



MSPeasy – BCDR verkaufen leicht gemacht

Leitfaden für ein erfolgreiches BCDR-Verkaufsgespräch –
von MSPs für MSPs

Einleitung

Viele Managed Service Provider (MSPs) tun sich schwer damit, ihren mittelständischen Geschäftskunden und/oder potenziellen Kunden den Wert einer zuverlässigen Business Continuity & Disaster Recovery (BCDR)-Lösung zu vermitteln. Dabei ist genau das wichtig: Laut einer [aktuellen Umfrage unter 250 deutschsprachigen MSPs](#) ist es eine der häufigsten Herausforderungen von MSPs, die Kosten für BCDR zu rechtfertigen. Was ist der Grund dafür?

Viele Geschäftsinhaber kennen unter Umständen den Unterschied zwischen einer BCDR-Lösung und herkömmlichen Backups nicht. Doch genau solche Argumente sind entscheidend. Denn ein kostenbewusster Geschäftsführer benötigt gute Gründe, um mehr für den Schutz von Daten auszugeben als in den Vorjahren, insbesondere, wenn es noch nie zu einem schweren Datenverlust oder einem Ausfall gekommen ist. Und viele Kunden unterschätzen das Risiko von Cybersicherheit oder Ransomware – und müssen erst noch überzeugt werden, sich dafür zu interessieren. Sie möchten das perfekte BCDR-Verkaufsgespräch? Dann sollten Sie sich auch die Zeit nehmen, Ihre Kunden und Interessenten zielgerichtet über diese Inhalte zu informieren.

In diesem eBook erfahren Sie, wie Sie Ihren Kunden die Vorteile einer vollständig gemanagten BCDR-Lösung gegenüber herkömmlichen Backup-Produkten vermitteln. Tipp-Geber sind MSPs, die schon erfolgreiche BCDR-Verkaufsgespräche geführt haben. Sie erhalten außerdem praktische Beispiele, wie BCDR-Produkte den finanziellen Schaden eines Ausfalls reduzieren können. Und dieses eBook enthält eine 1-seitige Anleitung mit den wichtigsten Argumenten für BCDR.

Downtime ist heutzutage nicht mehr akzeptabel. Die gute Nachricht: Mit BCDR-Lösungen sind Ausfallzeiten kein Thema mehr. Unternehmen, die BCDR nicht ernst nehmen, setzen sich allerdings einem großen Risiko aus.

BCDR verkaufen – Die Kosten der Downtime berechnen

Die Kosten von ein paar Stunden Downtime, geschweige denn von Tagen oder sogar Wochen, können für ein Unternehmen verheerend sein. Wenn ein Betrieb still steht, können Kunden weder Bestellungen aufgeben noch auf Account-Informationen zugreifen. Mitarbeiter können nicht mehr arbeiten. Die Umsatzeinbußen addieren sich schnell. Früher war es nicht existenzbedrohend, wenn es Tage oder Wochen dauerte, bis man wieder ganz regulär arbeiten konnte. Tape-Backups, die man noch zum Unternehmen bringen musste, waren für die damalige Zeit zuverlässig genug. Das ist heute anders. Unternehmen können nicht mehr Wochen oder Tage warten, um wieder voll einsatzbereit zu sein. Downtime ist heutzutage nicht mehr akzeptabel. Die gute Nachricht: Mit BCDR-Lösungen sind Ausfallzeiten kein Thema mehr. Unternehmen, die BCDR nicht ernst nehmen, setzen sich allerdings einem großen Risiko aus.

Von Server- und Stromausfällen bis zu Cyber-Bedrohungen: Downtime kann durch eine Reihe von Faktoren verursacht werden. Da Ransomware weiterhin Unternehmen weltweit attackiert, haben wir 2.400 MSPs, mit denen wir zusammenarbeiten, gebeten, [die Kosten dieser Angriffe](#) zu analysieren. MSPs berichteten, dass das durchschnittliche geforderte Lösegeld ca. €3.700 betrug, und die Kosten für Ausfallzeiten durch einen Angriff um mehr als das 10-fache höher waren – und zwar ca. €40.500.

Solche Beträge können sich die wenigsten Unternehmen leisten. Viele Mitarbeiter wären von dem Disaster betroffen, ihr Lohn könnte ggf. nicht mehr bezahlt werden, die damit verbundenen Overhead-Kosten und verlorenen Einnahmen noch nicht eingerechnet. Hinzu kommen die negativen Folgen für

datto
Kostenloses Tool:
So viel kostet Downtime
Recovery Time Calculator

Jetzt berechnen





Manuelle Backups und veraltete Technologien werden den Unternehmen von heute nicht mehr gerecht. 40 Jahre alte Lösungen wurden entwickelt, um die Probleme von vor 40 Jahren zu lösen.

die Reputation eines Unternehmens, die sich ebenfalls negativ auf den Erfolg eines Unternehmens auswirken.

Manuelle Backups und veraltete Technologien werden den Unternehmen von heute nicht mehr gerecht. 40 Jahre alte Lösungen wurden entwickelt, um die Probleme von vor 40 Jahren zu lösen. Backup-Tools, die einen erheblichen manuellen Mehraufwand für Mitarbeiter bedeuten, werden auch nicht optimal funktionieren, denn Menschen machen Fehler. Unternehmen sind also erheblich höheren Risiken ausgesetzt als früher.

Kunden, die weiterhin auf veraltete oder manuell gesteuerte Backup-Prozesse setzen, werden zwar so eventuell ihre Daten sichern, aber sie können weder deren Verfügbarkeit bei Bedarf garantieren, noch überprüfen, dass der Backup-Prozess tatsächlich funktioniert hat. Business Continuity kann nicht gewährleistet werden, wenn es sich um Backups handelt, bei denen die Mitarbeiter jeden Freitag daran denken müssen, eine Kopie der Daten zu erstellen. Automatisierung ist deshalb das Schlüsselwort. Gerade ein [hybrides Cloud Backup](#) trägt zur Continuity bei.

Die kostengünstigste Lösung für Unternehmen, die wichtige Daten sichern möchten, ist die Cloud. Widerstand gegen die Cloud, weil sie nicht zuverlässig sein soll, ist heute nicht mehr gerechtfertigt, sondern nur ein Hindernis für Unternehmen. Hybride cloudbasierte Backup-Lösungen ermöglichen Unternehmen den Zugriff auf ein lokales Backup, das vor Ort gespeichert ist, und eine zusätzliche Kopie ihres gesamten Netzwerks in der Cloud. Das lokale Backup bietet bei Bedarf einen schnellen Zugriff auf die Daten. Die umfangreichere Kopie in der Cloud kommt bei einem größeren Problem zum Einsatz, sodass eine längere Downtime vermieden wird. Hybrid Cloud Backup gibt Unternehmen also die Sicherheit, die sie benötigen, um bei kleinen und großen Daten-Katastrophen schnell wieder einsatzbereit zu sein.

Widerstand gegen die Cloud, weil sie nicht zuverlässig sein soll, ist heute nicht mehr gerechtfertigt, sondern nur ein Hindernis für Unternehmen.

Dies könnte Sie auch interessieren:

datto

Legen Sie die Messlatte für Zuverlässigkeit höher

Jetzt herunterladen



Kein Unternehmen ist zu 100 % geschützt vor Datenverlust. Doch wenn man sich die Kosten einer längeren Downtime vor Augen hält, wird klar, dass Unternehmen das Risiko ausschalten sollten. Veraltete Technologie ist keine Lösung. Unternehmen, die sich vor der wachsenden Zahl von Bedrohungen schützen wollen, müssen sich zwei Fragen stellen: 1. Was steht bei Downtime auf dem Spiel? 2. Welche Lösungen gibt es auf dem Markt, die meine Anforderungen erfüllen?

Das RTO/RPO-Argument eignet sich hervorragend, um die höheren Kosten einer All-in-One-Lösung für Business Continuity und Disaster Recovery (BCDR) gegenüber einer einfachen alten Backup-Lösung zu rechtfertigen. Ziel ist es, den Wert von Business Continuity gegenüber Backup hervorzuheben. Mit dem kostenlosen [Recovery Time Calculator](#) von Datto können Sie dies schnell und einfach durchrechnen. So funktioniert es.

Schritt 1 – Finden Sie heraus, mit welcher Downtime Unternehmen rechnen müssen

Bei Gesprächen mit potenziellen Kunden sollten Sie zunächst prüfen, wie lange es dauert, Daten – lokal oder aus der Cloud – im Falle von Datenverlust oder Störungen wiederherzustellen. Hierfür benötigen Sie die folgenden Informationen:

- Kritische Systemdaten: X GB
 - Als kritische Systemdaten bezeichnet man die Summe der Daten, die in einem bestimmten Szenario verloren gehen und zu Downtime für Mitarbeiter führen.
- Zeit zwischen Backups: X TAGE X STUNDEN X MINUTEN
- Das Intervall, in dem Ihre Backups erstellt werden. Dies wird zur Ermittlung des Recovery Point Objectives (RPO) verwendet.



- Start des Wiederherstellungsprozesses: X TAGE X STUNDEN X MINUTEN
 - Die Zeit, die man benötigt, um eine Wiederherstellung von Dateien oder Systemen einzuleiten. Dazu gehören die Benachrichtigung eines Managed Service Providers und die Konfiguration des Recovery Points.
- Geschätzte Downtime: X TAGE X STUNDEN X MINUTEN
 - Die Dauer der Downtime wird durch das Addieren der STARTZEIT DES WIEDERHERSTELLUNGSPROZESSES zu der Zeit, die für die vollständige Wiederherstellung der verlorenen Daten benötigt wird, bestimmt (LOKALE WIEDERHERSTELLUNGSZEIT).
 - Die Geschwindigkeit, mit der die verlorenen Daten wiederhergestellt werden, hängt davon ab, ob sie lokal oder aus der Cloud wiederhergestellt werden.
 - Lokale Geschwindigkeit: Die standardmäßige lokale Wiederherstellungs-Geschwindigkeit basiert auf einer typischen Gigabit-Verbindung.
 - Cloud: Die standardmäßige Wiederherstellungs-Geschwindigkeit aus der Cloud basiert auf der durchschnittlichen Geschwindigkeit der Internetverbindung von Unternehmen.
 - **Hinweis:** Da die lokale Wiederherstellung schneller ist als die Cloud-Wiederherstellung, kommt es durch die lokale Wiederherstellung zu weniger Downtime.

Beispiel:

- STARTZEIT DES WIEDERHERSTELLUNGSPROZESSES: 1 Std.
- LOKALE WIEDERHERSTELLUNGSZEIT: 1170 Sek.
- STARTZEIT DES WIEDERHERSTELLUNGSPROZESSES + LOKALE WIEDERHERSTELLUNGSZEIT = DOWNTIME
- 1 Std. + (100 GB / LOKALE GESCHWINDIGKEIT) = DOWNTIME
- 1 Std. + (819200 MB / 700 Megabits pro Sekunde (MBPs)* = DOWNTIME

- 1 Std. + 1170 Sek. = DOWNTIME
 - DOWNTIME = 1 Std. 20 Min.
- *Berücksichtigt den Netzwerk-Verkehr

Schritt 2 – Berechnen Sie die Kosten der Downtime

Sobald Sie eine ungefähre Angabe über die Dauer der Downtime haben, mit der das Unternehmen im Falle eines Datenverlustes oder Ausfalls zu rechnen hat, können Sie den Rechner verwenden, um die Kosten der Downtime pro Stunde zu ermitteln.

Die Kosten von Downtime werden zunächst durch die Gesamtkosten der Zeit aller Mitarbeiter bestimmt. Dazu gehören die Löhne der Mitarbeiter, Overhead-Kosten (Abonnement-Kosten, Sozialleistungen usw.) und Umsatzeinbußen durch Arbeitsausfall der Mitarbeiter (Verlust von Geschäftschancen). Dazu könnte auch eine eCommerce-Seite gehören, die offline keine Umsätze mehr generiert.

Beispiel:

- Betroffene Mitarbeiter: 10
- Durchschnittliches Gehalt: €20 / Std.
- Overhead-Kosten: €80 / Std.
- Umsatzeinbußen: €200 / Std.
- Gesamtkosten der Downtime: €480 / Std.

(MITARBEITER * GEHALT) + (OVERHEAD-KOSTEN + UMSATZEINBUSSEN) =
KOSTEN DER DOWNTIME (10 * €20 / Std.) + (€80 / Std. + €200 / Std.) = KOSTEN
DER DOWNTIME

(€200 / Std.) + (€280 / Std.) = KOSTEN DER DOWNTIME

KOSTEN DER DOWNTIME = €480 / Std.



Alle Backups sind gleich – das denken viele. Das stimmt auf eine Weise auch – alle Backup-Produkte erstellen eine Datenkopie. Aber nicht alle Backups sind gleich, wenn es um die Wiederherstellung von Daten und Anwendungen geht.



So fassen Sie das also zusammen: „Die Recovery Time Objective, kurz RTO, ist die Zeitspanne, die Sie benötigen, um den Betrieb nach einer Störung wieder zum Laufen zu bringen.“

Als nächstes erklären Sie Ihren Kunden, warum sie diese Kennzahl beachten sollten. „Sicher, Sie haben Backups. Was, wenn der Strom ausfällt? Haben Sie sich überlegt, wie lange es dauern würde, die Backups wiederherzustellen, falls der Strom ausfällt? Mit der Lösung, die Sie derzeit nutzen, kann das Tage dauern. Für einige Unternehmen ist das keine große Sache – sie können offline arbeiten. Wie viel Downtime kann sich Ihr Unternehmen leisten?“ Folgen Sie dieser Argumentation.

Alle Backups sind gleich – das denken viele. Das stimmt auf eine Weise auch – alle Backup-Produkte erstellen eine Datenkopie. Aber nicht alle Backups sind gleich, wenn es um die Wiederherstellung von Daten und Anwendungen geht.

„MSPs sollten mit ihren Kunden über die Zeitspanne reden, die sie benötigen, um das Unternehmen wieder fit zu bekommen“, sagt ein MSP. „Wir verkaufen Datto derzeit nur für den Schutz von Daten, aber wir haben eine Reihe älterer Kunden, die wir nicht von einem anderen Backup-Produkt auf Datto umstellen konnten. Einer von ihnen hatte kürzlich einen RAID-Fehler und es dauerte Tage, bis wir die Daten wiederhergestellt hatten und der Betrieb wieder aufgenommen werden konnte.“

Ein anderer MSP gibt einen ähnlichen Ratschlag: „Sie müssen dieses Gespräch führen. Fragen Sie sie: ‚Wenn Sie nicht arbeiten können, was kostet Sie das?‘ Erklären Sie ihnen, dass das System, das sie derzeit im Einsatz haben, sie nicht innerhalb eines tolerierbaren Zeitraums wieder online bringt. Viele Unternehmen wissen gar nicht, dass die Zeit für die Wiederherstellung zwischen den jeweiligen Lösungen stark variieren kann.“

Wenn Sie also mit potenziellen Kunden über BCDR sprechen, ist es sinnvoll, die Kosten von Downtime in Zahlen zu fassen. Ein wichtiger Ausgangspunkt für Ihre Argumentation ist dabei die Backup-Lösung, die der Kunde verwendet.

BCDR verkaufen – Das RPO-Argument

Szenario: Nehmen wir an, ein potenzieller oder aktueller Kunde verwendet Backup-Software XYZ, um täglich 500 GB Daten zu sichern. Aus Erfahrung wissen Sie, dass die Wiederherstellung von 500 GB Daten mit Produkt XYZ mindestens drei Stunden dauert, vorausgesetzt, Sie müssen keine neue Hardware installieren.

Fragen Sie zuerst: Wie viel Umsatz würden Sie verlieren, wenn Sie 3 Stunden lang offline wären? Wie viel in 24 Stunden?

Erklären Sie als nächstes: Sie müssen über das Recovery Point Objective, kurz RPO, Ihres Unternehmens nachdenken. Ihr RPO bezieht sich auf die Datenmenge, die Ihr Unternehmen zwischen den Backups verlieren könnte. Nehmen wir an, Sie haben 10 GB neue Daten an einem Tag erstellt und es kommt zu einem Rohrbruch, der einen Server um 16 Uhr überflutet. Wenn Ihr vorheriges Backup um 18 Uhr am Abend zuvor stattfand, sind 10 GB Daten für immer verloren. Deshalb ist es in modernen Unternehmen üblich, den ganzen Tag über regelmäßige Backups der Daten durchzuführen.

Fassen Sie zum Schluss alles noch einmal zusammen: Jetzt, wo Sie das alles wissen, ist es auch wichtig, dass Sie sich darüber im Klaren sind, dass es fast unmöglich ist, den ganzen Tag über regelmäßige Backups mit der XYZ-Backup-Software zu planen. Mit Ihrer aktuellen Lösung riskieren Sie den Verlust eines Arbeitstages (oder sogar mehr). Sie wissen sicher, dass dies garantiert zu Umsatzeinbußen führen wird.





Wenn ein Geschäftsinhaber die konkret bezifferten Einbußen realisieren kann, ist es viel einfacher, den Wert einer BCDR-Lösung zu erklären. Mit anderen Worten: Auf Umsatzeinbußen reagieren Entscheider eher als auf potenzielle Datenverluste.

Wenn ein Geschäftsinhaber die konkret bezifferten Einbußen realisieren kann, ist es viel einfacher, den Wert einer BCDR-Lösung zu erklären. Mit anderen Worten: Auf Umsatzeinbußen reagieren Entscheider eher als auf potenzielle Datenverluste.

BCDR verkaufen – Der Image-Faktor

Vor allem bei KMU ist die Wahrscheinlichkeit höher, dass Entscheider sich nicht bewusst sind, dass nicht alle Backup-Lösungen dieselbe Wiederherstellungszeit garantieren. Je nachdem, welche Produkte zum Einsatz kommen, kann die Wiederherstellung wichtiger Systeme sehr zeitaufwendig sein, und die finanziellen Folgen von Downtime können über den reinen Umsatzverlust weit hinausgehen. Downtime gefährdet die Reputation von Unternehmen.

Eine Möglichkeit, potenziellen Kunden die Folgen von Downtime vor Augen zu führen, ist, mit ihnen durchzuspielen, was passiert, wenn sie ihre Kunden plötzlich – zum Beispiel einen ganzen Tag lang – nicht bedienen können. Passen Sie dieses Szenario an die Branche an. So wird beispielsweise ein Tag mit IT-Downtime den Ruf eines Restaurants nicht in gleicher Weise beeinträchtigen wie den einer Anwaltskanzlei. Suchen Sie nach Beispielen in Ihrem eigenen Kundenstamm. Wenn Sie einen Kunden haben, der den IT-Dienstleister gewechselt hat, weil er die IT-Prozesse nicht schnell wiederherstellen konnte, bauen Sie eben diese Erfahrung in Ihren Pitch ein.

Sicherheitslücken können den Ruf eines Unternehmens nachhaltig schädigen, vor allem in Branchen, in denen Kundendaten besonders vertraulich behandelt werden müssen. Eine BCDR-Lösung ist kein Security-Tool, aber wichtig, um ein Unternehmen nach einem Ausfall schnell wieder zum Laufen zu bringen. „Es geht

Es gibt zwei Möglichkeiten, Sales-Expertise aufzubauen – stellen Sie jemanden mit Erfahrung im Verkauf ein oder wählen Sie einen Ihrer Mitarbeiter aus.

Dies könnte Sie auch interessieren:

datto
**MSPeasy – Vertrieb
leicht gemacht**

Jetzt herunterladen



nicht nur um Downtime, sondern auch um die Marke", sagt ein MSP. „Entscheidend ist, dass das System wieder in den Ursprungszustand gebracht werden kann, in dem es vor dem Angriff war.“

Bauen Sie Ihre Sales-Expertise auf

Sie haben jetzt alle Informationen, die Sie benötigen, um potenzielle Kunden über den Mehrwert von BCDR zu informieren. Das ist ein guter Anfang, aber die Technologie verkauft sich nicht von selbst. Sie sollten also Zeit und Ressourcen in den Vertrieb investieren.

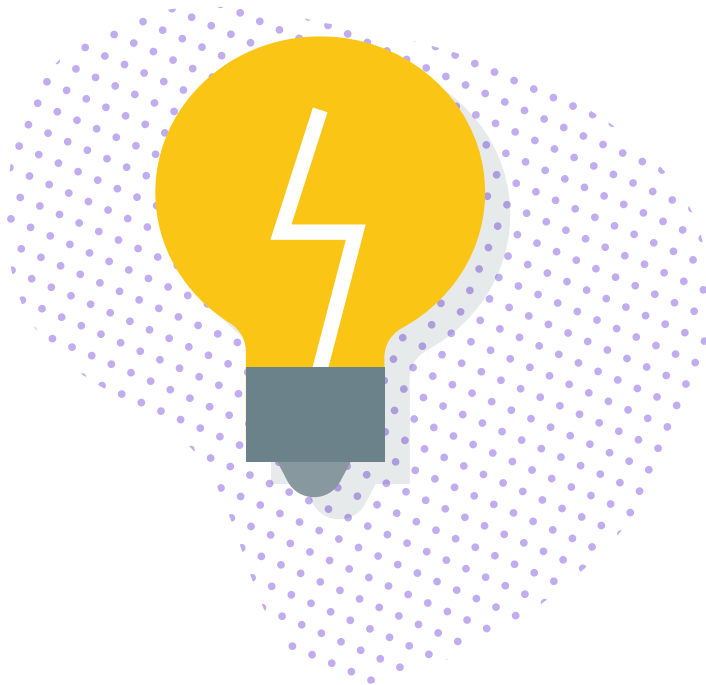
Wie bereits zu Beginn dieses eBooks erwähnt, gibt es zwei Möglichkeiten, Sales-Expertise aufzubauen – stellen Sie jemanden mit Erfahrung im Verkauf ein oder wählen Sie einen Ihrer Mitarbeiter aus. Wenn Sie wachsen möchten, macht die Einstellung von qualifizierten Vertrieblern einen großen Unterschied. Doch nicht jedes Unternehmen hat ein Budget, um sich auf Vertrieb und Business Development zu fokussieren. Sie haben bereits mit Ihrem Tagesgeschäft genug zu tun – Monitoring, Optimierung oder Reparatur der IT-Infrastrukturen der Kunden.

Wie findet man dennoch Zeit, sich Sales und Marketing zu widmen, auch wenn es zusätzlich zum Tagesgeschäft geschehen muss? Angenommen, Sie sind Geschäftsführer eines MSPs mit fünf Vollzeitbeschäftigten (einschließlich Ihnen selbst). Dann spricht doch nichts dagegen, Ihren erfahrensten Mitarbeiter für die Übernahme eines Teils Ihrer technischen Aufgaben auszubilden? Wenn Sie nicht gerade Sales-orientiert sind, ist einer Ihrer Mitarbeiter vielleicht der ideale Kandidat.

Der zweite Schritt ist es, Kunden zu finden, die zu Ihrem Unternehmen passen.



Hören Sie auf, jeder Chance hinterherzulaufen. Suchen Sie sich die richtigen Kunden aus. Man sollte wissen, wann man nein sagt.



Erfolgreiche MSPs betonen genau das – nicht jeder Kunde ist ein guter Kunde. Für Start-ups ist es natürlich schwieriger, sich an diese Maxime zu halten. Wenn Sie nicht viele Kunden haben, ist es schwierig, jemanden abzulehnen. Aber nach der Erfahrung erfolgreicher MSPs sollten Sie genau das tun.

Ein MSP empfiehlt, Informationen zu sammeln: „Was ist das für ein Unternehmen? Gelten für sie Compliance-Regelungen? Recherchieren Sie und stellen Sie fest, ob sie einer bestimmten Regulierung unterliegen und lassen Sie das in Ihren Pitch einfließen.“

Vor allem kleinere Unternehmen tendieren dazu, sich vor allem auf die Anschaffungskosten für Technologie zu konzentrieren. Sie übersehen dabei einen wesentlichen Aspekt: Die Kosten für Downtime sind für ihr Unternehmen unter Umständen viel höher. Ein Datto Partner berichtet, dass er nicht versucht, die Kunden, die dieses Prinzip nicht verstehen, mit allen Mitteln zu überzeugen. „Die meisten meiner Kunden verstehen es aber“, sagt er. „Und wenn nicht, dann gibt es wahrscheinlich zehn weitere Gründe, warum sie nicht gut zu uns passen. Bei manchen Kunden ist das eben so.“

Ein anderer MSP stimmt zu: „Bei uns bieten wir nur Datto an. Ich habe früher ein IT-Unternehmen geführt, das eine Reihe von verschiedenen Backup-Produkten verkauft hat, und es war schwer, Kunden von BCDR zu überzeugen“, sagt er. „Heute verkaufen wir nur noch an Kunden, die eigene IT-Mitarbeiter haben. Sie sind sich des Mehrwerts von BCDR meistens bewusst, was Verkauf und Zusammenarbeit einfacher macht.“

„Hören Sie auf, jeder Chance hinterherzulaufen. Suchen Sie sich die richtigen Kunden aus“, sagt ein MSP. „Man sollte wissen, wann man nein sagt.“

Fazit

Höhere Kosten von BCDR-Lösungen vor preissensiblen, kleinen Unternehmen zu rechtfertigen, ist definitiv eine Hürde. Wenn Sie sich jedoch darauf konzentrieren, die richtigen Unternehmen zu finden und die richtige Botschaft zu vermitteln, lässt sie sich leicht überwinden.

Informationen sind dabei der entscheidende Faktor für ein erfolgreiches Verkaufsgespräch. Auf der nächsten Seite finden Sie ein Handout, das die Vorteile von BCDR gegenüber anderen Lösungen für die Datensicherheit erläutert. Mit diesen überzeugenden und auch für technische Laien nachvollziehbaren Argumenten können Sie Unternehmen von BCDR überzeugen.

BCDR an potenzielle Kunden verkaufen

Warum Sie eine BCDR-Lösung benötigen

Ein guter Business Continuity und Disaster Recovery-Plan ist für Unternehmen jeder Branche unverzichtbar. Allerdings wird der Schutz von Daten nur selten so ernst genommen, wie er sollte – auch wenn das schwerwiegende Folgen haben kann. Das sind die Gründe, weshalb Sie sich unbedingt für BCDR interessieren sollten:

Downtime ist teuer

Wenn Ihre Mitarbeiter oder Kunden keinen Zugriff auf wichtige Anwendungen und Daten haben, hat dies direkte Auswirkungen auf Produktivität und Umsatz. Das klingt zwar offensichtlich, aber viele Unternehmen unterschätzen die wahren Kosten von IT-Ausfällen. Um das Problem der Downtime besser zu verstehen, erläutere ich Ihnen folgendes Beispiel: Angenommen, Ihr Unternehmen hat 100 Mitarbeiter, der durchschnittliche Stundenumsatz beträgt 1.500 Euro und der Backup-Datensatz 2 TB. Bei diesen Parametern würde eine vollständige Wiederherstellung aus einem lokalen Backup mit herkömmlicher Backup-Software über 8 Stunden dauern. Die daraus entstehenden Kosten für Downtime würden sich auf über 30.000 Euro an verlorenem Umsatz belaufen. Einige moderne Produkte für den Schutz von Daten bieten die Möglichkeit, Anwendungen über das Backup-Gerät oder in der Cloud auszuführen. Auf diese Weise können Benutzer den Betrieb fortsetzen, während die primären Anwendungsserver wiederhergestellt werden. Die Wahl einer BCDR-Lösung zur Reduzierung von Downtime ist daher wirtschaftlich sinnvoll.

Backup allein ist nicht genug

So gut wie jedes Unternehmen führt heute Datensicherungen durch. Aber was passiert, wenn ein Wasserschaden Ihre Haupt- und Backup-Server beschädigt? Eine Kopie der Daten off-site zur Wiederherstellung im Katastrophenfall zu speichern, sollte ebenfalls als unerlässlich angesehen werden. Früher bedeutete dies, dass Bänder an einen anderen Ort oder einen Bandspeicherplatz geschickt wurden. Wie bereits erwähnt, können moderne BCDR-Produkte Anwendungen aus Backup-Instanzen von virtuellen Servern ausführen, und einige können diese Fähigkeit

auf die Cloud ausdehnen. Dieser Ansatz wird häufig als Cloud DR oder Disaster Recovery as a Service (DRaaS) bezeichnet. Die Möglichkeit, Anwendungen in der Cloud auszuführen, während die Infrastruktur vor Ort wiederhergestellt wird, gilt weithin als ein entscheidender Faktor für Disaster Recovery.

„Kleinere“ Vorfälle

Nicht jeder Vorfall ist gleich eine Katastrophe. Tatsächlich sind die meisten IT-Ausfälle auf versehentliche (oder absichtliche) Datenlöschung, Schäden an der Computer-Hardware und schlechte Sicherheitsstandards zurückzuführen. So ergab beispielsweise eine aktuelle CompTIA-Studie, dass sich 94 % der Befragten trotz Sicherheitsrisiken routinemäßig im öffentlichen WLAN anmelden. Und 69 % greifen über das öffentliche WLAN auf arbeitsbezogene Daten zu. Ein Kryptolocker-Angriff oder ein Virus kann den Betrieb genauso einfach stoppen wie ein Rohrbruch oder ein Stromausfall. Diese „kleineren“ Vorfälle passieren regelmäßig und die damit verbundene Downtime läppert sich mit der Zeit. Eine Technologie, die es Ihrem Unternehmen ermöglicht, nach diesen kleinen „Katastrophen“ den Betrieb fortzusetzen, ist genauso wichtig, wenn nicht sogar wichtiger als der Schutz vor einem Totalausfall, der hoffentlich nicht eintritt.

Business Continuity geht jeden etwas an

Daten sind für alle Unternehmen unerlässlich, sodass der Zugriff auf Anwendungen und Daten nach einem Disaster unerlässlich ist. Aber das ist nur ein Teil des Puzzles. Bevor Business Continuity-Maßnahmen ergriffen werden, muss analysiert werden, wie der Status Quo ist, was die Fähigkeit des Unternehmens angeht, Daten wiederherzustellen. Eine solide Business Continuity-Planung erfasst das Unternehmen als Ganzes und macht es robuster gegen IT-Ausfälle. Tatsächlich beginnen viele Business Continuity-Planungen mit einer Business Impact-Analyse oder Risikobewertung – das kann die Schwächen Ihres Unternehmens aufdecken, Geschäftsprozesse aufrecht zu erhalten, die weit über die IT hinausgehen.