N-ABLE™

Kompendium: So verkaufen Sie Datensicherheit

Was die erfolgreichsten MSPs anders machen – und wie Sie das auch können

E-Book

Inhaltsverzeichnis

Im datenzentrierten Geschäft ist Sicherheit das A und O

Ob Großkonzern oder Freelancer im Homeoffice: Ohne Daten geht in Unternehmen nichts. Aus diesem Grund haben sich Backup- und Wiederherstellungslösungen zum Schutz vor Datenverlust als unverzichtbare Mittel etabliert.

Unternehmen, die groß genug sind, um eigene IT-Abteilungen zu unterhalten, sind dabei in der Regel recht gut aufgestellt. Ganz anders kleine und mittlere Unternehmen (KMU): Hier klaffen nicht selten große Sicherheitslücken.

Viele KMU behelfen sich in der Tat mit einem Potpourri an unzuverlässigen, zusammengewürfelten Backup-Systemen. Da in diesen Unternehmen oft extrem aufs Geld geachtet wird, ist es nicht immer einfach, sie davon zu überzeugen, zu einer neuen Lösung zu wechseln. Sie sind sich zwar der Problematik bewusst, möchten aber oft nicht wahrhaben, wie groß die Gefahr für sie persönlich ist oder was ihnen im Falle eines Datenverlusts droht.

Wie gehen erfolgreiche MSPs dieses Thema an, um auch in diesem Marktsegment Kapital aus dem Backup-Geschäft zu schlagen? Ganz bestimmt nicht durch den Verkauf einer weiteren reinen Backup-Lösung. Hier ist mehr gefragt – sprich: **umfassende Datensicherheit als Komplettpaket**.

WAS IST DER UNTERSCHIED ZWISCHEN BACKUP UND DATENSICHERHEIT?

Datensicherheit bietet etliche Funktionen, die weit mehr leisten als die bloße Ausführung von Backups. Folgendes sollen MSPs nach Ansicht der Unternehmen im Einzelnen abdecken:

- Daten vor Verlust durch Benutzerfehler, Hackerangriffe oder Systemausfälle schützen
- Komplexe Anforderungen zu Datensicherheit, Datenschutz und Data Governance berücksichtigen
- Jederzeit sicherstellen, dass Daten verfügbar und im Ernstfall sofort und ohne Systemausfall wiederherstellbar sind

Da Datensicherheit mit so vielen verschiedenen Serviceelementen einhergehen kann, lohnt es sich, ihr besondere Aufmerksamkeit zu widmen, wenn Sie wiederkehrende Umsätze generieren möchten:

Reaktiv	À la carte (Einzelprodukte)	Proaktiv	Managed
Unterstützt die bereits im Gebrauch befindliche Backup-Software des Kunden.	Verkauf von Software oder einfachen Services als monatlicher Posten für fortlaufendes Backup- und Reporting-Management.	Wird als Teil eines Pakets (nutzer-/gerätebasiert) verkauft; bietet fortlaufende Backup-, Reporting- und Wiederherstellungs-tests sowie Wieder-herstellungen im Bedarfsfall.	Wird als Teil eines gebündelten Pakets (nutzer-/gerätebasiert) verkauft; bietet fortlaufende Backup-, Reporting- und Wiederherstellungs-tests sowie Wieder-herstellungen gemäß definierter SLA-Stufen.
€	€€	€€€	€€€€

Je „gemanagter“ der Ansatz ist, desto mehr wachsen Ihre Chancen, daraus Kapital zu schlagen. Und desto mehr Wert liefern Sie Ihren Kunden.

IHRE AUFGABE IST KLAR

Viele Eigentümer haben ihr kleines Unternehmen über 10, 20 oder 30 Jahre mühsam aufgebaut. Jetzt verlassen sie sich darauf, dass Sie sie davor bewahren, ihre Existenzgrundlage und Vermögenswerte zu verlieren.

Das ist einer der Gründe, warum Sie ihnen mehr als nur Backup-Software in der Basisversion anbieten sollten.

WIE VERKAUFE ICH MEHR DATENSICHERHEIT?

Trotz der Herausforderungen im KMU-Segment muss Ihr Datensicherheitsgeschäft keine komplizierte Sache sein. Sie brauchen nur den richtigen Ansatz – und natürlich die richtige Lösung.

Sie können den richtigen Ansatz auf drei einfache Schritte herunterbrechen:

1. **Erfassen** Sie die Denkweise und Anforderungen Ihres Kunden
2. **Verdeutlichen** Sie dem Kunden den wahren Wert seiner Daten
3. **Individualisieren** Sie die Lösung für den Bedarf und das Budget des Kunden

Im Folgenden sind die einzelnen Schritte detaillierter aufgeführt.

Wussten Sie schon?

Knapp die Hälfte aller Datenschutzverstöße (43 %) betreffen kleine Unternehmen.[1]

[1] „2019 Data Breach Investigations Report“, Verizon. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf (aufgerufen im Juli 2019)

Erfassen Sie die Denkweise und Anforderungen des Kunden

WIE KANN ICH ERMITTELN, OB EIN KUNDE DATENSICHERHEIT BRAUCHT?

Viele MSPs neigen dazu, dem Kunden beim kleinsten Anzeichen von Interesse sofort eine Lösung zu präsentieren. Sie sollten jedoch lieber einen Gang zurückschalten.

Halten Sie inne und stellen Sie Fragen, um herauszufinden, was der Kunde wirklich will. Wenn Sie ihm die optimale Lösung anbieten möchten, müssen Sie seine Ziele und Erwartungen ermitteln, um festzustellen, was den Kern seines Geschäfts ausmacht.

Im Vertriebsjargon nennt man das die **Identifizierungsphase**.

Sie müssen dabei nicht nur die betrieblichen Anforderungen ermitteln, sondern auch herausfinden, wo sich die Daten befinden. In vielen KMU werden Daten auf Laptops, Telefonen und anderen Endgeräten gespeichert. Mit anderen Worten: Nicht nur die Server brauchen Backups.

Die Auswirkungen, die ein massiver Datenverlust auf das Geschäft hätte, müssen ebenso klar sein wie der Zeitaufwand für die Wiederherstellung dieser Daten. Außerdem müssen Sie die geltenden gesetzlichen Vorgaben rund um die Datensicherheit beachten, beispielsweise die DSGVO, und die Konsequenzen herausstellen, sollte es Nichtübereinstimmungen geben.

Wenn Sie das alles wissen, können Sie klar formulieren, wo genau Datensicherheit erforderlich ist. Außerdem können Sie das vorhandene Backup- und Wiederherstellungssystem besser einschätzen und mögliche optimierungsfähige Bereiche benennen.

Sie sind der Experte

Ihre Kunden engagieren Sie wegen Ihrer Fachkenntnisse und sehen in Ihnen einen IT-Berater, dem sie vertrauen können. Letztlich dürfte es ihnen relativ egal sein, welche Datensicherheitslösung Sie nutzen, Hauptsache sie funktioniert.

Wenn Sie diese Identifizierungsphase sauber durchlaufen, können Sie souverän eine Lösung anbieten, die den Anforderungen Ihrer Kunden entspricht und langfristig ihr Vertrauen sichert.

FRAGEN IN DER IDENTIFIZIERUNGSPHASE

So steigen Sie ein:

- Was unternehmen Sie derzeit für den Schutz Ihres Unternehmens?
- Gab es in Ihrem Unternehmen schon einmal Ausfallzeiten? Welche Auswirkungen hatten diese?
- Beschäftigen Sie die möglichen Auswirkungen von Ausfällen auf Ihr Geschäft?
- Haben Sie einen dezidierten Plan für den Fall, dass Ihre Systeme oder Daten nicht verfügbar sind?

- Inwiefern hat sich Ihre Abhängigkeit von Computersystemen in den letzten fünf Jahren verändert?
- Könnte der Geschäftsbetrieb aufrechterhalten werden, wenn Sie vorübergehend wieder mit Stift und Papier arbeiten müssten? Wie lange ginge das?
- Bereitet Ihnen Ihre aktuelle Situation schlaflose Nächte?
- Welche Ziele haben Sie für die kommenden zwei Jahre? Wie planen Sie die Modernisierung und das Wachstum Ihres Unternehmens?

Haken Sie nach:

- Wie viele Transaktionen pro Stunde verarbeitet Ihr Unternehmen normalerweise? Welche Kosten kämen bei Ausfällen pro Stunde auf Sie zu?
- Drohen rechtliche Konsequenzen, wenn Services plötzlich nicht mehr verfügbar sind?
- Wie lange ist Ihr Geschäftsbetrieb ohne Datenzugriff möglich?
- Welche Auswirkungen auf Ihren Ruf hätte ein eintägiger Ausfall Ihres Kundenservice? Was, wenn er eine ganze Woche dauern würde?
- Welche Geschäftsprozesse und Anwendungen sind am wichtigsten und müssen deshalb als Erste wiederhergestellt werden?
- Welche zugrundeliegenden Systeme und Datenarten bräuchten Sie, um den Betrieb zentraler Anwendungen wiederherzustellen? Auf welchen Servern oder Geräten befinden sich diese Systeme und Daten?

Stellen Sie abschließend Fragen zu den anderen Geschäftsanwendungen und Datenarten:

- Welche dieser anderen Anwendungen und Datenarten könnten ohne größere Auswirkungen auf den Geschäftsbetrieb auch gut für einen längeren Zeitraum offline oder gar nicht verfügbar sein?
- Was würde es umgerechnet auf Mitarbeiterzeit und -gehälter kosten, diese weniger wichtigen Daten wiederherzustellen, angenommen, sie wären vollständig verloren?

Drücken Sie sich verständlich aus

Sofern Ihr Kunde nicht extrem technisch ausgerichtet ist, brauchen Sie Fachwörter wie **RTO** (Recovery Time Objective) oder **RPO** (Recovery Point Objective) gar nicht zu erwähnen. Achten Sie jedoch darauf, dass Ihre Fragen auf diese Kennwerte abzielen.

Aufklärung des Kunden über den wahren Wert seiner Daten

WIE ÜBERZEUGE ICH EINEN KUNDEN VON DER NOTWENDIGKEIT FÜR DATENSICHERHEIT?

Versuchen Sie nicht, künftigen Kunden direkt bestimmte Produkte oder Lösungen zu verkaufen. Um sie davon zu überzeugen, dass sie Datensicherheit brauchen, sollten Sie ihnen zunächst den Wert ihrer Daten auf den Servern und Geräten verdeutlichen – und welchen Schaden der Verlust dieser Daten im Unternehmen anrichten kann.

Das Argument besteht im Grunde aus zwei Teilen:

Datenverlust kommt vor

Unternehmen können Präsentationen, Finanzberichte und andere wichtige Dateien auf alle erdenklichen Arten verlieren. Beschädigte Dateien, Hardwareausfälle, Malwareangriffe, versehentliches Löschen oder Naturkatastrophen: Kein Unternehmen ist davor gefeit. Auch wenn Ihre Kunden die Vorstellung, sie könnten unbeabsichtigt etwas Wichtiges entfernen, von sich weisen – versehentliches Löschen ist in der Tat eine der häufigsten Ursachen für Datenverlust. Und sie haben sicher schon von Unternehmen gehört, die Ransomware zum Opfer fielen. Sie müssen ihnen klarmachen, dass das auch ihnen selbst zustoßen kann.

Die Produktivität leidet

Der Verlust einer wichtigen Datei bedeutet, dass sie wiederhergestellt werden muss. Das kostet Zeit, die für andere wichtige Aufgaben genutzt werden könnte. Jedes Unternehmen verfügt über wichtige Daten, die nur schwer oder manchmal gar nicht wiederherstellbar sind. Über Monate oder Jahre zusammengetragene Finanzdaten sind unmöglich zu ersetzen. Und doch speichern viele Unternehmen ihre Buchhaltungsdaten und ähnlich Wichtiges auf einem einzigen Rechner ohne Sicherungskopie.

Wussten Sie schon?

Die Folgen nach massivem Datenverlust:[2]

- 19 % der KMU hatten weniger als eine Stunde Systemausfall
- 41 % hatten eine bis acht Stunden Systemausfall
- 40 % hatten über acht Stunden Systemausfall

[2] „Cisco Cybersecurity Special Report – Small and Mighty: How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats", Cisco. https://www.cisco.com/c/dam/global/hr_hr/solutions/small-business/pdf/small-mighty-threat.pdf (aufgerufen im Juli 2019)

ZEIGEN SIE DIE TATSÄCHLICHEN KOSTEN FÜR AUSFALLZEITEN AUF

Wenn Sie Datensicherheit verkaufen möchten, sprechen Sie dabei am besten über Geld – bei diesem Stichwort wird jeder Geschäftsführer hellhörig.

Zwei Dinge, die die Anschaffung von Datensicherheit rechtfertigen, sind Datenverluste, die zu massiven finanziellen Ausfällen führen, sowie Daten, deren Wiederherstellung oder Ersetzung Stunden oder gar Tage in Anspruch nähmen (was Zeit und Arbeitskraft der Mitarbeiter bindet).

Zur Konkretisierung bitten Sie Ihren Kunden, sich ein Szenario auszumalen, in dem die Systeme vollständig ausgefallen sind und es keinen Zugriff auf jedwede Dateien gibt. Und dann soll er ausrechnen, was das kosten würde. Im Vergleich dazu klingt Datensicherheit wie ein Schnäppchen.

Sie können das folgende Beispiel für Ihre Argumentation nutzen:

Konstruktionsfirma mit 25 Beschäftigten

100.000 € Umsatz pro Mitarbeiter und Jahr

25 Mitarbeiter x 100.000 € pro Jahr = 2,5 Mio. € Gesamtumsatz pro Jahr

250 Arbeitstage pro Jahr = 400 € Umsatz pro Tag

400 € x 25 Mitarbeiter = 10.000 € Umsatz pro Tag

AUSWIRKUNGEN INSGESAMT:

Produktivitätsverlust: 10.000 € pro Tag

Abhilfe: 800 € pro Tag

Rufrettung: unkalkulierbar

- Was, wenn ein Projekt nicht geliefert wird?
- Was, wenn ein Kunde abspringt?
- Wie hoch ist der Imageschaden?

Weitere Risikoarten

Neben finanziellen Risiken (Produktivitätsverluste, Wiederherstellungskosten und Rufschädigung) gibt es weitere Belange von Kleinunternehmen, derer sie sich annehmen sollten.

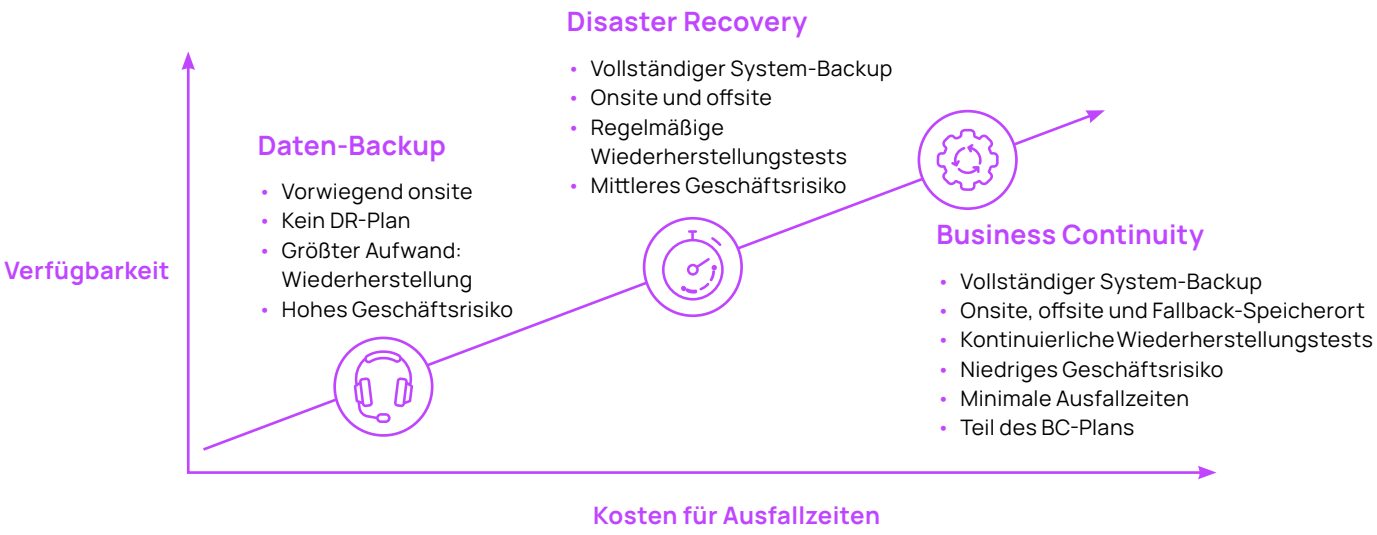
Muss Ihr Kunde zum Beispiel strikte Vorschriften in Bezug auf Schutz, Sicherung und Archivierung der Daten einhalten? Welche Konsequenzen drohen bei Verlust oder Diebstahl persönlicher, finanzieller oder medizinischer Daten?

Abstimmung der Lösung auf Bedarf und Budget des Kunden

GIBT ES EINE PAUSCHALE LÖSUNG?

Kurz gesagt: nein. Ihre Kunden brauchen nicht alle dasselbe Maß an Sicherheit (oder können es sich leisten). Deshalb ist es enorm wichtig, dass Sie Ihre Services auf die Erwartungen und Anforderungen Ihrer Kunden in Bezug auf Ausfälle und Verfügbarkeit ausrichten.

Nutzen Sie dazu das folgende Schaubild mit Reifegraden:



Wo würden Sie sich zurzeit in Bezug auf Backup-, Wiederherstellungs- oder Datensicherheitslösungen einordnen, die Sie Ihren Kunden anbieten? Können Sie die Anforderungen in allen genannten Bereichen effektiv erfüllen? Wenn Sie diese Frage bejahen können, dürften Sie höhere Margen und mehr Profit realisieren.

Tipp für die Praxis

Haben Sie einmal einen erfolgreichen Ansatz für den Vertrieb von Datensicherheit an einen Vertreter einer bestimmten Branche (beispielsweise eine Kanzlei oder einen Einzelhändler) erarbeitet, können Sie bei weiteren Kunden derselben Branche ähnlich verfahren.

WIE WERDE ICH DEN ANFORDERUNGEN ALL MEINER KUNDEN GERECHT?

Natürlich wäre es für Ihre Techniker deutlich bequemer, wenn Sie all Ihren Kunden dieselbe Lösung anböten. Die Customer Experience fiele dabei jedoch ziemlich mau aus. Andererseits: Würden Sie für jeden Kunden eigens eine Lösung erstellen, würde sich das Management für Sie ziemlich schwierig gestalten.

Wenn Sie **zwei oder drei Standardpakete** anbieten, können Sie die Anforderungen an die Wiederherstellung unter Beachtung der budgetären Rahmenbedingungen bei einem Großteil Ihrer Kunden effektiv abdecken.

Mit konsistenten Datensicherheitspaketen und Preisen auf verschiedenen Servicestufen (z. B. ein preiswertes Basismodell, ein mittelpreisiges Konzept und ein umfassendes Prämiumpaket) decken Sie für viele verschiedene Kunden und Datenarten genau das richtige Maß an Sicherheit ab. Es könnte folgendermaßen aussehen:

BRONZE Daten-Backup 75 € pro Server	SILBER Disaster Recovery 100 € pro Server	GOLD Business Continuity 150 € pro Server
• Vollständiger System-Backup	• Vollständiger System-Backup	• Vollständiger System-Backup
• Ein Backup pro Tag	• Zwei Backups pro Tag	• 12 Backups pro Tag
• 28 Tage Aufbewahrung	• 60 Tage Aufbewahrung	• 90 Tage Aufbewahrung
• Speicherung offsite	• Speicherung offsite	• Speicherung offsite
	• Hybrid-Backups zur schnelleren Wiederherstellung	• Hybrid-Backups zur schnelleren Wiederherstellung
	• Monatliche Archivierung	• Monatliche Archivierung
	• Vierteljährliche Wiederherstellungstests	• Monatliche Wiederherstellungstests
		• Standby-VM mit täglichem Screenshot
Für unkritische Daten beziehungsweise eher knappe Budgets eignet sich die Basisstufe. Sie sorgt für die Wiederherstellung innerhalb von 24 Stunden an variablen Wiederherstellungszielen.	Für weniger kritische Daten bietet sich Wiederherstellung aus der Cloud mit einem Wiederherstellungszeitfenster von vier bis 12 Stunden an.	Von einem Warm-Standby-Server lassen sich die wichtigsten Anwendungen und Daten der Kunden umgehend wiederherstellen.

Mit einem solchen Dreistufenmodell können sich Ihre Kunden auch für unterschiedlichen Schutz für unterschiedliche Daten entscheiden.

WORAUF MUSS ICH BEI DATENSICHERHEITSLÖSUNGEN ACHTEN?

Ihr Erfolg hängt letztlich von der richtigen Datensicherheitslösung ab – eine, die dem benötigten Funktionsumfang kleiner und mittlerer Unternehmen entspricht und nicht den Kostenrahmen sprengt.

Das optimale Datensicherheitstool sollte flexibel sein und sich so weit konfigurieren lassen, dass es für verschiedene Servicestufen und Pakete geeignet ist. Weitere Anforderungen:

Einfache Implementierung und Nutzung

Das Management Ihrer Kunden sollte für Sie so effizient wie möglich sein. Achten Sie auf ein webbasiertes Multi-Tenant-Dashboard, mit dem Ihre Techniker alle Kundendatenarten in verschiedenen Umgebungen auf nur einem Bildschirm einsehen können. So können sie den Backup-Status aller verwalteten Server und Geräte kontrollieren und einfach per Klick zu Detailansichten bei möglichen Problemen gelangen.

Vielseitigkeit

Ihre Angebotslösung sollte Daten an beliebigen Speicherorten sichern und wiederherstellen können, also auf physischen wie virtuellen Servern und Workstations sowie – als Teil von SaaS-Anwendungen wie Microsoft 365™ – in der Cloud. Die Lösung muss in der Lage sein, Daten über die verschiedensten Betriebssysteme und Hypervisoren zu sichern. Außerdem muss sie sämtliche Wiederherstellungsformen ausführen können, einschließlich Wiederherstellung auf Datei-/Ordnerebene, Bare-Metal-Restore und virtuelle bzw. kontinuierliche Wiederherstellung.

Cloud First

Der Vorteil von Onsite-Backups ist die schnellere Wiederherstellung, doch ist die lokale Speicherung für dieselben Schwachstellen anfällig wie die übrigen On-Premise-Systeme Ihres Kunden. Remote-Speicherung offsite und in der Cloud bietet hier deutlich höheren Schutz vor größeren Katastrophen. Die ideale Lösung bietet beide Optionen. Sie ist weder rein cloudbasiert, noch verlässt sie sich ausschließlich auf lokale Sicherung. Wir nennen diesen Ansatz „Cloud First“.

Wenn Sie über eine Lösung verfügen, die all diese Funktionen erfüllt, können Sie einfacher alle Servicestufen bedienen, die den diversen Anforderungen Ihrer KMU-Kunden entsprechen. Durch die höhere Effizienz und Automatisierung senken Sie damit zudem Ihre eigenen Serviceleistungskosten.

Machen Sie Ihre Techniker produktiver

Mit mehreren Backup-Tools arbeiten zu müssen, kostet wertvolle Zeit. Weniger Backup-Produkte und Dashboards einzusetzen, bedeutet also echten Produktivitätsgewinn. Techniker gewinnen so mehr Zeit für wertschöpfende, interessantere Aufgaben.

Tipps und Tricks für den Verkaufsabschluss

WANN SPRECHE ICH DATENSICHERHEIT AM BESTEN AN?

Im Katastrophenfall wenden sich Ihre Kunden zwangsläufig an Sie und erwarten, dass Sie sie retten. Dann ist es jedoch zu spät, sich über Datensicherheit zu unterhalten. Wenn sie noch keine adäquate Lösung haben, sind Ihre Hilfemöglichkeiten ziemlich begrenzt.

Wie lässt sich diese Situation am besten verhindern? **Schieben Sie nichts auf die lange Bank.** Sprechen Sie bei Ihrem nächsten Kundenbesuch das Thema Datensicherheit an – nach Möglichkeit in einem persönlichen Gespräch. Das ist besser als am Telefon oder per E-Mail. Übernehmen Sie das Ruder und steuern Sie das Gespräch so, dass Ihr Kunde am Ende ein Maß an Datensicherheit hat, das seinen Geschäftsanforderungen entspricht.

Upselling an Kunden mit bestehender Basislösung

Wenn Ihr Kunde kürzlich Daten verloren hat und Probleme bei der Wiederherstellung mit dem vorhandenen Backup-System hatte, haben Sie den perfekten Gesprächseinstieg. Erklären Sie, wie eine stabilere Datensicherheitslösung diesen Stress vermieden hätte.

Setzen Sie sich regelmäßig mit dem Kunden zusammen, um den Status seiner IT-Umgebung zu checken? Erstellen Sie regelmäßig Berichte zu seinen Backups – und können Sie benennen, wo das derzeitige System in puncto Speicher oder Wiederherstellung versagt? Hat der Kunde seit Ihrer letzten Überprüfung neue Services oder Plattformen eingerichtet oder wichtige Geschäftsanwendungen in die Cloud verlagert?

All diese Punkte sind Upselling-Möglichkeiten für eine stabilere, funktionsreichere Datensicherheitslösung.

Beim Upselling präsentieren Sie am besten zunächst das Mittelfeld. Wenn den Kunden der Preis schreckt, können Sie immer noch zurückrudern und stattdessen die preiswerteste Option anbieten. Wünscht er jedoch noch mehr Sicherheit, umso besser für ihn – und für Sie.

Nehmen Sie auf aktuelle Schlagzeilen Bezug

Beziehen Sie sich bei Ihren Kundengesprächen auf aktuelle Nachrichten über Datenschutzverstöße, Ransomware und andere Cyberangriffe.

Erzählen Sie ruhig, was aus dem Unternehmen um die Ecke wurde, das sämtliche Daten verlor – und wie Sie alles in Ihrer Macht Stehende tun wollen, damit Ihren Kunden nicht dasselbe widerfährt.

WIE GEHE ICH MIT EINWÄNDEN UM?

Der eine oder andere kostenbewusste Kunde mag die Investition vielleicht scheuen. Doch oft vergleicht er dabei Äpfel mit Birnen: Vielleicht hat er sich online umgesehen und ist auf eine wirklich günstige Backup-Lösung gestoßen. Und will nun nicht begreifen, warum Ihr Rundum-Angebot nicht zum selben Preis zu haben sein sollte.

Ihre Aufgabe besteht jetzt darin, ihm den Unterschied zwischen Äpfeln und Birnen zu erklären – und was die Datensicherheit, die Sie anbieten, alles mehr als bloße Backup-Software kann.

Machen Sie Ihrem Kunden klar, dass er neben Software und Speicher auch Datensicherheit mit Rundum-Service bekommt – einschließlich Backup-Monitoring und -Tests, Business Continuity und Datenwiederherstellung auf Zuruf, falls doch einmal etwas schiefgehen sollte.

Sie können Ihre Lösung auch als eine Art Versicherungspolice präsentieren: Gegen eine monatliche Gebühr erhält der Kunde eine Absicherung im Schadenfall. Sie können anbringen, dass er schließlich auch kein Ladengeschäft ohne Versicherung eröffnen würde und dies folglich auch für seine Daten gelten sollte.

Der Preis als Argument sticht nicht

Selbst wenn jemand den Preis anführt, werden Sie durch Nachfragen fast immer feststellen, dass es in Wahrheit gar nicht darum geht. Wenn der Nutzen Ihrer Leistungen klar wird, lösen sich Preisbedenken in der Regel von selbst auf.

UND WENN ICH DEN KUNDEN NICHT ÜBERZEUGEN KANN?

Bei Kunden, die Ihren Argumenten zum Trotz nicht in Datensicherheit investieren möchten, haben Sie drei Optionen:

- Bereiten Sie eine **Haftungsfreistellungserklärung** vor, die Ihr Unternehmen explizit von der Haftung für Datenverluste beim Kunden freistellt, sofern keine Backups vorgehalten werden. Viele Kunden überdenken ihre Entscheidung, sobald sie mit der Unterzeichnung einer solchen Erklärung konfrontiert werden.
- Richten Sie sich selbst eine Backup-Lösung ein und **kalkulieren Sie die Kosten für Datensicherung auf Dokumentenebene in Ihr Managed-Services-Angebot ein.** Dadurch werden Sie im Notfall zum strahlenden Retter und können bei Bedarf ein Upselling auf hochwertigere Datensicherheitsservices ansprechen. Bei diesem Ansatz berechnen Sie den Service nicht separat, sondern preisen die Kosten dafür in den Servicegrundvertrag mit dem Kunden ein.
- **Nehmen Sie bezahlte Datensicherheit als regulären Bestandteil in den Managed-Services-Vertrag auf.** Etwas so Wichtiges darf nicht optional sein. Alle Unternehmen, die mit Ihnen einen Servicevertrag schließen, buchen automatisch die Datensicherheit der Basisstufe mit. Sie ist als einzelne Position im Vertrag aufgeführt. Sollte der Kunde dies hinterfragen, können Sie sich mit ihm über Sicherheitsstufen und Preisoptionen unterhalten.

Holen Sie sich professionelle Unterstützung

Natürlich können Sie auch selbst eine Haftungsfreistellungserklärung formulieren, aber es empfiehlt sich, dass Sie dafür einen Rechtsanwalt zurate ziehen.

Sie möchten noch mehr Datensicherheit verkaufen? Wir können Ihnen helfen.

Um die Ratschläge in diesem Kompendium optimal umzusetzen, müssen Sie eine hervorragende Datensicherheitslösung für Ihre Kunden im Programm haben.

N-able™ Backup ist eine moderne Cloud-First-Lösung, die Daten jeglicher Art und beliebigen Umfangs zuverlässig sichern kann und von einzelnen Dateien bis hin zu kompletten Systemen alle Wiederherstellungsszenarien unterstützt. In nur einem Produkt sind Backup-Software, Cloud-Speicher und ein webbasiertes Dashboard zur Verwaltung all Ihrer Kunden vereint. Die Lösung ist zudem flexibel genug für mehrere Servicestufen, um individuellen Kundenansprüchen gerecht zu werden.

Weitere Informationen finden Sie auf https://www.n-able.com/de/products/backup

Außerdem bieten wir den nötigen geschäftlichen und technischen Support, damit Sie umfassende Datensicherheit verkaufen und bereitstellen können.

Wenn Sie mehr über Vertrieb und Marketing erfahren möchten, besuchen Sie das SolarWinds MSP Institute. Dort finden Sie ein umfassendes Angebot an Unterlagen und Praxistipps von renommierten Unternehmen, damit Sie Ihr Geschäft ausbauen können.

Stöbern Sie auch auf den Seiten des MSP Advice Project: Hier finden Sie praxiserprobte Tipps von anderen MSPs, die berichten, wie sich klassische geschäftliche Probleme entschärfen lassen.

Über N-able

Mit N-able können Managed Services Provider (MSPs) kleine und mittelständische Unternehmen effektiv bei der Digitalisierung unterstützen. Eine flexible Technologieplattform und leistungsstarke Integrationen erleichtern MSPs die Überwachung, Verwaltung und Sicherung der Systeme, Daten und Netzwerke ihrer Endkunden. Unser wachsendes Portfolio an Sicherheits-, Automatisierungs- sowie Backup- und Wiederherstellungslösungen richtet sich an Fachleute für das IT-Servicemanagement. N-able vereinfacht komplexe Umgebungen und sorgt dafür, dass Kunden ihre Probleme selbst in die Hand nehmen können. Wir bieten umfassenden, proaktiven Support in Form von hilfreichen Partnerprogrammen, praktischen Schulungen und wachstumsfördernden Ressourcen. So können MSPs hochwertige Services liefern und ihren Erfolg ausbauen.

n-able.com/de