CARBONITE an opentext company | WEBROOT an opentext company

Wie sicher sind Ihre Cloud-Daten?

Da Mitarbeiter mit höheren Raten remote arbeiten, sind Geschäftsdaten zunehmend gefährdet.

Die globale COVID-19-Pandemie hat eine massive Verlagerung zur Fernarbeit verursacht. Einer Schätzung zufolge ist die Anzahl der Telearbeitstage seit der Pandemie um 49% gestiegen.[1] Während die Pandemie die Verschiebung ausgelöst haben mag, gibt es keine Anzeichen dafür, dass sich die Dinge wieder normalisieren werden, sobald die Krise verblasst. In einer kürzlich durchgeführten Umfrage gaben 83% der Befragten an, dass flexible Arbeitsrichtlinien auf absehbare Zeit bestehen bleiben werden.[2] Es ist offensichtlich, warum – die Produktivität war laut 94% der Arbeitgeber gleich oder höher.

49%
Anstieg der Anzahl der Tage, die seit COVID-19 für Telearbeit aufgewendet wurden

83%
Umfrageteilnehmer, die sagen, dass flexible Arbeit bestehen bleibt

94%
Arbeitgeber, die sagen, dass die Produktivität gleich oder höher war

Während Fernarbeit und Produktivitätsraten hoch sind, kann das Gleiche nicht über die Sicherheit von Cloud-Daten gesagt werden, die Remote-Mitarbeiter generieren. In den meisten Fällen sind die Heimnetzwerke, persönlichen Geräte und Cloud-Apps, die Remote-Mitarbeiter verwenden, weniger sicher als die lokalen Geräte. Cloud-Produktivitätsanwendungen wie Microsoft 365 haben den Übergang zur Remote-Arbeit zu einer nahtlosen Angelegenheit gemacht. IT-Administratoren sind jetzt jedoch dafür verantwortlich, das gleiche hohe Sicherheitsniveau für Daten aufrechtzuerhalten, die mehr denn je verteilt sind, und für Netzwerke, die nicht den gleichen robusten Schutz wie Büronetzwerke bieten.

Wenn IT-Organisationen Microsoft 365 bereitstellen, entbinden sie sich von der Verantwortung für die Aufrechterhaltung eines komplexen Netzwerks von Hardware- und Infrastruktur-Abhängigkeiten. Dabei verlieren sie jedoch die detaillierte Kontrolle über die Container, in denen sich ihre Geschäftsdaten befinden. Solange alles reibungslos läuft, gibt es keinen Grund zur Sorge. Herausforderungen ergeben sich jedoch, wenn alltägliche Datenverluste auftreten: Ein verärgerter Mitarbeiter löscht seinen OneDrive und leert den Papierkorb. Jemand setzt die Berechtigungen für eine gesamte SharePoint-Sammlungswebsite zurück oder die routinemäßige Fluktuation führt dazu, dass Sie für Exchange-Lizenzen bezahlen, die Sie nicht wirklich benötigen.

70%
Unternehmen, die in SaaS-Umgebungen Daten verloren haben

35%
Organisationen, die mit SaaS-SLAs nur teilweise vertraut sind

33%
Unternehmen, die glauben, dass SaaS-Apps nicht gesichert werden müssen

37%
Unternehmen, die sich beim Datenschutz auf ihren SaaS-Anbieter verlassen

Es gibt ein weit verbreitetes Missverständnis, dass mit der Bereitstellung in der Cloud die Risikominderungsaufgaben der IT entfallen. Studien zeigen, dass mindestens 70% der Unternehmen in Software as a Service (SaaS) -Umgebungen wie Microsoft 365 einen gewissen Datenverlust erlitten haben.[3] Durch die Verwirrung in der Cloud besteht für Unternehmen ein höheres Risiko für Datenverlust, da sie den Betrieb schnell auf SaaS-Umgebungen verlagern. Untersuchungen zufolge geben 35% der Unternehmen an, die Service Level Agreements (SLAs) ihrer SaaS-Anbieter nur teilweise zu kennen. Noch besorgniserregender ist, dass 33% der Unternehmen der Meinung sind, dass SaaS-Anwendungen überhaupt nicht gesichert werden müssen, während 37% sich ausschließlich auf ihren SaaS-Anbieter verlassen, um ihre Anwendungsdaten zu schützen.

SaaS-Anbieter wie Microsoft sind nur für die Verfügbarkeit ihrer Infrastruktur und Dienste verantwortlich, nicht für die Daten, die ihre Kunden in der Cloud speichern. Für alltägliche Datenverlustszenarien wie versehentliches oder böswilliges Löschen oder Überschreiben von Berechtigungen muss das Unternehmen bei Datenverlust eine Wiederherstellung durchführen. Und ohne ein vollständiges Toolset für die Durchführung verschiedener Arten der Wiederherstellung ist der Prozess viel manueller und fehleranfälliger als der gleiche Vorgang, der mit speziell entwickelten Tools ausgeführt wird.

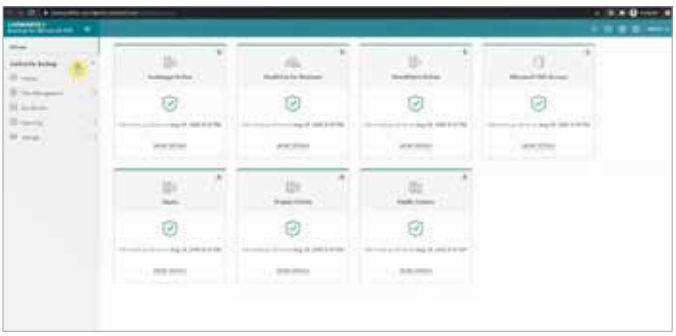
In vielen Szenarien könnte die IT Zeit und Ressourcen sparen, indem sie SaaS-Anwendungen mit Datenschutzlösungen unterstützt, die robuste Disaster Recovery-Funktionen enthalten, anstatt nur mit den eingeschränkten Funktionen bestimmter SaaS-Plattformen auszukommen.

Datenverlust in OneDrive

OneDrive ist ein sogenanntes Tool zum Synchronisieren und Freigeben von Dateien. Es ist sehr nützlich für den angegebenen Zweck, d.h. Ordner in der Cloud zu spiegeln und Mitarbeitern die Freigabe dieser Dateien zu ermöglichen. Aufgrund dieser Funktionen wird OneDrive auch als Tool für die Zusammenarbeit und Produktivität eingestuft. OneDrive ist nicht für die Sicherung und Wiederherstellung konzipiert, da es nicht über alle Funktionen für die Durchführung einer flexiblen Notfallwiederherstellung verfügt. Eine echte Sicherungslösung bietet IT-Administratoren mehrere Optionen zum Wiederherstellen von Dateien, Ordnern sowie Systemstatusinformationen. Abhängig von der Art des Datenverlustszenarios können diese Funktionen den Wiederherstellungsprozess vereinfachen und die Zeit für die Wiederherstellung von Daten verkürzen, die auch als Recovery Time Objective (RTO) bezeichnet wird.

93
Tage
Standardaufbewahrungsrichtlinie für den Papierkorb

Wenn bei OneDrive eine Datei - ob böswillig oder versehentlich - gelöscht wird, besteht die wahrscheinliche Vorgehensweise darin, im OneDrive-Papierkorb nach der gelöschten Datei zu suchen. Abhängig davon, wie viel Zeit seit dem Löschen der Datei vergangen ist, ist die Datei



möglicherweise vorhanden oder nicht. OneDrive verfügt über eine Standardaufbewahrungsrichtlinie. Nach Ablauf der Aufbewahrungsfrist (oder wenn die Person, die die Datei gelöscht hat, sie auch aus dem Papierkorb gelöscht hat) kann die Datei ohne eine Sicherungslösung eines Drittanbieters nicht wiederhergestellt werden.

Das Durchführen einer umfangreichen Datei- oder Ordnerwiederherstellung kann mit jedem Prozess, der mehrere manuelle Schritte umfasst, sehr zeitaufwändig sein. Ein speziell entwickeltes Sicherungs- und Wiederherstellungstool automatisiert viele der Schritte, die mit komplexen Notfallwiederherstellungsszenarien verbunden sind. Die speziell entwickelte Sicherung ermöglicht die Wiederherstellung von Dateien und Ordnern über ein administratives Dashboard.

Das Dashboard enthält auch Optionen für die Wiederherstellung zu einem bestimmten Zeitpunkt, die über eine Sicherungsplanungsfunktion aktiviert werden. Durch das Planen häufigerer Sicherungen können Administratoren das Fenster verkleinern, in dem Datenverluste auftreten können. Dies wird auch als Recovery Point Objective (RPO) bezeichnet. Den meisten Tools zum Synchronisieren und Freigeben von Dateien fehlen diese Funktionen, die in einer speziell entwickelten Sicherungslösung Standard sind, da sie nicht für die Sicherung ausgelegt sind.

Dieselben Funktionen, die das versehentliche Synchronisieren und Freigeben von Dateien so bequem machen, erleichtern die Verbreitung von Malware. Wenn ein Benutzer in einer E-Mail auf einen schädlichen Link klickt, werden nicht nur lokale Dateien mit Malware infiziert, sondern diese beschädigten Dateien werden auch mit der Cloud synchronisiert, sodass der Administrator keinen sauberen Wiederherstellungspunkt mehr hat. Das Ergebnis ist, dass die Dateien dauerhaft verloren gehen oder dass das Unternehmen bei Ransomware ein Lösegeld aushandeln muss, um einen Entschlüsselungsschlüssel zu erhalten.

90%

Neu erstellte Coronavirus-Domänen, die betrügerisch sind[4]

Sicherungen mit Carbonite® Backups für Microsoft 365 sind unveränderlich, d.h. sie können weder von Ransomware-Dieben noch von anderen geändert werden. Auf diese Weise wird sichergestellt, dass IT-Administratoren Zugriff auf sichere Wiederherstellungspunkte in der Cloud haben, sollten lokale Dateien je infiziert werden. Ransomware-Vorfälle nehmen zu, und es entstehen irreführende neue Varianten mit Coronavirus-Motiven. Benutzer, insbesondere Fernmitarbeiter in ungeschützten persönlichen WLAN-Heimnetzwerken, sind besonders anfällig für diese Art von Angriffen.

SharePoint-Berechtigungen und Websitesammlungen

IT-Administratoren müssen bei der Verwaltung von SharePoint-Umgebungen auch die gleichen Probleme

beim Löschen, Beschädigen und Synchronisieren von Dateien berücksichtigen. Websitesammlungen unterliegen ebenfalls der Richtlinie zur Aufbewahrung im Papierkorb. Dies bedeutet, dass gelöschte Websites über den Aufbewahrungszeitraum hinaus nicht wiederhergestellt werden können.

SharePoint-Berechtigungen können auch gelöscht oder ungültig gemacht werden, sodass bestimmte Gruppen oder sogar der Administrator selbst nicht auf die gesamte Website zugreifen können. In den meisten Fällen gibt es keine native Funktionalität, die den Zugriff auf diese Sites wiederherstellt. Aber mit Carbonit® Backup für Microsoft 365 können Administratoren die Sicherheitseinstellungen auf einzigartige Weise wiederherstellen, wenn Berechtigungen beschädigt werden oder auf andere Weise auf die Site nicht zugegriffen werden kann.

Die Lösung bietet Administratoren auch die Möglichkeit, eine gesamte Websitesammlung, ein Dokument oder eine Bibliothek wiederherzustellen, je nachdem, was zur Behebung des Schadens erforderlich ist. Es besteht auch die Möglichkeit, den Inhalt einer Site, einer Sammlung, eines Dokuments oder einer Dokumentbibliothek bei Bedarf zu Archivierungszwecken an einen anderen Speicherort zu exportieren.

Wiederherstellen von Teamgesprächen

Die heutigen Remote-Mitarbeiter verlassen sich mehr denn je auf Telekommunikationsplattformen wie Microsoft Teams für Chat- und Videokonferenzen. Je mehr Mitarbeiter in Teams interagieren und Geschäfte abwickeln, desto wichtiger ist es für IT-Administratoren, die Daten in Teams zu schützen. Ebenso wichtig ist die Möglichkeit, Konversationen einfach wiederherzustellen, ohne auf mehrere manuelle Schritte zurückgreifen zu müssen. Das Wiederherstellen von Gesprächen in Teams ist jedoch ein manueller und arbeitsintensiver Prozess. In vielen Fällen kann der ursprüngliche Beitrag nicht wiederhergestellt oder nur als Kommentar in einen anderen Beitrag eingefügt werden.

Mit Carbonit® Backup für Microsoft 365 kann der IT-Administrator die Sicherungsdaten von Teams am

ursprünglichen Speicherort wiederherstellen. Wenn eine Gruppe in Teams vom ursprünglichen Speicherort gelöscht wurde, kann der Administrator die Gruppe in Teams und die Berechtigungen des Eigentümers und aller seiner Mitglieder wiederherstellen.

Mit Carbonite® Backup für Microsoft 365 können Sie auch eine Gruppe mit weichen Löschvorgängen in Teams aus dem Microsoft 365 Papierkorb auf den letzten bekannten fehlerfreien Zustand zurücksetzen. Carbonite überprüft den Status der Gruppe in Teams, um sicherzustellen, dass Microsoft über diese Daten verfügt, und bietet Optionen für die Wiederherstellung, einschließlich der Verwendung der nativen Microsoft-Wiederherstellungsfunktion innerhalb des Aufbewahrungszeitraums oder der Verwendung von Carbonite-Sicherungsdaten, um das gesamte Team oder sogar granularen Inhalt zurückzusetzen, falls gewünscht.

Umgang mit Exchange-Postfächern

Wenn Mitarbeiter das Unternehmen verlassen, muss das Unternehmen entscheiden, wie mit dem Exchange-Postfach des verstorbenen Mitarbeiters umgegangen werden soll. Obwohl es viel kostet, weiterhin für Lizenzen zu bezahlen, nur um Postfächer zu behalten, tun viele Unternehmen genau das. Einige Unternehmen platzieren die E-Mails in einem freigegebenen Postfach, was aus mehreren Gründen nicht ideal ist. Es gibt Größenbeschränkungen, die bei Überschreitung weiterhin eine zugewiesene Lizenz erfordern. Außerdem ist eine Löschung des Postfachs möglich, wodurch der Archivierungspunkt zunichte gemacht wird. Wenn der IT-Administrator die Lizenz des ehemaligen Mitarbeiters einem neuen Mitarbeiter zuweist, gehen alle Daten des ehemaligen Mitarbeiters verloren.

Problemumgehungen bei der Archivierung sind aus mehreren Gründen unzureichend. Aus diesem Grund können Sie am besten mithilfe von Tools archivieren, die für diesen Zweck entwickelt wurden. Mit Carbonit® Backup für Microsoft 365 können IT-Administratoren Postfachinhalte einfach in einen Personal Storage Table (PST) als Teil eines Standard-Offboarding-Prozesses für Endbenutzer exportieren. Postfächer können an einen anderen Speicherort wie beispielsweise das Postfach eines anderen Benutzers exportiert werden. Dies ist hilfreich, wenn ein Postfach versehentlich gelöscht wird und von Grund auf neu erstellt werden muss. Postfächer können auch für Rechtsstreitigkeiten in ein E-Discovery-Tool importiert werden.

Umfassender Portfolio-Schutz

Bereits vor der COVID-19 Pandemie stellten Unternehmen ihre Mitarbeiter rasch auf Microsoft 365 Cloud Apps um. Da mehr Mitarbeiter als je zuvor remote arbeiten, sind Cloud-Plattformen und Tools für die Cloud-Zusammenarbeit für den Geschäftsbetrieb unverzichtbar geworden.

Während Unternehmen seit langem über ein umfassendes Toolset zum Schutz und zur Wiederherstellung lokaler Daten verfügen, hatten sie bei Cloud-Apps wie Microsoft 365 keinen Zugriff auf dieselben flexiblen Wiederherstellungsoptionen. Da Unternehmen kein klares Verständnis für Microsoft SLAs haben, bleibt ein Großteil der Daten, auf die sich Remote-Mitarbeiter verlassen, um produktiv zu bleiben, anfällig für eine Reihe von Risiken. Apps für die Zusammenarbeit und Produktivität sind zwar für den angegebenen Zweck sehr effektiv, jedoch nicht für die Notfallwiederherstellung konzipiert.

Carbonite® Backup für Microsoft 365 schützt die gesamte Suite von Microsoft 365 Apps. Es bietet IT-Organisationen die Tools, die sie für die Art von Datenverlustszenarien benötigen, mit denen sie routinemäßig konfrontiert sind. Dies spart Zeit und Ressourcen, wenn jemand versehentlich eine Datei in OneDrive löscht, die Berechtigungen in SharePoint ändert oder wenn Mitarbeiter das Unternehmen verlassen und ihre wichtige Geschäftskommunikation erhalten bleiben muss.

Während die Krise im Bereich der öffentlichen Gesundheit irgendwann nachlassen wird, dürften flexible Fernarbeitsregelungen bestehen bleiben. Remote-Mitarbeiter sind möglicherweise weiterhin so produktiv wie zuvor oder besser, jedoch nur dann, wenn ihre Cloud-Daten und -Anwendungen vor den häufigsten Ursachen für Datenverlust geschützt sind.

Kontaktieren Sie uns, um mehr zu erfahren – Webroot EMEA
E-Mail: carb-salesemea@opentext.com
Telefon: 1 800 303 388

Kontaktieren Sie uns, um mehr zu erfahren – Webroot APAC
E-Mail: carb-apac_sales_team@opentext.com
Telefon: 1 800 013 992

1. Gallup, USA, Fernarbeitstage haben sich während der Pandemie verdoppelt https://news.gallup.com/poll/318173/remote-workdays-doubled-during-pandemic.aspx

2. Eine Studie der Gesellschaft für Personalmanagement stellt fest, dass die Produktivität nicht durch Verlagerung auf Fernarbeit beeinträchtigt wird.https://www.shrm.org/hr-today/news/hr-news/pages/study-productivity-shift-remote-work-covid-coronavirus.aspx#:~:text=Ninety%2Dfour%20percent%20of%20800,with%20their%20employees%20working%20remotely

3. Enterprise Strategy Group, Data Protection Cloud Strategies (Juni 2019)

4. ZDNet, COVID Cyberkriminalität: 10 beunruhigende Statistiken, die Sie heute Abend wach halten (September 2020), https://www.zdnet.com/article/ten-disturbing-coronavirus-related-cybercrime-statistics-to-keep-you-awake-tonight/

Über Carbonite und Webroot

Carbonite und Webroot, OpenText-Unternehmen, nutzen die Cloud und künstliche Intelligenz, um Unternehmen, Einzelpersonen und Managed Service Providern umfassende Lösungen für mehr Cyberresilienz anzubieten. Cyberresilienz bedeutet, dass Systeme trotz Cyberangriffen und Datenverlusten jederzeit aktiv und betriebsbereit sind. Mit diesem Ziel haben wir unsere Kräfte gebündelt, um Endpunktschutz, Netzwerkschutz, Schulungen zur Steigerung des Sicherheitsbewusstseins, Datensicherungs- und Notfallwiederherstellungslösungen sowie Threat Intelligence-Services bereitzustellen, die von marktführenden Technologieanbietern weltweit verwendet werden. Webroot nutzt die Leistungsstärke des maschinellen Lernens zum Schutz von Millionen von Unternehmen und Einzelpersonen und sichert die vernetzte Welt. Carbonite und Webroot sind weltweit in Nordamerika, Europa, Australien und Asien tätig. Erfahren Sie mehr über Cyberresilienz unter carbonite.com und webroot.com.