SOPHOS
Security made simple.

Office 365 sicher nutzen

Die Vorteile von Office 365™ liegen auf der Hand. Warum sollten Sie Ihren eigenen Exchange Server einrichten oder Office-Software verwalten, wenn Microsoft® all dies für Sie erledigen kann?

Hierbei müssen Sie jedoch Folgendes beachten: Beim Hosten Ihrer Microsoft-Infrastruktur in Ihrem eigenen Rechenzentrum haben Sie auf ergänzende Sicherheitstechnologien von anderen Anbietern zurückgegriffen, um die Malware-Gefahr einzudämmen und Vorkehrungen gegen Ausfälle zu treffen. Diese Risiken sind auch in Ihrer neuen Cloud- und Office-365-Welt nicht verschwunden.

In diesem Whitepaper beschäftigen wir uns mit der Frage, warum Unternehmen auf Office 365 umstellen, und untersuchen, welche Sicherheitsprobleme sich hieraus ergeben. Anschließend gehen wir auf die Sicherheitstechnologien ein, die Unternehmen neben ihrer Office-365-Bereitstellung benötigen.

Office 365 wird immer beliebter

Office 365 kommt immer flächendeckender zum Einsatz. Schätzungen eines aktuellen Berichts von Gartner zufolge (Implementing Office 365: Gartner Survey Results and Analysis, 2016, veröffentlicht am: 4. Mai 2016) werden 78 % der Unternehmen innerhalb der nächsten sechs Monate Office 365 nutzen bzw. planen eine Nutzung. Dies entspricht einem Anstieg von 13 % gegenüber einer Umfrage aus dem Jahr 2014.

Die Vorteile von Office 365 für Unternehmen jeder Größe sind offenkundig. Sie erhalten Zugang zu modernen Kommunikations- und Kollaborationstools, die dem Branchenstandard entsprechen – ohne Vorab- und laufende Wartungskosten, die beim Betreiben dieser Dienste vor Ort für die Verwaltung von Hardware und Software anfallen. Für die Bereitstellung von Office 365 sind keine Upgrades, neuen Server oder zusätzlichen Sicherheitssysteme vor Ort erforderlich, um diese Infrastrukturen vor neuen Cyberangriffen zu schützen. Die Nutzungskapazität lässt sich durch Deaktivieren überflüssiger Accounts bzw. Einrichten zusätzlicher Accounts flexibel regulieren.

Sie outsourcen quasi die Wartung Ihrer Exchange-Server und Geschäftsanwendungen an Microsoft. Auf diese Weise entlasten Sie Ihre IT-Abteilung, sodass diese sich auf andere IT-Projekte konzentrieren kann.

Sicherheitsbedenken beim Einsatz von Office 365 bleiben

Office 365 ist zweifellos ein nützliches Tool, das der Geschäftsproduktivität sehr zuträglich ist, und Microsoft bietet leistungsstarke Sicherheitsfunktionen für in der Cloud gespeicherte Kundendaten. Es müssen jedoch viele weitere Sicherheitsfaktoren berücksichtigt werden. Gartner zufolge schützen 40 % aller Nutzer von Office 365 ihre Bereitstellung mit Sicherheitslösungen von Drittanbietern, um Sicherheitslücken zu stopfen. Ihre Benutzer, Workstations, Server und Daten außerhalb der Cloud benötigen zusätzliche Sicherheit. Hierbei gilt es, eine ganze Reihe von Punkten zu berücksichtigen:

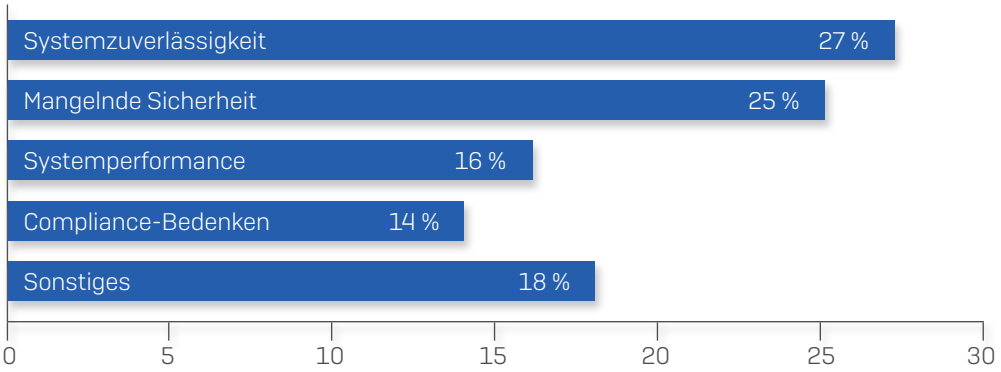
Firewall- und Web-Sicherheit: Mit Office 365 erhalten Sie kein Secure Web Gateway, um den Internetzugang der Enduser zu schützen und zu kontrollieren, und auch keine Firewall, um die Netzwerkgrenze Ihres Unternehmens abzusichern.

E-Mail-Sicherheit und unterbrechungsfreier E-Mail-Zugriff: Obwohl Microsoft Add-on-Subscriptions für E-Mail-Security-Funktionen anbietet, berichten viele Kunden dennoch von Problemen mit Spam und Malware und greifen daher lieber auf Lösungen von speziellen IT-Security-Anbietern zurück. Außerdem haben häufige Ausfälle von Office 365 in jüngster Zeit gezeigt, dass E-Mail-Continuity-Services erforderlich sind, z. B. E-Mail-Spooling und Notfall-Posteingang, damit die Benutzer beim Ausfall des Services weiterhin auf ihre E-Mails zugreifen können. Microsoft Exchange Online (enthalten in den Office-365-Plänen E1, E3 und E5) bietet Ihnen nicht die gleichen wichtigen E-Mail-Continuity-Funktionen, die Sie vor Ort bereitgestellt haben.

Next-Gen Endpoint Security: Office 365 sieht auf Endpoint-Ebene keinerlei Abwehrmaßnahmen zum Schutz vor gefährlichen Malware-Bedrohungen wie Ransomware vor.

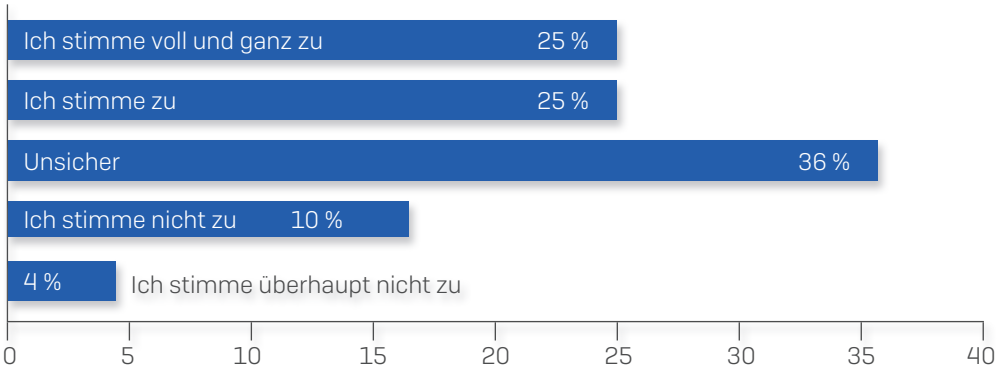
Die sich hieraus ergebenden Sicherheitsbedenken sind in Unternehmen heutzutage allgegenwärtig. Einer aktuellen Sophos-Studie zufolge sind „Systemzuverlässigkeit“ und „mangelnde Sicherheit“ die größten Problembereiche für Unternehmen, die Office 365 als E-Mail-Plattform nutzen.

Welches sind die größten Probleme beim Einsatz von Office 365 als Ihre E-Mail-Plattform?



50 % der Befragten stimmten zu bzw. stimmten voll und ganz zu, dass Sicherheitslösungen von Drittanbietern unerlässlich sind, um die unzureichende Sicherheit von Office 365 aufzustocken.

Sicherheitslösungen von Drittanbietern sind unerlässlich, um die unzureichende Sicherheit von Office 365 aufzustocken.



Es ist daher wenig verwunderlich, dass die meisten Unternehmen ihre Office-365-Implementierung mit Sicherheits- und Continuity-Lösungen von anderen Anbietern aufstocken. Der weiter oben bereits zitierte Gartner-Bericht (Implementing Office 365: Gartner Survey Results and Analysis, 2016, veröffentlicht am: 4. Mai 2016) führt zudem aus, dass 23 % auf die Frage hin, warum ihr Unternehmen Office 365 nicht nutzt und die Nutzung auch nicht in Betracht gezogen hat, als Hauptgrund auf rechtliche oder geschäftliche Datenschutzbedenken verweisen.

Unterbrechungsfreier E-Mail-Zugriff

E-Mail-Anwendungen sind für den Geschäftsbetrieb in den allermeisten Unternehmen unerlässlich und auch der Hauptgrund, warum Unternehmen auf Office 365 umstellen. In einer aktuellen Studie von Gartner (Implementing Office 365: Gartner Survey Results and Analysis, 2016, veröffentlicht am: 4. Mai 2016) stuften 70 % der Befragten Exchange Online als eine der drei wichtigsten Funktionen von Office 365 ein.

Office 365 ist in der Regel sehr zuverlässig und sichert eine 99,9%ige Verfügbarkeit zu. Eine Ausfallquote von nur 0,1 % entspricht jedoch mehr als 8¾ Stunden pro Jahr. Zudem kommt Osterman Research in seinem Whitepaper „Microsoft® Office 365® for the Enterprise: How to Strengthen Security, Compliance and Control" vom März 2014 zu folgendem Schluss:

„In einem durchschnittlichen Unternehmen beträgt der Produktivitätsverlust infolge von E-Mail-Ausfällen 20 Cents pro Benutzer und Minute. Ein einziger 30-minütiger Ausfall kostet ein Unternehmen mit 500 Benutzern also 3.000 USD."

Falls die Verfügbarkeit auf unter 95 % fällt, erstattet Microsoft die monatliche Gebühr zu 100 %. Wenn man jedoch Ostermans Zahlen zugrunde legt, kostet eine Ausfallquote von 5 % ein Unternehmen mit 500 Benutzern 216.000 USD pro Monat – also wesentlich mehr als das Office-365-Abonnement.

Und Ausfälle passieren. Das belegen mehrere Fälle aus den Medien, bei denen der Ausfall von Office 365 für Probleme sorgte – sowohl in den USA (http://www.theregister.co.uk/2016/06/30/office_365_down_in_nyc/) als auch in Europa (http://www.computing.co.uk/ctg/news/2447946/office-365-suffers-global-outage-due-to-high-resource-utilisation).

Office 365 mit Cloud Security ergänzen

Wie bereits erwähnt, ist eine Migration in die Cloud mit vielen Vorteilen verbunden – keine Upgrades, keine neuen Server, keine Wartung und erhebliche Zeitersparnis bei der Verwaltung. Es ist daher sinnvoll, nach einer Sicherheitslösung zu suchen, die dieselben Vorteile bietet. Hier finden Sie eine Übersicht der Funktionen, die in keiner Cloud-Security-Lösung zum Schutz von Office 365 fehlen dürfen:

1. Einfache cloudbasierte Verwaltung

Office 365 macht die Verwaltung einfach – genau das sollte auch Ihre Sicherheitslösung können.

Wie viele Dashboards müssen Sie momentan im Auge behalten? Stellen Sie sicher, dass Sie die von Ihnen gewählte Sicherheitslösung über eine zentrale Ansicht verwalten können. So sparen Sie wertvolle Zeit.

2. Integrierte Sicherheit für besseren Schutz

Office 365 bietet eine Vielzahl von ineinandergreifenden Funktionen – Gleiches sollte auch für Ihre Sicherheitslösung gelten.

Suchen Sie nach Sicherheitslösungen, die durch den Austausch relevanter Informationen schnellere, präzisere Entscheidungen ermöglichen und auf diese Weise besseren Schutz bieten. Bleiben Ihre Dateien beispielsweise geschützt, wenn Sie von der Cloud auf mobile Geräte oder Endpoints übertragen werden? Werden kompromittierte Geräte automatisch isoliert und in ihren Rechten beschränkt (z. B. Einziehen von Schlüsseln und Sperren des Netzwerkzugriffs)?

Darüber hinaus herrscht im IT-Security-Bereich ein eklatanter Fachkräftemangel. Einem aktuellen Bericht der Enterprise Strategy Group zufolge räumen 46 % aller Unternehmen mittlerweile ein, nicht genügend auf Cybersecurity spezialisierte Mitarbeiter zu haben. Dies entspricht einem Anstieg von 28 % gegenüber dem Vorjahr. Quelle: ESG Research Blog, High-Demand Cybersecurity Skill Sets, May, 2016

Am besten können Sie diesem Problem aus dem Weg gehen, indem Sie sich für ein integriertes, benutzerfreundliches System entscheiden.

3. Unterbrechungsfreier E-Mail-Zugriff

Wie bereits erwähnt, sind die finanziellen Folgen von E-Mail-Ausfällen nicht zu unterschätzen. Sie benötigen eine Lösung, die den E-Mail-Verkehr auch bei einem Ausfall von Office 365 aufrechterhält. Jede Sicherheitslösung sollte über Funktionen wie E-Mail-Spooling und Notfall-Posteingänge verfügen, damit Mitarbeiter auch bei Ausfällen auf ihre E-Mails zugreifen können. Achten Sie darüber hinaus auf leistungsstarke Antivirus-, Anti-Spam- und Anti-Phishing-Funktionen.

Sophos Central

Sophos Central ist eine Cloud-Verwaltungsplattform, mit der Sie alle erforderlichen Sicherheitsfunktionen in einem benutzerfreundlichen Paket erhalten. Sophos Central bietet leistungsstarken Schutz für Ihr gesamtes Unternehmensnetzwerk – für Endpoints, mobile Geräte, Internet, E-Mails, WLAN, Verschlüsselung, Server und Netzwerkkomponenten. Außerdem lässt sich Sophos Central einfach bedienen.

Da es sich um eine Cloud-Lösung handelt, benötigen Sie keine Upgrades, neuen Server oder Wartungsroutinen und profitieren durch den verringerten Verwaltungsaufwand von erheblichen Einsparungen. Und nicht zu vergessen: Sophos Central wird von einem bewährten IT-Security-Marktführer angeboten.

Einfache cloudbasierte Verwaltung

Sophos Central wird zentral über eine Ansicht verwaltet. Sie haben also von einem Ort aus Zugriff auf alle Sicherheitslösungen. Bei der Verwaltung Ihres E-Mail-Gateways erhalten Sie beispielsweise automatische Benachrichtigungen, wenn ein mobiles Gerät kompromittiert wurde, und müssen nicht jede Lösung einzeln auf Meldungen überprüfen.

Besserer Schutz mit Synchronized Security

Die Lösungen in Sophos Central basieren auf Synchronized Security. Das bedeutet, dass Kontextinformationen untereinander ausgetauscht werden, wodurch die Sicherheit weiter verbessert wird. Ein kompromittierter Endpoint kann beispielsweise automatisch vom Unternehmensnetzwerk isoliert werden. Demselben Gerät werden auch die Schlüssel entzogen, damit es nicht auf verschlüsselte Dateien zugreifen kann.

Wichtige E-Mail-Continuity- und Security-Funktionen

Sophos Email (in Sophos Central) ergänzt Office 365 mit E-Mail-Spooling und einem Notfall-Posteingang. Im Falle eines Ausfalls von Office 365 bleiben Ihre E-Mails so weiterhin verfügbar. Darüber hinaus bietet Sophos Email leistungsstarke Antivirus-, Anti-Spam- und Anti-Phishing-Funktionen zur Abwehr neuester Malware-Angriffe, Phishing-Kampagnen und infizierter Websites.

Zusammenfassung

Office 365 bietet im Hinblick auf die Unternehmensproduktivität viele Vorteile. Eine Umstellung auf Office 365 ist zweifellos attraktiv, beseitigt jedoch nicht alle Probleme, mit denen Sie bei der Sicherheit und E-Mail-Verfügbarkeit zu kämpfen haben.

Ihre Microsoft-Infrastruktur mit Technologien anderer Anbieter zu ergänzen, war schon sinnvoll, als Sie Ihre Umgebung noch selbst verwalteten. Die Gefahr durch Sicherheitsbedrohungen und E-Mail-Ausfälle ist auch in Ihrer neuen Cloud- und Office-365-Welt nicht gebannt. Für viele Unternehmen ist es sinnvoll, ihren Office 365 Service mit zusätzlichen, in der Cloud bereitgestellten Security- und Business-Continuity-Lösungen aufzustocken.

Sie haben gesehen, welche Vorteile die Migration Ihrer Microsoft-Geschäftsanwendungen sowie Ihrer Kommunikations- und Collaboration-Infrastruktur in die Cloud bietet. Es ist daher sinnvoll, auch Ihre Sicherheitssoftware in der Cloud bereitzustellen und zu verwalten. Entscheiden Sie sich für eine Lösung, mit der Sie Ihre E-Mail-Security gemeinsam mit Ihren Endpoints, Servern, Ihrem Web-Gateway und Ihrer Mobile-Security-Infrastruktur verwalten können – so sparen Sie Zeit und behalten den Überblick über Ihre Sicherheit und Ihr Budget.

Sophos Central kostenlos testen:
www.sophos.de/central

Sales DACH (Deutschland, Österreich, Schweiz):
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

© Copyright 2016. Sophos Ltd. Alle Rechte vorbehalten.
Eingetragen in England und Wales, Nr. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, GB
Sophos ist die eingetragene Marke von Sophos Ltd. Alle anderen genannten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken ihres jeweiligen Inhabers.

20.09.2016 WP-DE (NP)

SOPHOS