Gruppen nicht möglich. Außerdem wird die geänderte Gruppe zunächst nicht angezeigt, sodass Administratoren die Details des Überwachungsereignisses auf der Registerkarte Geänderte Eigenschaften (unten in Abbildung 4) prüfen müssen, um die geänderte Gruppe zu finden.

Eine weitere Möglichkeit ist der Export und die Analyse der Ergebnisse als Microsoft Excel-Arbeitsblatt, was ein Abonnement nicht nur von Office 365, sondern auch von Azure erfordert.

Quest

GRUPPEN IM EINHEITLICHEN AUDITPROTOKOLL FINDEN

Wie bei Rollenänderungen können Sie Informationen über Gruppenänderungen auch über das Office 365 Security & Compliance Center erhalten (siehe Abbildung 2), indem Sie eine Überwachungsprotokollsuche nach allen **Administrationsaktivitäten zu Azure AD-Gruppen durchführen**. Eine Suche nach **Mitglied zu Gruppe hinzugefügt** und **Mitglied aus Gruppe entfernt** (siehe Abbildung 5) ergibt die Änderungen bei der Mitgliedschaft.

Aber mit diesem Verfahren ist immer noch keine Direktsuche nach nur den gewünschten Gruppen möglich. Es ist erforderlich, nach Änderungen aller Gruppen zu suchen und dann die Daten zu untersuchen. Und auch hier befinden sich alle Überwachungsdetails in einer einzigen eingebetteten JSON, weshalb alle Details durchsucht werden müssen, wenn man feststellen will, welche Gruppe geändert wurde. Die Daten können in ein Tool wie etwa Excel exportiert werden, doch erschwert die JSON das Filtern nach den geänderten Gruppen.

Abbildung 5: Geänderte Eigenschaften im einheitlichen Überwachungsprotokoll

Quest

3. Änderungen – von Anwendungen

Azure AD ermöglicht eine vereinfachte Einrichtung zahlreicher Anwendungen und auch den Zugriff auf lokale Anwendungen.

Während SaaS-Anwendungen nicht schwer einzurichten sind, können sie durch falsch durchgeführte Änderungen leicht beschädigt werden. Außerdem verursachen nicht dokumentierte Änderungen durch die Lösung von Problemen Verluste an Zeit und Produktivität und beeinträchtigen die Unternehmensgewinne. Die Nachverfolgbarkeit von Anwendungsänderungen ist daher eine geschäftliche Notwendigkeit.

> Die Nachverfolgbarkeit von Anwendungsänderungen ist eine geschäftliche Notwendigkeit.

ANWENDUNGSÄNDERUNGEN IM AZURE-AUDITPROTOKOLL FINDEN

Im Azure-Portal ist der erste Schritt bei der Suche nach Änderungen einer bestimmten Anwendung der Abschnitt **Überwachungsprotokolle** zur jeweiligen Anwendung in Azure Active Directory. Das Problem ist, dass eine Vielzahl von repetitiven manuellen Schritten erforderlich ist, um Änderungen zu finden.

Quest

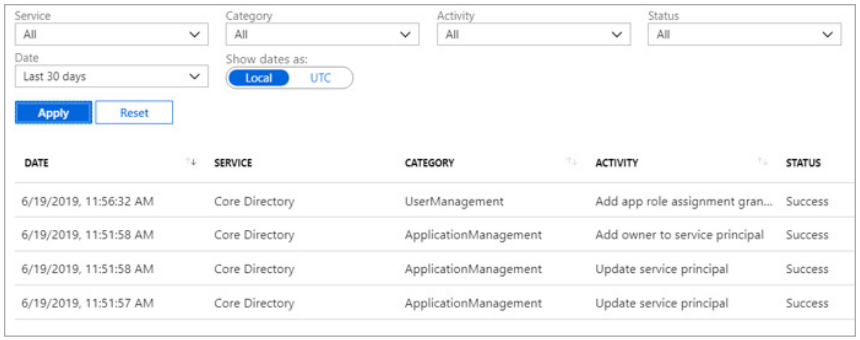


Abbildung 6: Im Azure-Überwachungsprotokoll aufgeführte Anwendungsänderungen

Wie in der Spalte Kategorie von Abbildung 6erkennbar, kommen die Überwachungsereignisse aus **ApplicationManagement** (Anwendungsverwaltung) und **UserManagement** (Benutzerverwaltung).

Bei einer Detailansicht der Kategorie **ApplicationManagement** (Anwendungsverwaltung) ergibt sich die Liste in Abbildung 7.

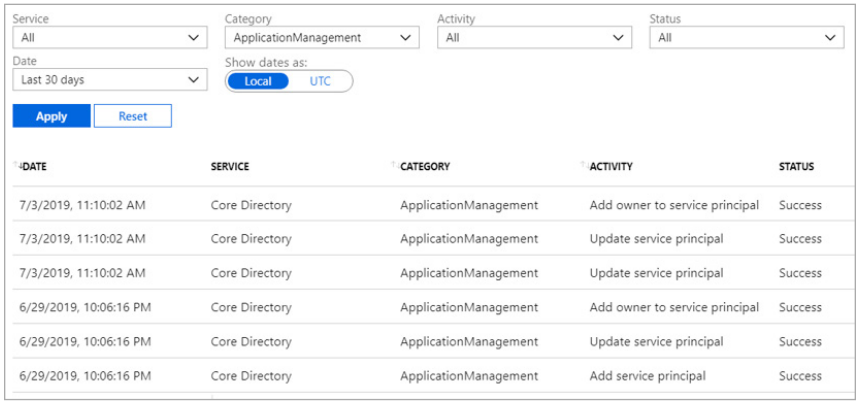


Abbildung 7: Suche in der Kategorie ApplicationManagement (Anwendungsverwaltung)

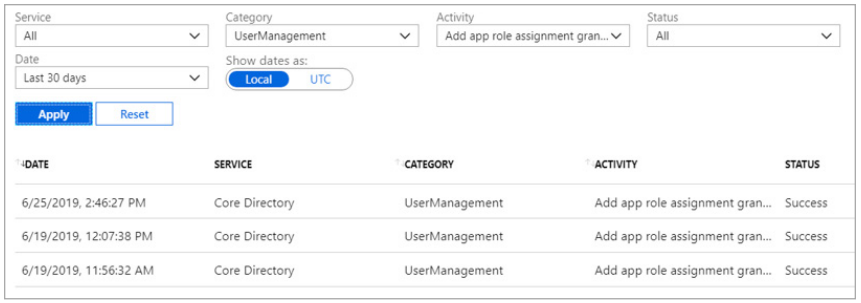


Abbildung 8: Suche in der Kategorie UserManagement (Benutzerverwaltung)

Um genauere Informationen zu den Anwendungsänderungen in Verbindung mit der **UserManagement** (Benutzerverwaltung) zu erhalten, müssen Sie in diese Kategorie wechseln und dann in der Dropdownliste **Activity** (Aktivität) fünf verschiedene Aktivitäten auswählen:

- Einem Benutzer die Erteilung einer Rollenzuweisung hinzufügen (siehe Abbildung 8)
- Ein Anwendungskennwort für einen Benutzer erstellen
- Ein Anwendungskennwort für einen Benutzer löschen
- Eine Anwendungsrollenzuweisung zu einem Benutzer entfernen
- Eine Anwendungszuweisung überprüfen

Es gibt also keine einfache Möglichkeit, nach allen Anwendungsänderungen zu suchen oder eine Liste mit den gewünschten Änderungen zu erstellen.

Quest

4. Ressourcener-stellung

Bei fast jedem Wechsel in die Cloud ergibt sich die Erstellung von Ressourcen, von denen einige (etwa eine Microsoft Teams-Site) wiederum eigene Ressourcen erstellen – etwa Office 365-Gruppen und SharePoint-Ressourcen. Die Nachverfolgbarkeit der Art und Anzahl der erstellten Ressourcen hilft den Administratoren, ihre kosten- und zeitaufwändige Verwaltung zu reduzieren.

ERSTELLTE RESSOURCEN IM AZURE-AUDITPROTOKOLL FINDEN

Beachten Sie die Ressourcen, die mit dem Erstellen von Benutzern und Gruppen in Verbindung stehen. Am besten lassen sich die verbrauchten Ressourcen – Hinzufügungen, Löschungen, Aktualisierungen, Lizenzänderungen, Zuweisungen von Anwendungsrollen – im Überwachungsprotokoll von Azure Active Directory innerhalb des Azure-Portals bestimmen.

Leider lässt sich jeweils immer nur eine Kategorie durchsuchen – **UserManagement** (Benutzerverwaltung) (siehe Abbildung 9), dann **GroupManagement** (Gruppenverwaltung) – Administratoren müssen also jeweils mehrere Abfragen durchführen, um die Informationen zu erhalten.

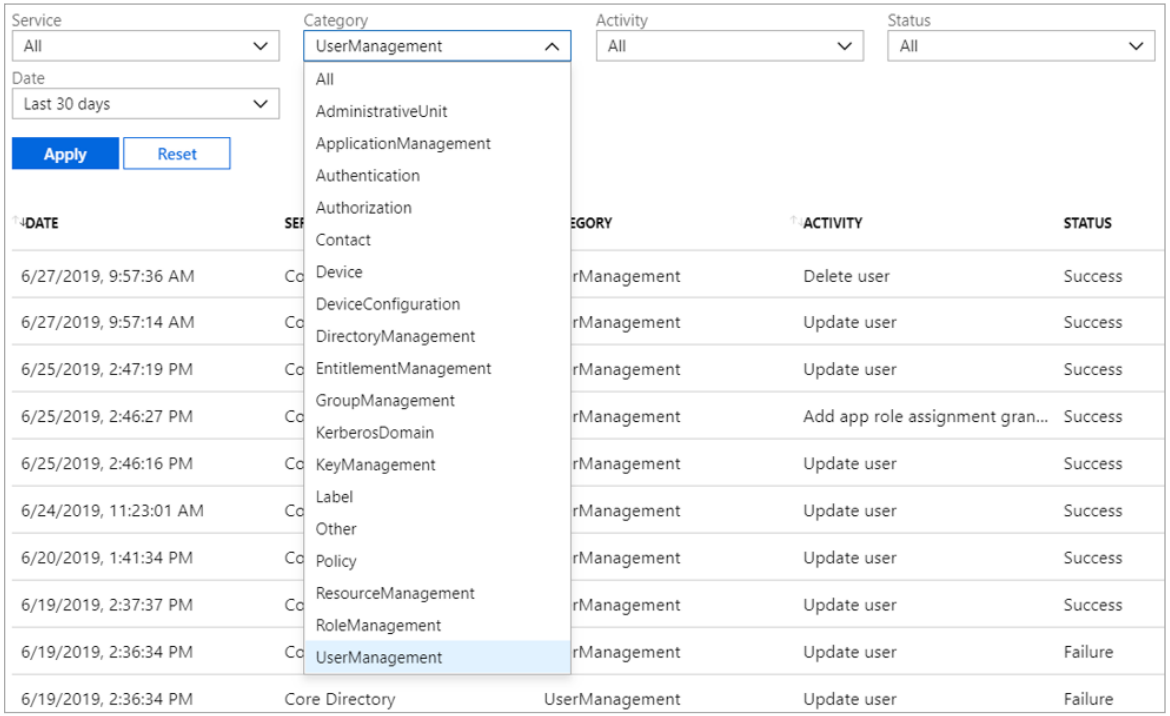


Abbildung 9: Im Azure-Überwachungsprotokoll aufgeführte erstellte Ressourcen

Die Nachverfolgbarkeit der Art und Anzahl der erstellten Ressourcen hilft den Administratoren, ihre kosten- und zeitaufwändige Verwaltung zu reduzieren.

Quest

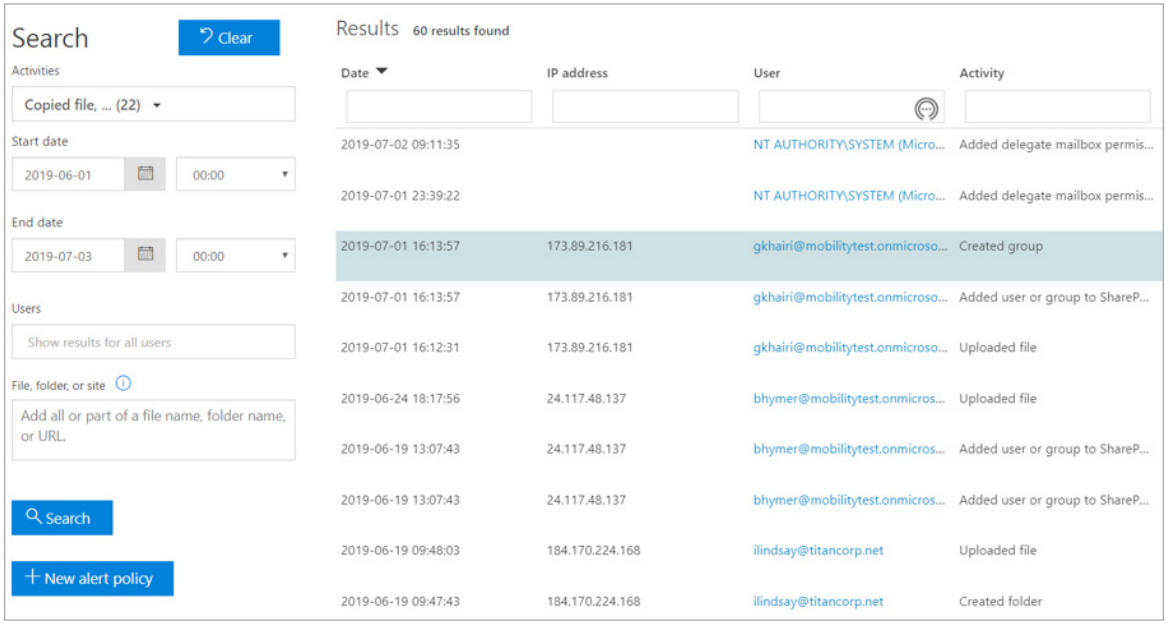


Abbildung 10: Im einheitlichen Überwachungsprotokoll aufgeführte erstellte Ressourcen

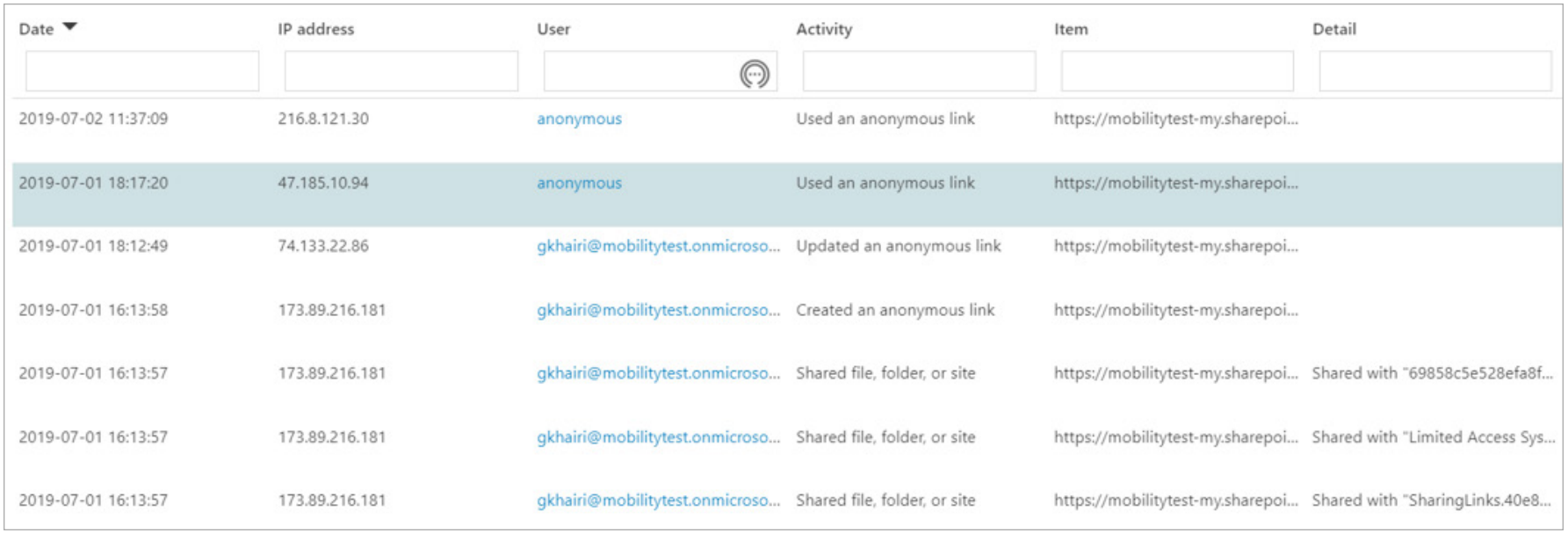
ERSTELLTE RESSOURCEN IM EINHEITLICHEN AUDITPROTOKOLL FINDEN

Die Auditprotokollsuche im Office 365 Security & Compliance-Portal (siehe Abbildung 10) bietet eine Übersicht verschiedener Ressourcen:

- Dateien: kopiert, verschoben, hochgeladen, umbenannt, wiederhergestellt
- Ordner: erstellt, umbenannt, verschoben, wiederhergestellt
- SharePoint-Sites: erstellte Liste, erstelltes Listenelement
- Site-Berechtigungen: hinzugefügter Sitesammlungs-Administrator, zu SharePoint-Gruppe hinzugefügte(r) Benutzer oder Gruppe, erstellte Gruppe
- Exchange: erstelltes Postfachelement, hinzugefügte Postfachberechtigungen
- Sway: erstelltes Sway
- Teams: erstelltes Team, hinzugefügte Registerkarte, hinzugefügter Konnektor, hinzugefügter Kanal, hinzugefügte Mitglieder, hinzugefügter Bot

Ein umfassendes Bild aller dieser Ressourcen zu erhalten erfordert mehrere Abfragen. Und wie bei jeder anderen Suche in Office 365-Überwachungsereignissen befinden sich die Details in der eingebetteten JSON, wodurch sie weniger zugänglich sind als ein einfaches Abfrageergebnis.

Quest



Date	IP address	User	Activity	Item	Detail
2019-07-02 11:37:09	216.8.121.30	anonymous	Used an anonymous link	https://mobilitytest-my.sharepoi...	
2019-07-01 18:17:20	47.185.10.94	anonymous	Used an anonymous link	https://mobilitytest-my.sharepoi...	
2019-07-01 18:12:49	74.133.22.86	gkhairi@mobilitytest.onmicroso...	Updated an anonymous link	https://mobilitytest-my.sharepoi...	
2019-07-01 16:13:58	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Created an anonymous link	https://mobilitytest-my.sharepoi...	
2019-07-01 16:13:57	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Shared file, folder, or site	https://mobilitytest-my.sharepoi...	Shared with "69858c5e528efa8f...
2019-07-01 16:13:57	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Shared file, folder, or site	https://mobilitytest-my.sharepoi...	Shared with "Limited Access Sys...
2019-07-01 16:13:57	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Shared file, folder, or site	https://mobilitytest-my.sharepoi...	Shared with "SharingLinks.40e8...

Abbildung 11: Im einheitlichen Überwachungsprotokoll aufgeführte Freigabeaktivitäten

5 & 6. Freigabe – wichtiger Dateien und anonymer Daten

Ein Wechsel zu SharePoint Online und OneDrive for Business führt zu einer neuen Art von Risiko, insbesondere im Zusammenhang mit Datenfreigaben. Wie bereits erwähnt, können Benutzer unabsichtlich sensible Daten freigeben, indem sie einen B2B-Benutzer aus einem anderem Unternehmen mit aufnehmen, ohne sich dessen bewusst zu sein. Zum Beispiel kann ein unberechtigter Benutzer, der einen Mit-allen-Teilen-Link zu Daten auf OneDrive erhält, anonym auf die Datei zugreifen.

Die Kehrseite erweiterter Freigabemöglichkeiten ist das erhöhte Risiko. Für die IT ist die Möglichkeit zum Generieren von Azure AD-Berichten zu Datenfreigaben noch wichtiger, wenn Unternehmen in die Cloud wechseln. Die Unternehmen haben starke Gründe dafür, die Freigabe bestimmter Dateitypen zu sperren oder streng zu kontrollieren.

Ein unberechtigter Benutzer, der einen Mit-allen-Teilen-Link zu Daten auf OneDrive erhält, kann anonym auf die Datei zugreifen.

FREIGABEN UND ZUGRIFFSANFORDERUNGEN IM EINHEITLICHEN ÜBERWACHUNGSPROTOKOLL FINDEN

Die Suche im Überwachungsprotokoll im Office 365 Security & Compliance-Portal gibt Informationen zu freigegebenen Dateien, Ordnern und Sites zurück. Abbildung 11 zeigt die Ergebnisse einer Suche in **Freigabe- und Zugriffsanforderungs-Aktivitäten.**

Das Problem ist, dass die Abfrage alle Daten für diese Aktivitäten zurückgibt. Eine effektivere und sinnvollere Abfrage würde die Ergebnisse auf die Erweiterungen der freigegebenen Dateien beschränken, etwa CER, DER, CRT, PEM, PFX, P7B, P7C, P12, PPK, PUB, SPC, STL, CRL, SSH, EVT, EXE, BAT, PIF. Oder sie würde die Ergebnisse auf Microsoft Office-Dateierweiterungen begrenzen – PPT, PPTX, XLS, XLSX, DOC, DOCX usw. Mit der Suche im Überwachungsprotokoll ist das nicht möglich.

Eine weitere Möglichkeit ist der Export der Obermenge der Daten aus dem Feld **AuditData** (Überwachungsdaten) im einheitlichen Überwachungsprotokoll in ein Tabellenkalkulationsformat. Dennoch ist immer noch einiges an Datenmanipulationen erforderlich, um die Ergebnisse auf die fraglichen Freigaben einzugrenzen.

Anonyme Freigaben, die von besonderem Interesse sind, sind einfacher abzufragen, indem man das Wort "anonym" im Aktivitätsfilter eingibt – siehe dazu Abbildung 12.

Durch das Setzen des Benutzerfilters auf anonym wird jede Datei zurückgegeben, auf die anonym zugegriffen wurde. Ähnliche Ergebnisse bringt das Filtern der Spalten **UserIds** oder **Vorgänge** in den exportierten Überwachungsvorgängen.

Date	IP address	User	Activity
			anonymous
2019-07-02 11:37:09	216.8.121.30	anonymous	Used an anonymous link
2019-07-01 18:17:20	47.185.10.94	anonymous	Used an anonymous link
2019-07-01 18:12:49	74.133.22.86	gkhairi@mobilitytest.onmicroso...	Updated an anonymous link
2019-07-01 16:13:58	173.89.216.181	gkhairi@mobilitytest.onmicroso...	Created an anonymous link
2019-06-27 11:26:26	24.117.48.137	bhymer@mobilitytest.onmicros...	Updated an anonymous link
2019-06-27 11:26:10	24.117.48.137	bhymer@mobilitytest.onmicros...	Updated an anonymous link
2019-06-19 13:10:43	68.0.116.100	anonymous	Used an anonymous link
2019-06-19 13:08:57	66.210.49.30	anonymous	Used an anonymous link
2019-06-19 13:07:43	24.117.48.137	bhymer@mobilitytest.onmicros...	Used an anonymous link

Abbildung 12: Suchergebnisse zu anonymen Freigabeaktivitäten

7. E-Mail – Weiterleitung von eingehenden Nachrichten

Das Weiterleiten von eingehenden Nachrichten an andere Adressen ist an sich weder gut noch schlecht. Es kann sein, dass Empfänger die Informationen einer Nachricht an externe Lieferanten oder Kunden weitergeben müssen. Berater und Auftragnehmer vor Ort ziehen es vielleicht vor, Nachrichten weiterzuleiten und alle ihre E-Mails in nur einem Konto zu konsolidieren. Benutzer können E-Mails manuell weiterleiten und für ein Postfach kann eine automatische Weiterleitung eingerichtet werden – durch einen Benutzer (per ForwardSMTP) oder durch einen Administrator (per ForwardAlias).

Automatisches Weiterleiten kann absolut harmlos sein, aber clevere Administratoren behalten E-Mail-Weiterleitungen im Auge, um Änderungen zu verhindern, die auf böswillige Aktivitäten hindeuten.

Leider lassen die Änderungsprotokolle in Azure Active Directory und Office 365 eine direkte Suche nach Änderungen von E-Mail-Weiterleitungen nicht zu.

Leider lassen die Änderungsprotokolle in Azure Active Directory und Office 365 eine direkte Suche nach solchen Änderungen nicht zu. Stattdessen müssen zur Erkennung von Änderungen in Exchange Online das gesamte Protokoll exportiert und dann die exportierten Überwachungsereignisse mit **{“name”:”DeliverToMailboxAndForward”,”value”:”True”}** im Parameterfeld der Überwachungsdetails durchsucht werden, damit die gewünschten Ereignisse zurückgegeben werden.

Quest

8. E-Mails – Aktivitäten von Nichtbesitzern

E-Mail-Aktivitäten von Nichtbesitzern sind gang und gäbe in großen Organisationen, wo Angestellte in der Verwaltung Zugriff auf die E-Mail-Konten der leitenden Mitarbeiter haben, für die sie arbeiten, oder wo mehrere Mitarbeiter sich ein Postfach teilen. Wenn ein Konto eines Nichtbesitzers kompromittiert wird, kann ein Angreifer Zugang zu sensiblen Informationen erhalten.

Im Rahmen der Verwaltung von Exchange Online können die Administratoren mit ihren Berechtigungen nahezu jede Aktivität ausführen – zum Beispiel können sie sich selbst das Recht zur Einsicht anderer Postfächer von leitenden Mitarbeitern zuweisen. Jede Organisation vertraut zwar ihren Administratoren hinsichtlich der Verwaltung und Pflege von Systemen, muss aber auch Ausschau nach böswilligen Aktivitäten halten.

Administratoren können mit ihren Berechtigungen nahezu jede Aktivität ausführen – zum Beispiel können sie sich selbst das Recht zur Einsicht anderer Postfächer von leitenden Mitarbeitern zuweisen.

AKTIVITÄTEN VON NICHTBENUTZERN IM EINHEITLICHEN ÜBERWACHUNGSPROTOKOLL FINDEN

Informationen über Aktivitäten von Nichtbenutzern stehen im einheitlichen Überwachungsprotokoll – siehe Abbildung 13. Bei der Suche nach den Aktivitätstypen, welche die meisten Nichtbesitzer in Postfächern ausführen, sollten Sie Folgendes berücksichtigen:

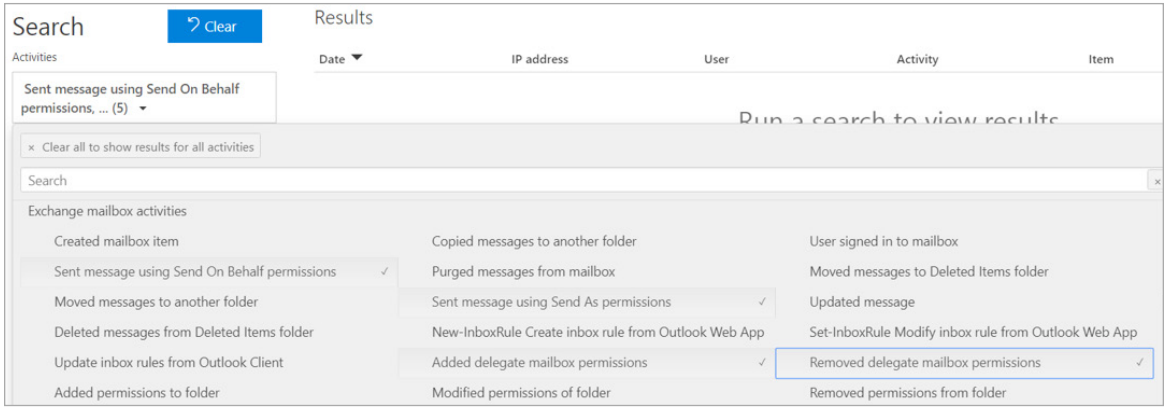


Abbildung 13: Im einheitlichen Überwachungsprotokoll aufgeführte E-Mail-Aktivitäten von Nichtbenutzern

Abbildung 14: Detail der Spalte AuditData (Überwachungsdaten)

- Mit Berechtigung "im Auftrag senden" gesendete Nachricht
- Hinzugefügter oder entfernter Benutzer mit Stellvertretungszugriff auf Kalender/Ordner
- Mit Berechtigung "Senden als" gesendete Nachricht
- Hinzugefügte Stellvertretungs-berechtigung für Postfach
- Entfernte Stellvertretungsberechtigung für Postfach

Beachten Sie jedoch, dass damit Aktivräten wie das Hinzufügen, Löschen und Verschieben von Ordnern und Nachrichten oder Änderungen mancher Berechtigungen – um nur ein paar Beispiele zu nennen – nicht abgedeckt sind. Für eine umfassende Suche müssen alle **Postfachaktivitäten** abgefragt und die Ergebnisse als Tabellenkalkulations-Arbeitsblatt exportiert werden.

Aber der nächste Schritt – das Finden von Überwachungsereignissen, bei denen **LogonUserSid** nicht **MailboxOwnerMasterSid** entspricht – ist arbeitsintensiv, weil die Informationen in der Spalte **AuditData** (Überwachungsdaten) mit dem Rest der Informationen aus dem Ereignis eingebettet sind (siehe Abbildung 14).[4]

4 Siehe auch "Auditing Privileged Operations and Mailbox Access in Office 365 Exchange Online" (Überwachen von privilegierten Vorgängen in Office 365 Exchange Online), https://www.quest.com/docs/auditing-privileged-operations-and-mailbox-access-in-office-365-white-paper-24932.pdf

Quest

9. Administrator-befehlsverlauf

Microsoft bietet Verwaltungstools wie Microsoft Management Console (MMC) für die lokale Verwaltung und Webportale für die Cloud-Verwaltung. Zunehmend betont Microsoft PowerShell als die Hauptadministrationsmethode. Tatsächlich führen viele MMCs PowerShell-Befehle auf der Grundlage von Ereignissen aus, die von der Benutzeroberfläche übergeben wurden; ein typisches Beispiel ist Exchange.

Doch wie wichtig es auch sein mag, sicherzustellen, dass Befehle korrekt ausgeführt werden – das Nachverfolgen des Befehlsverlaufs ist nahezu unmöglich. Zum Beispiel ist es sinnvoll, Anwendungszustimmungsereignisse und alle Änderungen von Richtlinien zum bedingten Zugriff in Azure AD nachzuverfolgen. Ein der falschen Anwendung gewährter Lese-/Schreibzugriff auf Objekte kann Sicherheitsrisiken zur Folge haben.

Das Problem ist, dass es derzeit keine Möglichkeit gibt, aus den Azure- und Office 365-Portalen einen Verlauf ausgeführter Administratorbefehle zu extrahieren.

Es gibt derzeit keine Möglichkeit, aus den Azure- und Office 365-Portalen einen Verlauf ausgeführter Administratorbefehle zu extrahieren.

Quest

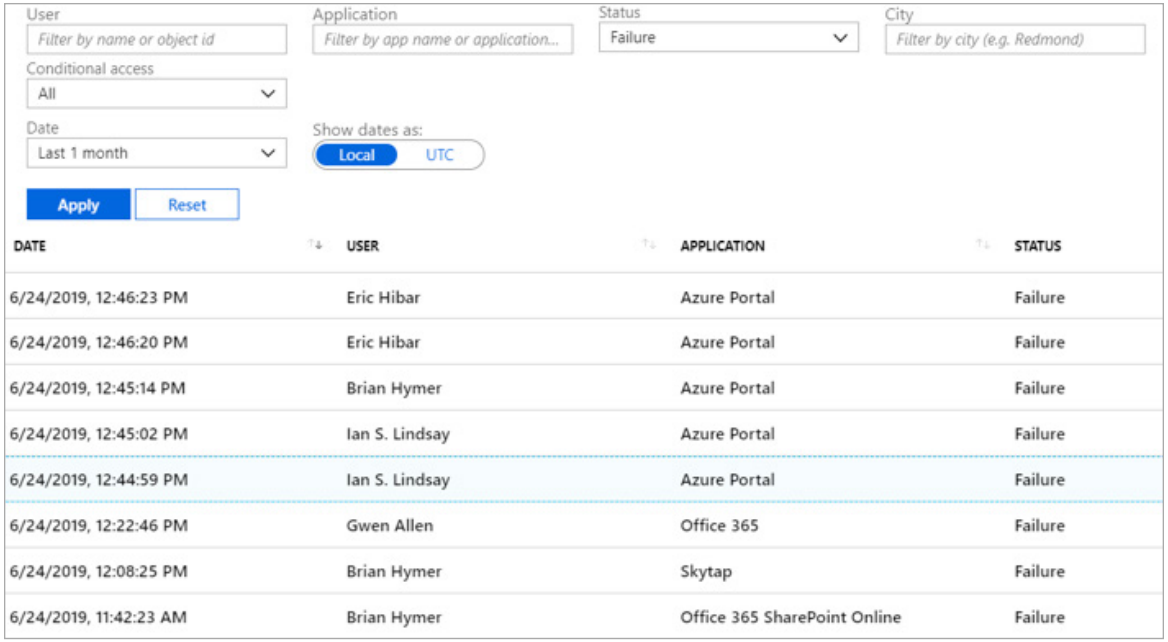


Abbildung 15: Suche nach fehlgeschlagenen Anmeldeversuchen in Azure AD

Wiederholte fehlgeschlagene Anmeldeversuche können auf böswillige Aktivitäten hinweisen – etwa darauf, dass böswillige Akteure versuchen, Kennwörter mit Brachialgewalt einzugeben.

10. Fehlgeschlagene Anmeldeversuche

Ob vor Ort oder in der Cloud – die Nachverfolgung fehlgeschlagener Anmeldeversuche gehört zu den Aufgaben eines Administrators. Gesperrt zu werden, führt zu Frustrationen bei Benutzern, die selten wissen, wie oder warum sie gesperrt wurden. Hybride Anmeldungen über Azure AD verschärfen das Problem noch, indem nun noch eine weitere Quelle hinzukommt, die für die Sperrung verantwortlich sein könnte. Wiederholte fehlgeschlagene Anmeldeversuche können aber auch auf böswillige Aktivitäten hinweisen – etwa darauf, dass böswillige Akteure versuchen, Kennwörter mit Brachialgewalt einzugeben.

Vor Ort werden Informationen zu fehlgeschlagenen Anmeldeversuchen in den Sicherheitsprotokollen aller Domänencontroller gespeichert. In der Cloud befinden sich diese Informationen in den Überwachungsereignissen von allen Azure-Mandanten. Wie in Abbildung 15zu sehen, gibt eine Suche nach **Fehler** im Bildschirm **Anmeldungen** unter **Monitoring** im Azure AD für die einzelnen Mandanten fehlgeschlagene Anmeldeversuche zurück.

Aber das Sammeln aller fehlgeschlagenen Anmeldeversuche ist erst der Anfang. Als Nächstes müssen alle Informationen auf Muster hin untersucht werden – eine Aufgabe, die durch den Mangel an Details in den Suchergebnissen nicht gerade einfacher wird.

Quest

Fazit – On Demand Audit von Quest

Wie wäre es, wenn Sie angesichts der Schwächen der nativen Tools für die Office 365- und Azure-Berichterstellung keine "Blindflüge" mehr nötig hätten?

Die Quest On Demand Audit Hybrid Suite for Office 365 bietet eine zentrale gehostete Ansicht der Benutzeraktivitäten in ganzen hybriden Microsoft-Umgebungen. Sie zeigt alle vorgenommenen Änderungen – egal ob in lokalen AD-, Azure AD- oder Office 365-Workloads wie Exchange Online, SharePoint Online und OneDrive for Business. Anstatt Teileinblicke in Überwachungsprotokolle durchkämmen zu müssen, können Sie jetzt eine reaktionsschnelle Suche in Daten mehrerer Jahre durchführen, um von einem einzelnen Fenster aus Ereignisse zu untersuchen und Berichte zu ihnen zu erstellen. Dank der Verknüpfung mit Power BI von Microsoft können Sie Berichte per interaktiver Datenvisualisierung generieren – siehe Abbildung 16.

Die On Demand Audit Hybrid Suite bietet einen granularen delegierten Zugriff und ermöglicht es Benutzern so, auf sichere Weise die benötigten Erkenntnisse zu gewinnen, ohne dass Konfigurationsänderungen oder die Einrichtung zusätzlicher Infrastruktur erforderlich werden. Mit nur wenigen Klicks können Sie Ihren Sicherheits- und Compliance-Teams, Helpdesk-Mitarbeitern, IT-Verantwortlichen und sogar externen Prüfern sowie Partnerngenau die Berichte an die Hand geben, die sie benötigen – und wirklich nur diese.

Weitere Informationen finden Sie unter quest.com/on-demand.

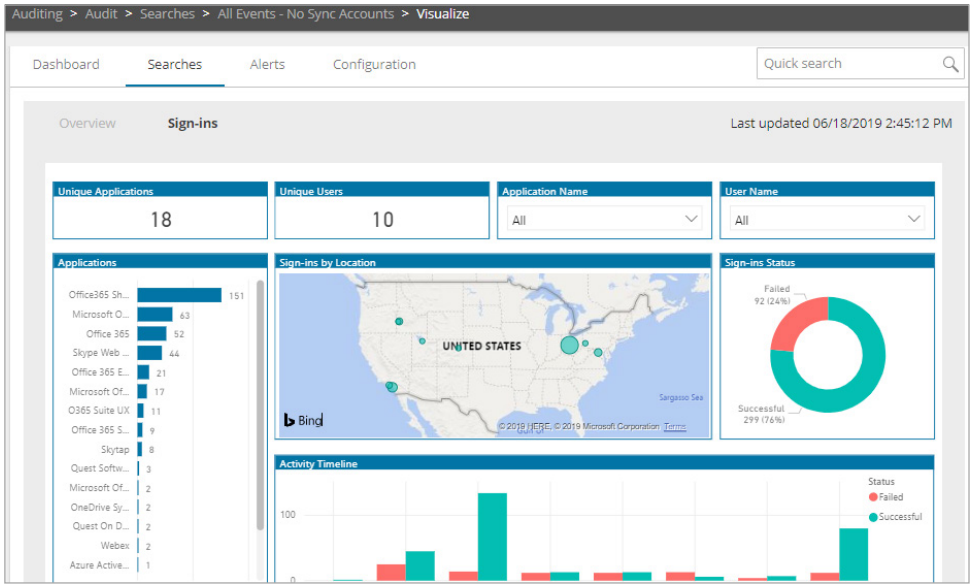


Abbildung 16: On Demand Audit

Die On Demand Audit Hybrid Suite bietet einen granularen delegierten Zugriff und ermöglicht es Benutzern so, auf sichere Weise die benötigten Erkenntnisse zu gewinnen, ohne dass Konfigurationsänderungen oder die Einrichtung zusätzlicher Infrastruktur erforderlich werden.

ÜBER QUEST

Quest liefert Softwarelösungen für die ständig im Wandel befindliche Welt der Unternehmens-IT. Wir helfen, die durch Datenexplosion, Cloud-Erweiterung, Hybrid-Rechenzentren, Sicherheitsbedrohungen und gesetzliche Bestimmungen hervorgerufenen Schwierigkeiten zu verringern. Wir sind der globale Anbieter für 130,000 Unternehmen in 100 Ländern, einschließlich 95 % der Fortune 500 und 90 % der Global 1000. Seit 1987 entwickeln wir eine Palette von Lösungen, die aktuell Datenbankverwaltung, Datensicherung, Identitäts- und Zugriffsverwaltung, Microsoft-Plattformverwaltung sowie die Verwaltung vereinheitlichter Endgeräte umfasst. Mit Quest investieren Unternehmen weniger Zeit in die IT-Administration und haben mehr Zeit für geschäftliche Innovationen. Weitere Informationen finden Sie auf www.quest.com.

Sollten Sie Fragen hinsichtlich der potenziellen Nutzung des Materials haben, wenden Sie sich bitte an:
www.quest.com/de-de/company/contact-us.aspx

Ebook-SecurityEventsToMonitor-US-GM-DE-WL-40070

Quest