10 Schritte für die Cyberresilienz von Microsoft 365

Inhalt

Der Anstieg der Cyberangriffe auf Microsoft 365

Der Schutz von Microsoft 365-Daten ist ein wichtiger Bestandteil einer modernen Cybersicherheitsstrategie, da die Anwendungen der Suite tagtäglich in zahllosen Unternehmen zum Einsatz kommen. Microsoft 365 umfasst eine Vielzahl von Produktivitäts-Tools wie z. B. Exchange, Teams, SharePoint und OneDrive und enthält damit sehr viele vertrauliche Informationen und kritische Geschäftsdaten. Aus diesem Grund investieren mehr Unternehmen denn je in Drittanbieter-Lösungen oder Managed Backup-Services zum Schutz dieser Daten.[1] Tatsächlich gibt es Hinweise darauf, dass Ransomware genau zu dem Zweck entwickelt wurde, Microsoft 365 und andere SaaS-Anwendungen zu infiltrieren. Laut einem Report von Coalition hat die Zahl der Lösegeldforderungen infolge von Ransomware-Angriffen in der ersten Jahreshälfte 2023 um 12% zugenommen. Die durchschnittliche Lösegeldforderung belief sich dabei auf 1,62 Millionen USD.[2] Als Folge ihrer weit verbreiteten Verwendung und da immer mehr Mitarbeiter Microsoft 365 auf Homeoffice-Computern installieren und verwenden, ist die Plattform besonders anfällig für Angreifer geworden, die aus dieser diversifizierten Infrastruktur Kapital schlagen.

12%

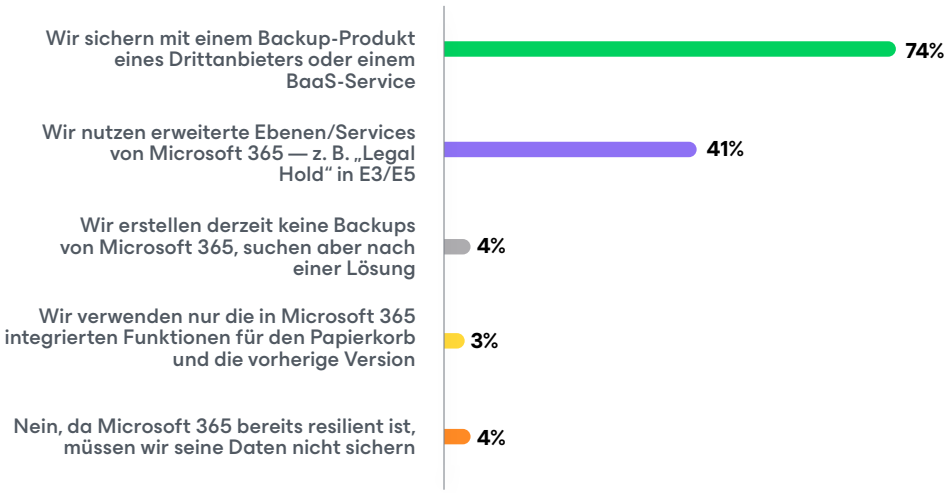
Anstieg der Cyberschäden imersten Halbjahr 2023

1,62

Millionen USD

beträgt die durchschnittliche Lösegeldforderung

Sichert Ihr Unternehmen Daten aus Microsoft 365?



[1] Report zu Trends im Bereich Datensicherung 2024

[2] Microsoft 365 Ransomware: Ihr umfassender Leitfaden zur Aufklärung, Prävention und Wiederherstellung

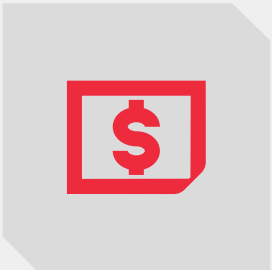
Die mit dem Verlust von Microsoft 365-Daten verbundenen Risiken sind daher nicht nur komplex, sondern sehr real. Datenverluste haben gravierende Betriebsstörungen zur Folge und können erhebliche finanzielle Schäden durch Ausfallzeiten und Produktivitätseinbußen verursachen. In einem Report schätzten IT-Verantwortliche die Kosten für Ausfallzeiten auf 1.467 USD pro Minute (88.000 USD pro Stunde)[3] — was angesichts der vielen Zeit, die die Benutzer an einem normalen Arbeitstag mit Microsoft 365 verbringen, und der vielen Arbeit, die sie damit erledigen, nicht überrascht. Wenn sensible Daten offengelegt werden, drohen Unternehmen hohe Bußgelder wegen Compliance-Verstößen und eine erhebliche Rufschädigung. Bei Verstößen gegen die DSGVO müssen sie mit Geldstrafen von bis zu 21 Millionen USD rechnen.[4] Da Microsoft 365-Daten für Unternehmen und ihre Mitarbeiter äußerst sensibel sind, ist es mehr als wahrscheinlich, dass ein Datenverlust nicht nur das Vertrauen der Kunden, sondern auch der Mitarbeiter erschüttern wird. Dies kann zu Umsatzeinbußen und langfristigen Imageschäden sowohl innerhalb als auch außerhalb des Unternehmens führen.

Die möglichen Folgen ungeschützter Microsoft 365-Daten können wohl gar nicht hoch genug eingeschätzt werden. Infolge von Sicherheitsverletzungen, bei denen personenbezogene Daten offengelegt werden, kann es zu Identitätsdiebstahl und Betrug kommen, sodass noch lange nach der eigentlichen Kompromittierung Schaden entsteht. Für Unternehmen kann der Verlust von geistigem Eigentum Wettbewerbsvorteile zunichte machen und kostspielige Rechtsstreitigkeiten oder Geldstrafen nach sich ziehen. Gerichtliche Auseinandersetzungen drohen auch Unternehmen, denen vorgeworfen wird, die Daten ihrer Kunden unzureichend geschützt zu haben.

Es führt kein Weg daran vorbei. Ein proaktiver Ansatz zur Sicherung von Microsoft 365-Daten ist mehr als eine innovative Idee — er muss sicherstellen, dass Unternehmen die Kontinuität gewährleisten, rechtliche und regulatorische Pflichten einhalten und das Vertrauen ihrer Kunden bewahren.

[3] 2022 Data Protection Trends Report
[4] What are the GDPR Fines?

Kosten im Zusammenhang mit Datenverlust



Die Kosten für Ausfallzeiten belaufen sich auf 1.467 USD pro Minute (88.000 USD pro Stunde).

Bei Verstößen gegen die DSGVO drohen Bußgelder in Höhe von bis zu 21 Millionen USD.

Infolge von Sicherheitsverletzungen, bei denen personenbezogene Daten offengelegt werden, kann es zu Identitätsdiebstahl und Betrug kommen.

Schritte zur Vorbereitung auf Angriffe

1. Multifaktorauthentifizierung

Multifaktorauthentifizierung (MFA) ist eine wesentliche Sicherheitsmaßnahme. Benutzer müssen dabei zwei oder mehr Verifizierungsfaktoren angeben, um Zugriff auf digitale Ressourcen wie E-Mail-Konten, Geschäftsanwendungen und Online-Services zu erhalten. MFA erhöht die Sicherheit erheblich, indem zusätzliche Schutzebenen hinzugefügt werden, die über ein Passwort hinausgehen. Selbst wenn Cyberkriminelle an das Passwort eines Benutzers gelangen, müssen sie die zusätzlichen Authentifizierungsfaktoren umgehen, um Zugriff zu erhalten. Dies ist nichts weniger als eine gewaltige Barriere gegen unbefugtes Eindringen.

MFA bietet zahlreiche Vorteile, insbesondere im Kontext von Microsoft 365, da damit ständig sensible Daten bearbeitet und Unternehmensmitteilungen ausgetauscht werden. MFA kann vor den Folgen häufiger Cyberangriffe wie Phishing schützen, bei denen Angreifer Benutzer dazu verleiten, Anmeldedaten preiszugeben. Für diesen zusätzlichen Authentifizierungsschritt kann etwas verwendet werden, das der Benutzer kennt (z. B. eine PIN oder Sicherheitsfrage), oder etwas, das der Benutzer besitzt (z. B. ein Smartphone oder Unternehmenshardware).

Selbst in Szenarien, in denen Kennwörter aufgrund schwacher oder wiederverwendeter Kennwörter kompromittiert werden, schützt MFA das Konto weiterhin vor unbefugtem Zugriff. Dieses Sicherheitsniveau ist in Microsoft 365-Umgebungen entscheidend, da hier standardmäßig ein Remote-Zugriff erfolgt und Benutzer möglicherweise über ungesicherte Netzwerke oder persönliche Geräte eine Verbindung herstellen. MFA schafft schlicht und einfach einen dynamischen Abwehrmechanismus, der sich an die sich ständig weiterentwickelnde Bedrohungslandschaft anpasst.

Vorteile der Multifaktorauthentifizierung

Schützt vor den Folgen häufiger Cyberangriffe

Schützt das Konto weiterhin vor unbefugtem Zugriff

Erstellt einen dynamischen Abwehrmechanismus, der sich an die Bedrohungslage anpasst

2. Zugriff nach dem Prinzip der geringsten Rechte

Das Prinzip der geringsten Privilegien ist ein Grundbestandteil effektiver Cybersicherheitspraktiken. Es ist untrennbar mit dem Konzept der Zero-Trust-Architektur verbunden und trägt entscheidend dazu bei, ein Unternehmen gegen potenzielle Cyberangriffe zu wappnen. Eine Zero-Trust-Architektur geht davon aus, dass Bedrohungen sowohl außerhalb als auch innerhalb des Netzwerks vorhanden sind, sodass keine Benutzer oder Systeme automatisch als vertrauenswürdig eingestuft werden.[5] Dies entspricht dem Prinzip der geringsten Privilegien, das besagt, dass Benutzern nur ein Mindestmaß an Zugriff (oder Berechtigungen) gewährt werden sollte, das für die Ausführung ihrer Aufgaben erforderlich ist — und nicht mehr. Für Microsoft 365 kann die Implementierung dieser Prinzipien bedeuten, dass der Zugriff auf bestimmte Dokumente, Ordner, Websites, administrative Einstellungen und Anwendungen basierend auf der Rolle des Benutzers innerhalb der Organisation eingeschränkt wird.

Durch die Einführung eines Modells für den Zugriff mit den geringsten Privilegien kann der Sicherheitsstatus Ihrer Microsoft 365-Umgebung deutlich verbessert werden. Zum einen minimiert sich die potenzielle Angriffsfläche der Suite für Cyberkriminelle. Wenn das Konto eines Benutzers kompromittiert wird, ist der Angreifer auf die Zugriffsrechte dieses Kontos beschränkt, die idealerweise so restriktiv wie möglich sein sollten. Wenn beispielsweise die Anmeldedaten eines Benutzers gestohlen werden, kann der Angreifer nicht auf vertrauliche Informationen zugreifen oder administrative Aufgaben ausführen, wenn diese Rechte nicht mit dem Konto des Benutzers verknüpft sind. Diese Schadensbegrenzung schafft eine Quarantänezone für Sicherheitsverletzungen und ist entscheidend, um die Ausbreitung von Angriffen innerhalb eines Unternehmens kontrollieren zu können.

[5] https://www.veeam.com/news/new-zero-trust-data-resilience-model-introduced-by-it-security-and-data-protection-experts.html

3. Regelmäßige Backups

Da Microsoft 365 ein Hauptziel von Cyberkriminellen ist, sind Backups äußerst wichtig. Dies gilt insbesondere angesichts des Shared Responsibility Model von Microsoft[6], wonach die Unternehmen selbst für die Sicherheit ihrer Daten verantwortlich sind. Ransomware stellt eine erhebliche Bedrohung für die Datenintegrität dar, da Angreifer versuchen, die Dateien eines Unternehmens zu verschlüsseln und für die Freigabe eine Lösegeldzahlung zu verlangen. Die Daten sind jedoch nicht nur durch böswillige Angriffe bedroht. Auch versehentliche Löschungen oder andere Pannen können Ihre Daten gefährden. Wenn ein Unternehmen seine Backups auf dem neuesten Stand hält, kann es schnell wieder auf seine Daten zugreifen, unabhängig davon, ob der Verlust auf Ransomware, menschliches Versagen oder einen der vielen anderen Gründe zurückzuführen ist, die die Unterhaltung von Microsoft 365-Backups so wichtig machen.[7] Dies minimiert nicht nur Ausfallzeiten, sondern signalisiert auch, dass das Unternehmen kein leichtes Ziel für zukünftige Angriffe ist.

Die Einführung einer regelmäßigen Backup-Routine bedeutet, einen Zeitplan festzulegen, der eine Balance zwischen der Menge der verarbeiteten Daten und den für Backups verfügbaren Ressourcen schafft. Dazu sollte die Sicherung von E-Mails, Dokumenten, Kontakten, Kalendern und anderen in der Microsoft 365 Suite gespeicherten Daten gehören.

Das ist so ähnlich wie bei einer Versicherungspolice. Sie ist vielleicht nicht jeden Tag notwendig, aber wenn eine Katastrophe eintritt, kann sie den Unterschied zwischen einer schnellen Wiederherstellung und einer tödlichen Katastrophe ausmachen.

[6] Gemeinsame Verantwortung in der Cloud

[7] 7 wichtige Gründe für die Sicherung von Microsoft 365

4. Unveränderliche Backups

Immutability spielt eine zentrale Rolle, wenn es darum geht, die digitalen Ressourcen eines Unternehmens vor Veränderung oder Löschung zu schützen, sei es durch Cyberbedrohungen oder menschliches Versagen. In Microsoft 365 werden routinemäßig riesige Datenmengen generiert, geteilt und gespeichert. Ein wesentliches Element einer robusten Strategie zur Bedrohungsabwehr besteht daher darin, sicherzustellen, dass Backup-Kopien nicht verändert werden können. Immutability garantiert, dass Informationen, sobald sie gesichert wurden, in einem makellosen Zustand bleiben und für einen bestimmten Zeitraum nicht verändert werden können.

Unveränderliche Backups schützen Unternehmen, die Microsoft 365 nutzen, vor Ransomware-Angriffen, die es nicht nur auf operative Live-Daten, sondern auch auf Backup-Repositories abgesehen haben. Einer Umfrage zufolge zielen fast alle Ransomware-Angriffe (93%) konkret auf Backups ab.[8] Für weitere Sicherheitsmaßnahmen ist eine unveränderliche Backup-Kopie der Daten wichtig. Durch die Erstellung und Durchsetzung von Aufbewahrungsrichtlinien, die Backup-Daten vor dem Überschreiben oder einer Manipulation schützen, können Unternehmen die betriebliche Kontinuität vor der unerwünschten Verschlüsselung oder Zerstörung von Daten schützen. Immutability sorgt dafür, dass Unternehmen trotz Sicherheitsverletzungen, die aktuelle Datenspeicher betreffen, den Geschäftsbetrieb unter Verwendung eines sauberen, unveränderten Backups wiederherstellen können.

93%

Der Angriffe mit Ransomware zielen speziell auf Backups ab.

[8] 2023 Ransomware Trends Report

5. Incident-Response-Plan

Ein Incident-Response-Plan ist gut strukturiert. Er beschreibt die Prozesse, denen ein Unternehmen im Falle von verschiedenen Cybersicherheitsvorfällen folgen muss, dient als Playbook für die Identifizierung, Eindämmung und Beseitigung von Sicherheitsbedrohungen und die anschließende Wiederherstellung. Darüber hinaus wird sichergestellt, dass alle Stakeholder informiert werden und bereit sind, zu handeln.

Für Unternehmen, die Microsoft 365 nutzen, bildet die Identifizierung kritischer Ressourcen innerhalb des Microsoft 365-Ökosystems die Grundlage eines soliden Incident-Response-Plan. Das bedeutet, genau zu bestimmen, wo sensible Daten gespeichert sind, sei es in OneDrive, SharePoint, Exchange Online oder anderswo. Sobald diese Assets identifiziert sind, sollte der Plan potenzielle Bedrohungen definieren und eine priorisierte Liste von Risiken sowie Strategien zu deren Minderung erstellen. Hierzu gehören der Einsatz von integrierten Tools für Monitoring und Entdeckung, Strategien zur sofortigen Eindämmung, die Beseitigung von Bedrohungen, eine robuste Kommunikation zwischen den Parteien sowie die Identifizierung und Wiederherstellung verlorener oder kompromittierter Daten.

Der Kitt, der einen Notfallplan zusammenhält, ist eine gründliche Vorbereitung. Dies geht über technische Tools, Schulungen und die Zusammenarbeit von IT- und Sicherheitsteams hinaus und betrifft alle Mitarbeiter. Für alle Benutzer von Microsoft 365 sollten Unternehmen regelmäßige Schulungen durchführen, die auf das komplexe Ökosystem zugeschnitten sind. Mitarbeiter, die Anwendungen in Microsoft 365 wie Outlook und Teams verwenden, müssen mit dem Wissen ausgestattet sein, verdächtige Aktivitäten zu erkennen und darauf zu reagieren, die in Form von scheinbar legitimen Nachrichten, gefälschten Besprechungseinladungen von Kollegen oder authentisch aussehenden E-Mails von Unternehmensleitern auftreten können. Menschen können für jedes Unternehmen eine Schwachstelle für die Cybersicherheit darstellen, aber gut geschulte Mitarbeiter haben das Potenzial, eine gewaltige Barriere gegen Bedrohungen zu bilden.

Ein Incident-Response-Plan beginnt mit

- **Umfassendes Incident-Response-Framework**
- **Identifizierung kritischer Ressourcen**
- **Bedeutung der Vorbereitung der Mitarbeiter**

6. Regelmäßige Audits und Penetrationstests

Regelmäßige Audits und Penetrationstests tragen wesentlich zum Erhalt einer resilienten Microsoft 365-Umgebung bei. Microsoft 365 selbst bietet eine Reihe von integrierten Tools für die Prüfung und Bedrohungserkennung[9], die als Grundlage zur Stärkung der Umgebung gegen verschiedene Sicherheitsbedrohungen dienen. Es handelt sich hier um proaktive Maßnahmen, mit denen Unternehmen Probleme erkennen und beheben können, bevor sie von Angreifern ausgenutzt werden können.

Audits des Microsoft 365-Ökosystems umfassen eine systematische Überprüfung verschiedener Aspekte wie Benutzerberechtigungen, Datenzugriffskontrollen und Sicherheitseinstellungen. Zwar können regelmäßige Audits mitunter kompliziert sein, sie tragen jedoch dazu bei, sicherzustellen, dass die Systemkonfigurationen den Best Practices und den Sicherheitsrichtlinien des Unternehmens entsprechen. Es ist daher ratsam, solche Audits einzuführen und beizubehalten. Da Microsoft 365 eine Vielzahl von Services umfasst, müssen diese Audits umfassend sein und jeden Service abdecken, um übersehene Schwachstellen zu vermeiden.[10]

Penetrationstests, die oft als „ethisches Hacking" bezeichnet werden, ergänzen die regelmäßigen Audits. Sie ermöglichen es den Unternehmen, die Wirksamkeit ihrer Sicherheitsmaßnahmen zu bewerten. Dabei werden Cyberangriffe auf die Microsoft 365-Infrastruktur simuliert, um Schwachstellen zu identifizieren, die von Angreifern im realen Geschäftsalltag ausgenutzt werden könnten. Für geeignete Unternehmen sollten Penetrationstests alle Schichten ihres Microsoft 365-Ökosystems untersuchen — von der Phishing-Resistenz der Mitarbeiter bis hin zur Ausfallsicherheit technischer Tools wie Firewalls, Bedrohungserkennungssystemen und Notfallplänen. Die aus diesen Tests gewonnenen Erkenntnisse helfen den Unternehmen bei der Feinabstimmung ihrer Schulungsprogramme und Sicherheitsstrategien. So können sie umfassendere und effektivere Abwehrmaßnahmen entwickeln, wenn unweigerlich eine Cyberbedrohung auftritt.

[9] Microsoft 365-Leitfaden für Sicherheit und Compliance

[10] Native Sicherheit in Microsoft 365: Freischaltung von Features für Compliance und Monitoring

7. Richtlinien zur Softwareeinschränkung

Eine Richtlinie zur Softwareeinschränkung (Software Restriction Policy, SRP) ist ein Sicherheitsfeature, das Unternehmen zur Identifizierung und Kontrolle der Ausführung von Software auf bestimmter Hardware verwenden können. In Unternehmen, die Microsoft 365 verwenden, kann die Einführung einer solchen Richtlinie als kritischer Mechanismus zum Schutz der vielen Geräte in ihrer Zuständigkeit dienen. Da Microsoft 365 eine Vielzahl unterschiedlicher Tools enthält, lädt es auch zu einer Reihe unterschiedlicher Bedrohungsvektoren ein, die ausgenutzt werden können. SRPs legen fest, welche Software auf einem System ausgeführt werden darf und welche nicht. Damit reduzieren sie effektiv die Angriffsfläche für böswillige Akteure.

Bei der Erstellung eines SRP für eine Microsoft 365-Umgebung soll sichergestellt werden, dass nur vertrauenswürdige Anwendungen, Skripte und Prozesse ausgeführt werden dürfen, einschließlich Whitelisting und Blacklisting von Bedrohungsvektoren nach Bedarf. Für maximale Effektivität sollten SRPs unter Berücksichtigung des Zugriffs mit den geringsten Rechten konfiguriert und regelmäßig aktualisiert werden, um Änderungen in der von einem Unternehmen verwendeten Software widerzuspiegeln. Dazu gehören Updates für Microsoft 365-Tools, das Hinzufügen neuer Software oder die Einstellung herkömmlicher Anwendungen.

Indem sie Malware daran hindern, gängige Exploit-Techniken zu nutzen, sind SRPs sehr effektiv bei der Unterbrechung der Infektionskette und der Aufrechterhaltung einer Quarantänezone. Die Integration von SRPs in eine Cybersicherheitsstrategie ist ein zukunftsorientierter Ansatz, der dazu beiträgt, die Infrastruktur eines Unternehmens vor der Ausführung nicht vertrauenswürdiger Software zu schützen - etwas, das mit dem Wachstum von Unternehmen und der Einstellung neuer Mitarbeitereine ständig wachsende Möglichkeit darstellt.

8. Monitoring und Protokollierung

Monitoring und Protokollierung sind wichtige Schritte für die Sicherheit und Integrität jeder Microsoft 365-Umgebung. Durch die Überwachung von Systemaktivitäten und umfassende Aufzeichnungen von Ereignissen können Unternehmen potenzielle Sicherheitsvorfälle in Echtzeit erkennen, Systemprobleme diagnostizieren, das Ausmaß von Sicherheitsverletzungen nachvollziehen und ihre allgemeine Sicherheitslage verbessern.

Für Microsoft 365-Administratoren kann es den Prozess erheblich vereinfachen, wenn die Protokolle in ein leistungsfähiges SIEM-System (Security Information and Event Management) importiert werden. Azure Sentinel beispielsweise ist ein Microsoft-natives SIEM, das ein Array vordefinierter Datenconnectors verwendet, um die Protokolldaten einer Organisation direkt in die SIEM-Anwendung zu streamen. Diese Daten werden dann normalisiert, um konsistente Datensätze zu erhalten, und durch integrierte Analysetools überwacht.

Für ein effektives Monitoring sollte ein breites Netz ausgeworfen werden, um mögliche Anomalien aufzuspüren, die auf eine Sicherheitsbedrohung hindeuten — von fehlgeschlagenen Anmeldeversuchen (ein Hinweis auf einen Brute-Force-Angriff) bis hin zu ungewöhnlichen Download-Mustern (ein Hinweis auf unerwünschte Datenexfiltration) und vielem mehr. Ebenso wichtig ist eine umfassende Protokollierung, die als Dokumentation aller überwachten Aktivitäten dient. Solche Protokolle sollten genügend Details erfassen, um die Rekonstruktion von Ereignissen über einen gesamten Vorfall hinweg zu ermöglichen — vor, während und nach dem Vorfall. Dies ist für die forensische Analyse nach einem Vorfall von unschätzbarem Wert, hilft aber auch bei Compliance Audits und der Optimierung von Sicherheitsmaßnahmen im Laufe der Zeit. Die Protokollierung muss sorgfältig konfiguriert werden, um sicherzustellen, dass die gesammelten Daten verwertbar sind und klare und relevante Informationen liefern, ohne das Rauschen, das durch einen zu ehrgeizigen Umfang erzeugt werden kann.

Im Laufe der Zeit liefern die aus Monitoring und Protokollierung gewonnenen Erkenntnisse den Unternehmen die benötigten Daten für proaktive Richtlinienänderungen und die Optimierung von Sicherheitsupdates.

9. Datentrennung

Die Trennung von Berechtigungen ist eine weit verbreitete und effektive Strategie von Unternehmen zur Verbesserung ihrer Sicherheitsinfrastruktur, die insbesondere bei der Integration datengestützter Services wie Microsoft 365 gut geeignet ist. Strategien wie mandantenfähige Architekturen, administrative Grenzen und bedingte Kontobeschränkungen konzentrieren sich auf die Strukturierung von Daten und ihren Berechtigungen, um unbefugten Zugriff zu reduzieren und potenzielle Schäden durch Sicherheitsverletzungen zu begrenzen. Durch die Trennung verschiedener Datensätze und die Unterteilung von Netzwerken in einzelne Segmente können Unternehmen das Risiko von Sicherheitsverletzungen erheblich verringern und eventuelle Ausbrüche effektiv isolieren.

Die Verwendung von Richtlinien zur Rechtetrennung in Microsoft 365 ermöglicht es Unternehmen, strenge Zugriffsregeln einzuhalten. Wie wir im vorherigen Abschnitt erwähnt haben, stellen die besten dieser Regeln sicher, dass Benutzer, Administratoren und Dienste nur die Berechtigungen erhalten, die zum Ausführen der erforderlichen Aufgaben erforderlich sind, und nicht mehr — z. B. das Prinzip der geringsten Rechte und rollenbasierte Zugriffskontrolle (RBAC/ Rollenbasierte Zugriffssteuerung).

Bei Unternehmen, die in verschiedenen Rechtsräumen tätig sind oder über mehrere Geschäftsbereiche verfügen, kann die Trennung von Microsoft 365-Mandanten über eine mandantenfähige Architektur helfen, Daten zu isolieren und den Zugriff zu kontrollieren. Dies bezieht sich auf die Schaffung unterschiedlicher administrativer Grenzen pro Mandant. Auf diese Weise werden die Umgebungen auf ihre eigenen Daten, Benutzerkonten und Zugriffskontrollen beschränkt und es wird sichergestellt, dass die Sicherheits- und Compliance-Anforderungen individuell erfüllt werden und Sicherheitsverletzungen oder -probleme bei einem Mandanten die Integrität der anderen nicht kompromittieren.

Innerhalb dieser administrativen Grenzen fügen Richtlinien für bedingten Zugriff und Kontobeschränkungen eine weitere Schutzebene hinzu und können direkt in Microsoft 365 implementiert werden. Diese Richtlinien ermöglichen es Unternehmen, kontextbasierte Regeln für ein bestimmtes Konto zu definieren und zu implementieren. So können die Sicherheitsregeln eines Unternehmens an die Risikostufe eines Kontos, den geografischen Standort oder dynamische Unregelmäßigkeiten wie verdächtige Anmeldungen oder Downloads angepasst werden.

Die methodische Trennung kann daher auf alle Ebenen der Unternehmenshierarchie angewendet werden und bietet eine zuverlässige Grundlage für den Schutz von Microsoft 365-Daten und anderen digitalen Ressourcen. Da die strategische Abschottung nicht nur das Risiko eines unbefugten Zugriffs mindert, sondern auch mehrschichtige Sicherheitsvorkehrungen und Fallbacks gegen Sicherheitsverstöße ermöglicht, hat sich die Trennung von Daten und Berechtigungen zu Recht als zuverlässiges Konzept für Unternehmen etabliert, um ihre Cyberabwehr zu stärken, die Business Continuity aufrechtzuerhalten und letztendlich Cyberresilienz in ihrer Microsoft 365-Umgebung zu erreichen.

10. Verschlüsselung

Verschlüsselung ist eine grundlegende Sicherheitsmaßnahme, die als primäre Verteidigung zum Schutz sensibler Informationen dient und sicherstellt, dass nur autorisierte Parteien mit dem richtigen Entschlüsselungsschlüssel auf die ursprünglichen Informationen zugreifen können. Sie gilt für die Daten unabhängig davon, wie diese verwendet oder bewegt und wo sie gespeichert werden. In Bezug auf Microsoft 365 bietet die Verschlüsselung eine Sicherheitsebene, die Unternehmen dabei hilft, ihre Kommunikation, ihre Dokumente und andere Daten zu schützen — unabhängig davon, wo sich diese in ihrer Cloud-Infrastruktur befinden.

Phishing-E-Mails und infizierte Websites sind oft die subtilen Vorboten schwerer Ransomware-Angriffe. In den letzten Jahren hat RobbinHood Ransomware Unternehmen verheerende Schäden bereitet und sie Millionen von Dollar an Lösegeld, Ausfallzeiten und Wiederherstellung gekostet — und das alles, weil versehentlich eine infizierte E-Mail heruntergeladen und die Malware in das System gelangt war.

Integrierte Tools wie die Vertraulichkeitsbezeichnungen (Sensitivity Labels) von Microsoft 365 helfen, dies zu verhindern, indem sie strenge Protokolle einhalten, die Dokumente und E-Mails automatisch verschlüsseln können. So kann eine Erstinfektion verhindert werden, indem verdächtigen E-Mails misstraut und der Benutzer vor potenziell gefährlichen Absendern gewarnt wird. Diese Bezeichnungen können mit Richtlinien für die Rechteverwaltung konfiguriert werden. Auf diese Weise können Administratoren bestimmen, wer auf Daten zugreifen kann und wie die Daten verwendet werden können. Es handelt sich hier um eine Ebene der Inhaltsklassifizierung und des Schutzes, die zentral von den Unternehmen verwaltet wird. IT-Administratoren können so die Handhabung, Freigabe und Bearbeitung von Daten regeln. Somit verfügen wohlmeinende Benutzer über mehrere Schutzmechanismen, um die Einschleusung oder Verbreitung von Malware zu verhindern (und dabei die laufenden Workflows nicht zu beeinträchtigen).

Effektive Verschlüsselung bildet letztendlich das Fundament, auf dem Privatsphäre und Einhaltung gesetzlicher Compliance aufgebaut sind. Unternehmen, die die Verschlüsselungsfunktionen von Microsoft 365 in effektiver Weise parallel zu ihren bereits bestehenden Sicherheitsrichtlinien nutzen, sind weitaus cyberresilienter als Unternehmen, die dies nicht tun. Solide Verschlüsselungspraktiken sind entscheidend für den Schutz wertvoller Daten vor Ransomware und Cyberbedrohungen. Sie stärken den Datenschutz, gewährleisten die Einhaltung gesetzlicher Compliance und unterstützen einen sicheren, gemeinschaftlichen Arbeitsbereich.

Microsoft 365 Cyberresilienz beginnt mit dem Backup

Mit Blick auf das Datenmanagement und die Sicherheit der Zukunft hat sich Backup-as-a-Service (BaaS) als bevorzugte Methode zum Schutz von SaaS-Anwendungen wie Microsoft 365 herauskristallisiert. BaaS ist ein cloudbasierter Ansatz, der Unternehmen ein Online-System zur Sicherung und Speicherung ihrer Daten an einem Remote-Standort bereitstellt. Die Integration von BaaS in eine Microsoft 365-Strategie steht im Einklang mit dem Bedarf an zuverlässigen, skalierbaren und flexiblen Datensicherungslösungen — alles entscheidende Komponenten für die Resilienz des Unternehmens.

Backup-Services bieten Unternehmen die Möglichkeit, ihre Backup-Anforderungen an spezialisierte Anbieter auszulagern. Mit den End-to-End-Lösungen dieser Anbieter können Backup-Prozesse automatisiert werden, es wird weniger lokale Infrastruktur benötigt und es stehen erstklassige Sicherheitsmaßnahmen zur Verfügung — das alles bei direktem Zugriff und direkter Kontrolle über die Daten. Für Benutzer von Microsoft 365 bedeutet BaaS verbesserte Datensicherheit, betriebliche Effizienz und ein Gefühl der Sicherheit.

Die Sicherung eines Microsoft 365-Ökosystems ist ein vielschichtigesUnterfangen, bei dem Unternehmen sowohl strategische Präventionsmaßnahmen als auch effektive Notfallpläne benötigen. Der Weg zur Cyberresilienz von Microsoft 365 ist noch nicht abgeschlossen und erfordert die effektive Nutzung technologischer Fortschritte. Hier gibt es spezialisierte Backup Anbieter, die speziell auf die Microsoft 365-Daten zugeschnitten sind.

Veeam Data Cloud *für Microsoft 365*

Veeam Data Cloud *for Microsoft 365* unterstützt eine maximale Ausfallsicherheit für Microsoft 365-Daten mit einem modernen Ansatz. Die branchenführende Backup-Lösung für Microsoft 365 — Veeam Backup *for Microsoft 365* — ist jetzt als Service verfügbar.

Vereinfachen Sie Ihre Backup-Strategie mit einem zentralen Cloud-Service, der Software, Backup-Infrastruktur und unbegrenzten Speicherplatz umfasst. Damit können Sie leistungsstarke Datensicherungs- und Sicherheitstechnologien in einer einfachen und nahtlosen Umgebung nutzen.

Veeam Data Cloud *for Microsoft 365* ist ein Backup-Service für die umfassende Datensicherung und -wiederherstellung für **Microsoft Exchange, SharePoint, OneDrive for Business und Teams**, mit dem Sie die volle Kontrolle über Ihre Microsoft 365-Umgebung behalten.

→ Fordern Sie eine Demo von Veeam Data Cloud for Microsoft 365 an

Mit **der Veeam Data Cloud *für Microsoft 365*** profitieren Sie von diesen Vorteilen:

- **Zuverlässige, branchenführende Technologie:** Eine äußerst umfangreiche Datensicherungslösung, mit mehr als einem Jahrzehnt kontinuierlicher Innovation, entwickelt, um zu skalieren.
- **Moderne, sichere und intuitive Plattform:** Über eine moderne Weboberfläche können Sie ganz einfach Backup-Jobs erstellen, Wiederherstellungen abschließen und Einblicke in Microsoft 365 gewinnen.
- **Rundum-Sorglos-Service:** Software, Backup-Infrastruktur und unbegrenzter Speicherplatz im Paket mit laufender Wartung durch Experten.

Seien Sie vorbereitet, bleiben Sie informiert

Ihr Weg zur Cyberresilienz von Microsoft 365 endet hier nicht — es ist erst der Anfang. Erweitern Sie Ihr Wissen, optimieren Sie Ihre Strategien und bleiben Sie den Entwicklungen auch 2024 immer einen Schritt voraus. Wir unterstützen Sie gerne dabei, Herausforderungen in Chancen umzuwandeln. Nutzen Sie unsere erweiterte Ressourcensammlung:

- 8 Vorteile eines Backup-Service für Microsoft 365
- Microsoft 365 Backup for Dummies
- Best Practices für die Wiederherstellung von Microsoft 365-Daten

Über Veeam Software

Veeam®, weltweit führender Anbieter von Lösungen für Datensicherung und Wiederherstellung nach Ransomware-Angriffen, möchte allen Unternehmen helfen, sich nach einem Datenausfall oder Datenverlust nicht nur wieder zu erholen, sondern auch Fortschritte zu machen. Mit Veeam erreichen Unternehmen maximale Ausfallsicherheit durch Datensicherheit, Datenwiederherstellung und Datenfreiheit für ihre Hybrid Cloud. Die Veeam Data Platform ist eine zentrale Lösung für cloudbasierte, virtuelle, physische, SaaS- und Kubernetes-Umgebungen. IT- und Sicherheitsverantwortliche haben somit die Gewissheit, dass ihre Anwendungen und Daten stets geschützt und verfügbar sind. Veeam hat seinen Hauptsitz in Seattle und ist mit Niederlassungen in mehr als 30 Ländern vertreten. Weltweit hat Veeam mehr als 450.000 Kunden, darunter 74% der Global 2000-Unternehmen, die auf Veeam vertrauen, um einen zuverlässigen Geschäftsbetrieb zu gewährleisten. Maximale Ausfallsicherheit beginnt mit Veeam. Erfahren Sie mehr unter www.veeam.com oder folgen Sie Veeam auf LinkedIn @veeam-software und X @veeam.