Channel Futures

CLOUD BACKUP UND CYBER PROTECTION

Der einfachste Weg für VARs, Service-basierte Einnahmen zu generieren

POWERED BY | Acronis

EINFÜHRUNG

Störungen sind die neue Normalität. Der digitale Transformationsmoloch definiert weiterhin praktisch alle Phasen und Facetten des globalen Geschäfts neu – das VAR-Segment (Value-Added-Reseller) eingeschlossen. Marktkräfte wie die Cloud, die explodierende Einführung neuer Geräte und ständig wachsende Datenmengen, eine immer breitere Palette von Software-as-a-Service-Lösungen (die auf eine immer breitere Palette von Geschäftsszenarien abzielen) sowie Innovationen in der Automatisierung formen das VAR-Modell radikal um und stellen die Frage, welche Rolle diese Faktoren spielen und wie sie den Geschäftserfolg im neuen Jahrzehnt definieren werden.

Zukunftsorientierte VARs, die sich an diese weitreichenden Änderungen anpassen wollen, verdienen Anerkennung – selbst wenn diese Anpassung langsam erfolgt. Viele haben Abonnement-Modelle, SaaS-Lösungen und Cloud-Infrastrukturen in ihr Produktportfolio aufgenommen – ein wichtiger Schritt in die richtige Richtung.

Aber es gibt noch viel zu tun in einer Welt, in der Unternehmen es zunehmend vorziehen, IT-Services von spezialisierten Providern anzumieten, statt entsprechende Lösungen selbst zu besitzen und zu betreiben. Neue „Everything-as-a-Service"-Startups breiten sich in der gesamten Wettbewerbslandschaft aus und erfinden die „Go-to-Market"-Formel mit schwindelerregender Geschwindigkeit neu. VARs müssen sich da wohl mitentwickeln – oder die Konsequenzen tragen.

Wie die nachfolgenden Seiten aufzeigen werden, kann ein VAR von diesem zunehmend lukrativen „as-a-Service"-Ansatz am direktesten profitieren, indem er selbst entsprechende Cloud Backup Services und Data Protection Services anbietet. Diejenigen mit den besten Geschäftsvisionen für dieses und die nächsten Jahre werden zunehmend mehr Cloud Services verwalten, Automatisierungstools zur Unterstützung ihrer Kunden einsetzen und kontinuierlich nach neuen Wegen suchen, um von den zahlreichen, im gesamten Technologie-Ökosystem entstehenden Plattformen zu profitieren. Wobei Plattformen mit umfassenden Automatisierungsangeboten eine besondere Rolle zukommt, weil sie VARs bei der Einführung hochwertiger Services effizient unterstützen. Es gibt beispielsweise neue Managed Services-Plattformen, um betriebskritische Informationen, Sicherheitsupdates, Infrastrukturverwaltungs- und Routineaufgaben besser zu handhaben.

Mit dem richtigen Plattform-Ansatz und einer kuratierten Liste von Lösungen können VARs ihren Kunden und Partnern verwaltete Services ohne die üblichen Probleme und Kosten anbieten, wie sie sonst beim Aufbau eines neuen Geschäftsmodells oder einer neuen Geschäftseinheit vorkommen. Wie dies geht, erfahren Sie auf den nachfolgenden Seiten.

Geschäftsmodelle für den Vertrieb hochwertiger Services

Es gibt eine Reihe überzeugender Gründe für VARs, ihr Angebotsportfolio mit hochwertigen abonnementbasierten und verwalteten Services zu erweitern. Einige sind ziemlich offensichtlich – wie etwa, dass regelmäßige Abonnementeinnahmen (statt sporadischer Einzelkäufe) eine höhere Geschäftsstabilität, Rentabilität und Kalkulierbarkeit bieten.

Am wichtigsten dürfte jedoch die Erkenntnis sein, dass VARs, die an klassischen Geschäftsmodellen festhalten (wie nur herkömmliche Lizenz-Erneuerungen, Support- und Service-Verträge sowie einfache Managed Services anzubieten) zunehmend gefährdet sind. Stattdessen auf Cloud Services zu setzen, kann VARs davor schützen, vom Markt überholt zu werden: denn die Cloud ist das am schnellsten wachsende IT-Service-Marktsegment. Laut Gartner wird sich der weltweite Markt für Public Cloud Services von 182,4 Milliarden US-Dollar in 2018 auf 331,2 Milliarden US-Dollar in 2022[i] entwickeln, weil Unternehmen zunehmend auf herkömmliche Angebote verzichten und stattdessen bei der Auswahl von IT-Produkten/-Services zunehmend eine „Cloud-first"-Mentalität entwickeln.[ii]

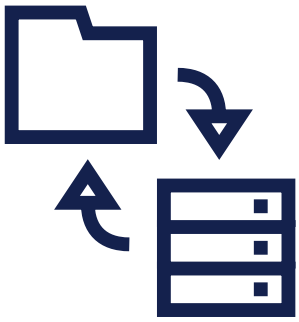
IT-Services: OBERSTE 5 und UNTERSTE 5

nach jähr. Wachstum (CAGR, in %) (2017-2022)

Quelle: Gartner Webinar („Top Trends Driving Change for IT Services.")

Oberste 5	CAGR % 2017-2022
IaaS	**26,6**
Infrastruktur-Utility-Services	**14,1**
Mobil (Managed Workplace Services)	**11,3**
Colocation	**11,0**
Hosting	**10,4**

Unterste 5	CAGR % 2017-2022
Desktop (Managed Workplace Services)	**-3,5**
Hardware-Support (Client-Geräte-Support)	**-3,4**
Kundendienst-Outsourcing	**-3,2**
Datenzentren-Outsourcing	**-2,5**
Enterprise-Netzwerke-Outsourcing	**-2,3**



Ein solches exponentielles Wachstum gibt es auch bei den Managed Cloud Services: laut Prognosen wird der weltweite Markt bis 2023 einen Umfang von 84,7 Milliarden US-Dollar erreichen. Gegenüber 2018 (mit 41,4 Milliarden US-Dollar) entspricht dies mehr als einer Verdoppelung.[iii] Gartner prognostiziert, dass Cloud-bezogene Services (wie Beratung, Implementierung, Migration und Managed Services) bis 2022 fast ein Drittel (28%) des gesamten Cloud-Budgets ausmachen werden.[iv]

Fazit: VARs, die ihre Geschäftskennzahlen verbessern und langfristig wachsen wollen, müssen ihr Managed Cloud Service-Portfolio erweitern. Die Welt wendet sich der Cloud zu – und damit von VARs ab, die diesem Trend nicht folgen wollen.

Ein Cloud Service-Portfolio aufbauen und verwalten

Wie kann ein VAR auf diese Zug aufspringen? Managed Cloud Services basieren auf zwei Kernelementen. Das erste Element ist eine **Plattform** für Service-Management, Onboarding, Integration und Anpassung.

Eine eigene Service-Management-Plattform aufzubauen, ist eine komplexe und anspruchsvolle Software-Entwicklungsaufgabe. VARs und MSPs sollten dafür besser mit einem kompetenten Technologiepartner zusammenarbeiten, der eine passende robuste, getestete und vorkonfigurierte Lösung anbieten kann – wie etwa **Acronis Cyber Cloud**. Mit einer solchen für Service Provider optimierten Plattform können VARs und andere Partner die für sie passenden Cloud Services ohne oder mit niedrigen Einstiegskosten schnell zusammenstellen und dann ihren Kunden anbieten. Die besten Plattformen ermöglichen es, differenzierte Angebote zu erstellen, Geschäfts- und Preismodelle zu entwickeln und die Cloud Services leicht in ein bestehendes Portfolio zu integrieren.

Unabhängig vom Provider muss eine Cloud Managed Service-Plattform folgende Funktionen bereitstellen:

- Mandanten-Fähigkeit mit sicherer Service-Partitionierung zur Unterstützung von Mehrfachkunden
- Die Möglichkeit, verschiedene Angebote und Services zu bündeln
- Einzelanmeldung (Single Sign-on, SSO) für Kundenkonten und Integration in externe SSO-Systeme
- Eine Richtlinien-Engine, die angepasste Nutzungs- und Sicherheitsrichtlinien (wie rollenbasierte Zugriffskontrollen) unterstützt
- Nutzungskontingente (Quotas)
- Vielfältige Zahlungsmodelle wie Pay-as-you-go, Jahresabonnements, reservierte Kapazitäten usw.

- Eine einheitliche Management-Konsole, die Mehrfachkunden-Umgebungen unterstützt
- Umfangreiche Nutzungsberichte, Dashboards sowie Monitoring- und Messfunktionen
- Integration in andere Systeme, inkl. Benutzer-Bereitstellung, Benutzer-Authentifizierung (IAM), Rechnungsstellung/Buchhaltung, Support/Ticket-Verwaltung, CRM
- Individuelles Branding (z.B. eine Whitelabeling-Möglichkeit)
- Eine REST-API, die die Entwicklung und Integration von kundenspezifischen Cloud Services erleichtert

Der Erfolg beim Vertrieb von Managed Cloud Services hängt auch von einer sorgfältig kuratierten **Service-Zusammenstellung** ab. Natürlich könnte ein VAR auch damit fortfahren, Hunderte von Lösungen von Hunderten von Herstellern zu verkaufen. Es ist jedoch sinnvoller, seine Angebotspalette zu vereinfachen und alle Anforderungen über eine Handvoll Hersteller abzudecken. Insbesondere mit Herstellern aus dedizierten Nischen – wie Netzwerke, Data Protection, IaaS (Infrastructure as a Service), Infrastruktur-Management, Produktivitätswerkzeuge – die Services für folgende geschäftskritische Bereiche bereitstellen:

- Endpunkte/Endgeräte (Desktop-PCs, Notebooks und Mobilgeräte)
- Internet und Mobile Data Services
- VoIP-Services
- Drucker
- Applikationen für Email und Office-Produktivität (wie Office 365 oder Google Apps)
- CRM-Applikationen
- Finanzapplikationen
- ERP-/HCM-Applikationen
- Marketing-Applikationen
- Endpunkt-Management (Desktop-PCs, Notebooks und Mobilgeräte)

Was Cyber Protection-Lösungen angeht, ist Acronis wie ein „Schweizer Taschenmesser“. Acronis wird Ihre Cloud Service-Bedürfnisse nicht zu 100% abdecken (kein einzelner Hersteller wird dies tun), aber doch zu einem bedeutenden Umfang. Dazu gehören Services für:

- Data Protection (Backup, Recovery)
- Geschäftskontinuität (Disaster Recovery)

- Endpunkt-Sicherheit (z.B. zur Ransomware-Abwehr)
- Speichern, Synchronisieren und Teilen von Dateien (EFSS-Lösungen)
- Beglaubigung/Zertifizierung, Authentizitäts/ Integritätsüberprüfung und digitales Signieren von Dateien

Für welchen dieser Bereiche Sie sich auch entscheiden – Acronis hat die passende Lösung, um Ihren Kunden einen Mehrwert zu bieten.

Data Protection: Die Grundlage eines jeden guten Cloud Service-Portfolios

Es ist immer eine gute Geschäftsstrategie, seine Produkt- und Service-Kategorien für einen großen Zielmarkt auszulegen. Und „Data Protection as a Service" (DPaaS) passt perfekt zu einer solchen Strategie. Denn laut IDC wird der DPaaS-Markt bis 2022 mit einer jährlichen Wachstumsrate (CAGR) von 16,2% auf 10,2 Milliarden US-Dollar zunehmen.[v]

Ein überzeugendes Data Protection Service-Portfolio beginnt mit einem sicheren **Backup Service** für klassische Server, Storage-Systeme, virtuelle Maschinen, virtuelle Storage-Umgebungen und Cloud-basierte Ressourcen. Ein Produkt wie **Acronis Cyber Backup Cloud** ermöglicht es VARs, alle geschäftskritischen Daten und Systeme eines Unternehmens mithilfe eines Hybrid-Storage-Designs zu sichern, welches sowohl lokale als auch Cloud-basierte Storage-Ressourcen unterstützt. Auf diese Weise sind die Kunden nicht an bestimmte Speicherorte, Standorte oder Umgebungen gebunden.

Ein Disaster Recovery as a Service-Angebot (DRAAS) ist eine weitere, entscheidende Komponente im Data Protection-Portfolio eines VARs. Damit kann man einen Backup Service um die Möglichkeit erweitern, Daten und Applikationen im Notfall schnell auf einer sekundären Infrastruktur (in der Regel eine Cloud Recovery Site) wiederherzustellen und auszuführen.

Die Prozessautomatisierung, eine überlicherweise notwendige Voraussetzung für einen zuverlässigen Disaster Recovery Service, kann einen erheblichen Software-Entwicklungsaufwand erfordern. VARs können diesen Aufwand durch den Einsatz eines SaaS-Produkts wie **Acronis Cyber Disaster Recovery Cloud** umgehen – und so ihr Cloud Service-Portfolio leicht um ein DR-Angebot erweitern. Dieses schlüsselfertige SaaS-Produkt unterstützt sowohl physische als auch virtuelle Workloads, bietet einen GUI-Editor zum Erstellen von DR-Automatisierungen und kann verschiedene Wiederherstellungsszenarien testen, ohne dass laufende Produktionssysteme dabei beeinträchtigt werden.

Der **File Sync & Share Service** stellt Cloud-basierte Funktionen zum unternehmensgerechten Speichern, Synchronisieren und Freigeben von Dateien sowie dazugehörige Sicherheits- und Zugriffskontrollfunktionen bereit. Zwar bieten auch viele gängige Public Clouds (teils auch in Enterprise-Varianten) ähnliche Funktionalitäten an. Jedoch handelt es sich dabei meistens um eigenständige Produkte bzw. Funktionalitäten, die nicht gut mit anderen, von Unternehmen verwendeten Storage-, Data Protection- und Security-Services zusammenarbeiten. **Acronis Cyber Files Cloud** ermöglicht VARs dagegen, einen umfassenden, integrierten und anpassbaren File Sync & Share Service auf Enterprise-Niveau anzubieten, der mit vorhandenen Storage-Systemen oder der Cloud-Infrastruktur von Acronis zusammenarbeiten kann. Wie die oben genannten Public Clouds unterstützt auch Acronis Cyber Files Cloud alle gängigen Mobilgeräte, Windows-Versionen, Macs und Webbrowser. Darüber hinaus stellt es weitere unternehmensgerechte Funktionen bereit – wie etwa die direkte Bearbeitung von Microsoft Office-Dokumenten in der Mobile App (auf dem Mobilgerät).

Und dann gibt es noch diese „Must-haves" für das moderne papierlose Büro: **Zertifzierungs-, Verifizierungs- und E-Signatur-Funktionen für Dateien** bieten einen sicheren, unwiderlegbaren Nachweis, um digitale Dokumente erst zu beglaubigen und dann später auf ihre Authentizität überprüfen zu können. Ein SaaS-Produkt wie **Acronis Cyber Notary Cloud** ermöglicht es VARs, einen Blockchain-basierten Service zur elektronischen Beglaubigung, Signierung und Verifizierung von Dokumenten bereitzustellen. Die entsprechenden Kunden können damit ihre geschäftskritischen Dokumente authentifizieren und so gesetzliche Vorgaben zur Datenintegrität und Datentransparenz erfüllen.

Was lohnende Geschäftsstrategien anbelangt, erweisen sich Data Protection Services immer wieder als eine der **einfachsten Vertriebsoptionen für Technologie-Provider.** Tatsächlich haben viele große MSPs zuerst mit dem Vertrieb von Backup-, Data Recovery- und Data Security-Lösungen angefangen und konnten von dieser Basis aus dann expandieren.

Gehen Sie über Data Protection hinaus, um wettbewerbsfähig zu bleiben

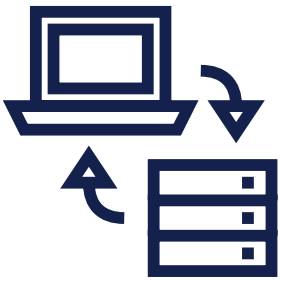
Klassische Data Protection-Herausforderungen (wie Stromausfälle und Naturkatastrophen) sind längst nicht mehr die Hauptgefahren, mit denen sich Unternehmen im 21. Jahrhundert konfrontiert sehen. Zur weltweit wohl größten Gefahr für Unternehmen sind vielmehr Cyber-Bedrohungen geworden. Laut dem Beratungsunternehmen Accenture[vi] haben digitale Sicherheitsverletzungen im Zeitraum von 2014-2018 um 67% zugenommen.

Das sind schlechte Nachrichten für Unternehmen – aber durchaus gute für VARs. In einer Welt, in der jede Minute 2,9 Millionen US-Dollar durch Cyber-Kriminalität verloren gehen[vii], können VARs einen erheblichen Wettbewerbsvorteil gewinnen, wenn sie ihr Portfolio weg von herkömmlichen, handelsüblichen Backup-Produkten und hin zu umfassenden Cyber Protection-Lösungen entwickeln. Acronis versteht unter Cyber Protection eine neue Generation von Data Protection, die Cyber Security-Fähigkeiten integriert und zudem alle fünf Vektoren der Cyber Protection adressiert, die Acronis unter dem Schlagwort **SAPAS** zusammenfasst. Mithilfe dieser Komponenten können VARs ihren Kunden differenzierte und sichere Data Protection Services anbieten.

Der erste Buchstabe des Akronyms SAPAS steht für **Safety**, womit die Verlässlichkeit gemeint ist, dass die gesicherten Datenkopien unverfälscht und jederzeit wiederherstellbar sein müssen. Der zweite Buchstabe („A“) steht für **Accessibility (Verfügbarkeit)**, weil die Kunden und Mitarbeiter von heute stets mobil und „always online“ sind, sodass Unternehmensdaten jederzeit und von überall verfügbar sein sollten. Der dritte Buchstabe („P“) steht für **Privacy (Vertraulichkeit)**. Denn eine moderne Cyber Protection-Lösung muss sowohl die sensiblen Unternehmensdaten vor den neugierigen Augen unautorisierter Personen schützen können – wie auch die notwendigen Kontrollfunktionen bereitstellen, damit berechtigte Benutzer jederzeit Zugriff erhalten. Nicht weniger entscheidend ist das für **Authentizität** stehende „A“. Denn es muss gewährleistet sein, dass die gesicherten und beglaubigten Datenkopien nicht heimlich verändert wurden, sondern weiterhin mit den Originaldaten identisch sind.

Und schließlich („S“) müssen VARs **Sicherheits**lösungen bieten, um die Daten, Systeme und Benutzer vor böswilligen Akteuren (wie externe Hacker oder auch übel gesinnte Mitarbeiter) bewahren zu können. Diese Sicherheitsfunktionen müssen die Daten sowohl bei Übertragungen (im Netzwerk/Internet) als auch Speichervorgängen (auf dem Endgerät/Storage/in der Cloud) schützen. Für dieses Ziel werden diverse Techniken eingesetzt: Verschlüsselung, Hash-Wert-Erstellung, digitale Signaturen, Monitoring, Angriffsabwehr und Wiederherstellungsmaßnahmen.

VARs und MSPs, die eine integrierte Suite von sicheren Data Protection Services anbieten wollen, müssen auch an eine leistungsfähige Ransomware-Abwehr denken. Unter Ransomware versteht man eine besondere Variante von Schadsoftware (Malware), die den Zugriff auf von ihr befallene Computersysteme und Daten blockiert – und den betroffenen Besitzern nur gegen eine Lösegeldzahlung



wieder Zugriff auf ihre Systeme bzw. Daten gewährt. Analysen gehen davon aus, dass **in 2019 ca. alle 14 Sekunden ein Unternehmen durch Ransomware angegriffen wurde.**[viii] Laut einem Bericht von Malwarebytes sind die Angriffe auf Unternehmen allein von Q4 2018 bis Q1 2019 um 195% angestiegen.[ix]

Acronis Active Protection verhindert, dass Dateien, Backups oder die Backup-Software selbst von Ransomware verschlüsselt bzw. deaktiviert werden können. Dazu werden alle Dateizugriffe und Dateiänderungen auf den geschützten Systemen überwacht, um potenziell schädliche Aktivitäten zu erkennen und zu blockieren, bevor ein Ransomware-Angriff verheerende Schäden anrichten kann. Sollte eine Ransomware diesen Schutzwall doch einmal durchbrechen können, wird Acronis Active Protection die verschlüsselten Dateien automatisch wiederherstellen. Service Provider können dadurch viel Zeit für ansonsten aufwendige Wiederherstellungen einsparen und entsprechende Ausfallzeiten vermeiden. Weil diese Technologie in Acronis Cyber Backup Cloud integriert ist, können Sie die Gefährdung durch Ransomware für sich und Ihre Kunden umgehend minimieren. Und Sie müssen nichts anderes auf den zu schützenden Systemen installieren als die Backup Agenten.

Cyber Protection-Lösungen mithilfe von Acronis bereitstellen

Acronis Cyber Cloud bietet noch mehr als Backup-, Disaster Recovery-, File Sync & Share-, Dokumentbeglaubigungs- und Data Security-Funktionalitäten. Es lässt sich auch in zentrale MSP-/CSP-Backoffice-Tools (z.B. für Service-Management, Support-Tickets, Monitoring, Alarmfunktionalität) integrieren, damit MSPs effizienter arbeiten können.

Außerdem ist Acronis Cyber Cloud die *einzige* Lösung, die neben der oben aufgeführten Reihe von begehrten Cyber Protection Services auch direkt eine umfassende Plattform zur Service-Bereitstellung und Benutzerverwaltung bietet. Dadurch können Service Provider alle Angebote an ihren üblichen Marktauftritt anpassen und ihre Kundenbindung stärken. Acronis Cyber Cloud ermöglicht außerden den Zugriff auf die Cloud-Infrastruktur von Acronis sowie die Unterstützung von privaten Systemen zur Service-Bereitstellung.

Wenn ein VAR sein Portfolio auf Basis einer soliden, von einem etablierten Software-Hersteller entwickelten SaaS-Lösung aufbaut, kann er Cloud Services mit **minimalen Einstiegskosten und geringem Zeitaufwand** anbieten – und von der Unterstützung durch einen Partner mit weitreichenden Erfahrungen in sicherer Data Protection profitieren.

Partner-Roadmap: So starten Sie den Vertrieb von Acronis Cyber Cloud

Neben seiner technischen Expertise sollte ein Cloud Service-Hersteller über sein Partner-Programm außerdem eine umfassende Unterstützung für Vertrieb und Marketing bereitstellen. Die Experten des Acronis Cloud Partner-Programms unterstützen VARs in allen Phasen des Service-Lebenszyklus – von der anfänglichen Markteinführung (bei der Acronis dem VAR durch alle Prozesse hilft, von der Service-Einführung über die Preisgestaltung bis zum Schnüren der Angebotspakete) über das Kunden-Onboarding bis hin zu Marketing-Kampagnen und dem Presales-Support.

Sichere Data Protection Services: Beispiele und Anwendungsszenarien

Auf Basis der sicheren Data Protection-Fähigkeiten von Acronis Cyber Cloud können VARs eine Fülle von allgemeinen oder angepassten Cloud Services anbieten, die für Unternehmen jeder Art und Größe attraktiv sind. Die beliebtesten Kategorien sind:

Vielfältige **Hybrid Data Protection Services**, die mit jeder Infrastruktur arbeiten – wozu auch lokale Server oder Disk-Arrays, VAR-verwaltete Systeme in einem Colocation-Rechnenzentrum oder Cloud Storage-Ressourcen gehören. Bei einem typischen Hybrid Storage-Szenario wird das Primärarchiv auf einem Cloud Storage gespeichert – und die optionalen sekundären Datenkopien auf einem lokalen Storage. Eine solche Hybrid-Implementierung kann der VAR außerdem zum Cross-Selling nutzen. Denn neben dem Cloud Service kann er dem Kunden auch ein passendes Hardware-/Software-Bundle für den lokalen Storage anbieten.

Eine weitere Geschäftschance ergibt sich aus der wachsende Popularität von SaaS-Applikationen wie Office 365, für die Cloud-basierte Data Protection Services wie Acronis Cyber Backup Cloud eine ideale Ergänzung sind. Viele VARs bieten **Office 365 im Bundle mit einer Backup-Lösung** an, die es den Kunden ermöglicht, ihre Data Protection-Ziele und (falls notwendig) gesetzlichen Compliance-Anforderungen einzuhalten.

SaaS-basierte Data Protection Services können mit **Cloud-basierten File Sync & Share Services** kombiniert werden. Diese verbessern die Zusammenarbeit zwischen Mitarbeitern bzw. mit Partnern und stellen Kontrollwerkzeuge bereit, um Datenzugriffe zu steuern und unberechtigte Daten-Exfiltrationen zu verhindern. Eine weitere Upselling-Option für Services zur Datenarchivierung sind.

Cloud-basierte Disaster Recovery Services. Sie stellen automatisierbare Prozesse und Cloud-Ressourcen bereit, um Daten und Systeme bei Betriebsausfällen auf einem vom Provider verwalteten Remote-Standort wiederherzustellen. Dadurch entfällt die Notwendigkeit für ein Unternehmen, eine solche kostenintensive, redundante Infrastruktur selbst vorhalten zu müssen. Je mehr Kunden bereit sind, zum Hosten ihrer Enterprise-Applikationen auf Cloud-Infrastrukturen zurückzugreifen, umso mehr können VARs ihr Angebot ausdehnen und IaaS-Ressourcen verwenden, um derartige Disaster Recovery-Standorte bereitzustellen.

Konvergente Data Protection: Security Services dienen als Bollwerk gegen die allgemeine Ransomware-Angriffswelle. Sie verhindern, dass Unternehmen Lösegeld für ihre wertvollen Daten zahlen müssen, weil diese von den Angreifern zuvor verschlüsselt oder anderweitig deaktiviert wurden. Wie leicht Daten ohne einen solchen modernen Schutz deaktiviert werden können, belegt die Unzulänglichkeit herkömmlicher Anti-Malware-Lösungen – und unterstreicht die Notwendigkeit, Data Protection- und Data Security-Technologien symbiotisch in einer konvergenten Cyber Security-Lösung zu vereinen. Viele herkömmliche, auf Signaturen basierende Antiviren-Lösungen bieten hier keine ausreichende Schutzwirkung mehr. Die wirkungsvollen modernen Abwehrlösungen basieren dagegen auf Technologien wie Acronis Active Protection, die Ransomware-Angriffe mit ausgeklügelten Machine Learning-Modellen erkennen und stoppen können. Für VARs und MSPs bedeutet dies, dass sie sich auf die Bereitstellung und Vermarktung dieser modernen Lösungen konzentrieren können, während die komplexe Implementierung und Verwaltung der zugrundeliegenden Technologien von einem Drittanbieter-Spezialisten übernommen wird.

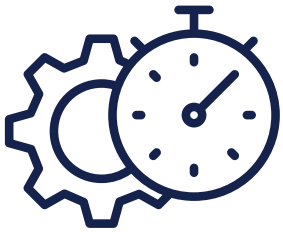
VARs und Partner können die allgemeinen Cyber Protection Services auch mit zusätzlichen Funktionen erweitern und anpassen, um ganz bestimmte Branchen und Kunden anzusprechen. Eine erweiterbare und per Whitelabeling anpassbare Plattform wie Acronis Cyber Cloud stellt sicher, dass Partner ihre Markendarstellung, Angebotsanpassung und Kundenbeziehung komplett in eigener Hand haben. VARs und MSPs können die Funktionen von Acronis Cyber Cloud mithilfe der Acronis Cyber Platform erweitern, welche eine Reihe von APIs und SDKs bereitstellt. Durch solche Anpassungen und Erweiterungen können VARs und MSPs einzigartige Angebote erstellen, mit denen sie der Konkurrenz einen Schritt voraus sind.

Typische Beispiele für derartig angepasste Services wäre etwa ein **Workstation-Backup in die Cloud** oder eine **Langzeitarchivierung von Daten in einem Storage-Depot**, um gesetzliche Compliance-Anforderungen zu erfüllen. Für letzteres sind spezielle Cloud Services ideal, die einen kostengünstige Cold Storage bereitstellen.

Eine weitere, hervorragende Marktchance eröffnet sich in der **Gesundheitsbranche**. Denn hier werden Storage- und Backup-Lösungen benötigt, die konform mit gesetzlichen Verordnungen wie der EU-DSGVO/GDPR (für Europa) oder HIPAA (für die USA) sind. Ein typisches Anwendungsbeispiel ist ein **auf Dienstleistungen für Zahnärzte spezialisierter MSP in den USA**. Dieser konnte mit Acronis Cyber Backup Cloud und der dort integrierten AES-256-Verschlüsselung einen HIPAA-konformen Data Protection Service bereitstellen – und durch den Wechsel von der zuvor verwendeten Backup-Software auch noch 30.000 US-Dollar einsparen. Ein weiteres Beispiel ist ein **führender amerikanischer Anbieter von Lösungen für elektronische Gesundheitsakten und automatisierte Praxisverwaltung**. Durch den Umstieg auf Acronis Cyber Backup Cloud konnte das Unternehmen seine Wiederherstellungszeiten um 90% senken und von der Skalierbarkeit des Cloud Services profitieren, sodass sein Kundenstamm in zwei Jahren um das Zehnfache anstieg.

Und noch eine weitere Möglichkeit, die Beachtung verdient: Cyber Protection Services für **Einzelhandel-, Logistik- und Versicherungsunternehmen**. Denn diese Branchen arbeiten meist mit einem verteilten Filialnetz, welches schwer zentral zu verwalten und zu schützen ist. Die Acronis Plattform bietet diesen Unternehmen folgende Möglichkeiten:

- Zentrale Cyber Protection für alle Niederlassungen, mit zentralen Backup-Richtlinien und Self-Service-Wiederherstellungsfähigkeiten.
- Remote-Wiederherstellungen, die von zentraler Stelle aus automatisier- und steuerbar sind.



- Automatisierbare Ein-Klick-Wiederherstellungen, für die keine speziellen IT-Mitarbeiter notwendig sind.
- Es sind keine Ausrüstungsinvestitionen für die einzelnen Zweigstellen erforderlich, weil alle Services in der Cloud laufen.
- Eine einheitliche, zentrale Verwaltung für die Sicherung der Server, Workstations und Office 365-Konten.

Zusammenfassung und Empfehlungen

Sichere Cloud-basierte Data Protection Services bieten VARs erhebliche Möglichkeiten, regelmäßige Umsätze mit hohen Margen zu erzielen sowie Kunden zu gewinnen und zu binden. Mit einem etablierten Software-Hersteller wie Acronis als Partner können sich VARs auf ihre wesentlichen Fähigkeiten fokussieren: durch die Kompetenz von Acronis entlastet, kann ein VAR seine ganze Energie auf **Angebotsdifferenzierungen und Service-Anpassungen** sowie **Umsatzsteigerungen und Kostensenkungen richten**. Desweiteren kann er seine Kunden vor **modernen Cyber-Bedrohungen (wie Ransomware) schützen, die Entwicklung und Bereitstellung seiner Service-Angebote beschleunigen** und das **Cross-Selling von passenden Zusatzprodukten/-diensten vorantreiben.** Durch all diese Möglichkeiten kann ein VAR eine **starke Marke entwickeln, die Neukunden anzieht und Bestandskunden bindet.**

Kontaktieren Sie den Acronis Vertrieb für eine Geschäftsbesprechung und eine Live-Produktdemo.

KONTAKT

Quellen

[i] Gartner. „Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019.“ Pressemitteilung 02. April 2019.

[ii] Gartner. „Top Trends Driving Change for IT Services.“ Webinar 25. März 2019.

[iii] IDC. „Worldwide Managed Cloud Services Forecast, 2019–2023: An Extraction View of Technology Outsourcing Services Markets.“ Marktprognose. September 2019.

[iv] Prabha, Anil. „Public Cloud Services Market to Hit $214bn.“ TechHQ, 8. April 2019.

[v] IDC. „Worldwide Data Protection as a Service Forecast, 2018–2022: Initial Market Sizing.“ Marktprognose. Juli 2018.

[vi] Accenture. Ninth Annual Cost of Cybercrime Study. 6. März 2019.

[vii] „Cybercrime Costs Global Economy $2.9m Per Minute.“ Infosecurity Magazine. 24. Juli 2019.

[viii] Morgan, Steve. „Global Ransomware Damage Costs Predicted to Hit $11.5 Billion by 2019.“ Cybercrime Magazine, 17. November 2017.

[ix] Zamora, Wendy. „Labs Cybercrime Tactics and Techniques Report Finds Businesses Hit with 235 Percent More Threats in Q1.“ MalwareBytes, 25. April 2019.