netskope

WHITE PAPER

Microsoft 365 Management Summary

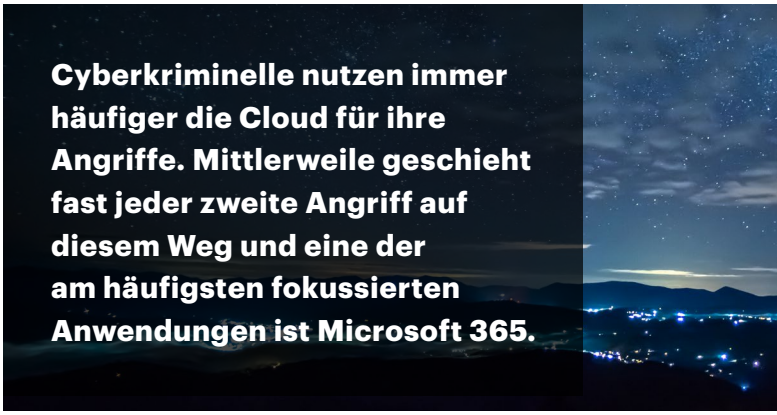
Microsoft 365 hat die Arbeit und Zusammenarbeit im Unternehmen deutlich verbessert. Als Cloud-basiertes Produkt ist es zudem ideal, die Flexibilisierung der Arbeit zu unterstützen und voranzutreiben. Doch durch den Einsatz von Microsoft 365 entstehen auch neue Sicherheitsrisiken. Um diese zu minimieren, bietet Microsoft in seinen Serviceplänen zahlreiche Sicherheits-Features an. Warum diese für einen umfassenden Schutz oftmals nicht ausreichen und weshalb es sinnvoll ist, Ihre Microsoft 365-Sicherheit mit unabhängigem Schutz vom Microsoft Gold-Partner zu vervollständigen und in Ihre Cloud-Security-Strategie zu integrieren, erfahren Sie hier.

GETEILTE VERANTWORTUNG: DAS SHARED RESPONSIBILITY-MODELL VON MICROSOFT

Zunächst ist es wichtig zu verstehen, dass die Sicherung von Microsoft 365 in der gemeinsamen Verantwortung von Microsoft und Ihnen als Unternehmen liegt. Während Microsoft seine Applikationen, Netzwerke und die Infrastruktur effektiv schützt, sind die Unternehmen für die Nutzeraktivitäten, die Daten und die Abwehr von Cyberbedrohungen wie Malware verantwortlich. Microsoft hat in den letzten Jahren viel in die Security investiert und bietet Ihnen verschiedene Servicepläne an. Aber auch der Abschluss solcher Lizenzen entbindet Sie nicht von Ihrer Verantwortung hinsichtlich Nutzerverhalten, Daten und Bedrohungen. Zudem erscheint es sinnvoll, dem von Microsoft bereitgestelltem Schutz eine weitere unabhängige Sicherheitsschicht hinzuzufügen, um insbesondere folgende Herausforderungen zu adressieren.

DATEN IM BLICK UND IM UNTERNEHMEN BEHALTEN

Daten sind Ihr wertvollstes Gut. Der Diebstahl von Kundendaten, geistigem Eigentum oder Produktionsplänen kann enorme Auswirkungen auf Ihr Unternehmen bedeuten – von Bußgeldern wegen Verstößen gegen die DSGVO über Reputationsverlust bis hin zu einer möglichen Insolvenz. Aber auch das Verschieben und Kopieren von Daten in andere Anwendungen oder Cloud-Speicher birgt Risiken. Ein Fünftel der Benutzer bewegt Daten zwischen verschiedenen Cloud-Anwendungen und kopiert beispielsweise Dokumente von OneDrive auf Google Drive oder teilt sie über Slack. Netskope erkennt diese Datenbewegungen – auch wenn sie in nicht gemanagte Applikationen oder private OneDrive-Speicher erfolgen. Microsoft ist hingegen beispielsweise nicht in der Lage, zwischen beruflichen und privaten Nutzerkonten zu unterscheiden. Und anstatt alles standardmäßig zu blockieren und damit auch die Effektivität der Mitarbeiter womöglich unnötig zu beschränken, erlaubt Netskope ein fein abgestimmtes Regelwerk und kann zudem die Nutzer per Nachricht auf nicht gewünschte oder verbotene Aktionen hinweisen. Auf diese Weise wird das Verständnis der Mitarbeiter gefördert und sie für das Thema Datensicherheit sensibilisiert.



MIT SICHERHEIT KREATIV ZUSAMMENARBEITEN

Mit Microsoft Teams beinhaltet Microsoft 365 eines der am meisten genutzten Tools für die Zusammenarbeit. Dabei ist das Teilen von Inhalten und Dokumenten bewusst einfach. Was den kreativen Austausch fördert, kann sich aber negativ auf die Sicherheit und Vertraulichkeit auswirken. Auch hier gilt: Es ist wesentlich effektiver, die Mitarbeiter auf ihr Fehlverhalten hinzuweisen, anstatt ihre Aktivitäten kommentarlos zu blockieren. Dies führt im Zweifelsfall nur dazu, dass sie auf andere Anwendungen ausweichen, über die Sie und Ihre IT-Abteilung keinerlei Kontrolle haben bzw. von der Sie nicht einmal etwas ahnen (die sogenannte Schatten-IT). Mit Netskope wird die Zusammenarbeit gefördert, ohne dabei die Sicherheit zu vernachlässigen: Die Mitarbeiter werden durch gezielte Coaching-Nachrichten auf potenziell gefährliches Verhalten aufmerksam gemacht und so die Datensicherheit gefördert.

ANGRIFFE ERFOLGREICH ABWEHREN

Cyberkriminelle nutzen immer häufiger die Cloud für ihre Angriffe. Mittlerweile geschieht fast jeder zweite Angriff auf diesem Weg und die am häufigsten fokussierte Anwendung ist Microsoft 365! Dabei setzen sie auf aus ihrer Sicht bewährte und Erfolg versprechende Techniken wie Phishing oder Malware, die sich über die Cloud wesentlich unauffälliger und vorbei an vielen herkömmlichen Sicherheitslösungen verbreiten können. Aber egal, welche Technik die Angreifer auch einsetzen: Netskope erkennt durch den Einsatz von künstlicher Intelligenz auch ausgefeilte und hoch entwickelte Angriffe und kann sie schnell und effektiv verhindern, bevor Schaden entsteht.

EFFIZIENZ UND GLEICHZEITIG SICHERHEIT STEIGERN

Auch wenn Ihre Mitarbeiter hauptsächlich mit Microsoft 365 arbeiten, so nutzen sie auch zahlreiche andere Dienste und Anwendungen, sei es um Dateien zu speichern, zusammenzuarbeiten oder Mails zu verschicken. Und obwohl in Unternehmen durchschnittlich nur 142 Anwendungen offiziell genehmigt werden, greifen Mitarbeiter bei ihren täglichen Aktivitäten auf weit mehr Applikationen zu – im Schnitt auf 2.400! Anstatt für jede einzelne Anwendung eigene Sicherheitsrichtlinien festzusetzen ist es sinnvoller und effektiver, eine einheitliche Richtlinie für alle Anwendungen zu etablieren und diese durchzusetzen – unabhängig davon, ob sie von der IT-Abteilung freigegeben wurden oder nicht (Schatten-IT). Mit Netskope können Sie Ihre komplette Cloud-Sicherheit einfach und effektiv von einer zentralen Stelle aus orchestrieren und genau festlegen, welche Nutzer was mit welcher Art Anwendungen tun dürfen. So sorgen Sie für mehr Sicherheit bei weniger Aufwand.

MICROSOFT 365—MIT SICHERHEIT PROFITABEL

Microsoft 365 fördert die Produktivität der Mitarbeiter, egal wo sie sich befinden. Damit Unternehmen hiervon aber wirklich profitieren können, muss die Sicherheit stets und überall gewährleistet sein. Microsoft unternimmt hier in seinem Verantwortungsbereich einiges, jedoch ist es auch an den Unternehmen, ihren Teil dazu beizutragen. Dies sollte idealerweise nicht durch einen Mehraufwand speziell zur Absicherung der Office-Suite gewährleistet werden, sondern im Rahmen einer effektiven, effizienten und umfassenden Cloud-Sicherheitsstrategie. Dies bedeutet mehr Sicherheit bei weniger Aufwand, mehr Kreativität und Produktivität bei weniger Störungen der Arbeitsabläufe.

Machen Sie die Probe aufs Exempel: Stellen Sie Ihrem CISO oder Sicherheitsverantwortlichen die folgenden Fragen:

- Erkennen wir, ob unsere Nutzer Unternehmensdaten in private OneDrive-Speicher kopieren?
- Bemerken wir, wenn sensitive oder interne Daten in einen öffentlichen MS Teams Channel geteilt werden?
- Wissen wir, welche Applikationen in unserem Unternehmen in welchem Umfang und für welche Aufgaben genutzt werden?
- Haben wir je nach genutztem Endgerät unterschiedliche Sicherheitsrichtlinien im Einsatz?
- Wie schnell bemerken wir einen Datenabfluss?
- Können wir unerlaubten Datenfluss in die Cloud verhindern?

Es ist heute wichtiger denn je, Sicherheit zu einer Top-Priorität zu machen und mit den Sicherheitsverantwortlichen ins Gespräch zu kommen, um die gemeinsamen Ziele abzustecken und Möglichkeiten zu identifizieren. Dabei steht Ihnen auch Netskope gerne zur Verfügung. Sprechen Sie mit uns, um herauszufinden, wie sich Microsoft 365 in Ihre Sicherheitsstrategie integrieren lässt, damit wir gemeinsam Ihre Daten wirkungsvoll schützen.

netskope

Die Netskope Security Cloud bietet umfassende Transparenz, Echtzeit-Daten und Bedrohungsschutz beim Zugriff auf Cloud-Dienste, Websites und private Anwendungen von überall und auf jedem Gerät. Netskope versteht die Cloud und bietet datenzentrierte Sicherheit aus einem der größten und schnellsten Sicherheitsnetzwerke der Welt. Damit verfügen die Kunden über das richtige Gleichgewicht zwischen Schutz und Geschwindigkeit, das sie benötigen, um ihre Geschäftsabläufe zu beschleunigen und ihre digitale Transformation sicher voranzutreiben.

Mehr Informationen unter https://www.netskope.com.

©2020 Netskope, Inc. Alle Rechte vorbehalten. Netskope ist ein eingetragenes Warenzeichen und Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index und SkopeSights sind Warenzeichen von Netskope, Inc. Alle anderen Marken sind Marken ihrer jeweiligen Eigentümer. 09/20 WP-407-1