ON-PREMISE VS. CLOUD: WARUM EIN WECHSEL VON MICROSOFT EXCHANGE ZU MICROSOFT 365 NÖTIG IST

UND SIE ZUSÄTZLICHEN SCHUTZ DURCH DRITTANBIETER BENÖTIGEN

Inhalt

Im Januar 2021 wurden **vier Zero-Day-Exploits in On-Premise Microsoft Exchange Servern entdeckt,** die Angreifern vollen Zugriff auf E-Mail-Konten und Passwörter auf den betroffenen Servern, Administratoren-Rechte sowie Zugriff auf angeschlossene Geräte im selben Netzwerk ermöglichten.

Es folgte eine **weltweite Welle an Cyberattacken - schätzungsweise 250.000 Server** waren von den Angriffen betroffen. Der Vorfall zeigt einmal mehr, wie riskant On-Premise Hosting für Unternehmen sein kann. In diesem Infopaper erfahren Sie, wie der **Wechsel von On-Prem zu Microsoft 365 Ihre Betriebsabläufe optimieren kann** und weshalb es wichtig ist, sich nicht nur auf die Sicherheitsfeatures von Microsoft zu verlassen, um Ihr Unternehmen vor Cyberbedrohungen zu schützen.

KAUM EIN WEG FÜHRT AM WECHSEL IN DIE CLOUD VORBEI

Der Microsoft Exchange Server-Hack, von dem **weltweit hunderttausende Server betroffen** waren, ist eine der schwerwiegendsten Cyberattacken der vergangenen Jahre. Nach der letzten Zählung sind mehr als **60.000 Unternehmen dem Angriff zum Opfer gefallen.**

Hochrangige Behörden wie das BSI (Bundesamt für Sicherheit in der Informationstechnik) sowie das Weiße Haus haben die betroffenen Organisationen aufgefordert, Security Patches in ihren jeweiligen Exchange-Systemen zu installieren. Doch **es ist nicht ausreichend, den eigenen Microsoft Exchange Server einfach nur zu patchen,** wenn ein Unternehmen bereits kompromittiert wurde.

Angreifer haben möglicherweise **Hintertüren (sog. Backdoors) installiert oder Konten erstellt** und sich so selbst Zugriffsrechte erteilt.

Betroffene Unternehmen müssen mit hohen Kosten und dem Verlust sensibler Daten rechnen

Betroffene Unternehmen müssen nicht nur den **Ausfall ihrer E-Mail-Kommunikation und Störungen des Betriebsablaufs** im Zuge des Patch-Prozesses hinnehmen, sondern werden im Falle eines erfolgreichen Angriffs mit weitaus schlimmeren Schäden konfrontiert:

Hacker können sensible Unternehmensdaten stehlen oder sich Zugang zu kritischen Geschäftsprozessen verschaffen: darauf können hohe Kosten, rechtliche Konsequenzen und andere Schwierigkeiten folgen.

Und selbst wenn die Exchange-Server gepatcht, die Hintertüren geschlossen und die Angreifer bereits ausgeschaltet sind, ist das noch nicht das Ende der Fahnenstange. Eine **Flut von Spear-Phishing-Attacken könnte folgen,** da die durch den Angriff gesammelten Informationen, wie E-Mails und Dateien, trotzdem weiter genutzt werden können:

Zum Beispiel **zur Erstellung von gezielten und besonders glaubwürdigen Betrugs-E-Mails.**

Cloud versus On Premise – What the experts say

Angesichts des Ausmaßes dieses Angriffs empfehlen die Sicherheitsexperten von Hornetsecurity Unternehmen dringend, **On-Premise-Dienste von Microsoft Exchange durch die cloudbasierte Alternative Microsoft 365** zu ersetzen.

Microsoft 365 befindet sich in der Cloud und ist daher nicht anfällig für Angriffe dieser Art oder Störungen, die durch physische Einflüsse, wie das Wetter, bedingt sind. Auch der **Funktionsumfang von Microsoft 365 ist deutlich größer** und bietet Unternehmen so ein großes Spektrum an Möglichkeiten.

Im Folgenden erfahren Sie **mehr zu den Vorteilen von Cloud-basiertem Hosting gegenüber On-Premise.**

WAS SIND DIE PROBLEME BEI ON-PREMISES-HOSTING?

Obwohl Cloud Computing bei Unternehmen weltweit auf dem Vormarsch ist, stehen Fragen zu möglichen Kosten, dem Aufwand und vor allem der Sicherheit bei einer endgültigen Entscheidung im Vordergrund. Schließlich **ist es essenziell, sensible Daten zu schützen und einen reibungslosen Betrieb aufrechtzuerhalten.**

Das Hosten und Betreiben von Software auf Inhouse-Servern bietet verschiedene Vorteile, wie die volle Kontrolle über die eigenen Systeme, die Tatsache, dass sich die gesamte IT-Infrastruktur im Unternehmen selbst befindet, die lokale Speicherung von Daten, auch ohne Internetverbindung, und die hohen Anpassungsmöglichkeiten. **Dem stehen jedoch einige Nachteile gegenüber, die beispielsweise auch bei Microsoft Exchange zum Tragen kommen:**

Das Unternehmen ist selbst für die Sicherheit einer Daten und das Schwachstellenmanagement verantwortlich:
Um die Datensicherheit muss sich das Unternehmen selbst kümmern. Dies erfordert geschultes IT-Personal, das über Sicherheitslücken Bescheid wissen sowie regelmäßig und schnell Updates installieren, Systemausfälle verhindern und im Ernstfall korrigierend eingreifen muss.

On-Premise-Software ist in den meisten Fällen nicht auf dem neuesten Stand, wodurch Unternehmen angreifbar werden:
Wenn Probleme in On-Premise-Software auftreten und Updates notwendig sind, ist das Unternehmen selbst dafür verantwortlich, diese Fehler zu beheben. Oftmals fehlen an dieser Stelle jedoch die notwendigen Ressourcen oder es fehlen lediglich Informationen zu neuen Patches, so dass es zu entscheidenden Verzögerungen kommt, bis die Software wieder ordnungsgemäß genutzt werden kann.

Kompletter Datenverlust ist möglich:
Das Unternehmen muss nicht nur dafür sorgen, dass die On-Premise-Software auf dem neuesten Stand ist, sondern auch dafür, dass der Hardware nichts passiert. Ohne Backup-Systeme kann zum Beispiel ein Feuer, eine Überschwemmung oder ein technischer Defekt zum Verlust wichtiger Daten führen.

On-Premise ist teuer und zeitaufwändig:
Ein weiterer Nachteil von On-Premise-Software sind die hohen Kosten. Die notwendige Hardware muss vom Unternehmen selbst angeschafft, finanziert und gewartet werden.

Besonders anfällig für Ransomware-Angriffe:
Unternehmen mit On-Premise-Setups waren häufiger Opfer von Ransomware-Angriffen - Eine Analyse der Daten von Ransomware-Leak-Sites durch das Hornetsecurity Security Lab ergab, dass unter den Opfern, deren Daten auf diesen Webseiten veröffentlicht wurden, 25 Prozent der Unternehmen ihre E-Mail-Server vor Ort hosten.

Im Vergleich dazu, zeigen die veröffentlichten Daten von Ransomware-Leak-Sites, die E-Mail nicht als primären Zugriffsvektor nutzen, dass nur 13 Prozent der Unternehmen ihre Mailserver vor Ort hosten.

Das bedeutet, dass das Risiko, Opfer eines E-Mail-basierten Ransomware-Angriffs zu werden, für Unternehmen, die ihre E-Mail-Server selbst hosten, doppelt so hoch ist, als bei Ransomware-Angriffen, die andere Angriffsvektoren nutzen.

WELCHE VORTEILE BIETET DIE CLOUD-BASIERTE MICROSOFT 365 SUITE?

Microsoft gilt als größter Treiber zum Umstieg in die Cloud und hat mit Microsoft 365 die weltweit meistgenutzte Office Suite in die Cloud gebracht. Für Unternehmen, die aktuell **die Risiken von Cyberangriffen auf Cloud-Dienste gegen die technologischen Chancen abwägen,** ist die folgende Liste hilfreich.

Neueste Sicherheitsupdates:
Unternehmen, die Microsoft 365 nutzen, haben automatisch stets Zugriff auf die neueste Version der Lösung, ohne sich selbst um das Patchen kümmern zu müssen. Microsoft liefert die Updates, die Cloud-Anbieter konzentrieren sich nur auf die Zuverlässigkeit und Sicherheit des Systems.

Und Unternehmen können ihrem Kerngeschäft nachkommen. Sollte es zu einem Angriff kommen, installiert der SaaS-Anbieter den Patch einfach selbst. Es ist nicht notwendig, dass jeder einzelne Kunde seine eigenen Patches installiert – das vereinfacht Sicherheitsmaßnahmen enorm.

Modernste Funktionen und eine Vielzahl von Zusatzfeatures:
Das bedeutet auch, dass die Nutzer von Microsoft 365 immer Zugriff auf die neuesten Funktionen haben. Die Updates erfolgen automatisch. Die im Paket enthaltenen Zusatzfunktionen wie Microsoft Teams, OneDrive, SharePoint etc. vereinfachen die Zusammenarbeit innerhalb des Unternehmens und erleichtern den Austausch von Daten.

Einfach zu bedienen und zu warten:
Die Bedienbarkeit von Cloud-basierten Anwendungen wie Microsoft 365 ist weniger komplex. Sie können in wenigen Minuten installiert werden und auch die Wartung von Hardware entfällt.

Ressourcen sparen:
Durch den Einsatz von Cloud-Software sparen Unternehmen nicht nur den Aufwand für den Betrieb von Rechenzentren und Serverräumen, sondern unter anderem auch die Beschaffung, Installation, Konfiguration, Wartung und Aktualisierung von Software.

Skalierbarkeit:
Da Microsoft 365 in der Cloud gehostet wird, lässt sich der benötigte Speicherplatz leicht skalieren.

Flexibel:
Unternehmen, die MS 365 nutzen, können von jedem Gerät aus, überall und synchron auf Dokumente zugreifen.

IST DER INTEGRIERTE SCHUTZ VON MICROSOFT 365 NICHT AUSREICHEND? WARUM BRAUCHT ES ZUSÄTZLICHE SICHERHEITSEBENEN?

Bei der Betrachtung von Microsoft 365 und seinen vielen Vorteilen machen sich Unternehmen oft Sorgen um die Sicherheit ihrer Daten aufgrund von Cyberangriffen - diese Sorge ist nicht unbegründet, aber lösbar. **Während Microsoft Schutzmechanismen beinhaltet, sind zusätzliche Ebenen des Schutzes durch Dritte Anbieter notwendig,** damit ein Unternehmen angemessene Sicherheit genießen kann. Das sind die Gründe dafür:

Massive Angriffe auf Microsoft 365:
Da Microsoft 365 für Unternehmen aller Größenordnungen die am meisten genutzte Office-Lösung weltweit ist, ist sie auch diejenige, die am meisten angegriffen wird. In den letzten Jahren sind zum Beispiel Phishing-Angriffe um 250 Prozent gestiegen.

Microsoft selbst stellte in seinem jüngsten Microsoft Digital Defense Report fest, dass die Bedrohungsakteure im vergangenen Jahr immer raffinierter geworden sind und Techniken einsetzen, die es ihnen erschweren, entdeckt zu werden.

Ransomware ist die größte Bedrohung:
Microsoft unterstreicht, dass Ransomware der häufigste Grund für ihre Incident-Response-Einsätze von Oktober 2019 bis Juli 2020 war. Die durchschnittlichen Kosten für einen Ransomware-Angriff liegen bei über 84.000 US-Dollar.

Microsoft's Filter sind nicht perfekt – Drittanbieter-Lösungen werden empfohlen:
Ein erfolgreicher Angriff auf Microsoft 365 kann für Cyberkriminelle sehr lukrativ sein. Das ist der Grund, warum Hacker so viele Ressourcen investieren, um Schwachstellen in Microsofts integrierten Sicherheitssystemen zu finden. Es ist daher nicht verwunderlich, dass Analysten, wie von Osterman Research, zusätzliche Schutzlösungen von Drittanbietern empfehlen, um die integrierten Filter von Microsoft zu ergänzen und so auf Nummer Sicher zu gehen.

Neue Studie deckt Schwachstellen in Microsoft 365 Accounts auf:
Laut Vectra AI könnten 71 % der Microsoft 365-Implementierungen im Jahr 2020 erfolgreich von Cyberkriminellen angegriffen worden sein. Die Studie zeigt außerdem, dass höhere Managementebenen ihre eigenen „Verteidigungsfähigkeiten" überschätzen.

Zudem ist die **Identifizierung eines Microsoft 365-Benutzers für einen Angreifer äußerst einfach,** da die MX-Records und Autodiscover-Einträge online öffentlich einsehbar sind. Um mögliche Angriffe auf Microsoft 365-Konten zu verhindern, müssen umfangreiche Sicherheitsfunktionen implementiert werden. Dabei gilt es zu bedenken, dass die Daten in der Cloud selbst - auch bei unberechtigtem Zugriff - von überall zugänglich sind.

Durch den Einsatz von Microsoft 365 fällt ein wichtiger Sicherheitsaspekt für Unternehmen weg: die Firewall. Gelingt es einem Angreifer, sich unbefugt Zugang zu einem Microsoft 365-Konto zu verschaffen, stehen ihm alle Daten uneingeschränkt zur Verfügung.

HORNETSECURITY

WIE KANN ICH DIE SICHERHEIT VON MICROSOFT 365 ERHÖHEN, UM UNTERNEHMENSDATEN ZU SCHÜTZEN?

Laut Statistik werden 95 % aller erfolgreichen Cyberangriffe auf ein Unternehmen per E-Mail durchgeführt. Die E-Mail-Kommunikation gilt als das Haupteinfallstor für jegliche cyberkriminelle Methoden, um auf interne Unternehmensdaten zuzugreifen, diese zu stehlen und zu verschlüsseln. Das gilt auch für die E-Mail-Kommunikation über Microsoft 365. Aus diesem Grund hat Hornetsecurity 365 Total Protection entwickelt - eine **branchenweit einzigartige Security- und Compliance-Suite, die speziell für Microsoft 365 entwickelt wurde** und umfassenden zusätzlichen Schutz bietet.

Der Service vereint alle notwendigen Sicherheitsfunktionen, die ein umfassendes E-Mail-Sicherheitsmanagement benötigt, wie z. B.:

- ✓ **Email Live Tracking:** Ermöglicht es einem Administrator, die gesamte E-Mail-Kommunikation des Unternehmens in Echtzeit zu überwachen.
- ✓ **Threat defense:** Mehrstufige Tiefenanalyse- und Filtersysteme erkennen selbst die neuesten Spam- und Phishing-Angriffe. Hornetsecurity bietet die höchsten Erkennungsraten von Spam und Viren auf dem Markt.
- ✓ **Global S/MIME & PGP encryption:** Schützt die gesamte E-Mail-Kommunikation vor dem Verändern oder Mitlesen durch Dritte.

Die Enterprise-Version enthält noch mehr Zusatzfunktionen, wie z. B.:

- ✓ **Forensic analysis mechanisms:** Intelligente Filter ermöglichen eine effiziente Erkennung und Filterung von Cyberbedrohungen, die per E-Mail in ein Unternehmen eingeschleust werden.
- ✓ **Erkennt selbst fortgeschrittene Bedrohungen** wie Ransomware, die Kompromittierung von Geschäfts-E-Mails oder CEO-Fraud.
- ✓ **Malware ex-post alert:** Ermöglicht es Administratoren, E-Mails zu löschen, die erst nachträglich als schädlich eingestuft werden.
- ✓ **ATP sandboxing:** Schützt vor gezielten Angriffen und Blended Attacks.
- ✓ **Email archiving:** E-Mails rechts- und revisionssicher archivieren.
- ✓ **URL malware control:** Identifiziert Links, die zu Websites führen können, auf denen Malware-Downloads angeboten werden.
- ✓ **Contingency covering:** Gewährleistet den permanenten Zugriff auf die E-Mails Ihres Unternehmens, auch wenn der Microsoft-Dienst vorübergehend nicht verfügbar ist.
- ✓ **Global security dashboard:** Das Global Security Dashboard fasst alle Funktionen und Ergebnisse Ihres 365 Total Protection Services zentral zusammen und bietet den vollen Überblick in Bezug auf Ihre Unternehmenssicherheit:

Noch heute kostenlos testen unter:
www.hornetsecurity.com/de/services/365-total-protection/