Security und Data Protection für KMU

DELL Technologies

Ohne Security kein Unternehmenserfolg

Bereits am Anfang stehen Data Security und Data Protection

Jedes Unternehmen ist von Cyberattacken bedroht, nicht nur die großen. Zudem muss sich jedes Unternehmen gegen Systemausfälle und Fehler schützen und benötigt Backups. Auch wenn ein Unternehmen klein anfängt und vielleicht nur ein Endgerät und verschiedene Cloud-Services nutzt, müssen bereits Data Protection und Data Security sichergestellt sein. Mit diesen Lösungen und Tipps sichern kleine wie große Unternehmen ihren Erfolg.

Cyberattacken und Datenverlust: Es kann jeden treffen

Der deutsche Mittelstand wiegt sich hinsichtlich seiner Cyberrisiken in falscher Sicherheit, so der GDV (Gesamtverband der Deutschen Versicherungswirtschaft). Obwohl jeder vierte Mittelständler schon Opfer von Cyberkriminellen geworden ist, sehen zwei Drittel kein hohes Risiko für das eigene Unternehmen, wie eine Umfrage des GDV zeigt. 70 Prozent der befragten kleinen und mittleren Unternehmen denken, ihre Daten seien uninteressant. 62 Prozent glauben, ihr Unternehmen sei zu klein, um ein mögliches Angriffsziel zu sein.

Tatsächlich aber sind alle Unternehmen jeder Größenordnung und aus jeder Branche gefährdet. Der Mittelstand ist sogar in besonderer Gefahr, denn dort sind viele Schutzmaßnahmen eher lückenhaft. So haben zum Beispiel nur 45 Prozent ein Notfallkonzept und 44 Prozent testen nicht regelmäßig, ob sie eine Datensicherung im Notfall auch wieder einspielen könnten.

Gebraucht werden Data Security und Data Protection

Sicherheit und Erfolg eines Unternehmens hängen inzwischen maßgeblich von der sicheren Digitalisierung ab. IT-Infrastrukturen wie Endgeräte und Speichermedien, genutzte Applikationen und Cloud-Dienste müssen ebenso geschützt werden wie die Daten des Unternehmens, Kundendaten, Lieferantendaten, Beschäftigtendaten, Finanzdaten, Auftragsdaten, Projektdaten bis hin zu den Betriebsgeheimnissen, die jedes Unternehmen hat, teils ohne sich dessen richtig bewusst zu sein.

Für die IT-Infrastruktur und die Daten müssen die Schutzziele der Vertraulichkeit, Verfügbarkeit und Integrität gewährleistet sein. Das bedeutet insbesondere, dass kein Unbefugter auf die Daten zugreifen können darf, dass die Daten nicht verloren gehen dürfen und dass die Daten gegen Manipulation, also ungewollte Veränderung, geschützt sein müssen.

Mit Maßnahmen der Data Security (Datensicherheit) schützen sich Unternehmen gegen unerlaubte Datenzugriffe und Manipulationen an Daten, die durch Cyberangriffe und andere Attacken auf Daten und Infrastruktur versucht werden. Dazu gehören zum Beispiel der Malware-Schutz und die Verwaltung und Kontrolle der Identitäten und Berechtigungen (IAM, Identity and Access Management).

Die Data Protection (Datensicherung) schützt das Unternehmen gegen Datenverlust und Ausfallzeiten. Dazu gehören Backups und das Testen der Wiederherstellung der Daten sowie das Recovery nach einem Vorfall.

Die besonders gefürchteten Ransomware-Attacken versuchen durch kriminelle Verschlüsselung der Daten deren Verfügbarkeit zu unterlaufen. Gleichzeitig wollen die Angreifenden die Daten ausspähen und stehlen, um deren Vertraulichkeit auszuhebeln und die betroffenen Unternehmen mit mehreren Druckmitteln zu erpressen – durch die Verschlüsselung der Daten und durch die Androhung, die >>

Inhalt

Ohne Security kein Unternehmenserfolg 2

Bereits am Anfang stehen Data Security und Data Protection

Sicheres Unternehmenswachstum 8

Das Unternehmen wächst, die IT-Infrastruktur und die Security-Anforderungen ebenso

Security as a Service 13

Fachkräftemangel kompensieren, Cyberrisiken minimieren

Bilder: Dell Technologies

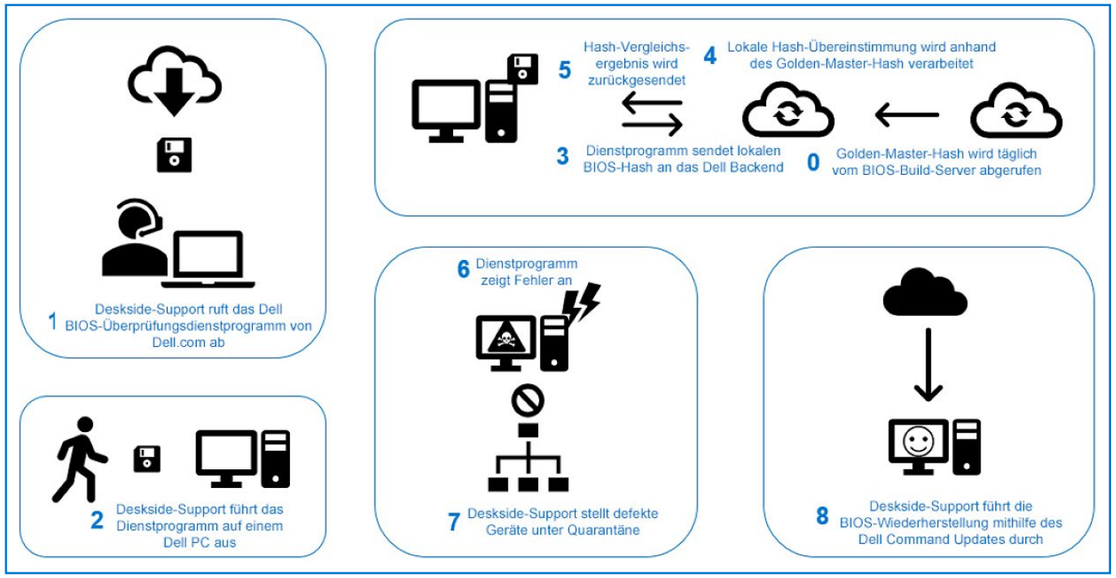
Daten zu veröffentlichen oder zu verkaufen, wenn kein Lösegeld gezahlt wird.

Was bereits Einzelunternehmen und Kleinstunternehmen benötigen

Selbst wenn ein Unternehmen nur aus einer Person besteht, mit einem Endgerät, auf dem Applikationen laufen und mit dem auf Cloud-Dienste zugegriffen wird: Auf Data Security und Data Protection kann man niemals verzichten. Jedes Unternehmen muss für den Schutz der Daten und Systeme sorgen, von Anfang an. Ob PC oder Notebook, das Endgerät des Einzelunternehmens oder die Endgeräte des Kleinstunternehmens mit beispielsweise fünf Beschäftigten sollten so viel integrierte Sicherheit aufweisen wie nur möglich.

Malware und Cyberattacken müssen erkannt und abgewehrt werden. Dazu gehört es, auch versteckte Angriffe, die bereits unterhalb der Betriebssystemebene starten, erkennen und eindämmen zu können. Daten auf Endgeräten, Datenträgern und in der Cloud müssen verschlüsselt werden. Die Zugangsdaten und digitalen Identitäten müssen sicher sein, aber auch die Daten, die auf dem Bildschirm des Gerätes zu sehen sind, müssen gegen Unbefugte geschützt werden.

Um Datenverlust und Ausfallzeiten zu vermeiden, die durch Cyberangriffe, aber auch durch IT-Störungen, Systemfehler und Missgeschicke der Nutzerinnen und Nutzer auftreten können, dürfen Backup und Funktionen für ein Recovery nicht fehlen.



Dell SafeBIOS führt eine Überprüfung außerhalb des PC-Clients anhand einer sicheren, von Dell Technologies gehosteten Datenbank durch und stellt ein korrumpiertes BIOS wieder her.

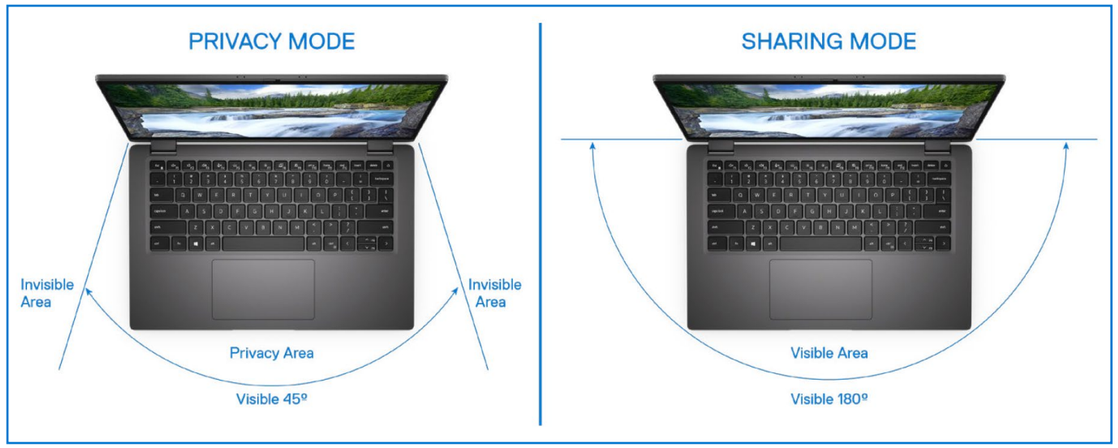
Für eine umfassende Data Security und Data Protection bieten sich diese Lösungen an:

Schutz vor Malware und Cyberangriffen

McAfee Small Business Security bietet umfassende Sicherheit für Endgeräte wie PCs, Notebooks, Tablets und Smartphones mit E-Mail-, Web- und Firewall-Schutz, sodass Unternehmen sich auf ihr Geschäft konzentrieren können, ohne sich Sorgen machen zu müssen, ob die Geräte oder Daten gefährdet sind. Die flexible Lizenzierung ermöglicht die Skalierung auf weitere Geräte, wenn das Unternehmen wächst. Der preisgekrönte Support sorgt dafür, dass das Unternehmen am Laufen bleibt.

Alternativ bietet sich VMware Carbon Black (Dell SafeGuard and Response) an. VMware Carbon Black Endpoint vereitelt Angriffe durch die Analyse von Milliarden Systemereignissen, um nachvollziehen zu können, welche Aktivitäten in der IT-Umgebung des Nutzenden normal sind, den Missbrauch zulässiger Tools zu verhindern und den Untersuchungs-Workflow für eine effiziente Reaktion zu automatisieren. VMware Carbon Black Endpoint konsolidiert mehrere Sicherheitsfunktionen für Endpunkte in einem Endpunkt-Agent und einer Konsole. Die Lösung beginnt ab 25 Lizenzen (Unternehmen, die mindestens 25 Endpoints sichern wollen).

Zusätzlichen Schutz gegen versteckte Angriffe unterhalb der Betriebssystemebene bietet Dell SafeBIOS. Dell SafeBIOS ist das fehlende Element in einer umfassenden Sicherheitsmanagement-Strategie zum Schutz von Hardware und vor Bedrohungen „unterhalb des Betriebssystems“. Zunächst führt Dell >>



Dell SafeScreen schützt Bildschirminhalte vor neugierigen, unerlaubten Blicken.

SafeBIOS eine Überprüfung außerhalb des PC-Clients anhand einer sicheren, von Dell Technologies gehosteten Datenbank durch. Alle Dell-Clients führen dies bei Systemstart oder spätestens alle 12 Stunden aus. Der PC-Client erhält ein positives oder negatives Ergebnis der Verifizierung, sodass eine schädliche Manipulation am Endgerät entdeckt wird. Die Dell SafeBIOS-Software unterstützt alle kommerziellen Dell-Business-Plattformen wie OptiPlex-, Latitude-, Precision- und XPS-Mobilgeräte und wird kontinuierlich mit den neuesten Schutzmaßnahmen für Dell-Clientgeräte aktualisiert.

Schutz der Daten auf dem Gerät und in der Cloud

Dell SafeData ermöglicht es Endnutzerinnen und Endnutzern, sicher zusammenzuarbeiten, indem sensible Daten auf Geräten geschützt und Informationen in der Cloud abgesichert werden.

Dell Encryption Enterprise bietet mit seiner flexiblen Verschlüsselungstechnologie unterschiedliche Möglichkeiten zum Schutz von Daten. Dazu gehören ein datenzentrierter und richtlinienbasierter Ansatz und ein Ansatz zur vollständigen Festplattenverschlüsselung. Dell Encryption steht für ein flexibles Angebot an optimierten Sicherheitslösungen, die Folgendes umfassen: dateibasierte Verschlüsselung, vollständige Festplattenverschlüsselung, verbesserte, zentralisierte Verwaltung nativer Verschlüsselungen (Microsoft BitLocker und Mac FireVault) sowie Datenschutz auf externen Medien, selbstverschlüsselnden Festplatten und mobilen Geräten. Alternativ empfehlen sich die Open-Source-Lösung Veracrypt sowie die kommerziellen Lösungen McAfee SafeBoot oder Cigent Secure.

Sichere Endnutzerzugangsdaten

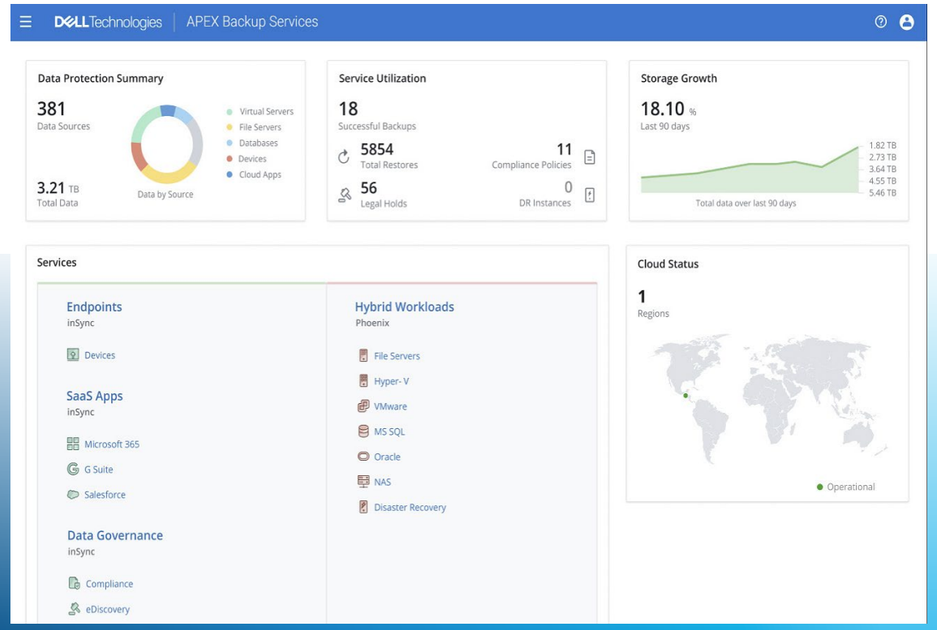
Dell SafeID wahrt die Sicherheit von Dell Endpoints und schützt vor Malware-Angriffen mit einem speziellen Sicherheitschip, der die Zugangsdaten von Endnutzerinnen und Endnutzern speichert. Mit dieser hardwarebasierten Speicherlösung sind die Daten besser geschützt, da sie isoliert und außer Reichweite von Angreifenden aufbewahrt werden.

Dell SafeScreen schützt vertrauliche Bildschirminhalte vor neugierigen, unerlaubten Blicken. Mit Look Away Detect wird der Bildschirm zudem automatisch abgeblendet, wenn die legitimen Nutzenden wegschauen, wodurch der Datenschutz weiter verbessert wird.

Backups und schnelle Wiederherstellung nach Vorfällen (Ransomware, Datenverlust)

Mit den SaaS-basierenden APEX Backup Services ermöglicht Dell Technologies einen durchgängigen Datenschutz mit zentraler Überwachung und Verwaltung für Anwendungen, Endpunkte und hybride Workloads. Dieses As-a-Service-Angebot lässt sich in wenigen Minuten einrichten und bei Bedarf skalieren, um steigenden Arbeitslasten gerecht zu werden. Verschiedene Sicherheitsfunktionen – inklusive sofortiger Erkennung, schneller Reaktion und beschleunigter Wiederherstellung – schützen vor Cyberangriffen und erhöhen die Resilienz.

Mit diesen Lösungen und Maßnahmen für Datensicherheit und Datensicherung hat ein Unternehmen das sichere Fundament, um erfolgreich zu wachsen. Mit dem Unternehmen wachsen dann auch die IT-Infrastruktur und die erforderlich IT-Sicherheit. Das zeigt das nächste Kapitel.



Auf einem zentralen Dashboard fassen die Dell APEX Backup Services alle Informationen zu Datensicherungs- und Restore-Vorgängen zusammen.

Sicheres Unternehmenswachstum

Das Unternehmen wächst, die IT-Infrastruktur und die Security-Anforderungen ebenso

Wachsende Unternehmen benötigen zusätzliche Schutzmaßnahmen für ihre IT-Infrastruktur, die Daten und die Zugriffe der Nutzerinnen und Nutzer. Ohne die richtige Sicherheit für die eigenen Endgeräte, Server, Netzwerke und Speicherlösungen gerät das Unternehmenswachstum schnell in Gefahr. Gerade die erhöhten Anforderungen an die IT-Administration dürfen nicht übersehen werden.

Die Vernetzung eröffnet neue Möglichkeiten, auch für Cyberkriminelle

Besteht ein Unternehmen nur aus einer einzelnen Nutzerin oder einem einzelnen Nutzer, beschränken sich die Verbindungen für den Datenaustausch auf Cloud-Dienste und das Internet. Doch mit einer Zunahme an Beschäftigten in Unternehmen, entsteht auch der Bedarf, sich untereinander zu vernetzen, zudem kommen eigene Server zum Einsatz. Gleichzeitig nehmen die Verbindungen ins Internet und zu den Cloud-Diensten zu.

Die internen Server, Verbindungen und Netzwerke müssen wirksam geschützt sein, und Lauschangriffe auf die Netze müssen ebenso verhindert werden wie ein Ausfall der Netzwerkverbindung oder der Server. Doch die gleichzeitige Nutzung interner Netzwerke und des Internets bringt weitere Risiken mit sich, nicht nur die erhofften Vorteile. Cyberkriminelle nutzen den Weg über das Internet ins Unternehmensnetzwerk, um dort Daten auszuspähen, Identitäten zu stehlen und Systeme lahmzulegen. Über unzureichend genutzte Netzwerkverbindungen könnten die Angreifenden auf die Server, die Endgeräte und auf die Speicherlösungen gelangen, die die Beschäftigten verwenden.

Die IT-Sicherheit muss erweitert werden: Schutz der Netzwerke

Wird das Unternehmen größer, steigt auch die Zahl der Nutzerinnen und Nutzer. Zusätzlich zu den erforderlichen Schutzmaßnahmen für Endpoints und Clouds kommen Themen wie Endpoint Management, sichere Server, sichere Vernetzung und geschützte Storage-Dienste hinzu.

Um die steigende Zahl an Endpoints abzusichern, bietet sich Dell SafeGuard and Response (VMware Carbon Black Cloud Endpoint Standard) an. Dell SafeGuard and Response ermöglicht es, Schadsoftware, unerwünschte Anwendungen und schädliche Aktionen innerhalb der eigenen Umgebung zu verhindern und alle erforderlichen Informationen bereitzustellen, um neue Bedrohungen oder Threat Actors zu erkennen, die möglicherweise auftreten.

Für den Schutz vor Endpoint-, Cloud- und Netzwerk-Risiken wird ab 50 Endpoints zudem SecureWorks Taegis XDR empfohlen. Secureworks Taegis XDR ist eine auf Bedrohungsdaten basierende Plattform für Sicherheitsanalysen mit integriertem Sicherheitskontext. Secureworks Taegis XDR ermöglicht es, komplexe Bedrohungen in der gesamten Endpunkt-, Netzwerk- und Cloud-Umgebung zu erkennen, zu untersuchen und darauf zu reagieren.

Für sichere Netzwerke sind zudem moderne Firewalls (Next Generation Firewalls) von zentraler Bedeutung, um die Datenverbindungen zu überwachen und zu kontrollieren. Damit wird die Schnittstelle zwischen dem Internet und den internen Netzwerken abgesichert. >>

Für Next Generation Firewalls gibt es verschiedene Optionen. Extended Technologies Complete (ETC) von Dell Technologies bietet umfassende, branchenführende Best-of-Breed-Partnerlösungen, die die Server-, Storage- und Netzwerkressourcen von Dell Technologies ergänzen:

- SonicWall bekämpft Cyberkriminelle mit Lösungen für die Erkennung und Verhinderung von Sicherheitsverletzungen in Echtzeit – einschließlich Firewalls der nächsten Generation.
- Die Sicherheitsbetriebsplattform von Palo Alto Networks kombiniert Netzwerk- und Cloud-Sicherheit mit Threat Intelligence und präzisen Analysen.
- Bei entsprechendem Bedarf kann auch SD-WAN (Software Defined WAN) zum Einsatz kommen, mit einem integrierten Firewall-Service, sodass Vernetzung und Netzwerksicherheit miteinander kombiniert werden.

Einsatz sicherer Server

Größer werdende Unternehmen verwenden häufig eigene Server zusätzlich zu den genutzten Cloud-Diensten. Hier spricht man dann von Hybrid Cloud Computing als Kombination von Cloud Services und On-Premises-IT. Die Server übernehmen zentrale Aufgaben im Unternehmensnetzwerk und müssen besonders geschützt werden, da die Endgeräte als Clients von den funktionierenden Serverdiensten abhängen.

Neben speziellen Lösungen zum Schutz der Server kommt es auf die integrierte Server-Sicherheit an, also auf ihre Eigensicherheit. Hier empfiehlt es sich, auf professionelle Systeme zu setzen, die nach dem „Security by Design“-Prinzip entwickelt wurden.

Die Dell PowerEdge Server wurden nach dem „Security by Design“-Prinzip entwickelt.

Beispiele dafür sind Serversysteme mit Sicherheitsfunktionen, die in die Plattform für Dell PowerEdge integriert sind. Sie reichen von der Zugriffskontrolle über die Datenverschlüsselung bis hin zur Lieferkettensicherheit. Dazu zählen VMware Carbon Black on Dell PowerEdge Server, Live-BIOS-Scanning, UEFI Secure Boot Customization, RSA SecurID MFA, Secure Enterprise Key Management (SEKM), Secured Component Verification (SCV), verbesserte System-Erase-Funktion, automatische Zertifikatregistrierung und -verlängerung, Cipher Select und CNSA-Support. Alle Funktionen nutzen Intelligenz und Automatisierung, um vor Bedrohungen zu schützen.

Sicherheit und Management für Storage-Lösungen

Nicht nur mit der Zahl der Beschäftigten nimmt das Datenwachstum immer weiter und immer schneller zu. Vielmehr ist es ist ein genereller Trend in der Digitalen Transformation. Da die Daten nicht nur das „neue Öl“ der digitalen Geschäftsmodelle sind, sondern entsprechend auch im Fokus der Cyberattacken stehen, müssen die Storage-Lösungen besonders geschützt und professionell administriert werden.

Um die Aufwände für den Schutz und das Management zu mindern, bieten sich Storage-Lösungen aus der Cloud an. Bei Bedarf können auch On-Premises-Storagelösungen genutzt werden oder eine Mischung aus On-Premises und Cloud.

Datensicherung und Recovery: Für den Ernstfall gerüstet

Die um sich greifenden Ransomware-Attacken sind nur ein Beispiel dafür, dass Cyberattacken zu Datenverlust, Systemausfall, Produktivitätsverlust und sogar Betriebsunterbrechung führen können. Entscheidend ist es deshalb, dass die komplette IT-Infrastruktur und damit sämtliche Daten über ein Backup gesichert werden. Kommt es zu einem Vorfall, müssen die betroffenen Daten schnell wiederhergestellt werden können. Hierfür werden Cyber-Recovery-Lösungen benötigt.

APEX Backup Services eignen sich für Unternehmen jeder Größe. Die Services sind eine Cloud-basierte Data-Protection-Lösung zu vorhersehbaren, kontrollierbaren Kosten. Die Lösung wird innerhalb weniger Minuten bereitgestellt und bietet unbegrenzte On-Demand-Skalierung, um sicherzustellen, dass wachsende Datenvolumen immer geschützt sind. Unternehmen mit mindestens 50 Endpunkten können auf diese Lösung zurückgreifen.

APEX Backup Services bieten Data Protection und Governance für SaaS-Anwendungen wie Microsoft 365, Salesforce und Google Workspace, für Endpunkte wie Desktop-PCs/Laptops und Mobile Devices und für hybride Workloads (Virtualisierung – VMware & Hyper-V, Datenbanken – Oracle & SQL, Dateiserver – Windows & Linux und NAS). >>

Für Backups, die für große Workloads On-Premises erstellt werden sollen, bieten sich PowerProtect-Appliances an. PowerProtect vereinfacht die Data-Protection-Abläufe und senkt die Risiken, sodass die Service Level Agreements (SLAs) bei gleichzeitiger Kostensenkung erfüllt werden können.

Die Appliances der PowerProtect-DP-Serie sind die integrierten Appliance-Lösungen aus dem PowerProtect-Appliances-Portfolio. Neben beschleunigten Backups und Recoverys bietet diese neue Generation der integrierten Data Protection Appliances (IDPA) Replikation, Deduplizierung sowie sofortigen Zugriff und Wiederherstellung dank enger VMware-Integration.

Appliances der Serie Dell EMC PowerProtect DD sind die bevorzugten Ziel-Appliances für Dell EMC PowerProtect Data Manager und unterstützen außerdem die Verbesserungen der Data Protection Suite zusammen mit vielen anderen Backupanwendungen und -softwareprogrammen von Drittanbietern.

Gegen den Fachkräftemangel: Managed Services

Gerade kleine und mittlere Unternehmen leiden unter dem bekannten IT-Fachkräftemangel. Bereits die zunehmende Zahl an Endpoints erhöht den Administrationsaufwand in wachsenden Unternehmen. Hinzu kommen die Aufgaben für Management und Absicherung der Netzwerke, Server und Speicherlösungen.

Um die eigene IT-Administration und die interne Security zu entlasten, bieten sich Managed Services an. Diese können noch weitaus mehr bieten als den Zugriff auf personelle Ressourcen und Expertise. Was durch Security Services noch alles möglich wird, zeigt das nächste Kapitel.

Dell PowerProtect-Appliances vereinfachen die Data-Protection-Abläufe.

Security as a Service

Fachkräftemangel kompensieren, Cyberrisiken minimieren

Nicht nur kleine und mittlere Unternehmen können von Security-Services profitieren. Doch im Mittelstand ist der Fachkräftemangel in der Cybersicherheit besonders zu spüren, bei gleichzeitig hohem Cyberrisiko. Ein Anbieter wie Dell Technologies hilft dabei, wirksame Security-Konzepte zu entwickeln und umzusetzen und bietet Security-Services und -Lösungen aus einer Hand, um bestehende Lücken in der Cybersicherheit eines Unternehmens zu schließen.

Die Cybersicherheit braucht den Lückenschluss

62 Prozent der Unternehmen befürchten, dass ihre Maßnahmen zur Datensicherung nicht ausreichen könnten, um mit Malware-Attacken wie etwa einem Ransomware-Angriff fertig zu werden, so der Dell Technologies 2021 Global Data Protection Index. 74 Prozent stimmen der Aussage zu, dass sie durch die wachsende Anzahl an Home-Office-Mitarbeitern einer steigenden Gefahr von Datenverlust ausgesetzt sind. Über zwei Drittel der Befragten (67 %) sind sich nicht sicher, ob sie nach einer Cyberattacke oder einem anderen Datenverlust ihre geschäftskritischen Daten wiederherstellen könnten.

Offensichtlich sind sich viele Unternehmen im Mittelstand der Cyberrisiken bewusst und erkennen, dass ihre bestehenden Maßnahmen für Cybersicherheit nicht ausreichen könnten, wenn es um drohenden Datenverlust geht. Trotzdem verbessert sich die Situation in der Cyber Security vieler Unternehmen seit Jahren nicht. Ein wesentlicher Grund: Es fehlt der Zugang zu den notwendigen Fachkräften und zu professionellen, bezahlbaren Lösungen. Selbst wachsende Unternehmen, die mehr und mehr Beschäftigte einstellen, können ihren Bedarf an Security-Fachkräften nicht decken – es gibt einfach zu wenige davon. Die verbleibenden wenigen Fachkräfte haben zudem meist hohe Honorarvorstellungen und suchen nach Tätigkeiten, die sich spannender anhören, als ein Mittelstandunternehmen abzusichern. Der Mittelstand in Deutschland kann es sich aber nicht leisten, die Sicherheitslücken offen zu lassen.

Managed Services und Security as a Service

Sowohl für Betrieb und Administration der IT als auch für die Cybersicherheit bieten sich professionelle, bezahlbare Services für den Lückenschluss an. Wichtige Funktionen und Aufgaben der Cybersicherheit wie das Erkennen und Abwenden von Angriffen (Incident Response), die aktive und vorbeugende

>>

Suche nach Cyberbedrohungen (Threat Hunting) und das Schließen von Schwachstellen (Vulnerability Management) können oftmals intern nicht umgesetzt werden, wohl aber durch die Beratung und Unterstützung seitens externer IT-Security-Spezialistinnen und -Spezialisten.

Dabei sollte ein Unternehmen darauf achten, dass die externen Services möglichst unkompliziert und einheitlich bezogen werden können, damit nicht das Management der Security Services zum großen und komplizierten Aufwand im eigenen Unternehmen wird. Ideal erscheint ein Anbieter, der möglichst viele Komponenten des Sicherheitskonzeptes bereitstellt und als zentraler Ansprechpartner für den Lückenschluss in der Cybersicherheit fungiert. Genau das bietet Dell Technologies mit seinen Lösungspartnerschaften in der Security.

Mit Services Angriffe erkennen und abwehren, aber auch für die notwendige Datensicherung sorgen

Mit Dell Technologies haben auch kleine und mittlere Unternehmen Zugang zu Lösungen und Services wie Managed EDR (Managed Endpoint Detection and Response), Managed XDR (Managed Extended Detection and Response) und Services für Backup und Cyber Recovery.

VMware Carbon Black EDR

Endpoint Security Services bieten individuelle Unterstützung, die kleine und mittlere Unternehmen zur Identifizierung von Risiken, zur Implementierung von Lösungen und zur Abwehr künftiger Bedrohungen benötigen.

VMware Carbon Black Endpoint führt verschiedene Funktionen für die Endpunktsicherheit in einem Agent und einer Konsole zusammen, wodurch Unternehmen schneller und effizienter agieren können. VMware Carbon Black Cloud ist eine SaaS-Lösung (Software as a Service), die die oftmals im Mittelstand noch fehlenden Lösungen Next-Generation Anti-Virus (NGAV), Endpoint Detection and Response (EDR) und Advanced Threat Hunting als Service aus der Cloud bereitstellen kann.

SecureWorks Taegis XDR

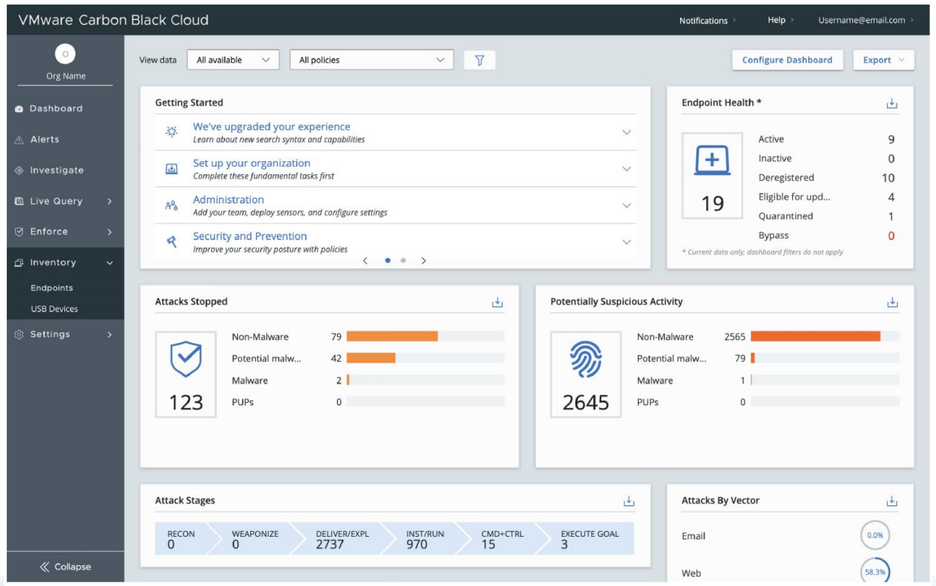
Bereits ab 50 Beschäftigten bietet sich der Einsatz einer „Managed Detection and Response"-Lösung auf Basis von SecureWorks Taegis XDR an. Dell Technologies Managed Detection and Response mit Unterstützung von Secureworks Taegis XDR ist ein vollständig verwalteter 24x7-End-to-End-Service zur Überwachung, Erkennung, Untersuchung und Reaktion auf Bedrohungen in der gesamten IT-Umgebung.

Unternehmen haben damit Zugang zu dem Fachwissen, das Dell Technologies durch jahrelange Erfahrung beim Schutz von Unternehmen auf der ganzen Welt gewonnen hat, und auf die Leistung der offenen Secureworks Taegis XDR Security-Analytics-Software, die auf mehr als 20 Jahren Know-how in der operativen Informationssicherheit, der Analyse und Erforschung realer Bedrohungen und umfassender Erfahrung in der Erkennung und Reaktion auf Advanced Threats basiert.

APEX Backup Services von Dell Technologies

APEX Backup Services von Dell Technologies bieten hochleistungsfähige und sichere Backups aus der Cloud, langfristige Aufbewahrung und automatisierte Compliance. Mit einer zentralen Konsole erhalten mittelständische Unternehmen vollständige Transparenz und eine einheitliche Managementerfahrung für SaaS-Anwendungen, Endpunkte und hybride Workloads. APEX Backup Services bieten Skalierbarkeit nach Bedarf und sorgen für planbare und kontrollierbare Kosten.

Es zeigt sich: Mit modernen End-to-End-Lösungen und Security-Services von Dell Technologies erhalten mittelständische Unternehmen das Vertrauen, die Kontrolle und die Skalierbarkeit, die sie benötigen, um die gerade bei Mittelständlern drängenden Sicherheitsherausforderungen zu bewältigen.



Dell SafeGuard and Response Offer Matrix	Next Generation AntiVirus (NGAV)	Behavioral Endpoint Detection & Response (EDR)	Taegis™ XDR
VMware Carbon Black Cloud Endpoint Standard	Yes	Yes	
VMware Carbon Black Cloud Endpoint Standard + Secureworks Taegis™ XDR	Yes	Yes	Yes

Dell SafeGuard and Response mit VMware Carbon Black und SecureWorks Taegis XDR bietet umfassende Sicherheitslösungen.

Bei Fragen können Sie uns jederzeit anrufen oder mit uns chatten:

0800 270 33 55

WhatsApp

Bitte teilen

DELL Technologies

Copyright © 2022 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Ultrabook, Celeron, Celeron Inside, Core Inside, Intel, Intel Logo, Intel Atom, Intel Atom Inside, Intel Core, Intel Inside, Intel Inside Logo, Intel vPro, Itanium, Itanium Inside, Pentium, Pentium Inside, vPro Inside, Xeon, Xeon Phi, and Xeon Inside are trademarks of Intel Corporation in the U.S. and/or other countries. Other trademarks may be trademarks of their respective owners. This brochure is for informational purposes only.