EIN UMFASSENDER LEITFADEN ZUM

Schutz vor Ransomware für Microsoft 365

Bauen Sie die Cyber-Resilienz Ihres Unternehmens auf

COHESITY

Inhalt

Datensicherheit ist wichtig

Hybrides Arbeiten und niedrigere Investitionskosten sind die Hauptgründe, warum Unternehmen schnell auf Microsoft 365 umgestiegen sind. Doch die abonnementbasierte Suite mit Exchange Online und anderen Office 365-Produktivitäts-Apps, OneDrive, SharePoint und Teams stellt seit zwei Jahren aufgrund der umfangreichen Benutzerbasis[1] und der schnell wachsenden Abonnementzahlen[2] ein verlockendes Ziel für Cyberkriminelle dar.

Wenn Ihr Unternehmen auf Microsoft 365 (M365) angewiesen ist, sollten Sie nicht nur die Minuten der Zusammenarbeit und die Benutzeranzahl im Auge behalten. Ransomware ist auf dem Vormarsch und Ihre sensiblen Daten in M365 werden immer häufiger zum Angriffsziel.

Kriminelle versuchen bereits, Ihre Daten mit Malware zu infizieren und zu verschlüsseln, um anschließend von Ihrem Unternehmen Lösegeld für die Rückgabe der Daten zu verlangen. Außerdem hoffen Cyberkriminelle, dass Ihre sensiblen Daten in M365 nur begrenzt geschützt sind, um diese zu exfiltrieren oder zu stehlen und dann Zahlungen zu erpressen, damit sie nicht an die Öffentlichkeit gelangen. Diese Vorgehensweise wird schnell Teil von Ransomware-Schemen mit „doppelter Erpressung".

Was auch immer der Plan von Angreifern sein mag, mit Ransomware können sie Ihr Geschäftsergebnis und das Ansehen Ihrer Marke schwer schädigen. Bleiben Sie einen Schritt voraus. Die Empfehlung von Microsoft zur Abwehr von Ransomware-Angriffen auf Ihre M365-Daten ist einfach: Sichern Sie Inhalte und Daten regelmäßig. Verwenden Sie zur Speicherung Anwendungen und Services von Drittanbietern.[3] Dies ist ein guter Rat. Aber das reicht wahrscheinlich nicht aus.

Lesen Sie weiter und erfahren Sie, warum und wie Sie Ihren Ransomware-Schutz für M365 verbessern können ›

66 % der Unternehmen waren von Ransomware betroffen

laut einer Studie zum Vorjahr.[4]

25 % gaben an, dass böswillige Datenlöschung

die Hauptursache für SaaS-Datenverluste ist.[5]

[1]Microsoft Q3 2022 Earnings Call Transcript – Fast 300 Millionen Benutzer verwenden Office 365
[2]Microsoft Q1 2022 Earnings Call Transcript – > 50 %
[3]Microsoft Service Agreement, Abschnitt 6b

[4]Sophos, „State of Ransomware 2022", 2022.
[5]Enterprise Strategy Group. „The Evolution of Data Protection Cloud Strategies", 2021.

Gemeinsame Verantwortung verstehen

Als Hyperscale-Cloud- und Anwendungsanbieter arbeitet Microsoft nach einem Modell der geteilten Verantwortung. Konkret bedeutet dies, dass sich Microsoft zu hohen Servicelevels in Bezug auf die Zuverlässigkeit und Verfügbarkeit der Infrastruktur, robuster Infrastruktursicherheit und begrenzter Datensicherung verpflichtet, einschließlich einiger Richtlinien zur Datenaufbewahrung und Versionierung, die wir im Folgenden behandeln werden. Microsoft sichert jedoch niemals die Verfügbarkeit Ihrer Inhalte zu. Soviel zum Anteil von Microsoft an der Verantwortung.

Ihr Anteil an der Verantwortung ist für die Wahrung des Rufs Ihrer Marke und des Vertrauens Ihrer Kunden ebenso wichtig. Sie sind Eigentümer Ihrer Inhalte. Die Verantwortung für den kurz- und langfristigen Schutz Ihrer Cloud-Daten liegt also bei Ihnen, denn Sie müssen Ihre geschäftlichen und gesetzlichen Anforderungen erfüllen. Ebenso ist es Sache Ihres Unternehmens, Ihre Daten im Falle eines Angriffs schnell wiederherzustellen. Ihr eigener Anteil an der Verantwortung für M365 bzw. eine für den Erfolg ausschlaggebende Umgebung ist ein äußerst wichtiger Aspekt. Überlegen Sie deshalb, ob Sie den Empfehlungen der Best Practices folgen und zusätzlich zum grundlegenden M365-Schutz Anwendungen und Services von Drittanbietern hinzufügen, die Ihre Daten vor Ransomware-Angriffen schützen.

Microsoft verfügt zwar über integrierte Möglichkeiten zur Aufbewahrung von Daten nach dem Löschen oder Ändern, doch diese Funktionen stellen einfach keine robusten, unveränderlichen Datensicherungen dar (mehr dazu später).

Native M365-Sicherungen auf einen Blick

Datensicherung ist wichtig für die M365-Apps, die Ihre wichtigsten Geschäftsabläufe unterstützen. Hier ist ein kurzer Überblick über die integrierten Funktionen von Microsoft:

Exchange Online	• Die Standardaufbewahrungsdauer für gelöschte Elemente beträgt 14 bis maximal 30 Tage, falls konfiguriert. • Die Standardaufbewahrungsdauer für gelöschte E-Mail-Postfächer beträgt maximal 30 Tage.
OneDrive	• Gelöschte Elemente im Papierkorb der Websitesammlung werden standardmäßig 93 Tage aufbewahrt. • Gelöschte Elemente im Papierkorb eines Benutzers werden standardmäßig 30 Tage aufbewahrt. • Die Wiederherstellung von Daten zurück bis zu einem bestimmten Zeitpunkt ist maximal 30 Tage möglich, falls konfiguriert.
SharePoint	• Gelöschte Elemente im Papierkorb der Websitesammlung werden standardmäßig 93 Tage aufbewahrt. • Gelöschte Elemente im Papierkorb eines Benutzers werden standardmäßig 30 Tage aufbewahrt. • Backups für gelöschte Elemente werden für zusätzliche 14 Tage aufbewahrt. • Administratoren können gelöschte Websitesammlungen und Inhalte innerhalb von 90 Tagen wiederherstellen.
Teams	• Die Standardaufbewahrungsdauer für Nachrichten beträgt 1 bis 7 Tage. • Die Aufbewahrungsdauer für andere Datentypen ist je nach Service begrenzt.

Denken Sie daran, dass jeder M365-Service im Kern auch auf Microsoft Azure Active Directory basiert. Daher ist es ebenfalls wichtig, einen Plan zur Sicherung dieses Repositorys zu haben, damit Sie den Endbenutzerzugriff schnell wiederherstellen können.

Ransomware kann jeden treffen

Malware kann in ein System eindringen und sich über Wochen oder Monate im Verborgenen auf andere Systeme ausbreiten, bis es schließlich zum eigentlichen Angriff kommt. Darüber hinaus reicht die Versionierung einfach nicht aus, um sich von Ransomware zu erholen. Wiederherstellungen müssen von einem bestimmten Zeitpunkt an für den gesamten Datensatz und nicht nur für einzelne Dateien erfolgen, damit sichergestellt ist, dass die von Ihnen wiederhergestellten Daten frei von Ransomware-Infektionen sind.

Die drohende Gefahr von Partnerschaftsmodellen für **Ransomware as a Service (RaaS)** macht es Angreifern leicht, ihre Aktivitäten zu skalieren und beliebige Branchen oder Unternehmen unabhängig von ihrer Größe ins Visier zu nehmen.[8]

Datensicherung vs. Versionierung

Wenn Sie weitere Beweise dafür benötigen, dass M365 alleine keine ausreichende Datensicherung bietet, sollten Sie sich darüber informieren, wie die Daten aufbewahrt werden. Im Gegensatz zu echten Datensicherungslösungen verwendet M365 eine Technik, die mehr der Versionskontrolle ähnelt, d. h. der Verwaltung mehrerer Revisionen derselben Informationen oder Dateien. Anders ausgedrückt: Die Versionierung erfolgt auf der Basis einzelner Dateien und jede Datei hat ihren eigenen Versionsverlauf. Die Herausforderung bei diesem Ansatz besteht darin, dass Ransomware-Angriffe zu bestimmten Zeitpunkten stattfinden und eine große Anzahl von Dateien gleichzeitig in Mitleidenschaft ziehen.

Sehen wir uns ein Beispiel in Abbildung 1 auf der nächsten Seite an. Eine heute neu erstellte PowerPoint-Präsentation liegt in der Version 2 vor, während eine jahrealte Kalkulationstabelle mit Umsatzprognose in der Version 1278 vorliegt (unter der Annahme, dass alles so eingerichtet ist, dass überhaupt so viele Versionen gespeichert werden). Diese Art der Versionsaufbewahrung macht es schwierig, wenn nicht gar unmöglich, Tausende von Dateien auf einmal zu einem bestimmten Zeitpunkt wiederherzustellen oder über Dokumente hinweg auf die Zeit vor einem Angriff zurückzusetzen.

[8]SecureWorks. „2021 State of the Threat Report“, 2021.

74 %
verlassen sich ausschließlich auf Microsoft 365

für die Datenwiederherstellung. Dies ergab eine kürzlich durchgeführte Befragung von 381 IT-Experten.[6]

Und

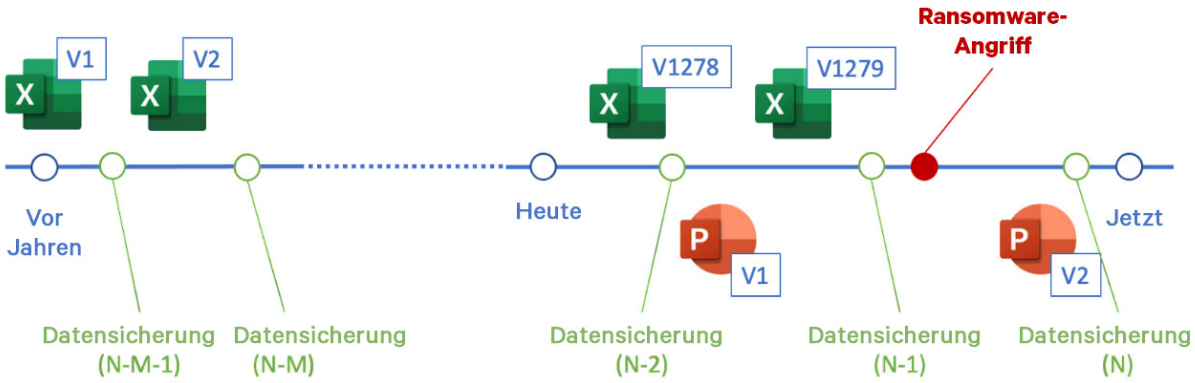
nur 15 % der Unternehmen gelang eine 100%ige Wiederherstellung

ihrer Daten.[7]

[6]Enterprise Strategy Group. „The Evolution of Data Protection Cloud Strategies—Key Findings Presentation“, März 2021.

[7]Enterprise Strategy Group. „The Evolution of Data Protection Cloud Strategies“, März 2021.

Abbildung 1: Datensicherung vs. Versionierung



Eine Next-Gen Data Management-Lösung mit moderner Datensicherung bietet Ihrem Unternehmen eine detaillierte Kontrolle darüber, wie lange Sie Daten aufbewahren können. Darüber hinaus bietet Sie Ihnen die Möglichkeit, alle Ihre Daten zu einem bestimmten Zeitpunkt wiederherzustellen, z. B. kurz vor einem Angriff oder einer Kompromittierung. So können Sie sicher sein, dass Ihrem Team eine saubere Kopie aller Dateien und Daten für eine schnelle Wiederherstellung zur Verfügung steht.

Rationalisierung der Compliance und Erfüllung interner Anforderungen

Neue und sich ändernde gesetzliche Vorschriften machen es für Ihr Unternehmen immer wichtiger, bei der Anpassung von Richtlinien zur Datenaufbewahrung flexibel zu sein. In regulierten Branchen wie dem Gesundheitswesen, den Finanzdienstleistungen und der öffentlichen Verwaltung wird von den Teams inzwischen regelmäßig verlangt, Daten länger als sieben Jahre (und manchmal sogar für immer) aufzubewahren.

Jedes Unternehmen, das sich bereits mit einem Rechtsstreit konfrontiert sah, weiß, wie wichtig flexible Aufbewahrungsrichtlinien sind. eDiscovery kann Monate oder gar Jahre dauern und M365-Daten wie E-Mails und Dokumente umfassen. Ohne Flexibilität bei der Aufbewahrungsdauer und den Zugriffszeiten auf die Daten riskiert das Unternehmen die Nichteinhaltung von Vorschriften oder Geldstrafen im Zusammenhang mit der Beantwortung rechtlicher Anfragen zur Offenlegung von Daten.

Führungskräfte passen auch immer häufiger interne Unternehmensrichtlinien an, um geschäftliche Anforderungen zu erfüllen und Daten im Zeitalter der Cloud zu schützen. Sie legen Richtlinien fest, die eine Auslagerung oder eine Verlagerung von Daten in eine andere Cloud vorsehen, um größtmögliche Sicherheit und geringste Anbieterabhängigkeit zu erreichen. Sie sollten unbedingt über einen Plan verfügen, um Ihre Daten im Falle einer Unterbrechung des M365-Services zu sichern. Dieser kann auch nützlich sein, wenn Sie eines Tages beschließen, von M365 zu einem anderen Cloud-Anbieter zu wechseln.

Bewertung des aktuellen M365-Schutzes

Wenn Ihr Unternehmen M365 eingeführt hat, haben die Standardeinstellungen bisher vielleicht funktioniert. Überlegen Sie sich nun anhand der folgenden Fragen, ob diese Vorgaben für Ihre Zukunft ausreichen:

- Sind Sie abgesichert, wenn M365 kompromittiert wird und die einzigen Kopien Ihrer Daten in der Microsoft Cloud gespeichert sind?
- Was würde mit der Marke und dem Ruf Ihres Unternehmens geschehen, wenn Daten exfiltriert und der Öffentlichkeit über das Darknet zugespielt würden?
- Wie würden Sie Daten wiederherstellen, die Sie für eDiscovery oder eine rechtliche Situation benötigen, die erst in Monaten oder Jahren eintritt?
- Wie unterstützen Sie Wiederherstellungszeiten (RTOs, Recovery Time Objectives) und Wiederherstellungspunktziele (RPOs, Recovery Point Objectives), wenn Microsoft keine Service Level Agreements (SLAs) anbietet?
- Wie gehen Sie mit den Compliance-Vorschriften für Ihre Daten um? Wie beabsichtigen Sie, Ihre Compliance nachzuweisen, wenn Sie angegriffen werden?
- Auf welche Lösungen können Sie bei Bedarf zurückgreifen, um Daten wieder vor Ort oder zu einem anderen Service zu migrieren?
- Welche Alternativen haben Sie, um M365-Daten in einer anderen Cloud zu sichern und Daten zu isolieren, falls die Microsoft Cloud angegriffen wird?

Gibt Ihnen eine oder mehrere der Antworten zu denken? Die standardmäßigen M365-Sicherheitsmaßnahmen können Ihr Unternehmen bzw. Ihre Daten **gefährden**.

Der Ernstfall: Wie Ransomware zu Chaos führt

Grundlegende Versionierungs- und Datenhaltungskapazitäten sind zwar bei Anwendungen vorhanden, doch Cyberkriminelle finden immer wieder Schwachstellen. Einige gängige Methoden, mit denen sie M365 mit Ransomware angegriffen haben, werden im Folgenden beschrieben.

Infektion

Erinnern Sie sich noch an die E-Mails vom wohlhabenden Prinzen, in denen Millionen von Dollar als Antwort versprochen wurden? E-Mail ist nach wie vor einer der Top-Infektionsvektoren, der für Ransomware ausgenutzt wird. Ein einfacher Klick auf einen Link oder das Herunterladen eines Dokuments reicht aus, um Malware auszulösen, die Daten und Systeme in Privathaushalten und Unternehmen verschlüsselt.

Mehr als acht von zehn Unternehmen (83 %) gaben an, dass sie im Jahr 2021 einen erfolgreichen E-Mail-basierten Phishing-Angriff erlebt haben, im Vergleich zu fünf von zehn (57 %) im Jahre 2020, so der Bericht „2022 State of the Phish“.[9] Die Bedrohung scheint nicht nachzulassen.

Erst kürzlich wurde das in Liverpool ansässige Bahnunternehmen Merseyrail Opfer eines Lockbit-Ransomware-Angriffs. Er verbreitete sich durch die erfolgreiche Kompromittierung eines privilegierten Office 365-Kontos. Die Infektion durch E-Mail, einschließlich Exchange Online, ist ein gängiger Ansatzpunkt für Angreifer, sich Zugang zu Unternehmenssystemen zu verschaffen. Sobald sie Zugriff haben, bewegt sich ihre Ransomware seitwärts und nutzt unter Rückgriff auf kompromittierte Anmeldedaten die Anfälligkeiten von ungepatchten Systemen aus.

Im Folgenden sind bekannte Beispiele für schädliche E-Mails aufgeführt, die in letzter Zeit in Bedrohungssignalen aufgetaucht sind:

- **Phishing** (auch Spear-Phishing): Angreifer versuchen, jemanden dazu zu verleiten, vertrauliche Informationen weiterzugeben, indem sie dringliche Benachrichtigungen versenden, die den Empfänger auffordern, auf einen Link zu klicken, um beispielsweise ein Passwort zurückzusetzen. Bei der Eingabe ihrer Anmeldedaten auf einer gefälschten Domain werden die Opfer oft auf eine legitime Website wie die Anmeldeseite für M365 umgeleitet, um ihre Anmeldedaten erneut einzugeben und so den Datendiebstahl und Betrug zu vollenden.

- **Malware-Zustellung**: Wenn eine kompromittierte Nachricht empfangen und geöffnet wird, kann sie mit einer bösartigen Website verknüpft sein, die Malware auf einen Unternehmenscomputer überträgt. Alternativ kann ein infiziertes Dokument Makros enthalten, die im Hintergrund Ransomware herunterladen und Systeme in Waffen verwandeln, um andere in der Umgebung anzugreifen.

Cerber-Ransomware ist ein bemerkenswertes Beispiel für Angreifer, die sich beim Versand von Phishing-E-Mails auf Microsoft (Office) 365-Benutzer konzentrieren.[10]

[9] VentureBeat. „22 Very Bad Stats on the Growth of Phishing, Ransomware“, 22. Feb. 2022.

[10] AFI. „Can Ransomware Hit Your Microsoft 365 Data?“ 22. Jan. 2022.

Selbst wenn Sie bei den fundamentalen M365-Sicherheitsmaßnahmen alles richtig gemacht haben, darunter die korrekte Konfiguration von Mailflow-Regeln für die SCL-Spam-Erkennung, Anti-Spam, Anti-Phishing, sichere Links, sichere Anhänge, Multifaktor-Authentifizierung und Anti-Malware-Einstellungen, gelangen dennoch einige E-Mails von Angreifern in die Postfächer von Unternehmen. Noch größer ist die Herausforderung bei OneDrive- und SharePoint-Dateien, bei denen das Risiko einer Verschlüsselung höher ist.

Wenn Angreifer zuschlagen, müssen Sie sicher sein, dass eine schnelle Wiederherstellung möglich ist, und zwar gemäß den SLAs des Unternehmens. Wenn Ihr Unternehmen Erwartungen an eine Wiederherstellungs-SLA (RTO und RPO) und ein bevorzugtes Wiederherstellungsformat nach unerwarteten Störungen wie einem Ransomware-Angriff hat, benötigen Sie eine Datensicherungslösung, die sich an den Geschäftsanforderungen ausrichtet und die Wiederherstellbarkeit gewährleistet. Das bedeutet, dass die Datensicherung Ihrer gesamten M365-Suite, einschließlich Exchange Online-E-Mails, Teil Ihres IT-Plans sein muss.

Datenverschlüsselung

Die Verschlüsselung von Daten ist seit Jahren die bevorzugte Strategie der Ransomware-Angreifer. Cyberkriminelle sperren Produktionsdaten und verlangen eine beträchtliche Zahlung, bevor sie versprechen, den Teams einen Verschlüsselungsschlüssel (oft eine Reihe von Schlüsseln, die durchsucht werden müssen) zu geben, um ihre Daten zu entschlüsseln und freizugeben. Ein Beispiel: OneDrive und SharePoint befinden sich bereits in den Händen von Angreifern. Diese Sammlungen können auf verschiedene Weise verschlüsselt werden. Infizierte lokale Dateien können zum Beispiel von einem Benutzersystem mit OneDrive oder SharePoint synchronisiert werden oder direkt von einem Server, der Dateien in großem Maßstab verschlüsselt und synchronisiert. Selbst wenn Sie Ihre Dateien mithilfe der Versionierung zurücksetzen könnten, ist dieser Prozess mühsam und kann keine zeitpunktgenaue Wiederherstellung gewährleisten – oft eine geschäftskritische Anforderung. In allen Fällen ist ein System zur unveränderlichen Datensicherung und -wiederherstellung eine wirksame Gegenmaßnahme.

Datendiebstahl und -exfiltration

Der unvorstellbare Erfolg hat Ransomware-Angreifer angespornt und ihre Kreativität beflügelt. Cyberkriminelle begnügen sich jetzt nicht mehr mit der Verschlüsselung von Dateien und Daten, sondern stehlen diese auch. Sie entfernen illegal große Mengen von Daten („Exfiltration“) und konzentrieren sich dabei auf sensible und vertrauliche Informationen wie Kreditkartennummern und personenbezogene Daten. Ihr Ziel dabei ist es, diese öffentlich zu machen oder im Darknet zu verkaufen, um von den geschädigten Unternehmen noch größere Summen zu erpressen.

Die Bedrohung durch Doppelerpressung mit Ransomware ist ideal für M365-Daten und furchterregend für Unternehmen. Mit M365 und anderen SaaS-Apps, die einen leichten Online-Zugriff und einfache Freigabekontrollen bieten, eröffnen sich Cyberkriminellen großartige Möglichkeiten – viele davon sogar mit weniger Hindernissen. Zu ihrer Bekämpfung müssen Unternehmen die Apps und die Benutzer, die auf Daten zugreifen, proaktiv auf Verhaltensweisen überwachen, die auf cyberkriminelle Aktivitäten hinweisen.

Bis zum Jahr 2025 werden Auszahlungen in Höhe von 1,75 Billionen US-Dollar im Zusammenhang mit Ransomware erwartet.[11]

Mehr als 83 % der Angriffe betreffen den Diebstahl von Unternehmensdaten und Dateiverschlüsselung.[12]

[11] Cybersecurity Ventures. „CISO Report: Ransomware Business is Booming“, 10. Dez. 2021.

[12] Coveware. „Ransomware Attackers Down Shift to ‚Mid-Game‘ Hunting in Q3 2021“, 21. Okt. 2021.

Umsetzbare Schritte zur Datensicherheit und Risikominderung

Integrierte M365-Sicherheitsvorkehrungen sind nicht mit einer modernen Datensicherung gleichzusetzen. Sie bieten auch keinen mehrschichtigen Ansatz für den Schutz vor M365-Ransomware. Mit einer Next-Gen Data Management-Lösung sind Sie besser auf Ransomware-Angriffe vorbereitet und können drei wichtige Schritte zum Schutz Ihrer Daten durchführen.

1. Schnelle, flexible Datensicherung und -wiederherstellung

Ganz egal, ob sich Ihr Unternehmen von einem Ransomware-Angriff erholen oder jahrelang archivierte Dateien finden muss (weit über die standardmäßigen Aufbewahrungsfristen von M365 hinaus), Sie benötigen eine moderne Backup-Lösung, die Daten zu jedem Zeitpunkt wiederherstellen kann – und zwar schnell. Eine Backup as a Service (BaaS)-Lösung für das Next-Gen Data Management bietet Ihnen automatisierte Datensicherungen sowie vollständige und granulare Datenwiederherstellung in Verbindung mit On-Demand-Zugriff und Benutzerfreundlichkeit.

Schnelle skalierbare Wiederherstellung

Mit der richtigen BaaS-Lösung lassen sich im Falle eines groß angelegten Angriffs, einer Naturkatastrophe oder eines menschlichen Versagens schnell Hunderte, sogar Tausende von Postfächern oder Dateien wiederherstellen. Die Wiederherstellung im großen Maßstab sollte nicht nur auf M365 beschränkt sein, sondern auch die schnelle Wiederherstellung von Hunderten von VMs, großen Datenbanken oder großen Mengen unstrukturierter Daten zu jedem Zeitpunkt und an jedem beliebigen Zielort erlauben.

Zeitpunktgenaue Wiederherstellung

Innerhalb von M365 kann ein Mitarbeiter eine andere Version eines einzelnen Dokuments oder einer Präsentation aufrufen und schnell wiederherstellen. Doch mit der Versionierung in M365 kann Ihr Unternehmen keinen bestimmten Zeitpunkt wählen, um einen Snapshot der letzten fehlerfreien Kopie aller Daten vor der Kompromittierung zu erhalten. Eine Next-Gen-Lösung für die Datensicherung bietet genau das. Mit BaaS können Sie große Datenmengen nach einem Angriff oder einer Störung schnell und in großem Maßstab wiederherstellen und die Einhaltung Ihrer RTOs und RPOs sicherstellen.

Saubere Wiederherstellung, wo Sie sie benötigen

Für eine verlässliche und vollständige Wiederherstellung kann eine moderne BaaS-Lösung mit integrierter Machine-Learning-Engine (ML) die letzte bekannte saubere Kopie ermitteln. So können Sie bei einer Wiederherstellung sicher sein, dass die Snapshot-Daten frei von Anomalien und Ransomware sind. Stellen Sie sicher, dass Ihre Lösung auch eine direkte Wiederherstellung der Daten am ursprünglichen Speicherort oder an einem neuen Speicherort erlaubt, z. B. bei einem Ausfall des M365-Services oder einer Kompromittierung Ihrer Konten.

2. Zuverlässige Datensicherung

Da Cyberkriminelle mittlerweile erkannt haben, dass Repositorys für die Datenaufbewahrung und Backups wie Versicherungspolicen sind, muss Ihr Unternehmen mehr für den Schutz Ihrer wertvollen Backup-Daten tun. Wählen Sie für ein optimales Ergebnis ein BaaS-Angebot mit strengen Sicherheitskontrollen. Ziehen Sie außerdem BaaS in Betracht, bei dem die Daten in einem separaten Cloud-Dienst außerhalb von Microsoft aufbewahrt werden und bei dem keine zusätzlichen Gebühren für Datenabgänge anfallen.

Unveränderliche Snapshots

Für Cyberkriminelle sind Produktionsdaten nach wie vor ein Hauptziel. Doch inzwischen versuchen sie auch immer häufiger, Backups zu verschlüsseln oder zu löschen, um Ihnen jede Möglichkeit zu nehmen, Ihre Produktionsdaten nach einem Angriff schnell wiederherzustellen. Eine Next-Gen-BaaS-Lösung, die Unveränderlichkeit bietet, hilft dabei, diese beiden Szenarien zu verhindern, denn die Daten sind in einem unveränderlichen Snapshot gespeichert, der weder versehentlich noch in böswilliger Absicht modifiziert, geändert oder manipuliert werden kann.

Write Once Read Many (WORM)

Mit WORM kann Ihr Team durch Richtlinien eine zeitgebundene Sperre für Daten erstellen und anwenden und diese dann ausgewählten Jobs zuweisen, um die Unveränderlichkeit geschützter Daten zu verbessern. Da dies ein Schutz ist, den weder Sicherheitsbeauftragte noch Sicherheitsadministratoren ändern oder löschen können, müssen Sie sich nicht so viele Gedanken über potenzielle Insider-Bedrohungen machen. Dies ist eine Next-Gen Data Management-Funktion, die M365 von Haus aus nicht bietet.

Datenverschlüsselung

Versuchen Sie, eine Lösung zu finden, die FIPS 140-2 entspricht, dem Standard der US-Regierung für kryptografische Module. Damit haben Sie die Gewähr, dass das Moduldesign und die Implementierung der kryptografischen Algorithmen sicher und korrekt sind. Nach dem FIPS-Standard validierte Verschlüsselung in modernem BaaS wird weltweit als die beste Methode zum Schutz von Daten während der Übertragung und im gespeicherten Zustand geschätzt.

Trennung der Backup-Daten von der Produktion

Die Speicherung Ihrer Backup-Daten außerhalb der Microsoft Cloud kann dazu beitragen, eine Art Trennung von „Off-Site“-Daten zu erreichen und zugleich helfen, Ransomware-Zahlungen entgegenzuwirken. BaaS hilft Ihnen, Ihre RTO/RPO-Anforderungen mit geeigneten Sicherheitskontrollen in Einklang zu bringen, indem Backup-Daten in der Cloud oder an einem anderen Ort gespeichert werden. Ihre Backup-Daten stehen so auch während eines M365-Ausfalls zur Verfügung und sind vor Manipulationen durch Cyberkriminelle geschützt, da sie in einem unveränderlichen Snapshot gespeichert sind.

3. Erfüllung von SLAs und Vereinfachung des Hybrid-Cloud-Betriebs

BaaS erhöht nicht nur Ihre Datensicherheit, sondern bietet auch einen umfassenden Satz von unternehmensgerechten Merkmalen, mit denen Sie entscheiden können, wann, wo und für welche Dauer Sie wichtige Informationen aufbewahren möchten. Dies bietet Ihrem Unternehmen die größtmögliche Auswahl und Flexibilität dahingehend, wie Sie Ihre Daten sichern und die geschäftlichen Anforderungen von heute und morgen erfüllen.

Flexible Aufbewahrung

Im Hinblick auf die Erfüllung komplexer Compliance-Anforderungen gibt es keine bessere Option als eine moderne Datensicherung durch einen Drittanbieter. Bei dieser Option bestimmen Sie, für welche Dauer Ihre M365-Daten aufbewahrt werden (für Monate oder sogar Jahre) und die entsprechenden Richtlinien werden für Sie verwaltet. Auch eine flexible langfristige Aufbewahrung, die über M365-Standards hinausgeht, hilft sicherzustellen, dass Ihr Unternehmen bei einer Störung Daten von einem beliebigen Zeitpunkt an wiederherstellen kann.

Einheitliche Datensicherung (M365 plus andere Datenquellen)

Möglicherweise möchten Sie aus geschäftlichen Gründen oder aus Gründen der Compliance nicht alle Workloads in die Cloud verlegen. Daher sollten Sie eine Datensicherungslösung wählen, mit der Sie M365, andere SaaS- und Cloud-Datenquellen sowie lokale Workloads wie VMs und Datenbanken sichern können.

Flexible Preisgestaltung

Eine solide Datenmanagementstrategie berücksichtigt bei der Auswahl einer Datensicherungslösung auch andere Aspekte als Ransomware. Beispielsweise ist es sehr wichtig, das Budget für die M365-Datensicherung auf die Arbeitsweise Ihres Unternehmens abzustimmen. Zahlen Sie entsprechend der Anzahl der Benutzer und gleichen Sie die Backups mit den M365-Plänen ab oder konsolidieren Sie die Backup-Daten über eine Vielzahl von Quellen hinweg und bezahlen Sie nach Kapazität? Letztere Option bietet Ihnen durch eine einzige Rechnung, die auf ein und derselben Metrik beruht, einen besseren Einblick in die Kosten. Next-Gen BaaS ist für eine flexible Preisgestaltung optimiert.

Checkliste für Microsoft 365 Backup und Ransomware-Schutz

Funktionen		Anbieter 1	Anbieter 2	Anbieter 3
Schnelle, flexible Datensicherung und -wiederherstellung	Schnelle skalierbare Wiederherstellung	☐	☐	☐
	Zeitpunktgenaue Wiederherstellung	☐	☐	☐
	Saubere Wiederherstellung, wo Sie sie benötigen	☐	☐	☐
Zuverlässige Datensicherung	Unveränderliche Snapshots	☐	☐	☐
	Write Once Read Many (WORM)	☐	☐	☐
	Datenverschlüsselung	☐	☐	☐
	Trennung der Backup-Daten von der Produktion	☐	☐	☐
Erfüllung von SLAs und Vereinfachung des Hybrid-Cloud-Betriebs	Flexible Aufbewahrung	☐	☐	☐
	Einheitliche Datensicherung (M365 plus andere Datenquellen)	☐	☐	☐
	Flexible Preisgestaltung	☐	☐	☐

Cohesity verstärkt den Schutz von Microsoft 365 vor Ransomware und anderen Bedrohungen

Cyberkriminelle nehmen immer wieder Datenquellen ins Visier, die hohe Lösegeldzahlungen abwerfen können. Mit Cohesity kann Ihr Unternehmen all seine Daten schützen, unabhängig davon, wo sie sich befinden.

Cohesity DataProtect wird als Service bereitgestellt und bietet umfassendes Backup as a Service (BaaS) für M365-Dienste. Dazu zählen z. B. Exchange Online und andere Office 365-Produktivitäts-Apps, OneDrive, SharePoint, Teams sowie weitere cloudgestützte (AWS) und On-Premises-Datenquellen wie VMs, Dateien und Datenbanken. Damit verfügt Ihr Unternehmen über einen unveränderlichen Snapshot, der getrennt von Microsoft gespeichert wird und Ihre Sicherungsdaten vor böswilliger Manipulation oder Löschung schützt. Dies erlaubt eine schnelle Wiederherstellung im Falle eines Ransomware-Angriffs oder Ausfalls und bietet Ihnen eine flexible Datenaufbewahrung, damit Sie Ihre Geschäfts- und Compliance-Anforderungen optimal erfüllen können. Ganz gleich, ob Sie eine Lizenzierung nach Benutzern oder nach Kapazität bevorzugen, Cohesity BaaS ermöglicht Ihnen eine flexible Preisgestaltung, sodass Sie das Modell wählen können, das Ihren Anforderungen am besten entspricht.

Melden Sie sich jetzt für eine
kostenlose 30-Tage-Testversion von DataProtect delivered as a Service an
und beginnen Sie in Minutenschnelle mit der Sicherung Ihrer Microsoft 365-Daten.

Erfahren Sie mehr unter Cohesity.com/de.

COHESITY