Osterman Research

WHITEPAPER

Whitepaper von Osterman Research
Veröffentlich im **Februar 2019**
Gesponsert von **Cyren**

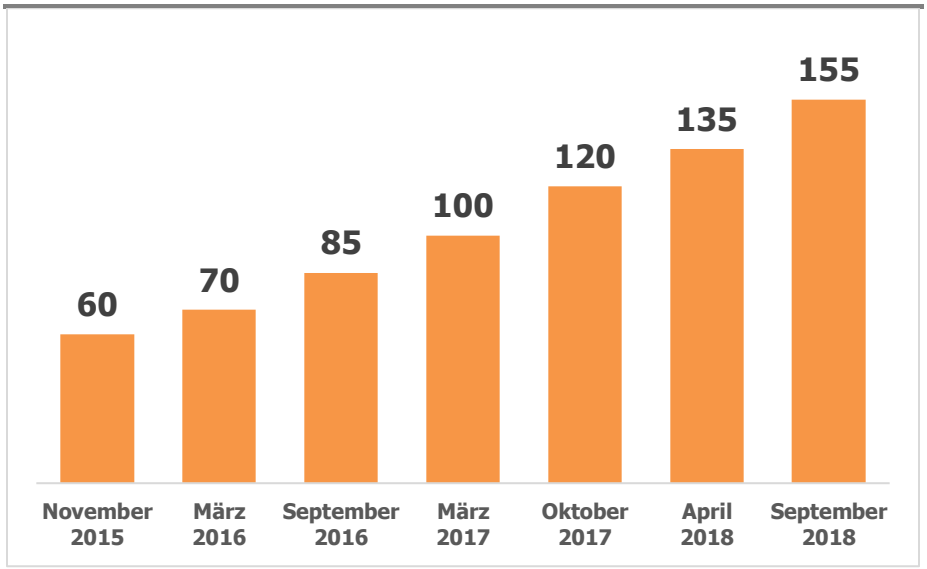
Warum Ihr Unternehmen Drittanbieter-Lösungen für Office 365 benötigt

Inhaltsverzeichnis

Kurzfassung

Office 365 ist eine robuste Kommunikations- und Kooperationsplattform mit umfassendem Funktionsangebot. Microsoft hat eine ganze Reihe von Features und Funktionen zusammengestellt, die eine breite Palette von Unternehmensanforderungen in Bezug auf E-Mail, Voice, Desktop-Produktivität und Kooperation bedienen und sich als extrem erfolgreich erwiesen haben, was durch das signifikante Wachstum der Benutzerzahlen der Plattform belegt wird (siehe Abbildung 1).

Abbildung 1
Microsoft Office 365-Abonnentenzahlen in Unternehmen
Millionen Abonnenten



Quelle: Microsoft

Microsoft ist bemüht, einen umfassenden Cloud-Service zur Unterstützung von Produktivität, Sicherheit, Compliance und Datenschutz bereitzustellen. Das ist eine wichtige Aufgabe mit vielen Komplexitäten und Abhängigkeiten, die genau gegeneinander abgewogen werden müssen. Wie jede große Plattform mit einem umfassenden und vielfältigen Benutzerstamm bietet auch diese in vielen Bereichen Kapazitäten, die „gut genug" sind, aber nicht die Tiefe an Funktionen oder spezialisierten Lösungen bereitstellen, die Kunden mit mehr als nur grundlegendem Bedarf und entsprechenden Anforderungen verlangen. Dabei kann es sich um Unternehmen handeln, die tiefgehendere Funktionen oder eine bessere Performance in spezifischen Bereichen benötigen, aber auch um Unternehmen mit ganz speziellen Anforderungen wie z. B. Firmen in regulierten Sektoren oder solche, die neuen sektorübergreifenden Datenschutzgesetzen unterliegen und ihre rechtlichen, regulatorischen oder Best Practices-Anforderungen erfüllen müssen.

Die engen Verknüpfungen zwischen mehreren Diensten schaffen auch einzelne Fehlerstellen (Points of Failure), wie z. B. die Ausfälle bei der Multifaktor-Authentifizierung im November 2018. Darüber hinaus hat Osterman Research festgestellt, dass viele Drittanbieterlösungen oft eine bessere Alternative für einige der nativen Funktionen der Office 365-Plattform darstellen.

Kurz gesagt: Osterman Research zufolge sind Office 365 und Exchange Online wichtige und fähige Plattformen, die für die Nutzung jeder Organisation ernsthaft in Erwägung gezogen werden sollten. Entscheidungsträger sollten aber auch mit ihren eigenen Anforderungen vertraut sein und alle Feature- oder Leistungslücken in Bezug auf die Plattform identifizieren. Office 365 bietet eine solide Grundlage; dennoch sollten

Microsoft hat eine ganze Reihe von Features und Funktionen zusammengestellt, die eine breite Palette von Unternehmensanforderungen in Bezug auf E-Mail, Voice, Desktop-Produktivität und Kooperation bedienen.

Organisationen Drittanbieter-Lösungen nutzen um mehr Sicherheit, ein besseres Content-Management, bessere Verschlüsselung und andere Kapazitäten bereitzustellen. Wir möchten betonen, dass die Nutzung von Drittanbieter-Lösungen oft die Verwendung weniger kostspieliger Office 365-Abonnements ermöglicht, wodurch die Gesamtbetriebskosten im Vergleich zur Nutzung teurerer Office 365-Abonnements gesenkt werden können.

WICHTIGSTE ERGEBNISSE

- **Viele Organisationen werden Drittanbieter-Lösungen implementieren**
  Unser Recherchen haben ergeben, dass fast ein Drittel der Organisationen, die Office 365 implementieren, vorhaben, eine Kombination kostengünstigerer Abonnements in Verbindung mit Drittanbieter-Lösungen zu verwenden, die Sicherheits-, Archivierungs- oder andere Funktionen als die in der Office 365-Plattform nativ vorhandenen bieten. Ganze 37 Prozent des typischen Office 365-Budgets im Jahr 2019 werden für Sicherheits-, Archivierungs- und andere Lösungen von Drittanbietern ausgegeben werden.

- **E-Mail ist ein fundamentaler Antriebsfaktor für Office 365**
  Es überrascht nicht, dass die überwältigende Mehrheit (93 Prozent) der Organisationen E-Mail als wichtige oder äußerst wichtige Funktion in Office 365 angeben. Im Gegensatz dazu werden andere Office 365-Funktionen als nicht so wichtig angesehen, darunter Skype for Business (54 Prozent), SharePoint Online (47 Prozent) und OneDrive for Business (45 Prozent).

- **Einschränkungen bei zielgerichteten und fortgeschrittenen Bedrohungen**
  Die meisten Organisationen, die Office 365 abonnieren, verlassen sich auf die grundlegenden, nativen Sicherheitsfunktionen der Plattform. Organisationen, die eine Version mit Microsoft Advanced Threat Protection (ATP) verwenden, genießen ein besseres Sicherheitsangebot, das aber auch bestimmte Beschränkungen aufweist, wie etwa die Tatsache, dass nicht alle Inhalte in SharePoint Online, OneDrive for Business und Microsoft Teams aktiv an Ort und Stelle auf eingebettete Bedrohungen gescannt werden. Das Scannen von E-Mail-Anhängen auf unbekannte Bedrohungen mit ATP kann außerdem die Lieferung verzögern und sich negativ auf die Benutzerproduktivität auswirken. Office 365-Abonnenten, die an ATP interessiert sind, sollten Sicherheitsoptionen von spezialisierten Sicherheitsanbietern in Betracht ziehen.

- **Keine konsolidierte Bedrohungsansicht**
  Die verschiedenen Bedrohungsberichte im Security & Compliance Center bieten keine konsolidierte Ansicht, wie sie von manchen Drittanbieter-Sicherheitslösungen bereitgestellt wird.

- **Hybrides Management muss in Erwägung gezogen werden**
  Viele Organisationen steigen bei ihrer Migration zu Office 365 auf hybride Umgebungen um. Unseren Recherchen zufolge planen 13 Prozent der Organisationen, langfristig eine hybride Konfiguration zu pflegen, wobei größere Organisationen mit höherer Wahrscheinlichkeit hybride Bereitstellungen nutzen werden als kleinere. Hybride Umgebungen sind mit zusätzlichen und manchmal unvorhergesehenen Management- und Administrations-Komplexitäten verbunden. Wenn diese nicht korrekt durch neue Prozesse und Drittanbieter-Tools angesprochen werden, besteht dabei das Risiko, dass viele der Vorteile einer Office 365-Implementierung nicht zum Tragen kommen.

- **Manche Anwendungen werden weiterhin nur in der Cloud vorhanden sein**
  Während Benutzer, die weiterhin lokal arbeiten, eine höhere Parität mit den verfügbaren Optionen in der Cloud genießen (insbesondere mit dem Office 2019-Release[i]), gibt es weiterhin bestimmte Anwendungen wie z. B. Workplace Analytics[ii], die nur als Cloud-Service bereitgestellt werden. Für Organisationen, die

… 37 Prozent des typischen Office 365-Budgets im Jahr 2019 werden für Sicherheits-, Archivierungs- und andere Lösungen an Drittanbietern ausgegeben.

solche Lösungen nutzen möchten, ist ein gewisser Grad an Integration unabdingbar.

- **Beschränkungen bei der Verhinderung der Nachahmung**
  Die Nachahmung in Form von nachgestellten, gefälschten und ähnlich klingenden Domains ist hinsichtlich Phishing- und Spear-Phishing-Versuchen ein schwerwiegendes Problem. Office 365 benachrichtigt den Empfänger einer verdächtigen Nachricht, die den Domainnamen der Organisation per Spoofing nachstellt, doch muss die Übereinstimmung exakt sein: Office 365 kann nicht mit Fast-Übereinstimmungen umgehen, bei denen Domains verwendet werden, die ähnlich wie die Domain der Organisation aussehen oder klingen.

- **Beschränkungen bei der Verhinderung von Datenverlust (Data Loss Prevention, DLP)**
  DLP-Richtlinien in Office 365 werden nach Priorität oder Ausführungsreihenfolge evaluiert. Die erste Regel, die mit dem identifizierten Inhalt einer E-Mail-Nachricht oder einem Dokument übereinstimmt, wird angewendet. Es gibt keine Möglichkeit, die Priorität oder Ausführungsreihenfolge von DLP-Richtlinien festzulegen, außer der zeitlichen Reihenfolge ihrer Erstellung.

- **Probleme mit Verschlüsselungsfunktionen**
  Microsoft stützt sich für Empfänger ohne Outlook auf linkbasierte Nachrichten. Das bedeutet, dass verschlüsselte Nachrichten wie Phishing-Nachrichten aussehen können, insbesondere weil sie dann zur Anmeldung nach einem Benutzernamen und Passwort fragen. Weil ein häufiger Phishing-Vektor darin besteht, einen gefälschten Office 365-Anmeldebildschirm zu verwenden, bearbeiten argwöhnische Benutzer verschlüsselte Nachrichten evtl. nicht weiter, oder manche Benutzer werden der Phishing-Gefahr gegenüber desensibilisiert und öffnen versehentlich eine Phishing-Nachricht und gewähren den Zugriff auf ihre Anmeldedaten.

- **Beschränkungen bei der eDiscovery**
  Es besteht kein Workflow oder Projekt-Tracking eines eDiscovery-Falles in Office 365. Suchen nach Schlüsselwörtern, die in der Content-Suche beginnen, können nicht in einen eDiscovery-Fall importiert werden.

- **Eine beschränkte Anzahl von Dateitypen wird indexiert**
  Bei einer eDiscovery-Suche und Durchführung einer frühzeitigen Fallbewertung (Early Case Assessment) wird jede Datei, die nicht in den 58 von Microsoft unterstützten Dateitypen enthalten ist, als nicht verarbeitet gekennzeichnet.

- **Keine langfristige Speicherung von Audit-Protokollen zu Compliance-Zwecken**
  Das Office 365-Überwachungsprotokoll speichert Audit-Ereignisse nur 90 Tage lang. Es gibt keine Möglichkeit, diesen Zeitraum zu verlängern (obwohl Office 365 Enterprise Plan E5 Speicherung für ein Jahr ermöglicht). Dies hat signifikante Auswirkungen auf Organisationen, die rechtlichen oder regulatorischen Aufbewahrungsanforderungen entsprechen müssen, die eine Aufbewahrung dieser Daten für viel längere Zeiträume vorschreiben.

ÜBER DIESES WHITEPAPER

Dieses Whitepaper wurde von Cyren gesponsert. Am Ende des Dokuments finden Sie Informationen über das Unternehmen. Dieses Whitepaper enthält Daten aus einer detaillierten Studie von Osterman Research im Oktober 2018. Wir befragten 124 Organisationen mit einer mittleren Mitarbeiterzahl von 1400 Beschäftigten, um uns über die Probleme zu informieren, die beim Management von Office 365 auftreten, um zu erfahren, welche weiteren Funktionen sie gerne haben würden und um andere relevante Informationen über die Office 365-Umgebungen der Befragten einzuholen. Die Daten aus der Studie werden in einem separaten Umfragebericht veröffentlicht werden, der auf die Veröffentlichung dieses Whitepapers folgen wird.

Dieses Whitepaper enthält Daten aus einer detaillierten Studie von Osterman Research im Oktober 2018.

Erwägungen zur Office 365-Sicherheit

ZUGRIFF AUF DIE SPAM-QUARANTÄNE

Hinsichtlich der Spam-Quarantäne von Office 365 sollten Entscheidungsträger bei der Beurteilung von Drittanbieter-Lösungen, die bessere Sicherheitsfunktionen bereitstellen könnten, einige Probleme in Erwägung ziehen.

- In der Spam-Quarantäne können nur 500 Nachrichten angezeigt werden und es gibt keine Möglichkeit, mehr anzuzeigen. Ein Endbenutzer kann versuchen, seine Liste von Spam-Nachrichten zu filtern, um legitime Geschäfts-E-Mails zu finden, die als Spam erfasst wurden, doch die Benutzeroberfläche und das Nachrichtenlimit machen dies zu einem sehr umständlichen Vorgang. Es ist wahrscheinlicher, dass legitime Nachrichten, die als Spam gekennzeichnet wurden, unentdeckt bleiben.

- Ein Administrator kann nicht alle Nachrichten in Quarantäne in einer einzigen Liste einsehen. Die Liste muss in die unterschiedlichen Nachrichtentypen unterteilt werden, die sich in Quarantäne befinden, wie Spam, Malware, Phishing und Massen-E-Mail.

- Spam-Nachrichten in Quarantäne werden maximal 30 Tage lang aufbewahrt (im September 2018 eingeführt). Danach werden sie gelöscht und sind nicht wieder abrufbar. Microsoft zufolge beträgt die Standarddauer ebenfalls 30 Tage, doch eine Überprüfung mehrerer Mandanten ergab, dass die Standardeinstellung immer noch 15 Tage beträgt. Ein Administrator kann diese maximale Dauer verringern, aber nicht erhöhen. Wird eine legitime Geschäfts-E-Mail fälschlicherweise als Spam gekennzeichnet und prüft der Endbenutzer den Quarantäne-Inhalt mehr als 30 Tage lang nicht, gehen diese Nachrichten unwiederbringlich verloren.

- Es ist nicht möglich, unterschiedliche Richtlinien zum Umgang mit verschiedenen Arten von Spam- und Massen-E-Mail wie Spam-, Malware-, Phishing- und Massen-E-Mail-Übereinstimmungen zu erstellen. Eine Anti-Spam-Richtlinie kann anhand des Empfängers differenziert werden, aber nicht basierend auf dem Nachrichtentyp.

- Wird ein X-Header in einer Richtlinie hinzugefügt, muss er für jede Art von Spam- oder Massen-Nachricht gleich sein. Es gibt keine Option, den X-Header basierend auf Typ (z. B. Spam, Malware, Phishing oder Massen-E-Mail) zu differenzieren.

- Während Spam nur eine Kategorie von Nachrichten ist, die unter Quarantäne gestellt werden könnten, legt eine einzige Einstellung unter Anti-Spam den Quarantänezeitraum für alle Kategorien von Nachrichten fest, die unter Quarantäne gestellt werden. Es gibt keine Option, unterschiedliche Aufbewahrungsdauern für verschiedene Arten von unter Quarantäne gestellten Nachrichten festzulegen.

- Für Endbenutzer gibt es keinen Workflow zur Freigabe von Spam aus der Quarantäne. Möchte ein Benutzer eine Nachricht in seinen Posteingang verlegen, wird die Aktion direkt ausgeführt. Es besteht keine Möglichkeit, eine Nachricht zur Freigabe zu kennzeichnen und zu ermöglichen, dass ein Administrator die Nachricht prüft, bevor sie freigegeben wird.

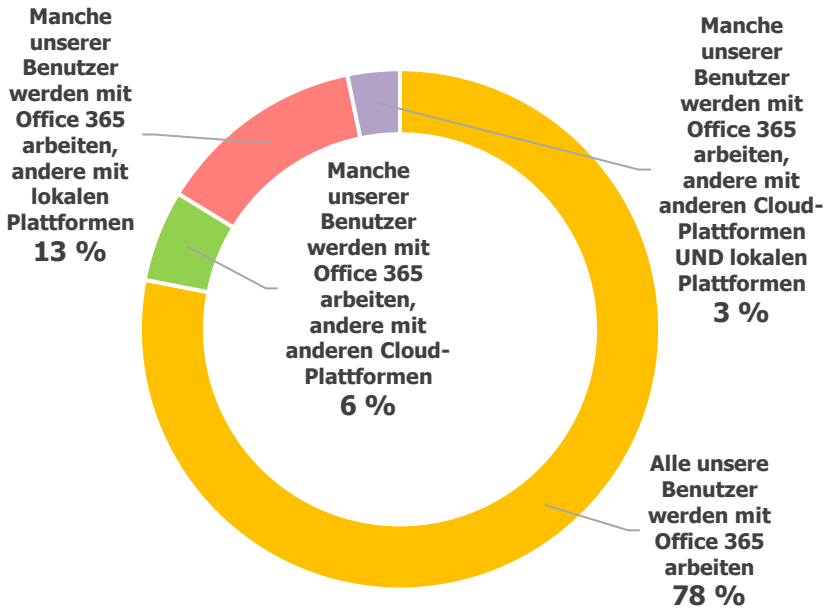
- Nachrichten von blockierten Absendern werden weiterhin in die Spam-Quarantäne aufgenommen, anstatt sofort gelöscht zu werden. Dadurch kann die Quarantäne mit möglichen Spam-Nachrichten wie auch E-Mail von blockierten Absendern überfüllt werden.

Es ist nicht möglich, unterschiedliche Richtlinien zum Umgang mit verschiedenen Arten von Spam- und Massen-E-Mail zu erstellen.

- Die Quarantäne gibt Benutzern keine Informationen, wie viele ähnliche Nachrichten mit einer ähnlichen Betreffzeile und einem ähnlichen Absender von anderen Personen in der Organisation empfangen wurden. Eine höhere Zahl würde bedeuten, dass die Wahrscheinlichkeit groß ist, dass es sich bei der Nachricht um einen Spam- oder Phishing-Versucht handelt. Solche Daten, die Benutzern helfen, informierte Entscheidungen darüber zu treffen, ob eine Nachricht eine böswillige Intention hat, werden aber nicht angeboten.

- Die neue Funktion „Automatische Bereinigung zur Nullstunde" (Zero-Hour Auto Purge, ZAP) von Microsoft unterstützt die Spam-Quarantäne nicht. Während es automatisch Nachrichten, die fälschlicherweise als Spam oder sauber klassifiziert wurden, neu klassifizieren und Nachrichten zwischen dem Posteingang des Benutzers und dem Junkmail-Ordner verschieben kann, kann es Nachrichten nicht automatisch zwischen der Spam-Quarantäne und dem Posteingang verschieben. Darüber hinaus funktioniert ZAP nur mit Exchange Online-Posteingängen, was für Organisationen mit einer hybriden Umgebung ein Problem darstellt. Dies ist ein besonders wichtiges Thema angesichts der vielen Organisationen, die Office 365 mit vielen anderen Lösungen zusammen verwenden, wie in Abbildung 2 dargestellt.

Abbildung 2
Bereitstellungsumgebungen nach der vollständigen Bereitstellung von Office 365



Quelle: Osterman Research, Inc.

- Ein Administrator kann Spam-Benachrichtigungen für Endbenutzer aktivieren. Dabei handelt es sich um eine einmal am Tag versandte E-Mail-Nachricht, in der Nachrichten an den Benutzer aufgeführt werden, die unter Quarantäne stehen und als Spam klassifiziert wurden. Dabei muss aber Folgendes hervorgehoben werden:
    - Die Benachrichtigung erfolgt nur für Spam. Andere an die Quarantäne gesandte Nachrichten sind ausgeschlossen.
    - Benachrichtigungen in Bezug auf Spam-Nachrichten unter Quarantäne können nur an alle oder niemanden gesendet werden. Office 365 bietet keine Feineinstellungsmöglichkeit, um vorzugeben, welche Benutzer Benachrichtigungen erhalten sollten und welche nicht.
    - Es ist nicht möglich, die Tageszeit für die Lieferung der Spam-Benachrichtigungs-Nachricht aus der Quarantäne festzulegen. Es kann außer der Tageseinheit auch nicht festgelegt werden, wie oft dies erfolgen soll (z. B. gibt es keine Möglichkeit, eine Benachrichtigung nach jeweils einer bestimmten Anzahl von Stunden anzufordern). Wenn die Spam-Benachrichtigung mitten in der Nacht ankommt, könnten Benutzer sie verpassen.
    - Nachrichten können zwar über die Benachrichtigungs-E-Mail aus der Quarantäne entlassen werden, doch muss jede einzeln bearbeitet werden. Dadurch muss für jede Nachricht, die der Benutzer an seinen Posteingang freigeben möchte, ein neues Browser-Fenster geöffnet werden.
    - Die Benachrichtigungs-E-Mail listet unter Quarantäne gestellte Nachrichten für alle Benutzer in koordinierter Weltzeit (UTC) auf. Dabei werden die jeweiligen Datums-/Zeitzoneneinstellungen des Benutzers außer Acht gelassen und

Nachrichten können zwar über die Benachrichtigungs-E-Mail aus der Quarantäne freigegeben werden, doch muss jede einzelne Nachricht einzeln bearbeitet werden.

Nachrichten in einem zwar technisch korrekten, aber für den Benutzer irrelevanten Format angezeigt.

- Es ist nicht möglich, eine Spam-Benachrichtigungs-E-Mail zu generieren, sobald eine neue Spam-Nachricht eingeht. Benachrichtigungen werden einmal täglich gesendet, nicht häufiger.

ZIELGERICHTETE UND FORTGESCHRITTENE BEDROHUNGEN

Advanced Threat Protection (ATP), ein in Office 365 Plan E5 angebotener (oder als Standalone-Service verfügbarer) Sicherheits-Service, bietet Schutz vor fortgeschrittenen Bedrohungen, die in URLs, Phishing-Nachrichten und Dokumenten verborgen sind. ATP ist mit zusätzlichen Kosten verbunden, doch müssen einige Probleme in Erwägung gezogen werden. Während Organisationen, die bestimmten Anwendungsfällen entsprechen, evtl. einen besseren Schutz durch ATP erhalten als durch den Standard-Office 365-Service, bedeutet die Risikolandschaft, dass Organisationen Drittanbieter-Angebote nutzen sollten, die einen besseren Schutz bieten. Wir sind sogar einigen Organisationen mit Office 365 ATP begegnet, die zusätzlich eine weitere Sicherheitsebene darüber implementiert haben. Einige zu erwägende Probleme:

- ATP bietet die Möglichkeit, Anhänge und Links auf unbekannte oder neue Bedrohungen zu prüfen. Zuvor muss ein Administrator aber Richtlinien zur Anwendung von sicheren Links und sicheren Anlagen für Einzelpersonen, Gruppen und die gesamte Organisation einrichten. Standardmäßig ist kein Bedrohungsschutz aktiviert, und selbst wenn er aktiviert ist, müssen Benutzer eine Verbindung mit Office 365 herstellen, damit sichere Links und sichere Anlagen funktionieren.

- Während ATP jetzt auch ruhende Inhalte in SharePoint Online, OneDrive for Business und Microsoft Teams unterstützt, werden nicht alle Inhalte aktiv vor Ort auf eingebettete Bedrohungen gescannt. Dateien werden basierend auf verschiedenen Auswahlkriterien gescannt, wie z. B. Freigabeaktivitäten, Gastzugriff und andere Bedrohungssignale. ATP kann kein Echtzeit-Dashboard bösartiger Dateien in Office 365 bereitstellen. Darüber hinaus speichern viele Organisationen Inhalte in anderen SaaS-Anwendungen wie z. B. Box oder G-Suite, die nicht von ATP abgedeckt werden.

- Das Scannen von E-Mail-Anhängen auf unbekannte Bedrohungen mit ATP kann die Lieferung verzögern und die Benutzerproduktivität beeinträchtigen. Als ATP eingeführt wurde, beschwerten sich manche Kunden darüber, dass E-Mails durchschnittlich um 10 bis 15 Minuten und zu Spitzenzeiten um bis zu drei bis fünf Stunden verzögert wurden. Ende 2017 gab Microsoft die durchschnittliche Latenz mit ca. 60 Sekunden an. Manche Kunden beschwerten sich aber auch 2018 noch über nicht akzeptable durchschnittliche Verarbeitungszeiten. Microsoft führte verschiedene Gegenmaßnahmen ein, um die wahrgenommene Verzögerung zu reduzieren, darunter dynamische Zustellung und Dokumentvorschau. Letztere ermöglicht dem Benutzer, eine sichere Version des Dokuments anzuzeigen und zu bearbeiten, während das vollständige Dokument noch gescannt wird. Wir werden sehen, wie lange diese durch die Dokumentvorschau bereitgestellten sicheren Versionen sicher bleiben, während Bedrohungsakteure verbissen daran arbeiten, die neuen Kontrollen zu umgehen.

- Die Funktion „Sichere Links" prüft eine URL zum Zeitpunk des Klicks auf Übereinstimmung mit bekannten Blacklists bösartiger Websites. Sie evaluiert aber nicht auf das Vorhandensein von Bedrohungen an der Ziel-URL zum Zeitpunkt des Klicks. Mit „Sichere Links" kann ein Benutzer trotzdem auf eine bösartige Website weitergeleitet werden, wenn diese Website nicht auf der Blacklist bekannter bösartiger Websites aufgeführt ist. Manche Drittanbieterlösungen bieten dynamische URL-Scans, um verdächtige URLs vor dem Klicken zu prüfen.

Wir sind einigen Organisationen mit Office 365 ATP begegnet, die zusätzlich eine weitere Sicherheitsebene darüber implementiert haben.

- „Sichere Links" evaluiert URLs zum Zeitpunkt des Klicks. Wird ein Link aber als bösartig eingeschätzt, wenn ein Benutzer darauf klickt, gibt es keine Möglichkeit, dass Advanced Threat Protection Instanzen der gleichen E-Mail aus den Postfächern anderer Benutzer entfernt.

- Microsoft ergänzt sein Prüfrepertoire derzeit durch teilweises Hinzufügen von Detonationsfunktionen mithilfe einer Integration mit „Sichere Anlagen". Über eine URL in einer E-Mail oder einem Dokument verlinkte Dokumente werden jetzt zum Zeitpunkt des Klicks in sicheren Anlagen „gesprengt" (unterstützte Dateitypen: Word, Excel, PowerPoint und auch PDF). Microsoft wird in Zukunft voraussichtlich tatsächliche Detonationsfunktionen für alle URLs nutzen, doch ist dies noch nicht verfügbar. Andere Best-in-Class-Lösungen bieten vollständige URL-Detonation, um Angriffe ohne Malware wie z. B. Anmeldedaten-Phishing zu erfassen.

- „Sichere Links" ist in erster Linie auf Benutzer von Word, Excel und PowerPoint ausgelegt, so lange sie Office 365 ProPlus-Versionen auf Windows- oder iOS- und Android-Geräten verwenden und beim Office 365-Dienst angemeldet sind. Es prüft Links in anderen Dateiformaten nicht und auch nicht, wenn der Benutzer an einem Mac arbeitet. Wie bereits erwähnt wird der Link nur mit kontrollierten Blacklists verglichen, anstatt dass geprüft wird, ob der Link wirklich derzeit für den Endbenutzer sicher ist.

- „Sichere Anlagen" nutzt virtuelles Sandboxing, um auf die Anwesenheit von Malware und anderen Bedrohungen in einem Dokument zu prüfen. Dieser Ansatz ist bei bestimmten Arten von Bedrohungen wie z. B. passwortgeschützter Ransomware, die mit dem Passwort im Text der E-Mail geschickt wird, nicht effektiv. Konkurrenzangebote gehen über das Sandboxing auf virtuellen Maschinen hinaus und umfassen die nächste Generation fortgeschrittener Detektionsmechanismen, wie z. B. Deep Content Inspection, rekursive Analyse eingebetteter Dokumente, Evaluierung von Bedrohungen unterhalb der Anwendungs- und Betriebssystemebene, Identifizierung von derzeit inaktivem Programmcode, Sandboxing auf kontrollierten physischen Maschinen zur Analyse auf Malware, die virtuelle Sandboxing-Detonation umgeht, und mehr. Unserer Einschätzung zufolge ist Microsoft ATP nicht so gut wie einige fortgeschrittene Best-in-Class-Drittanbieter-Produkte auf dem Markt.

- „Sichere Links" wurde bereits getäuscht, sodass bösartige Links für Endbenutzer genehmigt wurden. Die Punycode-Einschränkung wurde z. B. ausgenutzt, um die Prüfung auf bösartige Links mit der sicheren ASCII-Version zu täuschen und dann die Unicode-Version des Links zu verwenden, um den Browser auf eine bösartige Website zu führen. Bösartige Akteure evaluieren ständig, wie die Kontrollen von Microsoft umgangen werden können.

- Weder „Sichere Anlagen" noch „Sichere Links" sind gegen CEO-Betrug/Business Email Compromise (BEC)-Nachrichten effektiv, die in der Regel keine gefährlichen Links oder Anlagen enthalten. Manche Drittanbieter-Lösungen bieten dedizierten Schutz vor diesen Bedrohungen einschließlich Schutz vor Homograph-Domain-Attacken.

- Kunden können den Status von ATP in Office 365 überwachen. Die Integrität des Dienstes ist mit der anderer Dienste gebündelt. Das bedeutet, dass Kunden die zusätzlichen Kosten für den Service bezahlen, ohne zu wissen, ob er derzeit von einem Ausfall oder einer anderen Beeinträchtigung betroffen ist oder einfach nicht funktioniert.

- ATP weist keine hybriden Fähigkeiten auf. Das bedeutet, dass Kunden mit z. B. lokalem Exchange oder SharePoint ein zweites, separates Bedrohungsschutz-Angebot nutzen müssen. ATP geht nur mit bestimmten Office 365-Workloads unter spezifischen Bedingungen um und lässt Daten und Systeme außerhalb von Office 365 ganz außer Acht. Dies kann bei vielen Kunden, die eine hybride Umgebung betreiben, zu Problemen führen.

Office 365 bietet zwei Engines zur Verhinderung von Datenverlust (Data Loss Prevention, DLP)-Engines.

- Microsoft zufolge identifizieren ATP und Exchange Online Protection (EOP) jeden Monat zusammen lediglich 600 Millionen E-Mails von 400 Milliarden Nachrichten als bösartig. Das bedeutet eine Erfassungsrate für bösartige E-Mails von 0,15 Prozent. Das ist signifikant niedriger als die z. B. von FireEye erzielte Erfassungsrate für bösartige E-Mail-Nachrichten von 0,99[iii].

FUNKTIONEN ZUR VERHINDERUNG VON DATENVERLUST

Office 365 bietet zwei Engines für die Verhinderung von Datenverlust (Data Loss Prevention, DLP): den älteren, etablierten Ansatz, der vom lokalen Exchange Server übernommen wurde, und den neueren, vereinheitlichten Ansatz über das Security & Compliance Center. Beide bieten DLP-Funktionen, haben aber eine ganze Reihe von Schwächen.

DLP in Exchange Online:

- DLP-Regeln unterstützen nur grundlegende Aktionen, wenn sensible Informationen identifiziert werden. Manche der Funktionen von Konkurrenzangeboten können sie nicht bieten. Während DLP-Regeln z. B. verhindern können, dass eine Nachricht und bestimmte Arten von Dokumenten Exchange Online durchlaufen, wenn sensible Informationen identifiziert werden, ist es nicht möglich, die sensiblen Informationen in der Nachricht oder im Dokument zurückzurufen oder zu bereinigen bzw. sie ggf. automatisch zu verschlüsseln. Die Nachricht wird weiter bis zum Empfänger geleitet. Es ist ein menschlicher Eingriff durch den Originalabsender oder einen Administrator erforderlich, um das identifizierte Problem zu beheben. Dadurch kann ein Backlog von Nachrichten auflaufen, die einer manuellen Beurteilung und Intervention bedürfen.

- Eine grundlegende Funktion für digitale Fingerabdrücke ist verfügbar. Hierbei kann eine Vorlage eines sensiblen Dokuments gespeichert und für die Identifizierung zukünftiger Dokumente verwendet werden, welche die gleiche Struktur aufweisen. Es werden aber nur völlige Übereinstimmungen mit dem spezifischen Dokumentenfingerabdruck identifiziert. Teilweise Übereinstimmungen bleiben unentdeckt.

- Eine Nachricht, die eine DLP-Regel verletzt, kann nur zur Prüfung oder Genehmigung an eine ausdrücklich genannte Person oder den Vorgesetzten des Absenders weitergeleitet werden. Es gibt keine nuancierten Optionen wie z. B. die Durchführung einer Verzeichnissuche anhand des Namens des Absenders oder einer Abteilung, um den lokalen Compliance-Beauftragten zu finden, oder die Weiterleitung von Nachrichten in die Quarantäne, wo sie von einer Administratorengruppe analysiert werden.

- DLP-Regeln erfassen sensible Informationen nur in einem spezifischen Satz von 58 Dateitypen, wobei die verschiedenen Varianten von Word, Excel, PowerPoint und andere Office-Dateiformate viel stärker berücksichtigt werden. Nicht unterstützte Dateitypen, die sensible Informationen enthalten, werden nicht erfasst, wenn sie über Exchange Online gesendet werden. In Bildern verborgene sensible Informationen werden ebenfalls nicht erfasst, weil Office 365 keine OCR an gescannten Dokumenten oder Screenshots vornehmen kann.

DLP in Office 365 Security & Compliance Center ist der neuere, derzeit noch in der Reifephase befindliche Ansatz, der über mehrere Office 365-Workloads (aber nicht alle) hinweg funktioniert und die Kapazitäten des Exchange Online-Ansatzes übertrifft. Kunden sollten dabei folgende Probleme in Erwägung ziehen:

- DLP-Richtlinien können E-Mail-Sendefehler, wie z. B. das Adressieren von E-Mail an den falschen Empfänger, aufgrund von Fehlern bei der automatischen Vervollständigung nicht proaktiv mit Flags kennzeichnen. Office 365 analysiert die normalen Sendemuster eines Benutzer nicht, um vor falsch adressierten Nachrichten zu warnen, und hat keine Anomalie-Detektionsfunktionen, um böswillige Intentionen beim E-Mail-Sendeverhalten zu erfassen.

- DLP-Richtlinien werden nach Priorität oder Ausführungsreihenfolge evaluiert. Die erste Regel, die mit dem identifizierten Inhalt einer E-Mail-Nachricht oder einem Dokument übereinstimmt, wird angewendet. Es gibt keine Möglichkeit, die Priorität oder Ausführungsreihenfolge von DLP-Richtlinien festzulegen, außer der zeitlichen Reihenfolge ihrer Erstellung. Wenn eine neue Richtlinie erstellt wird, wird sie am Ende der Prioritäts- oder Ausführungsreihenfolge hinzugefügt. Um eine neue DLP-Richtlinie in der Ausführungsreihenfolge höher zu positionieren, müssen daher aktuelle Richtlinien gelöscht und nach dem Erstellen der neuen DLP-Richtlinie erneut erstellt werden. Dadurch werden zweifelsohne Fehler eingeführt.

- Es gibt keine ausgeglichene Analyse, welche DLP-Richtlinie am besten auf eine spezifische Nachricht oder ein Dokument angewandt werden sollte, und keinen Versuch, die „beste Übereinstimmung" auf Einzelnachricht- oder Einzeldokumentbasis zu identifizieren. Anders gesagt: Eine allgemeine Richtlinie mit höherer Priorität oder Position in der Ausführungsreihenfolge wird vor einer spezifischen Richtlinie mit niedrigerer Priorität oder Position in der Ausführungsreihenfolge angewandt.

- Es gibt keine Workflow-Optionen für Nachrichten und Dateien, die eine DLP-Richtlinie verletzen. Wenn eine E-Mail-Nachricht z. B. eine Richtlinie auslöst, wird sie entweder blockiert oder verschlüsselt. Es gibt keine Option für Richtlinienaktionen zur Weiterleitung der gegen die Richtlinie verstoßenden Nachricht an einen Administrator oder in eine Administratorwarteschlange, wo sie geprüft werden könnte. Wie bei DLP in Exchange Online bietet DLP im Security & Compliance Center keine nuancierten Optionen, um eine Prüfung durch jemand anders als den Originalendbenutzer anzufordern.

- Während Office 365 zwar DLP-Funktionen bietet, sind diese auf Exchange Online, SharePoint Online und OneDrive for Business beschränkt. Die neueren Konversationstools in Office 365 wie Yammer und Microsoft Teams sind ausgeschlossen; dasselbe gilt für andere Dokumentspeicher- und Konversationssysteme außerhalb von Office 365. Diese nur teilweise Abdeckung der Office 365-Workloads bedeutet, dass Office 365 keine einheitlichen DLP-Regeln und keine Abhilfe-Engine bietet, die unternehmensweit für alle im Dokument verwendeten Dokumentspeicher- und Konversationssysteme eingesetzt werden können, und somit nicht alles in Office 365 zu schaffen ist. Microsoft hat die Fähigkeit zum Blockieren von Chat-Nachrichten in Microsoft Teams vor Ende März 2019 versprochen.

DLP-Richtlinien können E-Mail-Sendefehler, wie z. B. das Adressieren von E-Mail an den falschen Empfänger, nicht proaktiv mit Flags kennzeichnen.

- Die Analyse von Inhalten auf sensible Daten stützt sich auf die von Microsoft bereitgestellten Typen sensibler Informationen oder eine vom Kunden erstellte spezifische Definition. Der Abgleich sensibler Daten ist einfach zu umgehen, um Daten auszufiltern. Die Vergleichsalgorithmen suchen nach genauen Übereinstimmungen und sind einfach auszutricksen.

- Während eine DLP-Richtlinie basierend auf dem Inhalt der Betreffzeile einer E-Mail ausgelöst werden kann, gilt: Besteht die Richtlinienaktion darin, die Nachricht zu verschlüsseln, dann bleibt die Richtlinie ohne Wirkung, weil die Office 365-Nachrichtenverschlüsselung die Betreffzeile in Klartext weiterleitet. Sie wird nicht verschlüsselt.

- In Office 365 sind keine speziell auf die jeweilige Organisation zugeschnittenen DLP-Richtlinien automatisch aktiviert. Jede muss manuell konfiguriert und fein eingestellt werden. Zu wenige Organisationen weisen das nötige Cybersicherheits-Know-how auf, um DLP-Richtlinien effektiv zu konfigurieren. Microsoft führte vor Kurzem neue Intelligence-Funktionen zur Erfassung sensibler Informationen ein, die durch eine DLP-Richtlinie geschützt werden sollten. Mit diesen Funktionen wird ein Administrator benachrichtigt, dass eine bestimmte Art von Abhilfemaßnahme ergriffen wird. Ob dieser „weiche Empfehlungsansatz" ausreicht, wird sich erst noch herausstellen. Es gibt auch keine Standard-DLP-Richtlinie, die nach der Präsenz von Kreditkartennummern sucht, die an jemanden außerhalb der Organisation gesendet werden. Diese Funktion befindet sich im Richtlinientipps-Modus und der Endbenutzer erhält eine Benachrichtigung.

- DLP-Richtlinien können nicht auf spezifische Gruppen oder Regionen zugeschnitten werden, um globale Unternehmen dabei zu unterstützen, unterschiedliche regulatorische Anforderungen weltweit zu erfüllen. Die Ausnahme dabei scheinen Organisationen zu sein, die den neuen Multi-Geo-Dienst verwenden, der ein spezifisches Anpassen basierend auf der Geografie (aber nicht notwendigerweise dem jeweiligen Land) ermöglicht.

- Dokumente in SharePoint Online und OneDrive for Business, für die eine DLP-Richtlinie festgestellt hat, dass sie sensible Informationen enthalten, werden an Ort und Stelle blockiert, um den Zugriff durch andere Personen als den Dokumenteigner, die Person, welche die letzte Änderung vorgenommen hat, und den Website-Eigner zu verhindern. Es besteht keine Möglichkeit, das Dokument automatisch von sensiblen Informationen zu reinigen oder die sensiblen Informationen innerhalb des Dokuments zu verschlüsseln, während der Rest des Dokuments verfügbar bleibt. Noch signifikanter ist, dass es keine Vorkehrungen für Personen außerhalb der drei genannten Personen gibt, die evtl. einen legitimen Grund für den Zugriff auf das Dokument mit intakten sensiblen Informationen haben. Die Blockieren-und-Verhindern-Haltung von Office 365 verursacht bei legitimen Geschäftsprozessen Probleme.

- Aktionen durch einen Administrator beim Erstellen oder Ändern einer DLP-Richtlinie werden nicht im Office 365-Überwachungsprotokoll protokolliert. Dadurch ist es unmöglich, zu wissen, wer eine DLP-Richtlinie erstellt hat und wie sie (von wem) im Zeitverlauf geändert wurde.

- DLP-Richtlinien und sensible Informationstypen können gegen Richtlinien verstoßenden Text in gescannten Bildern oder gescanntem Text nicht identifizieren. OCR wird nicht unterstützt.

MANGELNDE EINZELBILDSCHIRM-TRANSPARENZ BEI MALWARE- UND NICHT-MALWARE-BASIERTEN ATTACKEN

Die verschiedenen Bedrohungsberichte im Security & Compliance Center bieten nur eine bruchstückhafte Ansicht der Bedrohungen, denen eine Organisation durch verschiedene Malware- und Nicht-Malware-Angriffsvektoren ausgesetzt ist, aber keine konsolidierte Ansicht. Die verschiedenen, separaten Berichte konzentrieren sich auf

Die verschiedenen Bedrohungsberichte im Security & Compliance Center bieten nur eine bruchstückhafte Ansicht der Bedrohungen, denen eine Organisation gegenübersteht.

bestimmte Angriffstypen. Das bedeutet, dass ein Sicherheitsadministrator manuell Korrelationen für die gesamte Organisation herstellen muss, um eine Gesamtansicht zu erhalten.

Office 365 bietet die folgenden Bedrohungsberichte über den Sicherheitsrisiken-Explorer (Bedrohungsverwaltung > Explorer):

- **Malware (in E-Mail-Nachrichten)**
  Zeigt Malware-Bedrohungen an, die in E-Mails per Virusscan, ATP-Detonation oder Reputationserfassung festgestellt wurden. Zeigt die Top-Malware-Familien und Top-Benutzer an, die von Malware ins Visier genommen werden.

- **Phish**
  Zeigt E-Mail-Nachrichten an, die bösartige URLs enthalten, und gibt an, wie sie erfasst wurden (nach URL, Reputation, heuristisch oder durch Machine Learning). Zeigt auch an, auf welche URLs geklickt wurde und ob die fraglichen URLs blockiert wurden oder nicht.

- **Vom Benutzer gemeldet**
  Zeigt Nachrichten an, die Benutzer für die Neuklassifizierung gemeldet haben, wie z. B. eine E-Mail, die geliefert wurde, von der der Benutzer aber annimmt, dass es sich um eine Phishing-E-Mail handelt oder dass sie Malware enthält. Zeigt auch Einreichungen falscher Positiver an, bei denen ein Benutzer versichert, dass eine als Junk-Mail eingestufte Nachricht legitim ist.

- **Gesamte E-Mail**
  Zeigt eine Liste der gesamten E-Mail-Aktivität zwischen Benutzern sowie alle E-Mail-Nachrichten an, die von externen Quellen an den Office 365-Mandanten gesendet wurden.

- **Malware (in Dateien)**
  Führt die in Office 365 gespeicherten Dateien auf, die beim Advanced Threat Protection-Dateidetonationsprozess als Malware erfasst wurden. Dies umfasst nur Dateien, die per ATP-Dateidetonation analysiert wurden. Dies stellt keine Sicherheitsgarantie für alle vorhandenen Dateien dar (z. B. solche, die nicht detoniert oder geprüft wurden).

Es gibt keine Möglichkeit, eine einzige, konsolidierte Liste aller Bedrohungstypen anzuzeigen und dann mithilfe von Facetten genauer zu filtrieren.

ANMELDEDATEN-PHISHING UND E-MAIL-BETRUG

Wir haben mehrere Probleme bei Office 365 im Kontext von Anmeldedaten-Phishing und E-Mail-Betrug festgestellt:

- Microsoft scheint nicht in der Lage zu sein, Anmeldedaten-Phishing-Versuche, die zu einem gefälschten Office 365-Anmeldebildschirm führen, zuverlässig zu identifizieren. Im Jahr 2018 wurden viele solcher E-Mails an Endbenutzer zugestellt. Weil weder Payload noch der Link selbst bösartig ist, bietet ATP keinen Nutzen. Microsoft identifiziert nachgestellte Nachrichteninhalte für seinen eigenen Dienst nicht beständig.

- Office 365 benachrichtigt den Empfänger über eine verdächtige Nachricht, die den Domainnamen der Organisation nachstellt, doch muss die Übereinstimmung exakt sein. Dies erfolgt über den Exact Domain Spear Phishing Protection-Dienst in Exchange Online Protection. Office 365 berücksichtigt Fast-Übereinstimmungen nicht, bei denen Domains verwendet werden, die ähnlich aussehen oder klingen wie die Domain der Organisation (z. B. rnicrosoft.com vs. microsoft.com). Ohne zusätzliche Microsoft-Cloud-Dienste hat Office 365 Probleme, E-Mail-Betrugsnachrichten zu identifizieren, die von kompromittierten internen Konten gesendet wurden. Angesichts der steigenden Zahl von Nachahmungsangriffen

Wir haben mehrere Probleme bei Office 365 im Kontext von Anmeldedaten-Phishing und E-Mail-Betrug festgestellt.

durch Übernahme legitimer Postfächer ist der Mangel an fortgeschrittenen Detektionsfunktionen von Office 365 beunruhigend.

- Der Schutz der Benutzer vor einer Nachahmung durch andere erfordert manuelle Eingriffe durch einen Administrator, um eine Anti-Phishing-Richtlinie zu erstellen und jeden spezifischen zu schützenden Absender aufzuführen. Diese Liste muss manuell vom Administrator gepflegt werden, weil eine Integration mit Azure AD basierend auf Jobrollen nicht unterstützt wird, z. B. um einen neuen Vice President oder CEO zu schützen.

- Herkömmliche Methoden zur Klassifizierung von Spam anhand des Nachrichtenvolumens funktionieren für die Klassifizierung von Anmeldedaten-Phishing- und E-Mail-Betrugsnachrichten nicht. Der Betrug kann bereits mit einer einzigen Nachricht stattfinden.

- Office 365 bietet keine einfache Methode, um Phishing- und Nachahmungs-E-Mails, die es durch die Filter geschafft haben, aus den Postfächern zu entfernen. Ohne auf PowerShell zurückzugreifen, gibt es keine Möglichkeit, eine E-Mail in mehreren Postfächern zu entfernen, und auch keine Möglichkeit, einen Rückruf rückgängig zu machen (manche Drittanbieter-Lösungen ermöglichen dies auf recht einfache Weise). Das gleiche Problem gilt für DLP in Office 365: Bei internen Informationslecks müssen Maßnahmen ergriffen werden, um diese Informationen zu entfernen. Beispiel: Weil der *New-ComplianceSearchAction* PowerShell-Befehl zum Entfernen von Phishing-E-Mails Nachrichten nur vorläufig löscht, bleiben Phishing-E-Mails für Endbenutzer zugänglich, wenn sie gelöschte Objekte per Outlook oder Outlook Web Access wiederherstellen. Die automatische Bereinigung zur Nullstunde (Zero-Hour Auto Purge, ZAP) funktioniert nur bei Spam- und Malware-basierten Nachrichten, nicht bei Phishing- oder Nachahmungs-Nachrichten.

- Spoof Intelligence verwaltet Benutzer, Adressen und Domains, denen das Spoofing der Domain der Organisation gestattet ist. Dies bietet einen Schutz für die eigenen internen Benutzer und alle Geschäftspartner oder Kunden, die legitime oder illegitime E-Mail von ihrer Domain erhalten. Spoof Intelligence ist Teil des Security & Compliance Center. Es ist zu beachten, dass für Spoof Intelligence keine granuläre Richtlinienkontrolle verfügbar ist. Stattdessen kann die Funktion nur aktiviert oder deaktiviert werden. Darüber hinaus ist die Berichterstattungs-Funktionalität für dieses Tool stark eingeschränkt. Spoof Intelligence wurde ursprünglich für Kunden mit dem Enterprise E5-Abonnement (oder solche mit dem ATP-Add-on) konzipiert, aber als Teil von EOP im August 2018 allen Benutzern zur Verfügung gestellt.

- Gebräuchliche E-Mail-Authentifizierungs-Mechanismen wie SPF, DKIM und DMARC können Brand-Spoofing identifizieren, sofern sie korrekt implementiert werden. Beim Identifizieren von Brand-Spoofing, bei dem ähnlich aussehende oder klingende Domainnamen mit ihrer eigenen starken E-Mail-Authentifizierung verwendet werden, sind sie aber weniger effektiv. Zur Erfassung und ordnungsgemäßen Klassifizierung solcher Nachrichten muss man jedoch über gewöhnliche E-Mail-Authentifizierungs-Ansätze hinausgehen.

UNTERSTÜTZUNG HYBRIDER ARCHITEKTUREN

Die Sicherheitsfunktionen in Office 365 bieten unvollständige Unterstützung für Organisationen mit hybriden Architekturen:

- ATP weist keine hybriden Fähigkeiten auf. Das bedeutet, dass Kunden mit z. B. lokalem Exchange oder SharePoint ein zweites, separates Bedrohungsschutz-Angebot nutzen müssen. ATP geht nur mit bestimmten Office 365-Workloads unter spezifischen Bedingungen um und lässt Daten und Systeme außerhalb von Office 365 ganz außer Acht. Dies kann bei vielen Kunden, die eine hybride Umgebung betreiben, zu Problemen führen.

- Die im Security & Compliance Center definierten DLP-Richtlinien gelten nur für spezifische Office 365-Workloads. Diese Richtlinien werden nicht zusätzlich für lokale Server von Microsoft oder anderen Anbietern durchgesetzt.

- eDiscovery im Security & Compliance Center ist nur für bestimmte Office 365-Workloads vorgesehen und funktioniert nicht mit lokalen Exchange-, SharePoint- und OneDrive for Business-Umgebungen.

Jede Organisation, die in Office 365-Sicherheitsfunktionen (mit allen mit ihnen verbundenen Problemen) investiert, muss trotzdem einen völlig separaten Satz von Sicherheits-Services für Nicht-Office-Workloads und Daten erwerben.

Die Sicherheits-funktionen in Office 365 bieten unvollständige Unterstützung für Organisationen mit hybriden Architekturen.

PARALLELE DRITTANBIETER-SICHERHEITSLÖSUNGEN

Selbst die besten Angebote in Office 365 sprechen all die Sicherheitsbedrohungen, die Organisationen haben, welche die teureren Office 365-Abonnements (wie E3 und E5) nutzen, nicht an. Phishing-E-Mails erreichen z. B. trotzdem Endbenutzer-Posteingänge und erhöhen das Risiko von Anmeldedaten-Diebstahl und Kontokompromittierung. Microsoft zieht es vor, seine eigene Monokultur von Sicherheits-Services zu liefern, anstatt hoch funktionale Integrationspunkte für Drittanbieter-Angebote bereitzustellen, die den Kundensupport insgesamt verbessern würden. Auf der Ignite 2017 z. B. prahlte Microsoft mit dem eigenen Marktanteil im Anti-Malware-Sektor und damit, dreimal so viele Kunden zu haben wie sein nächster Wettbewerber. In der sich schnell entwickelnden Bedrohungslandschaft, in der Organisationen operieren müssen, würde es sowohl Microsoft als auch seinen Kunden besser dienen, wenn Microsoft bessere Möglichkeiten für Drittanbieter von Sicherheitslösungen zur Bereitstellung komplementärer Sicherheits-Services anbieten würde, welche die Sicherheitsfunktionen von Office 365 verbessern und ergänzen.

RÜCKRUF-FUNKTIONEN

Der Outlook-Client bietet eine Nachrichtenrückruf-Funktion, mit der eine Nachricht im Postfach eines Empfängers unter bestimmten Bedingungen gelöscht oder ersetzt werden kann. Der Nachrichtenrückruf ist eine Option für den Endbenutzer vom Diensttyp „Beste Leistung" im Outlook-Client und steht in Outlook Web Access oder als Office 365-Service-Level-Option nicht zur Verfügung. Der Rückruf funktioniert, wenn die Originalnachricht noch nicht gelesen wurde, sie im Posteingang des Empfängers verbleibt, der Outlook-Client des Empfängers geöffnet ist und der Empfänger sich im gleichen Office 365-Mandanten befindet. Für den Nachrichtenrückruf gelten folgende Einschränkungen:

- Er versagt, wenn die Nachricht bereits gelesen wurde. Sowohl die Original- als auch die Rückrufnachricht verbleiben im Posteingang des Empfängers.

- Befindet sich der Empfänger in einem anderen Office 365-Mandanten, verwendet er nicht Outlook oder hat er die Nachricht (über eine automatisierte Regel oder manuelle Aktion) in einen anderen Ordner als den Posteingang verschoben, schlägt die Rückruffunktion fehl.

- Zurückgerufene Nachrichten können vom Empfänger über die Wiederherstellungsfunktion für gelöschte Elemente wiederhergestellt werden. Weil die zurückgerufene Nachricht endgültig gelöscht wird (also in den Ordner „Wiederherstellbare Elemente" und nicht in den Ordner „Gelöschte Elemente" verschoben wird), kann der Empfänger diese Elemente innerhalb des Wiederherstellungszeitraums wiederherstellen.

An die zurückgerufene Nachricht angehängte Dokumente unterliegen den gleichen Bedingungen und Einschränkungen. Der Rückruf mag funktionieren, doch gelten viele Bedingungen, unter denen das nicht der Fall ist.

Archivierung und Content Management

Wenn Office 365 in Erwägung gezogen wird, besteht eine der wichtigsten Fragen für Organisationen darin, ob es einen vollständigen Ersatz für alle lokalen Microsoft-Server und -Funktionen oder vielmehr eine Ergänzung aktueller lokaler Kapazitäten darstellt.

Innerhalb von Office 365 besteht die Designabsicht darin, dass neue Inhaltsquellen (z. B. Microsoft Teams) und neue Inhaltstypen (wie Microsoft Teams-Konversationen, Office 365-Nachrichtenverschlüsselung, Planer, Stream und mehr) hinzukommen. Diese zusätzlichen Inhalte müssen geschützt, kontrolliert und Regeln unterworfen werden.

Aus der breiteren Perspektive stellt sich die Frage, ob die nativen Funktionen in Office 365 ausreichende Unterstützung für Nicht-Microsoft-Inhaltsquellen und selbst für Microsoft-Inhaltsquellen außerhalb von Office 365 bieten.

ES GIBT KEINE ENTSPRECHUNG FÜR EIN E-MAIL-JOURNAL

Statt eines herkömmlichen E-Mail-Journals hat Microsoft sein Office 365-Modell erweitert, um das gleiche „Compliance-Ergebnis" wie bei einem Journal-Service zu bieten. Kurz gesagt: Indem alle relevanten Postfächer auf „Beweissicherungsverfahren" oder „In-Situ Speicher" gestellt werden, werden alle gesendeten und empfangenen E-Mails unbegrenzt lange aufbewahrt und können von Benutzern nicht gelöscht werden. Inaktive Postfächer (z. B. solche von ehemaligen Mitarbeitern) können ebenfalls auf unbegrenzte Aufbewahrung eingestellt werden (derzeit ohne Lizenzstrafe, doch kann sich dies ändern).

Hat eine Organisation ein bestehendes Journal, wenn sie zu Office 365 migriert, benötigt sie daher einen Plan für Folgendes:

- Migration des bestehenden Journalinhalts zu Office 365 oder

- Verschieben des bestehenden Journals in einen Drittanbieter-Journaldienst und Fortsetzung dieses Journals von Office 365 aus

Die erste Option kann mithilfe von Spezial-Migrationssoftware umgesetzt werden, doch bleiben Microsofts Vorgaben zum Migrationsort für Journalinhalte unklar. Es gelten verschiedene Einschränkungen, wie Postfächer in Office 365 genutzt werden können, um E-Mail aufzubewahren, die zu mehreren Benutzern gehört[iv]. Obgleich vorgeschlagen wird, korrekt lizenzierte, freigegebene Postfächer zu nutzen, muss eine Organisation evtl. Hunderte (oder gar Tausende) freigegebener Postfächer verwenden,

Wenn Office 365 in Erwägung gezogen wird, besteht eine der wichtigsten Fragen für Organisationen darin, ob es einen vollständigen Ersatz für alle lokalen Microsoft-Server und -Funktionen oder vielmehr eine Ergänzung aktueller lokaler Kapazitäten darstellt.

um den Journal-Rückstand aufzuarbeiten. Dadurch wird die eDiscovery komplizierter und es besteht das Risiko, dass Legacy-Journale ausgeschlossen werden.

Die zweite Option bedeutet, dass zwei Speicherorte gepflegt und durchsucht werden müssen, um Informations-Governance- und eDiscovery-Anforderungen zu erfüllen, kann aber zu niedrigeren Kosten und einer praktischeren Lösung führen, insbesondere wenn eine Organisation Journale über viele Jahre hinweg aufbewahren muss.

VERSCHLÜSSELUNG

Die erste Version der Office 365-Nachrichtenverschlüsselung litt an verschiedenen Schwächen, darunter Kapazitätsmangel, mangelhaftes Reporting und eine nicht ausreichende Benutzeroberfläche für Empfänger. Auf der Ignite-Konferenz 2017 kündigte Microsoft eine neue Version an, die einige der Schwächen der ersten korrigieren sollte (darunter Benutzerkonto- und Client-Anforderungen). Mehr als ein Jahr nach dem Release von Version 2 der Office 365-Nachrichtenverschlüsselung (kurz OMEv2), kämpft das Produkt weiterhin mit Leistungs- und Kapazitätsproblemen. Zum Beispiel:

- Die Verschlüsselungseinstellung „Nicht weiterleiten", die ursprünglich mit OMEv2 eingeführt wurde, erlegten der Nachricht und allen Anlagen sowohl Verschlüsselungs- als auch Rechtemanagement-Einstellungen auf. Kunden fanden diese Einstellung für die allgemeine Verwendung zu restriktiv. Es ist nicht klar, was sich Microsoft dabei dachte, diese beiden Funktionen zu kombinieren.

- Die Verschlüsselungseinstellung „Nur verschlüsseln", die im 1. Quartal 2018 eingeführt wurde, sprach im Prinzip mehrere der Kritikpunkte gegen „Nicht weiterleiten" an, wie z. B. das Rechtemanagement nach der Zustellung. In der Praxis hat Microsoft immer noch keine Verschlüsselungsoption geliefert, die in Outlook für Windows und Mac zuverlässig funktioniert. Microsoft musste neue Einstellungen auf Mandantenebene einführen, um Probleme nach der Zustellung anzusprechen, bei denen Empfänger verschlüsselte Anlagen nicht lesen konnten. Die neue Einstellung entfernt die auf Anlagen für bestimmte Empfänger unter bestimmten Umständen angewendete Verschlüsselung, was den Hauptgrund für eine Verschlüsselung unterminiert.

- Manche Office 365-Kunden haben sich über spezifische und sich ständig ändernde Versionsanforderungen für Outlook (sowie Bugs in den verschiedenen Versionen mit dem Resultat, dass der Dienst nicht funktionierte), die Unmöglichkeit, verschlüsselte Nachrichten unter verschiedenen Bedingungen an andere Office 365-Mandanten zu senden und die Nichtoffenlegung der Einstellungen in Office 365 auf Mandantenebene durch Microsoft beschwert. All das verhindert, dass Verschlüsselung für alle funktioniert.

- Microsoft hat versucht, einen nahtlosen End-to-End-Verschlüsselungs-Service zu liefern, der inline im Outlook-Client funktioniert. Doch war das Unternehmen dazu seit der Ankündigung von OMEv2 Ende 2017 nicht in der Lage, und es gibt bestimmte Anzeichen (wie z. B. die Verknüpfung neuerer Funktionen in OMEv2 mit linkbasierten Nachrichten, die in einem Anzeigeportal statt inline in Outlook angezeigt werden), dass es sich von diesem Designziel nach und nach verabschiedet.

- Verschlüsselte Nachrichten, die mithilfe von Google Gmail und Yahoo Mail an Empfänger gesendet werden, können ihre Google- oder Yahoo-Identität für die Verschlüsselung der Nachricht im Anzeigeportal verwenden. Dabei handelt es sich um einen für den Empfänger transparenten Vorgang. Allerdings bedeutet dies auch: Sendet der Absender die verschlüsselte Nachricht an den falschen Empfänger, so ist dieser in der Lage, lediglich über seine Google- oder Yahoo-Anmeldedaten auf die verschlüsselte Nachricht zuzugreifen. Der Absender und die Absenderorganisation können keine weitere Identitätsbestätigung fordern, um sicherzustellen, dass die Nachricht vom korrekten Empfänger entgegengenommen wurde (wie z. B. Multifaktor-Authentifizierung). Dies führt zu einer

Microsoft hat versucht, einen nahtlosen End-to-End-Verschlüsselungs-Service zu liefern, der inline im Outlook-Client funktioniert.

Datenschutzverletzung, die für die Absenderorganisation nur schwer zu identifizieren ist.

- Ähnlich liegt der Fall, wenn das Google- oder Yahoo-Konto eines Benutzers kompromittiert wurde. Der Hacker kann dann den transparenten Entschlüsselungsprozess nutzen, um auf verschlüsselte Nachrichten zuzugreifen. Dies führt ebenfalls zu einer Datenschutzverletzung, die für die Absenderorganisation nur schwer zu identifizieren ist.

- Ist das Google- oder Yahoo-Konto eines Empfängers kompromittiert, kann der Hacker auch verschlüsselte Antworten an den Originalabsender sowie an andere Empfänger senden. Dies könnte zur Verbreitung von verschlüsselten Phishing-Nachrichten eingesetzt werden, die schwieriger zu erfassen sind.

- Microsoft stützt sich für Empfänger ohne Outlook auf linkbasierte Nachrichten. Das bedeutet, dass verschlüsselte Nachrichten wie Phishing-Nachrichten aussehen können, insbesondere weil sie dann zur Anmeldung nach einem Benutzernamen und Passwort fragen. Dieses Design löst alle Alarmzeichen für Phishing-Versuche aus. Andere E-Mail-Dienste wie z. B. Gmail können OMEv2-Nachrichten als Phishing klassifizieren und den Empfänger warnen, nicht auf den Link zu klicken. Anders gesagt: OMEv2-Nachrichten weisen alle Merkmale einer Phishing-Nachricht auf und unterminieren die Fähigkeit des Absenders, wichtige Informationen dem Empfänger zu übermitteln.

- OMEv2 verschlüsselt die Betreffzeile der Nachricht nicht. Sie wird vielmehr in Klartext weitergeleitet. Das war in OMEv1 zwar nicht anders, doch falls die Betreffzeile sensible Informationen enthält, werden diese nicht durch die Verschlüsselung geschützt, obgleich die Nachricht und alle Anlagen verschlüsselt werden.

- Es gibt keine Option für den Endbenutzer, automatisch alle Nachrichten, die per Outlook versendet werden, zu verschlüsseln. Dies muss für jede Nachricht einzeln durch einen Endbenutzer erfolgen.

- Wie bei der Originalversion bietet OMEv2 nach der Zustellung keine Einsicht- oder Meldefunktionen für den Absender der Nachricht. Das Office 365 Security & Compliance Center bietet einen neuen Bericht zu verschlüsselten Nachrichten für Office 365-Administratoren, doch steht diese Funktion Endbenutzern nicht zur Verfügung und sie meldet auch keine Aktionen durch den Empfänger nach der Zustellung. Dies hat mehrere Auswirkungen auf den Workflow. So ist es z. B. dem Absender unmöglich, nachzusehen, ob die Nachricht vom Empfänger geöffnet wurde. Separate Nachrichten oder ein Anruf sind erforderlich, um den Empfang zu bestätigen. Das bedeutet, dass der Absender den Verschlüsselungsstatus oder die Rechte nicht mehr ändern kann, sobald die Nachricht gesendet wurde. Stellt ein Absender fest, dass er eine Nachricht an den falschem Empfänger gesendet hat, kann er nicht wissen, ob es zu einer Datenschutzverletzung kam oder nicht. Wird darüber hinaus eine verschlüsselte Nachricht als Spam markiert oder als Junk-Mail ausgefiltert, kann der Absender nicht wissen, ob seine Nachricht erwartungsgemäß zugestellt wurde. Es sind separate E-Mails oder ein Anruf erforderlich.

- OMEv2 bietet dem Absender nicht die Möglichkeit, den Zugriff auf die Nachricht zu widerrufen, wenn diese über Outlook oder Outlook im Web gesendet wurde.

- Microsoft stellte im vierten Quartal 2018 einen Widerrufprozess (lediglich als Vorschau) vor, mit dem ein IT-Administrator Nachrichten im Auftrag des Absenders widerrufen kann. Dies erfordert allerdings, dass der Administrator die Nachrichten-ID für die jeweilige Nachricht findet (z. B. mittels der Nachrichtensuche in Exchange Online) und PowerShell-cmdlets verwendet, um den Widerrufprozess abzuschließen.

Es gibt keine Option für den Endbenutzer, automatisch alle Nachrichten, die per Outlook versendet werden, zu verschlüsseln.

- Der Widerruf durch einen IT-Administrator ist ein globaler Vorgang. Die Nachricht wird für alle Empfänger widerrufen. Es ist nicht möglich, den Zugriff nur für einen bestimmten Empfänger aufzuheben oder einen neuen Empfänger zur zuvor gesendeten Nachricht hinzuzufügen. Diese mangelnde Nuancierung verkompliziert alle vom Original ausgehenden Diskussionen zu verschlüsselter E-Mail und verursacht eine Unterbrechung des Workflows für alle Empfänger.

- Allgemein bietet OMEv2 Verschlüsselung nur für Microsoft Office-Dateitypen, nicht für andere Dateitypen wie z. B. PDF. Es fokussiert auf Organisationen, die Word-, Excel-, PowerPoint-, InfoPath- und XPS-Dokumente verwenden. Für Organisationen, die häufig Nicht-Microsoft-Dateitypen benutzen, hat OMEv2 keinen großen Wert. Im September 2018 kündigte Microsoft an, bis Ende 2018 PDF-Dokumente zu unterstützen. Im Kleingedruckten steht allerdings, dass PDF-Dokumente im Transit zwar verschlüsselt werden, aber nicht nach der Zustellung der Nachricht. Das bedeutet, dass PDF-Dokumente anders behandelt werden als Office-Dokumente, was mit Sicherheit zu Datenschutzverletzungen durch Endbenutzer führen wird, die von einer dauerhaften Verschlüsselung für jede E-Mail-Anlage ausgehen.

ARCHIVIERUNG

Archivierung, also das Verschieben von Geschäftsdaten von einem Geschäftssystem zu einem separaten, geschützten Speicherort, um Aufbewahrung, Unveränderbarkeit und bessere Daten-Governance zu optimieren, wird für manche wichtige Inhaltstypen in Office 365 nicht unterstützt. Dies umfasst SharePoint, Skype for Business, zusätzliche Nachrichtentypen und Drittanbieterinhalte.

Archivierung wird für bestimmte Inhaltstypen in Office 365 nicht angeboten.

- SharePoint-Inhalte wie z. B. Dokumente und Listenpunkte können an Ort und Stelle mithilfe von Retentionsrichtlinien aufrechterhalten oder an einen anderen Speicherort in SharePoint verschoben werden, wenn ihre Frist abgelaufen ist oder sie irrelevant geworden sind. Diese Retentions- oder Verschiebungsaktionen können nur anhand spezifischer, datums- und ereignisbasierter Trigger ausgelöst werden. Für Organisationen, die innerhalb ihrer zugewiesenen Speichergrenzen für SharePoint bleiben, kann die Datensatzverwaltung an Ort und Stelle in SharePoint ausreichen. Nicht möglich ist allerdings die Archivierung von nicht mehr aktuellen SharePoint-Inhalten, auf alternativen und kostengünstigeren Speichersystemen. Es ist zwar möglich, unbegrenzte SharePoint-Speicherkapazität zu kaufen; dies ist jedoch mit Premium-Preisen verbunden. Organisationen mit großen Mengen an SharePoint-Daten werden nicht gut bedient, wenn sie schlanke und aktuelle SharePoint-Inhalte pflegen möchten, ohne zusätzlich langfristige SharePoint-Speichergebühren bezahlen zu müssen, oder wenn sie Inhalte basierend auf Ereignisauslösern jenseits von datumsbasierten Metadaten außerhalb von SharePoint Online archivieren möchten. Darüber hinaus ist SharePoint nicht Write Once, Read Many (WORM)-kompatibel, was für Organisationen in regulierten Branchen ein großes Problem ist.

- Skype for Business Online nutzt Exchange Online für die Archivierung, wenn bestimmte Bedingungen erfüllt sind. Es steht kein nativer Archivierungsdienst für Skype for Business Online zur Verfügung. Standardmäßig werden Skype-Instant-Messaging-Aufzeichnungen im Ordner „Unterhaltungsverlauf" im Exchange Online-Postfach jedes Benutzers aufbewahrt. Ein Benutzer kann aber mit Ausnahme von Postfächern, für die eine Aufbewahrungspflicht aus juristischen Gründen gilt, seine Instant-Messaging-Aufzeichnungen nach Belieben löschen, was ein zuverlässiges, unveränderbares Archiv alter Nachrichten verhindert. Die Notwendigkeit einer Aufbewahrungspflicht aus juristischen Gründen zum Erzwingen des Speicherns von Skype-Nachrichten bedeutet, dass für alle Exchange Online-Mailboxen jederzeit eine Aufbewahrungspflicht gelten muss, damit dies funktioniert – unserer Meinung nach ein sehr seltsames Design. Gilt für ein Postfach die Aufbewahrungspflicht, werden Peer-to-Peer-Instant-Messages und solche mit mehreren Teilnehmern sowie Aktivitäten zum Hochladen von Inhalten während Besprechungen gespeichert. Andere Aktionen in Skype for Business werden beibehalten, wie etwa Peer-to-Peer-Dateitransfers, Audio/Video für Peer-to-Peer-Instant-Messages und

Konferenzen, Anwendungsfreigabe und Konferenzanmerkungen.

- SMS-Nachrichten auf BlackBerry-Geräten werden in Office 365 archiviert, sofern eine Drittanbietervereinbarung zum Erfassen dieser Nachrichten implementiert ist. SMS-Nachrichten auf anderen Geräten einschließlich iOS und Android werden nicht erfasst. Der Marktanteil von BlackBerry ist inzwischen im Vergleich zu iOS und Android sehr gering, wodurch das Erfassen ausschließlich von BlackBerry-Nachrichten nicht besonders nützlich ist.

- Inhalte aus spezifischen Drittanbieter-Messaging-, Kooperations-, Social Media- und anderen Inhaltsquellen können in Exchange Online in Office 365 als konvertierte E-Mail-Nachrichten archiviert werden, sofern Vereinbarungen mit einem Drittanbieter-Datenpartner gelten. Nachrichten werden im Exchange Online-Postfach des jeweiligen Benutzers gespeichert. Für Inhalte, die nicht einer genau bezeichneten Einzelperson zugeordnet werden können, wird ein allgemeines Postfach verwendet. Der Großteil des Inhaltskontexts aus Twitter, Facebook, Yahoo! Messenger, DropBox und Salesforce Chatter geht verloren, wenn diese Rich Media-Quellen in E-Mail-Nachrichten umgewandelt werden. Dadurch ist es schwierig, eine historisch korrekte Ereigniskette nachzustellen.

eDISCOVERY

eDiscovery ist ein grundlegender Bestandteil von E-Mail- und Kooperations-Plattformen, denn es müssen Informationen erzeugt werden, um Bemühungen bei Rechtsstreits zu unterstützen. Außerdem wird in der Regel ein großer Teil der Unternehmensdaten auf E-Mail- und Kooperationsplattformen von Organisationen gespeichert. Office 365 bietet einige nützliche Funktionen im Zusammenhang mit eDiscovery, doch gelten bestimmte Einschränkungen. Zum Beispiel:

- Microsoft bietet kein Service Level Agreement (SLA) für eine Inhalts- oder eDiscovery-Suche, gibt aber an, dass 100 Postfächer in 30 Sekunden und 10.000 Postfächer in vier Minuten durchsucht werden können. In der Praxis nehmen Suchen aber viel mehr Zeit in Anspruch.

- Für das Postfach eines Benutzers und sein Online-Archiv können keine separaten Retentions-, Erhaltungs- und Vernichtungsrichtlinien erstellt werden. Was für das Postfach gilt, gilt auch für das Online-Archiv, was für Organisationen, die separate Richtlinien definieren möchten, ein Problem darstellt.

- Die erweiterte eDiscovery-Fähigkeit Office 365 ist nicht „an Ort und Stelle" vorhanden. Die erweiterten Tools bieten eDiscovery-Funktionen innerhalb der Office 365-Anwendungs-Suite und sind nicht direkt in die Datenquellen integriert. Daher ist ein aus zwei Schritten bestehender Prozess erforderlich, wobei eine Suche und ein Export der Daten mithilfe der begrenzten Fähigkeiten des Security & Compliance Center durchgeführt werden müssen. Zunächst muss das erweiterte eDiscovery-Center als Ziel ausgewählt werden, bevor die erweiterten Tools überhaupt ausgeführt werden können. Daher gibt es keine Möglichkeiten für Iteration und Suchen in den Quelldaten ohne mehrere, manuelle und repetitive „blinde" Vorgänge.

- Es gelten keine Limits mehr für die Anzahl der Postfächer, die durchsucht werden können. Dies war bei eDiscovery in Exchange Online der Fall, wurde aber in der eDiscovery im neuen Security & Compliance Center gelöst/entfernt.

- Aufbewahrungspflichten aus juristischen Gründen können bei Daten an Office 365-Speicherorten (vielen, nicht allen) oder an Drittanbieter-Daten durchgesetzt werden, die in Office 365 importiert wurden (und dann im Exchange-Postfach des Benutzers gespeichert werden).

- 2018 fand eine dramatische Verlagerung der Datenschutzvorschriften statt, die über die Vorschriften traditioneller Datensicherheitsmandate weit hinaus ging. Damit einher ging die Erwartung, in der Lage zu sein, Suchen

Microsoft bietet eine Reihe von eDiscovery-Funktionen für die Suche nach relevantem Material in Office 365 an.

(Zugriffsanforderungen) und dem Recht auf Vergessenwerden (Discovery und Löschen) Rechnung tragen zu können. Office 365 weist zwar grundlegende Funktionen zur Unterstützung dieser Anforderungen auf, doch sind weiterhin die IT-Abteilungen dafür verantwortlich, diesen mittels IT-zentrischer Prozesse und Admin-Schnittstellen gerecht zu werden. Mit der DSGVO und dem neuen California Consumer Privacy Act (kalifornisches Verbraucherschutzgesetz) werden solche Aufforderungen 2019 wahrscheinlich stark zunehmen. Daher müssen Organisationen darauf vorbereitet sein, dass die Arbeit der IT-Abteilung durch viele Anfragen unterbrochen wird, die eigentlich im Verantwortungsbereich rechtlicher oder Kundenerfolgsabteilungen liegen sollten. Es stehen Drittanbieter-Tools zur Verfügung, um diese Compliance-Anforderung zu unterstützen und zu verhindern, dass dadurch ein IT-Engpass entsteht.

Microsoft bietet eine Reihe von eDiscovery-Funktionen für die Suche nach relevantem Material überall in Office 365 sowie einen erweiterten eDiscovery-Dienst namens Advanced eDiscovery, der zusätzlich Textanalysen, Machine Learning sowie Relevanz- und prädiktive Programmierung für die frühzeitige Fallbeurteilung bietet. Advanced eDiscovery ist im Rahmen des Premium-Enterprise E5-Abonnements sowie als zusätzliches kostenpflichtiges Add-on für das Enterprise E3-Abonnement verfügbar. Allerdings gilt:

- Es gibt keine Workflow- oder Projektverfolgung eines eDiscovery-Falles wie z. B. zum Status des Falles (außer „aktiv" und „abgeschlossen"), zu den Beteiligten und den Aufgaben, an denen gearbeitet wird.

- Ein eDiscovery-Falladministrator kann im Security & Compliance Center keine Benachrichtigungen zur Aufbewahrungspflicht aus juristischen Gründen senden, auch keine Erinnerungen oder Eskalationen. Diese müssen extern bearbeitet werden. Wie oben angegeben ist der Mangel an Workflow- und Projektverfolgungs-Fähigkeiten nicht ideal.

- Suchen nach Schlüsselwörtern, die im Tool für die Inhaltssuche begonnen werden, können nicht in einen eDiscovery-Fall importiert werden. Die beiden Dienste sind unterschiedlich und bieten keine Integration. Die einzige Möglichkeit, damit eine Suche in einem eDiscovery-Fall funktioniert, besteht darin, sie innerhalb des Falles zu erstellen.

- eDiscovery-Fälle bestehen aus Sperren und Suchen. Keine zwei Suchen innerhalb eines eDiscovery-Falls in der Organisation können denselben Namen haben. Office 365 erlaubt im gesamten Mandanten nur eine einmalige Verwendung eines bestimmten Namens in eDiscovery-Fällen.

- Alle Fälle werden auf Ad-hoc-Weise erstellt und verwaltet. Ein Compliance-Beauftragter gibt die Ad-hoc-Suchbegriffe ein. Es ist nicht möglich, eine Fallvorlage für Wiederholbarkeit und Auditing zu erstellen, mit Standardsuchanfragen und -orten, Schlüsselaktionen und Anforderungen, die abgeschlossen werden müssen, sowie einem Audit-Pfad der erfolgten bzw. unterlassenen Aktionen. Das ist besonders für Organisationen problematisch, die nicht ständig eDiscovery betreiben. Der Ad-hoc-Ansatz bedeutet, dass frühere Erkenntnisse und Ansätze in einem aktuellen eDiscovery-Fall wahrscheinlich vergessen und übersehen werden, wodurch einer Organisation aufgrund unzureichender Beweisbereitstellung Sanktionen auferlegt werden könnten.

- Es ist eDiscovery-Managern nicht möglich, einen stärker eingeschränkten Suchumfang für OneDrive- und SharePoint Online-Repositorys und Exchange-Postfächer zu konfigurieren. Jeder eDiscovery-Manager kann jeden OneDrive-Ordner, jede SharePoint Online-Site oder jedes Exchange-Postfach weltweit durchsuchen. Es sollte möglich sein, dies nach geografischer Region oder Land einzuschränken, um Daten zu schützen.

- Es ist nicht möglich, den Suchumfang für E-Mail-Nachrichten so festzulegen, dass der Signaturblock ausgeschlossen wird. Erscheint ein Suchbegriff in E-Mail-Signaturen, generiert er eine hohe Rate an falschen Positiven.

- Die eDiscovery-Funktionen im Security & Compliance Center verfolgen einen einheitlichen Ansatz bei relevanten Inhalten in drei Speichercontainern in Office 365: Benutzer- und Gruppen-Postfächer in Exchange Online, Sites in SharePoint und OneDrive sowie öffentliche Exchange-Ordner. Workloads, die Inhalte in diesen Containern speichern, können durchsucht werden. Andere Workloads, bei denen das nicht der Fall ist, werden jedoch ausgeschlossen (z. B. Yammer, Microsoft Stream und Microsoft Planner). Darüber hinaus kann ein eDiscovery-Fall, der im Security & Compliance Center erstellt wird, nicht nach relevanten Inhalten in Nicht-Office 365-Inhaltsspeichern suchen, wie z. B. lokal oder in anderen Cloud-Diensten gepflegten Speichern. Dieser begrenzte Ansatz bedeutet, dass jede Organisation mit Inhalten außerhalb von Office 365 (einschließlich lokales SharePoint 2013 und 2016) mehrere eDiscovery-Tools benötigt, und das zusätzlich zu der Notwendigkeit, mehrere eDiscovery-Fälle in jedem separaten Tool zu instanziieren, auszuführen und zu koordinieren.

- Bei Suchen in öffentlichen Exchange-Ordnern gilt das Motto: Alles oder nichts. Es besteht keine Möglichkeit, die Suche auf eine gezielte Liste einzuschränken.

- Suchergebnisse für Exchange Online, SharePoint Online und OneDrive müssen aus Office 365 exportiert werden, um die Prüfung zu erleichtern: der Exchange-Inhalt als eine oder mehrere PST-Dateien und der SharePoint- und OneDrive-Inhalt als einzelne Dateien (mit einer Option für alle Versionen). Mit dem Office 365-Ansatz sind mehrere Probleme verbunden: Es entsteht ein doppelter Satz von Inhalten außerhalb von Office 365, die geschützt werden müssen. Es gibt keine Berichterstattung zu an den exportierten Inhalten im eDiscovery-Fall in Office 365 vorgenommenen Aktionen, weil Office 365 gegenüber Aktionen nach dem Export blind ist. Wird die Suche erneut in Office 365 ausgeführt, sind ein darauffolgender Export sowie die Integration mehrerer Sätze der Daten erforderlich. Dabei gibt es keine Verbindung zwischen den erfassten Informationen und den an diesem Inhalt getroffenen Programmierungsentscheidungen, die für zukünftige Fälle herangezogen werden und das Volumen des potenziell relevanten Inhalts in Office 365 reduzieren könnte. Die Notwendigkeit, Inhalte nach Azure zu exportieren (mit den Zeitverzögerungen, die von Office 365 nach Azure und dann von Azure zu einem lokalen Computer verursacht werden), sorgt für nicht dienliche Verzögerungen bei einem für Compliance-Beauftragte dringenden Vorgang. Mit der Einführung der DSGVO Ende Mai 2018 führt die potenzielle Existenz von personenbezogenen Daten an zusätzlichen Orten zu signifikanten Daten-Governance-Problemen.

- Exporte aus Office 365 werden nicht geschützt. Dadurch besteht das Risiko, dass sie verändert oder unbrauchbar gemacht werden. Die Ausgabe erfolgt in rohem nativem Exportformat und nicht in einem Erhaltungsformat wie z. B. einem forensischen Bildformat, wie es viele eDicsovery-Erfassungs-Tools bieten. Darüber hinaus bietet Microsoft keine zusätzlichen Verschlüsselungsoptionen für den Export.

Es ist eDiscovery-Managern nicht möglich, einen stärker eingeschränkten Suchumfang für OneDrive- und SharePoint Online-Repositorys zu konfigurieren.

OFFICE 365 INDEXIERT NICHT ALLE WICHTIGEN DATEITYPEN

Bei einer eDiscovery-Suche und Durchführung einer frühzeitigen Fallbewertung (Early Case Assessment) wird jede Datei, die nicht in den 58 unterstützten Dateitypen enthalten ist, als nicht verarbeitet gekennzeichnet. Wenn DLP-Regeln angewendet

werden, lösen nicht in den 58 enthaltene Dateitypen die Erfassungsregeln nicht aus. Das bedeutet, dass diese nicht unterstützten Dateitypen durch einen Compliance- oder Sicherheitsbeauftragten geprüft werden müssen, was für zusätzliche Kosten sorgt und den Informationsaustausch verzögert.

Schlüsselwortsuchen fehlen aufgrund der Verwendung eines „Beste Leistung"-Indexes relevanter Inhalte. Verwendet eine Organisation regelmäßig nicht unterstützte Dateitypen, sollte sie Drittanbieter-Tools zur Indexierung zusätzlicher Dateitypen in Erwägung ziehen.

SENSIBLE DATEN

Office 365 weist mehrere Einschränkungen bei der Suche nach sensiblen Daten in E-Mail-Nachrichten auf:

- Die Analyse von Inhalten auf sensible Daten stützt sich auf die von Microsoft bereitgestellten Typen sensibler Informationen oder eine vom Kunden erstellte spezifische Definition. Der Abgleich sensibler Daten ist einfach zu umgehen, um Daten auszufiltern. Die Vergleichsalgorithmen suchen nach genauen Übereinstimmungen und sind einfach auszutricksen. Zum Beispiel:
    - Der Vergleich einer Kreditkartennummer kann durch Ändern einer der 16 Ziffern in das entsprechende Wort umgangen werden. Wenn z. B. die letzten vier Ziffern als „997vier" geschrieben werden, findet kein Vergleich mit den Kreditkarten-RegEx (regulären Ausdrücken) statt.
    - Das Abstimmen eines SWIFT-Codes kann ebenfalls umgangen werden, indem eine Ziffer in ein Wort oder ein Buchstabe in die Entsprechung aus dem phonetischen NATO-Alphabet abgeändert wird. Ein Beispiel: Anstatt den SWIFT-Code WPACNZ2W zu schreiben (der mit dem sensiblen Informationstyp verglichen werden soll), wird durch Schreiben als WPACNovemberZ2W kein Vergleich ausgelöst, und die DLP-Regel greift nicht. Dies gilt sogar, wenn die E-Mail-Betreffzeile und der E-Mail-Text angeben, dass in der Nachricht ein SWIFT-Code enthalten ist.
- Selbst wenn nicht versucht wird, das Vorhandensein sensibler Informationen absichtlich zu verschleiern, werden Nachrichten, die sensible Informationen erhalten, durch DLP-Richtlinien nicht erfasst, wenn erklärende Metadaten in der E-Mail fehlen. Ein Beispiel: Eine E-Mail mit einer Ausweisnummer und ohne den erklärenden Ausdruck „Ausweisnummer" löst keine DLP-Richtlinie aus, die nach Ausweisnummern sucht.

Office 365 weist mehrere Einschränkungen bei der Suche nach sensiblen Daten in E-Mail-Nachrichten auf.

Zusammengefasst gilt: Der Abgleich sensibler Daten erfordert zu viel Perfektion bei der Formulierung dieser Daten in einer Nachricht, und es wird keine ausgeglichene Evaluierung auf das Vorhandensein sensibler Daten genutzt.

KEINE LANGFRISTIGE SPEICHERUNG VON ÜBERWACHUNGSPROTOKOLLEN ZU COMPLIANCE-ZWECKEN

Das Office 365-Überwachungsprotokoll bewahrt Audit-Ereignisse nur 90 Tage lang auf (für Office 365-Abonnenten mit Enterprise E3 oder darunter). Es gibt keine Möglichkeit, diesen Zeitraum zu verlängern. Das bedeutet, dass das Überwachungsprotokoll nichts für eine Organisation tun kann, die ein Problem rückverfolgen möchte, das vor mehr als drei Monaten auftrat. Die Ausnahme sind Überwachungsprotokoll-Einträge für Exchange Online, bei denen ein Administrator die Voreinstellung von 90 Tagen nur für Exchange-Überwachungsprotokoll-Einträge ändern kann. Für Kunden mit Office 365 E5 und Microsoft 365 können Überwachungsprotokoll-Einträge maximal ein Jahr lang aufbewahrt werden. Diese Änderung wurde zur öffentlichen Vorschau im Oktober 2018 eingeführt, gilt aber nur für Überwachungsprotokoll-Datensätze, die nach dem Inkrafttreten dieser längeren Aufbewahrungsdauer generiert wurden. Bestehende Protokolleinträge sind von der längeren Aufbewahrungsdauer nicht betroffen.

Die Überwachungsprotokoll-Funktionen in Office 365 weisen mehrere Probleme auf, darunter:

- E-Mail-Flussereignisse in Exchange Online erstellen keine Überwachungsprotokoll-Einträge. Das bedeutet: Wenn eine E-Mail-Flussregel durch eine E-Mail-Nachricht ausgelöst wird, wird kein Datensatz dieses Vorgangs protokolliert.

- Einträge im Überwachungsprotokoll können nicht aufgrund juristischer Zwecke gesperrt werden, um spezifische, von Benutzern über Zeit ergriffene Aktionen anzuzeigen, die einer Discovery-Aufforderung unterliegen oder Teil einer frühzeitigen Fallbeurteilung sind.

- Der Export von Überwachungsprotokoll-Elementen aus Office 365 ist auf 5000 Einträge beschränkt, außer es werden alle Ergebnisse exportiert (das Limit beträgt dann 50.000 Elemente). Eine Organisation, welche die Auditing-Funktion aktiviert hat, generiert mindestens 10–20 Audit-Elemente pro Person und Tag für einen nicht allzu aktiven Benutzer und möglicherweise Hunderte von Elementen pro Tag für einen aktiven Informationsarbeiter. Manche mittelgroße oder große Organisationen erreichen daher täglich das Limit von 50.000 Elementen. In diesem Szenario muss ein Administrator mindestens einen Export pro Tag festlegen und generieren und hoffen, dass die zeitliche Verzögerung bei der Erfassung der Überwachungsprotokoll-Einträge nicht bedeutet, dass Elemente, die erfasst werden sollten, im Bericht fehlen.

- Ereignisse werden weder in Echtzeit protokolliert, noch stehen sie zur Echtzeitanalyse zur Verfügung. Microsoft zufolge kann dies je nach dem jeweils zu protokollierenden Ereignis von 30 Minuten bis zu 24 Stunden dauern. Kunden haben angegeben, dass es sogar noch länger dauern kann und manche Audit-Ereignisse gar nie erscheinen.

- Exporte werden als CSV-Dateien ausgegeben und lokal gespeichert (außerhalb von Office 365), sodass deren Erfassung und Sammlung verwaltet werden muss. Paradoxerweise gibt es für diese exportierte Datei von Audit-Elementen nichts, das verhindern könnte, dass ein fehlgeleiteter Administrator den Nachweis eigener Fehlhandlungen entfernt. Die exportierte Datei garantiert die Authentizität der darin enthaltenen historischen Informationen nicht.

- Der Grund für spezifische, von einem Admin-Benutzer an einem Office 365-Dienst ergriffene Aktionen wird nicht im Überwachungsprotokoll erfasst oder angezeigt. Es ist unmöglich, anhand der allgemeinen im Überwachungsprotokoll enthaltenen Informationen die Gründe für eine Änderung im Nachhinein zusammenzustückeln.

- Der Office 365-Überwachungsprotokoll-Dienst erfasst keine Ereignisse von lokalen Microsoft-Servern für Organisationen mit hybridem Setup wie z. B. Exchange Server und SharePoint Server zusätzlich zu Office 365. Er kann daher keine konsolidierte Ansicht der überwachungsfähigen Aktivitäten für Organisationen mit hybrider Infrastruktur bereitstellen.

In der kostenlosen und Basic Edition von Azure AD werden Aktivitäts- und Sicherheitsüberwachungs-Elemente maximal nur sieben Tage aufbewahrt. Einblicke in kompromittierte Konten zu gewinnen ist z. B. nur dann möglich, wenn das Problem praktisch unmittelbar festgestellt wird. Mit einem Azure AD Premium P2-Abonnement kann dies auf maximal 30 Tage für Aktivitäts- und 90 Tage für Sicherheitselemente erhöht werden.

Organisationen, die einen langfristigen Zugriff auf Audit-Berichtselemente benötigen (wie z. B. Daten über sieben Jahre, wie es manche Compliance-Vorschriften vorgeben), sollten sich der Einschränkungen des Office 365-Überwachungsprotokoll-Dienstes bewusst sein.

In der kostenlosen und Basic Edition von Azure AD werden Aktivitäts- und Sicherheits-überwachungs-Elemente maximal nur sieben Tage aufbewahrt.

eDISCOVERY FÜR DATEN EHEMALIGER MITARBEITER

Die Durchführung einer vollständigen eDiscovery bedeutet, dass Daten zu ehemaligen Mitarbeitern eingeschlossen werden. Bis dato hat die Microsoft-Funktion zu inaktiven Postfächern ermöglicht, dass die Postfächer von ehemaligen Mitarbeitern unbefristet kostenlos beibehalten werden können. Im Oktober 2017 wurde jedoch die Intention, 3,00 US-Dollar pro Postfach und Monat bzw. 36,00 US-Dollar pro Postfach und Jahr zu berechnen, signalisiert. Nach negativem Feedback von Kunden und MVPs hat Microsoft die Einführung dieser Kosten jedoch bis auf Weiteres zurückgezogen.

Wir prognostizieren, dass das exponentielle Wachstum bei Daten ehemaliger Mitarbeiter es unvermeidlich machen wird, dass für inaktive Postfächer 2019 oder 2020 neue Lizenzbedingungen gelten werden. Dies wird Unternehmen wahrscheinlich dazu motivieren, kostengünstigere Strategien für das Hosting der Daten ehemaliger Mitarbeiter zu verfolgen.

Andere zu erwägende Probleme

VERWALTUNG HYBRIDER UMGEBUNGEN

Die Nutzung hybrider Umgebungen in Office 365 – entweder lokales Exchange oder lokale Systeme bzw. andere Cloud-Lösungen – ist mit neuen Herausforderungen verbunden. Beispielsweise führen Office 365-Hybridbereitstellungen eine ganze Reihe nicht verbundener Schnittstellen lokal und in der Cloud ein, welche die tägliche Verwaltung und Automatisierung erschweren. Darüber hinaus macht die Synchronisierung von Identitäten zwischen lokalen und Cloud-fähigen Regeln es schwierig, ohne komplexe Skripte und Konten mit hohem Berechtigungen Änderungen vorzunehmen. Daher können bestimmte Helpdesk-Aufgaben in hybriden Umgebungen nicht mehr so einfach vom Helpdesk wahrgenommen werden, wodurch die zusätzliche Verwaltungslast in der hybriden Umgebung die wahrgenommenen Vorteile von Office 365 zunichte machen kann.

Organisationen, die in hybriden Umgebungen operieren, sollten Drittanbieter-Lösungen verwenden, um den durch solche hybride Umgebungen entstandenen Herausforderungen zu begegnen. Dies gilt insbesondere für größere Organisation mit einem höheren Anteil an lokalen Benutzern und Anwendungen, selbst nach der Migration zu Office 365.

Organisationen, die in hybriden Umgebungen operieren, sollten Drittanbieter-Lösungen verwenden, um Herausfoderungen die durchsolche hybride Umgebungen entstandenen zu stellen.

AUTHENTIFIZIERUNG MIT AZURE AD FÜHRT ZU EINEM SINGLE POINT OF FAILURE

Als nicht regionaler Dienst kann Azure AD bei Störungen in einer Region zu kaskadierenden Auswirkungen auf andere Datenzentren und Regionen führen. Die Intention ist zwar, dass Azure AD global resilient ist. Die Microsoft-Architektur für Azure hat aber noch keinen ausfallsicheren cloudbasierten Authentifizierungsdienst bereitgestellt. Zum Beispiel unterbrach ein Blitzschlag am 4. September 2018 in Texas die Kühlsysteme des US South Central-Datenzentrums in San Antonio. Dies hatte umfassende Auswirkungen sowohl auf Office 365- als auch Azure-Dienste und Kunden außerhalb der Region US South Central hatten Azure AD-Authentifizierungsprobleme.

Die Einführung neuer Funktionen für MFA durch Microsoft stört oft aktuelle Authentifizierungsrechte, beispielsweise wenn betroffene Benutzer verschiedene Office 365-Dienste nicht mehr verwenden können. Für Kunden ist das ärgerlich und störend.

Die Implementierung von MFA in Azure und Office 365 durch Microsoft führt zu einem Single Point of Failure. Fällt MFA aus, können sich die betroffenen Benutzer nicht anmelden. Dies war seit November 2018 bereits zweimal der Fall. Manche Benutzer, die MFA-Dienste von Drittanbietern zusammen mit Office 365 verwenden, haben angegeben, dass sie von solchen Ausfällen nicht betroffen sind, wie etwa Kunden, die Duo und Okta verwenden.

AUFSICHTSÜBERPRÜFUNG (ZUR FINRA-COMPLIANCE)

Bestimmte Branchenvorschriften, wie etwa die der Financial Industry Regulatory Authority (US-amerikanische Regulierungsbehörde im Wertpapiermarkt; FINRA), erfordern die Erfassung und Prüfung der Kommunikation zwischen bestimmten Personen oder Personen in einer spezifischen Gruppe, um zu gewährleisten, dass keine illegalen oder nicht autorisierten Themen offengelegt oder besprochen werden. Office 365 bot bereits in der Vergangenheit eine Aufsichtsüberprüfungs-Funktion, die mit Exchange Online-Nachrichten funktionierte, aber eine Reihe von Problemen aufwies.

Im Mai 2017 ersetzte Microsoft die Legacy-Aufsichtsüberprüfungsfunktion mit einem neuen Aufsichts-Tool, für das ein Enterprise E5-Abonnement oder das Advanced Compliance-Add-on erforderlich ist. Administratoren mit den entsprechenden Zugriffsberechtigungen können eine oder mehrere Aufsichtsrichtlinien einrichten.

- Jede Person, die von einer Aufsichtsrichtlinie betroffen ist, erfordert eine Enterprise E5-Lizenz oder das Advanced Compliance-Add-on. Dabei sind einzelne Benutzerlizenzen erforderlich; es gibt keine Option auf Organisationsebene.

- Aufsicht funktioniert nur mit Exchange Online in Office 365, lässt Microsofts andere Kommunikations-Tools wie Microsoft Teams, Yammer und Skype for Business aber außer Acht. Unserer Meinung nach ist dieser Abdeckungsumfang zu gering.

- Nach Einrichtung einer Aufsichtsrichtlinie wird für den Empfang erfasster Nachrichten ein privates, freigegebenes Postfach bereitgestellt. Aufsichtsprüfer müssen eine Verbindung mit dem freigegebenen Postfach herstellen, um jede Nachricht zu prüfen und zu beurteilen.

- Es gibt keinen integrierten Workflow, der Prüfer über eine neue Aufsichtsrichtlinie informiert und ihnen ermöglicht, Nachrichten zu prüfen. Beratende Prüfer müssen extern von der Person, welche die Aufsichtsrichtlinie eingerichtet hat, herangezogen werden.

- Jemand kann sich als Person, die unter Aufsichtsüberprüfung gestellt werden soll, und als Prüfer für eine bestimmte Richtlinie einrichten. Es gibt keine Prüfung, um die Trennung dieser Rollen durchzusetzen.

- Es ist nicht möglich, die sensiblen Informationstypen von Microsoft in Aufsichtsrichtlinien zu benutzen.

- Wenn die Aufsichtsrichtlinie um Bedingungen ergänzt wird, müssen die Wörter oder Ausdrücke genau übereinstimmen. Eine falsch buchstabierte Variante löst die Aufsichtsregel nicht aus. Es wäre nützlich, wenn Office 365 die Möglichkeit zur Verwendung einer Fuzzyübereinstimmung nutzen würde, um einen umfassenderen Eindruck davon zu geben, was über Exchange Online abläuft.

- Die Nutzung von Outlook als Aufsichtsschnittstelle bedeutet, dass die Standard-Outlook-Funktionen, wie z. B. Erstellung einer neuen E-Mail, Antworten auf und Löschen einer Nachricht, in der Schnittstelle sichtbar sind. Es ist zu beachten, dass die Löschoption für eine einzelne Nachricht in der Symbolleiste ausgegraut ist. Durch Klicken auf die Löschschaltfläche in einer einzelnen Nachricht wird eine Meldung angezeigt, die besagt, dass die Nachricht nicht gelöscht werden kann. Durch Klicken auf die Option „Alle löschen" in der Symbolleiste werden alle Nachrichten im Postfach gelöscht. Ein Hintergrundprozess legt dann aber alle Nachrichten wieder in das Postfach. Diese Schnittstellenelemente sind verwirrend und unnötig.

- Die in Outlook bereitstehenden Filteroptionen ergeben in puncto Aufsicht keinen Sinn. Es besteht keine Möglichkeit, Nachrichten anhand des für die Aufsichtsrichtlinie relevanten Inhalts oder der relevanten Metadaten zu sortieren und filtern.

Es gibt keinen integrierten Workflow, der Prüfer über eine neue Aufsichtsrichtlinie informiert und ihnen ermöglicht, Nachrichten zu prüfen.

- Der Versuch, alle Nachrichten in einem Aufsichts-Postfach zu löschen, wird nicht im Überwachungsprotokoll für die Nachrichten aufgezeichnet.

- Ein Vorgesetzter kann innerhalb des Aufsichts-Postfachs auf eine Nachricht antworten oder diese weiterleiten. Es gibt aber keine Möglichkeit, zu prüfen, welche Nachrichten aus dem Aufsichts-Postfach versendet wurden.

- Microsoft bietet keine Workflow- oder Fallmanagement-Funktionen für Nachrichten im Aufsichts-Postfach. Dafür muss ein externer Prozess genutzt werden.

- Ein Prüfer mit Zugriff auf mehrere Aufsichts-Postfächer muss jedes davon einzeln durchsuchen. Es gibt keine Möglichkeit, eine gemeinsame Ansicht der verschiedenen Aufsichtsrichtlinien zu erhalten.

- Außer dem Namen des Aufsichts-Postfachs gibt es keinen Hinweis darauf, wie die Aufsichtsrichtlinien-Einstellungen lauten oder warum Nachrichten im Postfach erfasst werden.

- Die Aufsichtsüberprüfung funktioniert nur in Outlook im Web. Es wurde zwar ein Outlook-Client-Add-in versprochen (und eines steht zur Installation zur Verfügung, allerdings mit PowerShell-Befehlen), doch ist es nicht funktionstüchtig.

- Es gibt keine Migrationsunterstützung zwischen der alten Funktion „Aufsichtsüberprüfung" und der neuen Funktion „Aufsicht". Richtlinien aus dem vorherigen Ansatz müssen gelöscht werden. Sie können nicht migriert und aktualisiert werden und werden nicht automatisch von Microsoft aktualisiert.

- Während Nachrichten für die Prüfung nach der Zustellung erfasst werden, besteht keine Möglichkeit, eine Richtlinien verletzende Nachricht unter Quarantäne zu stellen und so weiterzuleiten, dass ihre Freigabe genehmigt werden muss. Zu diesem Zeitpunkt könnte der Schaden bereits angerichtet sein, denn die Nachricht wurde bereits gesendet und zugestellt.

- Das Office 365-Überwachungsprotokoll ist Aufsichtsrichtlinien gegenüber blind. Die Erstellung, Bearbeitung und das Löschen von Aufsichtsrichtlinien werden nicht im Überwachungsprotokoll aufgezeichnet.

Microsoft hat seit Mai 2017 keine Änderungen an der Funktion „Aufsicht" vorgenommen. Kunden mit dringendem Bedarf an einer robusten Aufsichtsüberprüfungs-Funktion sollten Drittanbieter-Angebote in Erwägung ziehen.

ANDERE ZU ERWÄGENDE PROBLEME

- Azure AD-Authentifizierungsprotokolle werden für viele Office 365-Kunden nur sieben Tage lang aufbewahrt. Das bedeutet, dass z. B. Aufzeichnungen zu einem erfolgreichen Phishing-Versuch, der zur Kompromittierung von Kontoanmeldedaten führte, unmöglich zurückzuverfolgen sind, weil Azure AD die historischen Datensätze gelöscht hat.

- Office 365 unterstützt keine Passphrasen (in der Regel längere Ausdrücke, die mehrere Wörter in natürlicher Sprache enthalten, die leichter zu merken sind als ein Passwort mit einem schwierigen Muster). Eine Passphrase könnte z. B. lauten: „Ich bin Clarke Kent und ich bin Superman." Dabei handelt es sich um ein aus 34 Zeichen bestehendes „Passwort", das für den Endbenutzer einfach zu merken, aufgrund seiner Länge aber gleichzeitig für Angreifer schwieriger zu erraten oder zu knacken ist. Office 365 unterstützt Passphrasen nicht, weil Azure AD-Konten die Verwendung von Leerzeichen nicht unterstützen und auf maximal 16 Zeichen begrenzt sind.

- Admins können keine neuen Berichte zum Zugriff und zur Authentifizierung erstellen.

Zusammenfassung

Office 365 ist eine robuste und leistungsfähige Plattform. Osterman Research empfiehlt, dass Organisationen ihre Verwendung ernsthaft in Erwägung ziehen sollten. Eine Plattform mit dem Umfang und im Maßstab von Office 365 kann aber nicht alles für jede Organisation und jedes Szenario sein. Die Vorteile der Migration zu dieser Plattform müssen deren Einschränkungen überwiegen. Daher sollte die Bereitstellung von Drittanbieter-Lösungen entweder als Ersatz für die nativen, von Microsoft bereitgestellten Funktionen oder als deren Ergänzung zur Bereitstellung weiterer Funktionen für die Erfüllung spezifischer organisatorischer Anforderungen ernsthaft in Erwägung gezogen werden.

Sponsor dieses Whitepapers

LITERATUR

[i] https://www.microsoft.com/en-us/microsoft-365/blog/2018/09/24/office-2019-is-now-available-for-windows-and-mac/

[ii] https://www.microsoft.com/microsoft-365/partners/workplaceanalytics

[iii] https://www.fireeye.com/content/dam/fireeye-www/offers/pdfs/pf/email/ig-it-only-takes-one-email.pdf

[iv] https://technet.microsoft.com/en-GB/library/exchange-online-limits.aspx