Cloud Security Services

Microsoft 365 Top 6 Security Use Cases

ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

Microsoft 365 hat sich zur Standard-Produktivitätssuite für grosse und kleine Unternehmen entwickelt. Über eine Cloud-Plattform mit Software können Unternehmen die Zusammenarbeit und Kommunikation im gesamten Unternehmen ihrer Organisation verbessern. Als cloudbasierte Plattform für die Zusammenarbeit versetzt Microsoft 365 Unternehmen in die Lage, Word, Excel, PowerPoint und Outlook für ihre Mitarbeitenden, unabhängig von deren Standort, zur Verfügung zu stellen. Produktivitätsanwendungen, wie SharePoint, OneDrive, Yammer, können nahtlos in diese Bereitstellung integriert werden, um die Produktivität am Arbeitsplatz und die Zusammenarbeit zu verbessern.

Wenn Unternehmen jedoch zu den Cloud-basierten Anwendungen, wie Microsoft 365, wechseln, benötigen sie einen anderen Ansatz für die Sicherheit und die Einhaltung von Datenschutzvorgaben. Im Folgenden sind die sechs wichtigsten Anwendungsfälle aufgeführt, auf die Kunden bei der Evaluierung eines CASB (Cloud Access Security Broker) zum Schutz ihrer geschäftskritischen Microsoft 365-Implementierungen achten sollten.

1 Entfernen Sie öffentliche Freigaben von sensiblen Daten von OneDrive und SharePoint

OneDrive und SharePoint sind cloudbasierte Collaboration-Tools, die die Zusammenarbeit von Unternehmensanwendern erleichtern. Eingesetzt in Tausenden von Unternehmen, kann die Leichtigkeit, mit der Mitarbeitende Dokumente erstellen, hochladen und freigeben können, den Sicherheitsteams erschweren, die schiere Anzahl von Dokumenten, die innerhalb und zwischen Organisationen ausgetauscht werden, zu verwalten.

Es ist nicht ungewöhnlich, dass Unternehmen Links zu sensiblen Daten freigeben, die auch für Geschäftspartner zugänglich sind oder sogar im Internet öffentlich zugänglich bleiben, lange nachdem ein Projekt oder eine Partnerschaft beendet ist. Einfach vergessen, werden diese Links oft erst entdeckt, wenn eine kritische Schwachstelle entdeckt wird, und zwingen die Sicherheitsteams dazu, immer aufholen zu müssen. Mit der Zeit kann Microsoft 365 zu einem Chaos aus öffentlich zugänglichen Links, ungehindertem Zugang zu sensiblen Daten und einem Alptraum aus Berechtigungen werden, der eine zeitraubende Schritt-für-Schritt-Evaluierung für Sicherheitsrisiken notwendig macht.

Netskope kann Microsoft 365-Umgebungen analysieren, einschliesslich OneDrive- und SharePoint-Unternehmensimplementierungen, und Richtlinienverstösse bei Freigaben für Unternehmensdaten, erkennen. Unternehmen können Tausende von Dateien speichern, die bis in den Terabit-Bereich-Speicherplatz reichen. Netskope kann schnell eine umfassende DLP-Analyse über gespeicherte Unternehmensdaten skalieren und nach Freigaben für sensible Daten suchen, die nicht mit den Sicherheitsrichtlinien des Unternehmens übereinstimmen, wie sie von Sicherheitsteams definiert wurden. Alle Verstösse werden sofort entfernt und freigegebene Links, die keine nützliche Funktion mehr für das Unternehmen haben, können gelöscht werden.

Funktionale Anforderungen

- Fähigkeit, sensible Daten zu finden und zu melden, die extern oder öffentlich freigegeben wurden.
- Umfassende DLP für Daten im Ruhezustand in verwalteten Cloud-Diensten.
- Laufende und rückwirkende Richtlinien, die Aktionen unterstützen, wie Entfernen von öffentlichen oder externen Freigaben oder Einschränkung des Zugriffs auf die Ansicht.

Anforderungen für die Bereitstellung

- API (Out-of-Band)

Tipp

Erkundigen Sie sich bei Ihrem CASB-Anbieter, wie tief die Integration mit Microsoft 365 ist. Erlaubt der Grad der granularen Integration die Erkennung aller öffentlichen Datenfreigaben, die sensible Daten enthalten?

2 Erhalten Sie Echtzeit-Transparenz und Kontrolle über risikobehaftete Aktivitäten in allen Anwendungen von Microsoft 365

Microsoft 365 fungiert als IT-Zentralnervensystem und ermöglicht, die Zusammenarbeit unterschiedlicher globaler Teams zu verbessern. Die gleichen Systeme, die eine enorme positive Produktivität ermöglichen, können für riskantes Verhalten missbraucht werden, was dazu führen kann, dass sensible Daten dauerhaft aus dem Unternehmen entweichen. Sicherheitsteams benötigen Tools, mit denen sie das Risikoverhalten überwachen und kontrollieren können, ohne die alltäglichen Geschäftstätigkeiten zu beeinträchtigen. Herkömmliche Sicherheitstools haben weder Einblick noch Kontrolle über die Benutzeraktivitäten in Cloud-basierten Anwendungen wie Microsoft 365.

Netskope für Microsoft 365 hilft Sicherheitsteams, die Aktivitäten, Daten und den Kontext der Arbeitsabläufe in Microsoft 365 und Tausenden von Cloud-Diensten zu verstehen. Eine granulare und detaillierte Ansicht von Microsoft 365-Aktivitäten und Datenflüssen in Ihrem Unternehmen kann Ihren Sicherheitsteams wertvolle Einblicke geben, wie auf Daten zugegriffen wird und von welchen Benutzern und Gruppen. Dies schafft die Voraussetzungen für die Umsetzung von Sicherheitsrichtlinien, die in Echtzeit für alle Microsoft 365-Transaktionen angewendet werden. Über einen Forward Proxy werden Cloud-Services, einschliesslich Microsoft 365, für die Sicherheitsanalyse in Echtzeit an die Netskope Cloud weitergeleitet. Mit Hilfe von Cloud XD kann Netskope granularen Kontext erhalten, indem es Cloud-Apps dekodiert, verschlüsselten Datenverkehr untersucht, Tausende von Cloud-Apps in verwaltete und nicht verwaltete Gruppen unterteilt und dann spezifische Risikobewertungen durchführt. Nach der Entdeckung können Sicherheitsteams alle entdeckten Cloud-Apps, die potenziell als Kanal dienen, um sensible Daten aus dem Unternehmensbereich herauszuschleusen, entfernen.

Funktionale Anforderungen

- Fähigkeit, granulare Aktivitäten, Daten und den Kontext über M365-Anwendungen und Tausende von Cloud-Diensten hinweg zu verstehen.
- Fähigkeit zur Anwendung von Echtzeitrichtlinien zur Einschränkung riskanter Aktivitäten über M365-Anwendungen hinweg.
- Durchführung von DLP-Analysen für M365-Anwendungen und Tausende von Cloud-Diensten.

Anforderungen für die Bereitstellung

- Forward Proxy (Inline)

Tipp

Fragen Sie Ihren CASB-Anbieter, welche Bereitstellungsmodi er unterstützt, um Microsoft 365 zu schützen. Eine Bereitstellung nur im API-Modus bietet eine begrenzte Anzahl von unterstützten Fällen. Die Kombination von API mit dem CASB-Inline-Modus bietet den umfassendsten Schutz für Microsoft 365.

3 Verhindern Sie die Datenexfiltration von Microsoft 365 hin zu nicht verwalteten Cloud-Diensten

Unternehmen investieren oft beträchtliche Summen in die Sicherheit, um Microsoft 365 zu sichern und zu schützen. Die Sicherheitsrichtlinien sind oft auf die Beschränkung des Zugriffs für nicht autorisierte Personen und Geräte ausgerichtet. Doch der grösste, blinde Fleck, der häufig übersehen wird, sind nicht verwaltete Anwendungen, die auf verwalteten Geräten mit Zugriff auf Unternehmensinstanzen von Microsoft 365 liegen. Ein Szenario, das sich in Tausenden von Unternehmen wiederholt, ist ein Mitarbeitender, der rechtmässig Dateien von einer Unternehmensinstanz von Microsoft 365 herunterlädt. Sobald die Dateien auf ein verwaltetes Gerät heruntergeladen wurden, kann ein Mitarbeitender dieselben Dateien auf eine nicht verwaltete Cloud-Anwendung hochladen, wie z. B. eine persönliche Instanz von Microsoft 365, und dabei die etablierten Microsoft 365-Kontrollen vollständig umgehen. Netskope hat seine CASB-Sicherheitsplattform von Grund auf so konzipiert, dass alle Wege aus dem Unternehmen verschlossen sind, sodass sensible Daten nicht nach aussen, ausserhalb der Unternehmensgrenzen, dringen können. Netskope versteht in Echtzeit Tausende von Cloud-Anwendungen, die in Ihrem Unternehmen eingesetzt werden und ermöglicht Ihnen, granulare Sicherheitsrichtlinien zu entwickeln, die Sicherheitsleitplanken für die legitime Nutzung installieren und riskante Aktivitäten verhindern.

Mit Cloud XD kann Netskope Tausende von Cloud-Anwendungen identifizieren, verwaltet oder nicht verwaltet, und sogar zwischen Unternehmens- und privaten Instanzen von Microsoft 365 unterscheiden. Im Gegensatz dazu erlauben granulare Sicherheitskontrollen entweder den Zugriff auf Microsoft 365 oder und sie bieten indirekt die Möglichkeit zum Hochladen sensibler Daten auf persönliche Instanzen von Microsoft 365 oder andere nicht verwaltete Cloud-Anwendungen, wobei die etablierten Microsoft 365-Sicherheitskontrollen umgangen werden können.

Funktionale Anforderungen

- Die Fähigkeit, granulare Aktivitäten, Daten und kontextbezogene Details über Microsoft 365-Anwendungen und Tausende von Cloud-Diensten zu kontrollieren.
- Die Fähigkeit zur Warnung oder Verhinderung von Datenexfiltrationsaktivitäten, die von Microsoft 365 zu anderen Anwendungen stattfinden.
- Durchführung von DLP-Analysen für Microsoft 365-Anwendungen und Tausende von Cloud-Diensten.
- Fähigkeit zur Unterscheidung zwischen Instanzen von Microsoft 365 (z. B. privat vs. Unternehmen).
- Durchführung von Richtlinien auf der Ebene der Cloud-Services-Kategorie mit Erlauben und Blockieren von Aktionen je nach Instanz.

Anforderungen für die Bereitstellung

- Forward Proxy (Inline)

! Tipp

Erkundigen Sie sich bei Ihrem CASB-Anbieter nach dem Umfang der Sicherheits-Cloud-Anwendungen, die sie schützen. Eine vollständig gesicherte Microsoft 365-Bereitstellung kann von einem Benutzer auf einem nicht verwalteten Gerät oder durch ungehinderten Zugriff auf eine nicht verwaltete Cloud-Anwendung umgangen werden.

4 Sicherstellung der Compliance für Microsoft 365

Die Microsoft 365-Suite von Anwendungen dient als Repository für Unternehmensdaten. Daten werden erstellt, hochgeladen, heruntergeladen und von Unternehmensanwendern gemeinsam genutzt - eine Möglichkeit, die von riskanten Insidern missbraucht werden könnte. Sensible Daten können leicht nach aussen dringen und die gesamte Compliance und die Datensicherheitsanforderungen eines Unternehmens gefährden. Sicherheitsteams müssen die Sichtbarkeit und Kontrolle haben, um sicherzustellen, dass sensible Daten kontinuierlich überwacht werden, unabhängig davon, wo sie transportiert werden, um jede Möglichkeit des Datenmissbrauchs zu verhindern.

Wenn Kunden Microsoft 365 einsetzen, sind sie verantwortlich für Massnahmen zur Einhaltung von Vorschriften, die kontrollieren, wie auf regulierte Daten zugegriffen wird und von welchem Benutzer oder welcher Gruppe. Neue Leitplanken sind erforderlich, um sicherzustellen, dass auf Daten nicht zugegriffen wird, sie nicht angezeigt, heruntergeladen oder andere Aktionen durchgeführt werden, die die gesamte Organisation dem Risiko der Nichteinhaltung von Vorschriften aussetzen.

Netskope bietet eine zusätzliche Ebene von Sicherheitskontrollen, die Unternehmen dabei hilft, die gesetzlichen Vorschriften einzuhalten. Granulare Transparenz und Kontrollen ermöglichen es Sicherheitsteams, eine umfassende DLP-Durchsetzung zu etablieren, wie zum Beispiel die sofortige Blockierung der Exfiltration von regulierten Daten nach ausserhalb des Unternehmensperimeters. Vorgefertigte Vorlagen beschleunigen die Entwicklung von Compliance-Richtlinien und ermöglichen Sicherheitsteams deren Anpassung an die Anforderungen des Unternehmens.

Funktionale Anforderungen

- Die Fähigkeit, granulare Aktivitäten, Daten und kontextbezogene Details über Microsoft 365-Anwendungen und Tausende von Cloud-Diensten zu verstehen.
- DLP-Analyse für Microsoft 365-Anwendungen und Tausende von Cloud-Diensten.
- DLP-Analyse mit Vorlagen zur Einhaltung von Vorschriften und der Möglichkeit, den Kontext über einen Richtlinienassistenten zu definieren.
- Berichtsfunktion zur Erfüllung der Anforderungen von Prüfern, um Compliance-Massnahmen zu verifizieren.

Anforderungen für die Bereitstellung

- Forward Proxy (Inline)

Tipp

Fragen Sie Ihren CASB-Anbieter, wie viele vorgefertigte Compliance Vorlagen bereitgestellt werden. Vermeiden Sie die Aufgabe, jede Compliance-Richtlinie von Grund auf neu zu erstellen, was stundenlange manuelle Arbeit erfordern kann und anfällig für Fehler ist.

5 Schutz vor hochentwickelten, modernen Cyberbedrohungen in Microsoft 365

Microsoft 365 ist zunehmend zum Ziel geworden, da Cyberkriminelle ihre Angriffsvektoren dorthin verlagern, wo Unternehmensanwender zusammenarbeiten, kommunizieren und sensible Informationen aufbewahren. Mit globalem Zugriff der Cloud eröffnet Microsoft 365 Cyberkriminellen potenziell mehrere Möglichkeiten, in das System einzudringen und auf sensible Unternehmensdaten zuzugreifen. Sicherheitsteams benötigen einen fortschrittlichen Microsoft 365 Bedrohungsschutz, der gegen die neuesten Angriffskampagnen schützt, die auf ihr Unternehmen abzielen.

Netskope für Microsoft 365 bietet eine umfassende Sicherheitsplattform zur Abwehr fortschrittlicher Cyberbedrohungen, einschliesslich Bedrohungen wie Cloud-Phishing. Der Netskope Inline Schutz kann bösartige Links und Malware in Echtzeit verhindern, die tief in den Cloud-Traffic des Unternehmens eingebettet sind – einschliesslich des Datenverkehrs von Microsoft 365. Darüber hinaus kann Netskope den Microsoft 365-Datenverkehr aufschlüsseln und mit Entschleierungswerkzeugen, Sandboxing und maschinellem Lernen nach bösartigen Mustern, Verhaltensweisen und Indikatoren, die auf Cyberbedrohungen hindeuten, suchen. Organisationen können durch Netskope Malware und bösartige Links, die bei Phishing-Angriffen verwendet werden, verhindern, erkennen und unter Quarantäne stellen. In SharePoint und OneDrive eingebettete Malware wird beim Herunterladen auf Endgeräte der Unternehmensnutzer blockiert, um zu verhindern, dass Malware in Ihrem Unternehmen Fuss fassen kann.

Funktionale Anforderungen

- Fähigkeit zur Erkennung und zum in Quarantäne setzen bösartiger Malware in OneDrive und SharePoint.
- Analyse von Cloud-Diensten und Web-Traffic in Echtzeit, um bösartige Malware zu verhindern.
- Fähigkeit, über Ransomware-Infektionen zu berichten und Ermöglichung der Rückkehr zu einem Zustand vor der Infektion der Daten.
- Erkennung von anomalem Verhalten durch Entschärfungstools, Sandboxing und maschinelles Lernen, um punktgenau unbekannte cyberkriminelle Aktivitäten oder böswillige Insider zu entdecken.

Anforderungen für die Bereitstellung

- API (Out-of-Band)
- Forward Proxy (Inline)

! Tipp

Fragen Sie Ihren CASB-Anbieter, ob er Malware-Prävention und -Erkennung in Echtzeit bieten kann, wenn Daten zwischen Unternehmensanwendern und Ihren Cloud-Anwendungen hin- und hergehen. Fragen Sie, wie sie vor unbekannten und versteckten Bedrohungen schützen, einschliesslich Cloud-Phishing unter Verwendung betrügerischer oder kompromittierter Instanzen. Warten sie, bis bösartige Dateien und Links in Ihrer Cloud-Anwendung gespeichert werden, und bieten dann nur über die API Abhilfe?

6 Transparenz und Kontrolle über nicht verwaltete Geräte, die auf Microsoft 365 zugreifen

Microsoft 365 bietet eine Plattform für Zusammenarbeit und Produktivität für Mitarbeitende, unabhängig von ihrem Standort und den verwendeten Geräten. Dieser universelle Zugang bietet enorme Flexibilität für die unterschiedlichen Anforderungen am Arbeitsplatz. Da die Mitarbeitenden jedoch von ihren persönlichen Geräten aus auf Microsoft 365 zugreifen, entstehen neue Risiken für Unternehmen. Mit dem Zugang zu Microsoft 365 können Mitarbeitende Unternehmensdaten auf persönliche Geräte herunterladen. Unternehmen haben oft keinen Einblick in diese Aktivitäten ihrer Mitarbeitenden, wodurch ein Schleier der Unklarheit über potenziell kritische Aktivitäten, bei denen sensible Daten auf persönliche Geräte heruntergeladen werden, entsteht - direkt vor der Nase der Sicherheitsteams. Schlimmer noch: Mitarbeitende, die das Unternehmen verlassen und Unternehmensdaten auf ihren privaten Geräten mitnehmen, ohne dass ein Einblick oder eine Kontrolle durch die Sicherheitsteams erfolgt.

Netskope kann durch Cloud XD zwischen unternehmenseigenen (verwalteten) und privaten (nicht verwalteten) Geräten unterscheiden und Sicherheitsteams ermöglichen, fein abgestufte Kontrollen durchzuführen, die auf Sicherheitsrichtlinien basieren, die regeln, welche Geräte auf Unternehmensdaten zugreifen, Daten herunterladen oder bearbeiten können.

Funktionale Anforderungen

- Fähigkeit zur Echtzeit-Zugangskontrolle für Benutzer, Geräte, Aktivitäten, Daten.
- Fähigkeit zur Erkennung von Malware oder fortgeschrittenen Bedrohungen, die von nicht verwalteten Geräten ausgehen, die auf M365 zugreifen.
- Fähigkeit zur Unterscheidung zwischen einem verwalteten und einem nicht verwalteten Gerät.
- Fähigkeit zur Durchführung von Zugriffsbeschränkungsrichtlinien (nur anzeigen, sperren usw.) auf der Grundlage des DLP-Profils der Daten.

Anforderungen für die Bereitstellung

- Reverse Proxy (Inline)

Tipp

Fragen Sie Ihren CASB-Anbieter, wie er den Zugriff von nicht verwalteten Geräten auf verwaltete Cloud-Anwendungen regelt. Wenn sie eine Reverse-Proxy-Bereitstellung haben, fragen Sie nach der Anzahl der verwalteten Cloud-Anwendungen, die offiziell unterstützt werden.

Häufigste Bereitstellungsmodi

Schutz von Daten in Microsoft 365 und anderen genehmigten Cloud-Diensten

Bereitstellungsoption	Beschreibung	Wichtigste Vorteile	Einschränkungen
API (out-of-band)	■ Daten und Bedrohungsschutz nahezu in Echtzeit ■ Schutz vor Bedrohungen für Data-at-Rest in verwalteten Cloud-Diensten	■ Schützt Daten im Ruhezustand (Data-at-Rest)	■ Nur verwaltete Anwendungen ■ Nicht in Echtzeit
Reverse proxy	■ Echtzeit-Zugang zu Aktivitäten, Daten und Malware-Bewegungen über einen Browser auf verwalteten und nicht verwalteten Geräten für verwaltete Anwendungen	■ Sichtbarkeit und Kontrolle für nicht verwaltete Geräte	■ Nur verwaltete Anwendungen ■ Nur Browser
Weiterleitungs-Proxy-Netskope-Client	■ Zugang in Echtzeit zu Aktivitäten, Daten und Malware-Bewegungen von einem Browser oder einer nativen App auf verwalteten Geräten	■ Mobile und entfernte Benutzer ■ Native Anwendungen ■ Verwaltete und nicht verwaltete Cloud-Dienste ■ Webtraffic	■ Nur verwaltete Geräte

Eine Kombination dieser 3 Modi bietet eine 100%ige Abdeckung der Anwendungsfälle.

Wir beraten Sie gerne.
Senden Sie uns Ihre Anfrage: cloudsecurity@ispin.ch

ISPIN AG
Grindelstrasse 6
CH-8303 Bassersdorf
Tel.: +41 44 838 31 11
www.ispin.ch

netskope