heise Business Services

Ein eBook von

Powered by DELL EXPERT NETWORK

Einfach, effektiv und kostengünstig

Sicherheit für kleine und mittlere Unternehmen

- ☐ **Ransomware**
  So schützen sich KMU vor Erpressungstrojanern
- ☐ **Data Protection**
  Das sind entscheidende Lösungsmerkmale
- ☐ **Managed Security Services**
  Verbündete im Kampf gegen Cyberbedrohungen

Titelbild: Aleksandra Bogusławska, Unsplash

Bild: Usis, BigStock

Editorial

Wenn es um IT-Sicherheit geht, unterscheiden sich die Anforderungen von kleinen und mittleren Unternehmen (KMU) nicht wesentlich von denen großer Organisationen. Auch sie benötigen einen ganzheitlichen Schutz, der alle Systeme, Netze und Kommunikationskanäle umfasst und bei Sicherheitsvorfällen schnelles und effektives Agieren ermöglicht.

Nur so lassen sich Gefahren wie Ransomware-Attacken abwehren – eine für KMU potenziell existenzgefährdende Bedrohung, die in den vergangenen Jahren drastisch zugenommen hat. Ein mehrstufiges Sicherheitskonzept, das Angriffe durch Erpressungstrojaner zuverlässig erkennt und abwehrt, ist deshalb unabdingbar für die Risikominimierung.

Und für den Schutz und zur Sicherung ihrer Daten benötigen KMU nicht nur leistungsfähige Lösungen, die bestimmte Kriterien erfüllen müssen, sondern auch entsprechendes Knowhow.

Da es jedoch gerade für kleine und mittlere Unternehmen nahezu unmöglich ist, sämtliche sicherheitsrelevanten Anforderungen in Eigenregie abzudecken, ist die Zusammenarbeit mit externen Experten der beste Weg, maximale IT-Sicherheit zu erreichen, ohne dass Kosten und Aufwand aus dem Ruder laufen.

Lesen Sie in diesem eBook, …

- welche Komponenten ein Sicherheitskonzept zur Ransomware-Abwehr umfassen sollte,
- welche Eigenschaften eine Data-Protection-Lösung aufweisen sollte und
- welche Vorteile sich aus der Zusammenarbeit mit einem Managed-Security-Service-Providern (MSSP) ergeben.

Bernd Müller &
Dr. Thomas Hafen

Heise Medien GmbH & Co.KG
Abt. Heise Business Services
Hans-Pinsel-Straße 10b
85540 Haar bei München

Registergericht:
Amtsgericht Hannover HRA 26709

Persönlich haftende Gesellschafterin:
Heise Medien Geschäftsführung GmbH

Registergericht:
Amtsgericht Hannover, HRB 60405

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

Verantwortlich für den Inhalt:
Heise Business Services
Thomas Jannot, tj@heise.de

Haben Sie Fragen zu diesem eBook oder haben Sie Interesse an einer eigenen Produktion, dann schicken Sie bitte eine E-Mail mit dem Betreff **„HBS-eBook“** an hbs@heise.de

Inhalt

ÜBER DIE AUTOREN

Bernd Müller hat Physik, Journalistik und Innovationsmanagement studiert. Er war Redakteur bei bekannten Wissenschafts- und Wirtschaftsmedien. Heute arbeitet er als freier Autor für Magazine und Technologieunternehmen. Seine Themenschwerpunkte sind IT, Energie und Management.

Dr. Thomas Hafen war über 15 Jahre als Redakteur, Moderator und Manager für verschiedene IT-Fachverlage tätig. Seine fachlichen Schwerpunkte liegen in den Bereichen Digitale Transformation, Cloud Computing und Advanced Analytics. Thomas Hafen lebt und arbeitet heute als freier Journalist und Moderator in München.

Bild: Panoramaimages, BigStock

Ransomware – so schützen sich KMU vor Erpressungstrojanern

Erpressungstrojaner können für KMU zur existenzbedrohenden Gefahr werden. Ein mehrstufiges Sicherheitskonzept, das Ransomware-Angriffe zuverlässig erkennt und abwehrt, ist deshalb eine unabdingbare Komponente der Risikominimierung.

Thomas Hafen

Die Bedrohung durch Erpressungstrojaner hat in den vergangenen Jahren kontinuierlich zugenommen. Waren laut dem 2020 Cyberthreat Defense Report der CyberEdge Group 2017 noch 55 Prozent der Unternehmen von Verschlüsselungsattacken betroffen, so meldeten zwei Jahre später bereits 62 Prozent entsprechende Angriffe. Vor allem kleine und mittlere Unternehmen geraten ins Visier der Kriminellen. Bereits 2018 zielten fast zwei Drittel aller Ransomware-Attacken auf kleine Unternehmen. Darüber hinaus sind dem CyberEdge-Report zufolge immer mehr Unternehmen bereit, Lösegeld für ihre Daten zu bezahlen. Betrug der Anteil 2018 noch unter 40 Prozent, so stieg er innerhalb von zwei Jahren auf fast 58 Prozent. Die durchschnittliche Lösegeldsumme beträgt nach Berechnungen des Softwareanbieters Datto 5.900 US-Dollar. Die Kosten durch Betriebsunterbrechungen sind allerdings nicht nur um das 23-Fache höher als das erpresste Lösegeld, sie steigen Jahr um Jahr auch noch um 200 Prozent!

Anatomie eines Ransomware-Angriffs

Ransomware zielt darauf ab, Nutzern den Zugang zu Computersystemen und den sich darauf befindenden Informationen zu verwehren und sie nur gegen Zahlung eines Lösegeldes wieder freizugeben. Einfache Varianten blockieren beim Start des Rechners mit einem Sperrbildschirm den Zugriff, die meisten befallen gezielt Nutzerdaten und verschlüsseln sie, andere machen auch das Betriebssystem oder sogar die Speicher-Hardware unbrauchbar. Aufgrund der zunehmenden Nutzung von Cloud-Ressourcen suchen aktuelle Trojaner gezielt nach typischen Cloud-Speicheranwendungen wie Dropbox oder OneDrive, um nicht nur die lokal gespeicherten Daten, sondern auch die im Netz befindlichen Kopien unbrauchbar zu machen.

Bild: Pavlo Kolotenko, BigStock

Für die Infektion nutzen die Angreifer vor allem Phishing, indem sie E-Mails mit kompromittierten Links oder Anhängen versenden. Öffnet der Adressat die Datei oder klickt er auf den Link, wird der Trojaner aktiviert und beginnt im Hintergrund mit der Verschlüsselungsarbeit. Oft ist die Ransomware-Komponente mit anderen Tools aus dem Malware-Baukasten kombiniert, die beispielsweise Kontakt zu einem Command-and-Control-Server aufnehmen, um Daten und Passwörter an die Angreifer zu senden oder weitere Schadkomponenten nachzuladen. Manche Trojaner missbrauchen darüber hinaus Schwachstellen in Applikationen, Betriebssystemen und Netzwerkprotokollen, um sich im Firmennetz auszubreiten und weitere PCs oder Server zu befallen. So nutzte beispielsweise der 2017 bekannt gewordene Erpressungstrojaner Wannacry eine Sicherheitslücke im Windows-Dateifreigabesystem SMB (Server Message Block), um weitere Rechner zu kompromittieren.

Was KMU gegen Erpressungstrojaner tun können

Knappe Budgets und ein Mangel an Fachpersonal stellen kleine und mittlere Unternehmen bei der Abwehr und Bekämpfung von Ransomware vor besondere Herausforderungen. Um finanzielle und personelle Ressourcen optimal zu nutzen, sollten sich die Maßnahmen deshalb auf eine effektive Risikominimierung konzentrieren. Speziell auf KMU zugeschnittene Sicherheitslösungen und Service-Angebote, wie sie etwa Dell Technologies bietet, erleichtern diese Aufgabe erheblich.

Folgende Aspekte spielen beim Kampf gegen Ransomware die größte Rolle:

- **Abwehr:** Am besten ist es natürlich, wenn es gar nicht erst zu einer Infektion mit Ransomware kommt. Daher ist ein effektiver Schutz von Endgeräten und der E-Mail-Kommunikation entscheidend für den Kampf gegen Erpressungstrojaner. Neben einer signaturbasierten Erkennung, die bereits bekannte Trojaner identifiziert, spielt die verhaltensbasierte Detektion eine große Rolle. Sie erkennt beispielsweise, wenn ein Programm ohne Berechtigung auf Dateien zugreift und diese verschlüsselt, und blockiert es. Moderne Lösungen wie Dell SafeGuard and Response nutzen außerdem Künstliche Intelligenz und maschinelles Lernen, um Angriffe erkennen und abwehren zu können. Zusätzlichen Schutz können in die Hardware integrierte Sicherheitsmechanismen wie „SafeID" von Dell bieten. SafeID speichert die Zugangsdaten für ein Endgerät auf einem dedizierten Sicherheitschip und schottet sie so vor Malwareangriffen von außen ab..

- **Schulung:** Die besten Sicherheits-Tools helfen wenig, wenn Mitarbeiter bereitwillig auf verdächtige Links klicken oder unkritisch jeden Dateianhang öffnen. Schulungen und Trainings sind daher ein wichtiger Baustein jeder Sicherheitsstrategie. Dabei kommt es vor allem auf Regelmäßigkeit und Wiederholung an. Nur wenn das richtige Verhalten den Mitarbeitern in „Fleisch und Blut" übergeht, werden sie sich auch in Stresssituationen richtig verhalten.

> Ransomware-Infektionen erfolgen häufig via Phishing – dazu versenden die Angreifer E-Mails mit kompromittierten Links oder Anhängen.

- **Qualifiziertes Backup-Konzept:** Der beste Schutz gegen Ransomware ist ein qualifiziertes Backup-Konzept, in dem alle zu sichernden Systeme und Daten, die Art der Sicherung und regelmäßige Wiederherstellungstests definiert sind. Laut dem DsiN-Praxisreport 2020 Mittelstand@IT-Sicherheit der Initiative Deutschland sicher im Netz verfügen allerdings nur 30 Prozent der KMU in Deutschland über ein solches Konzept. Ein Viertel führt gar keine oder nur unregelmäßige Sicherungen durch – angesichts der zunehmenden Bedrohungen eine höchst gefährliche Strategie. Dabei ist die Umsetzung eines Backup-Konzepts gar nicht so kompliziert. Hersteller Dell bietet beispielsweise mit Dell EMC PowerProtect Cyber Recovery eine Lösung, die Datensicherungs-Workflows automatisiert, geschäftskritische Daten vor unautorisiertem Zugriff schützt und im Schadensfall eine schnelle Wiederherstellung ermöglicht.

Fazit

Erpressungstrojaner können für KMU zur existenzbedrohenden Gefahr werden. Ein mehrstufiges Sicherheitskonzept, das Ransomware-Angriffe zuverlässig erkennt und abwehrt, ist deshalb eine unabdingbare Komponente der Risikominimierung. Es muss mit Security-Awareness-Schulungen der Mitarbeiter kombiniert werden, um Bewusstsein für die Gefahren zu schaffen und richtiges Verhalten einzuüben. Die wichtigste Komponente in der Ransomware-Abwehr ist und bleibt allerdings ein qualifiziertes Backup-Konzept. Kommt es trotz aller Vorsichtsmaßnahmen doch zu einer Infektion, können die verschlüsselten Daten schnell und zuverlässig wiederhergestellt werden. Um dieses Konzept wirkungsvoll umsetzen zu können, sollten sich kleine Unternehmen Unterstützung holen, wie sie etwa die Dell Technologieberater bieten. Sie helfen, sich in der Vielzahl der Technologien zurechtzufinden und bieten fortlaufenden Support. ■

Bilder: LinchK32 / visual28, BigStock

Bild: Monsitj, BigStock

Data Protection – das sind entscheidende Lösungsmerkmale

Auch kleine und mittelständische Unternehmen brauchen leistungsfähige Lösungen zum Schutz und zur Sicherung von Daten. Hierbei gilt es, auf eine Reihe entscheidender Kriterien zu achten.

Bernd Müller

Die Corona-Pandemie ist ein Schub für die Digitalisierung. Das ist gut, setzt aber vor allem kleine und mittelständische Unternehmen noch stärker unter Druck. Die Mengen an Daten, Nutzern und Apps steigen schneller als zuvor, Daten wandern in die Cloud, die Virtualisierung von IT-Architekturen nimmt zu – das Einzige, was nicht mehr wird, ist das Geld, mit dem all das bezahlt werden muss. Zusätzlich hängt das Thema Datenschutz und IT-Sicherheit wie ein Damoklesschwert über den IT-Abteilungen. Erfreulich ist, dass die Unternehmen dennoch handeln: Laut der ESG-Erhebung „2020 Technology Spending Intentions" hatten das Backup und die Wiederherstellung von Daten im vergangenen Jahr oberste Priorität bei der IT-Modernisierung. Backup und Archivierung waren der zweitwichtigste Anwendungsfall für die Cloud-Nutzung.

Bild: Klyaksun, BigStock

Auf die Umsetzung kommt es an

Problem erkannt, Gefahr aber noch nicht gebannt, denn bei der Einrichtung einer Sicherheitsarchitektur kommt es drauf an, wie diese umgesetzt wird: So sicher, aber auch so einfach wie möglich und mit dem größten Nutzen pro Euro. soll Unternehmensdaten in kleinen und mittelständischen Unternehmen vor dem versehentlichen Verlust oder Beschädigung sowie vor Diebstahl und bösartigen Angriffen schützen. Das umfasst Aufgaben wie Backups von Daten, die vor Ort, an externen Standorten und/oder in der Cloud gespeichert sind, und den Einsatz von Technologien, Policies und Verfahren zum Schutz von Datenbeständen vor Malware-Attacken, Computerausfällen sowie Einrichtungs-, Anwendungs- und Nutzerfehlern.

Sechs Eigenschaften, die eine Data-Protection-Lösung aufweisen sollte

Das sind die Basics. Darüber hinaus sollten KMU auf der Suche nach einer Lösung zur Datensicherung auf folgende sechs Eigenschaften achten:

1. Einfachn

Die Lösung sollte Hardware und Software in einer einzigen Anwendung vereinen und das Monitoring und Management mit einer intuitiven Nutzeroberfläche erlauben, auch wenn dahinter komplexe Infrastrukturen aus mehreren Plattformen hängen. Alle Abläufe wie die Erkennung von Angriffen oder der Schutz von Daten in der Cloud sollten automatisiert ablaufen. Dazu gehören automatisierte Datenbackup-Lösungen für VMware-basierte Hybrid-Cloud-Umgebungen und moderne „Tanzu"-Anwendungen.

2. Skalierbar

Auch kleinere Unternehmen – und ihre Datenmengen – wachsen. Daher sollte die Lösung viel Spielraum für Erweiterungen lassen, bis in den Petabyte-Bereich. Sie sollte Daten schützen, egal wo sich diese befinden: lokal, virtualisiert oder in Public- oder Hybrid-Clouds.

3. Effizient

Natürlich kann man Berge an Festplatten anschaffen oder Cloudspeicher buchen, doch das ist teuer. Backup-Lösungen sollten also möglichst große Datenmengen mit möglichst wenig Speicher sichern.

4. Schnell

Ein hoher Datendurchsatz und viele Backups in kürzerer Zeit senken den Speicherbedarf und reduzieren die Anforderungen an die Übertragungsbandbreite.

5. Kostengünstig

Für 35 % der IT-Manager, die mit der Implementierung von DataProtection-Prozessen und -Technologien betraut sind, sind regelmäßig die Kosten eine der größten Herausforderungen. Eine Technologie zur Deduplizierung von Daten hilft, Speicherplatz zu sparen und reduziert die Übertragungskosten. Je nach Anwendungsfall erreicht eine gute Lösung Deduplizierungsraten von mindestens 10 zu 1 bis idealerweise über 100 zu 1, was bedeutet: 100 Petabyte an Daten lassen sich in weniger als einem Petabyte Speicherplatz sichern. Oft gibt aber auch versteckte Kosten, etwa für eine längere Support-Laufzeit – es lohnt sich also, auch anderweitig genau hinzusehen. Ein Online-Kostenkalkulator hilft, die echten Kosten und Einsparungen zu berechnen.

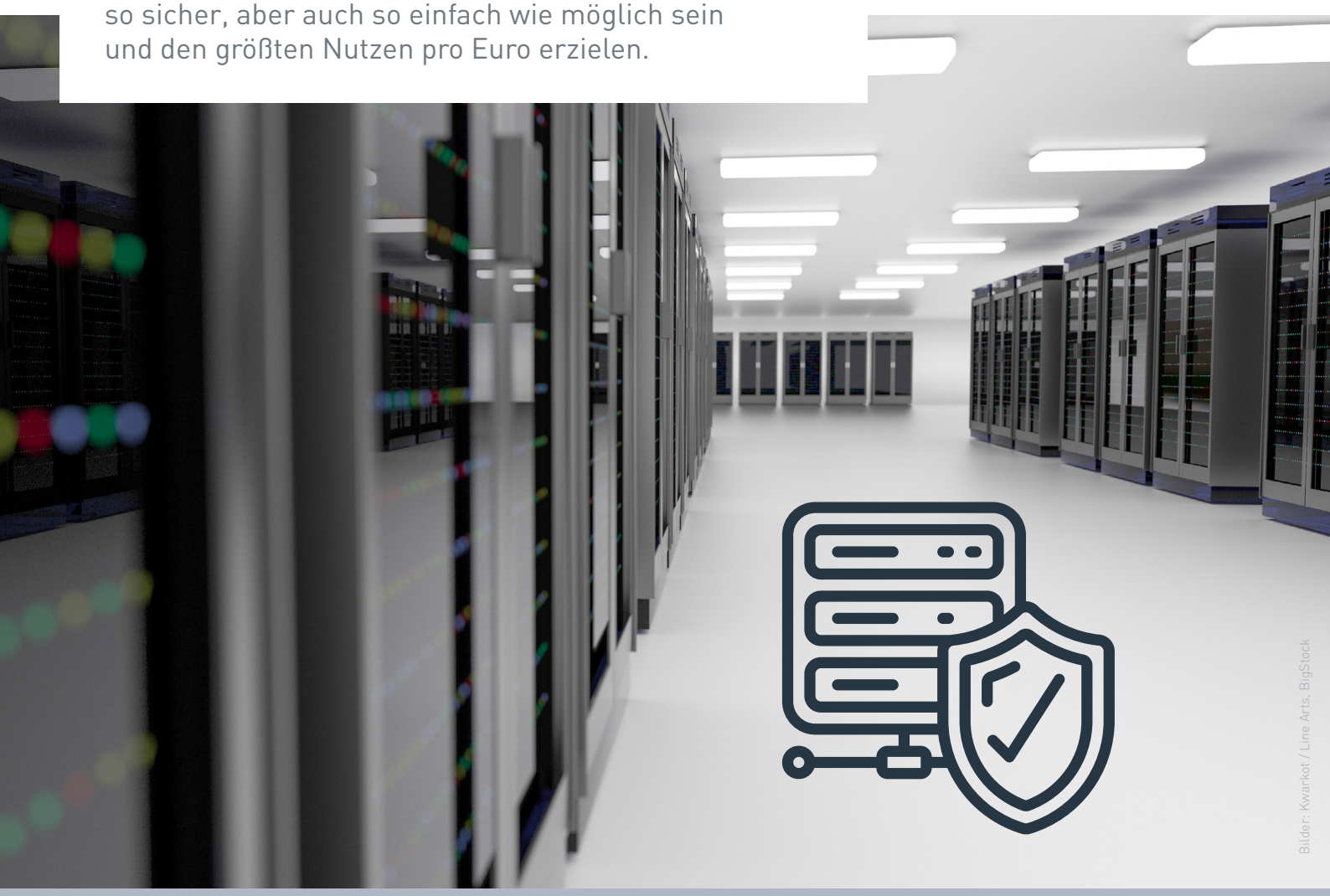
6. Zukunftssicher

Viele KMU zögern mit der Anschaffung einer umfassenden Sicherheitslösung, weil sie befürchten, die Lösung könnte bereits in wenigen Monaten veraltet sein – was einerseits stimmt, da sich die Technik rasant weiterentwickelt. Andererseits geben gute Anbieter langfristige Garantien für die Optimierung des IT-Lebenszyklus. Ein Beispiel: eine dreijährige Zufriedenheitsgarantie, nahtlose Upgrades und sorgenfreie Datenmigrationen.

Orientierungshilfe Gartner Magic Quadrant

Zugegeben, all diese Eigenschaften bei der Vielzahl von Angeboten auf dem Markt abzufragen ist eine Fleißaufgabe. Da hilft ein Blick in Gartners Magic Quadrant Data Center Backup & Recovery Solutions 2020. Dort ist Dell Technologies im Gartner Quadrant der „Leader" weit vorn aufgeführt – wie schon seit dem Jahr 1999. Die Autoren der Studie loben vor allem die Effizienz bei der Datenreduzierung, die hohe Qualität und die niedrige Ausfallrate der Produkte sowie die globale Präsenz des Anbieters. ■

> Die Umsetzung einer Sicherheitsarchitektur sollte so sicher, aber auch so einfach wie möglich sein und den größten Nutzen pro Euro erzielen.



Bilder: Kwarkot / Line Arts, BigStock

Foto: AndreyPopov, BigStock

Managed Security Services: Verbündete im Kampf gegen Cyberbedrohungen

Wenn es um IT-Sicherheit geht, unterscheiden sich die Anforderungen von KMU nicht wesentlich von denen großer Organisationen. Auch sie benötigen einen Schutz, der alle Systeme, Netze und Kommunikationskanäle umfasst.

Thomas Hafen

IT-Sicherheit hat für kleine und mittlere Unternehmen eine große Bedeutung. Dem DsiN-Praxisreport 2020 Mittelstand@IT-Sicherheit der Initiative „Deutschland sicher im Netz" zufolge spielt die Integrität, Vertraulichkeit und Verfügbarkeit von Unternehmensdaten für 87 Prozent der KMU eine wichtige Rolle, bei 38 Prozent hängen Betriebsabläufe unmittelbar von der IT ab.

In den meisten Unternehmen mangelt es allerdings an Fachpersonal, um die notwendige IT-Sicherheit auch wirklich zu gewährleisten. Nur in 17 Prozent der für den Praxisreport befragten Unternehmen ist ein IT-Sicherheitsbeauftragter für die IT-Sicherheit verantwortlich, in 28 Prozent der Betriebe muss sich jeder Mitarbeiter selbst um den Schutz seiner Hard- und Software kümmern. Diese Nachlässigkeit hat Folgen: Rund die Hälfte der Studienteilnehmer war bereits mit Cyberangriffen konfrontiert, 74 Prozent der betroffenen KMU mussten Schäden verzeichnen, bei 14 Prozent kam es zu erheblichen oder sogar existenzbedrohenden Belastungen.

Externe Unterstützung noch zu wenig genutzt

Es ist nachvollziehbar, dass sich kleine und mittlere Unternehmen keine große IT-Sicherheitsmannschaft leisten können – ganz abgesehen davon, dass der Markt für Security-Experten praktisch leergefegt ist. Weniger verständlich ist jedoch, warum viele KMU die Unterstützung nicht wahrnehmen, die staatliche Stellen und Verbände zur Verfügung stellen. Nur 20 Prozent nutzen beispielsweise IT-Sicherheitsstandards, wie sie das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit seinem IT-Grundschutz-Kompendium formuliert hat. Seit Januar 2021 bietet zudem die Transferstelle IT-Sicherheit im Mittelstand (TISiM) umfangreiche Informationen und Hilfsangebote für kleine und mittlere Unternehmen. Auch die Plattform Mittelstand Digital informiert KMU über die wichtigsten Aspekte der IT-Sicherheit.

> Noch nutzen zu wenige KMU die Security-Unterstützung von staatlichen Stellen und Verbänden.

Hilfe von außen

Für alle diese Hilfsangebote gilt allerdings, dass ihre Umsetzung meist nicht ohne externe Hilfe gelingt. Daher sind KMU gut beraten, mit Managed Security Service Providern (MSSP) zusammenzuarbeiten. Als Serviceorganisation eines Herstellers wie Dell oder als eigenständiges Unternehmen sind sie auf das professionelle Monitoring und Management von Sicherheitslösungen spezialisiert. Zu den angebotenen Dienstleistungen gehören beispielsweise der Schutz vor Viren und Spam, die Erkennung und Abwehr eingedrungener Malware, das Management von Firewalls und anderen Security-Lösungen, die Einrichtung und der Betrieb eines Virtual Private Networks (VPN), das Patch-Management von Applikationen und die Überwachung sämtlicher sicherheitsrelevanter Systeme und Vorkommnisse in einem Security Operation Center (SOC).

Für KMU ergeben sich aus der Zusammenarbeit mit einem MSSP vor allem folgende Vorteile:

- **Zugang zu Expertenwissen:** Egal ob Applikations-, Netzwerk-, Cloud-, Server- oder E-Mail-Security: Die verschiedenen Bereiche der IT-Sicherheit sind derart komplex und umfangreich geworden, dass ein einzelner IT-Sicherheitsbeauftragter sie unmöglich in der Tiefe abdecken kann. MSSP haben dagegen für jedes Spezialgebiet einen Experten oder ganze Teams, die sich spezifisch um einen Sicherheitsaspekt kümmern. Kleine und mittlere Unternehmen erhalten so Zugang zu einem Wissen, das sie in Tiefe und Umfang niemals selbst aufbauen könnten.
- **Überprüfung der IT-Sicherheit:** Wie gut eine IT-Umgebung wirklich geschützt ist, zeigt sich erst im Stress-Test. MSSP nutzen daher Methoden wie „Red Teaming“, um die Sicherheit von Unternehmensnetzwerken zu überprüfen. MSSP-Mitarbeiter versuchen dabei als „Red Team“ in die Infrastruktur einzudringen, indem sie nach Schwachstellen in Applikationen und Protokollen suchen, Phishing-Mails versenden oder präparierte USB-Sticks als „Köder“ im Firmengebäude auslegen. Das Ergebnis solcher Tests ist ein ungeschminktes Bild der tatsächlichen IT-Sicherheit. Unternehmen erhalten darüber hinaus Auskunft über das sicherheitsrelevante Verhalten der Mitarbeiter und können so Schulungsbedarf identifizieren. Solche Security-Awareness-Trainings lassen sich entweder direkt beim MSSP buchen, oder dieser kann einen Schulungsanbieter empfehlen.
- **Leistungsfähigere Security-Tools:** Sicherheitslösungen wie SIEM (Security Information and Event Management) sind nicht nur komplex in der Implementierung und Bedienung, sie sind auch für die meisten KMU zu kostspielig. MSSP können die Tools für mehrere Kunden nutzen und so die Kosten für jeden Mandanten in einen erschwinglichen Bereich bringen.
- **Kürzere Reaktionszeiten:** Ein 24x7-IT-Security-Monitoring ist in kleinen und mittleren Unternehmen nicht zu leisten. MSSP betreiben dagegen in der Regel ein Security Operations Center (SOC), das rund um die Uhr die IT-Systeme ihrer Kunden überwacht. Wie bei den Tools verteilen sich die Kosten auf viele Schultern, so dass dieser Service auch für KMU erschwinglich wird.

- **Schutz vor rechtlichen Konsequenzen:** Unternehmen, die zu regulierten Branchen oder der kritischen Infrastruktur (KRITIS) gehören, unterliegen beim IT-Schutz besonderen rechtlichen Rahmenbedingungen. Dies betrifft auch viele kleine und mittlere Unternehmen wie Arztpraxen, Rechtsanwaltskanzleien oder Steuerberater. Alle Betriebe sind zudem verpflichtet, die Bestimmungen der Datenschutzgrundverordnung (DSGVO) einzuhalten. Kommen personenbezogene Daten durch unzureichenden IT-Schutz abhanden, drohen empfindliche Strafen. MSSP wissen, welche Zertifizierungen für die jeweilige Branche sinnvoll und nötig sind und wie man diese erhält. Im Schadensfall leisten sie außerdem Unterstützung bei der forensischen Aufklärung. Betroffene können damit gegenüber den Behörden nachweisen, dass ihre IT-Sicherheit dem geforderten Stand der Technik entspricht, und sich so vor rechtlichen Folgen schützen.

Fazit

Wenn es um IT-Sicherheit geht, unterscheiden sich die Anforderungen von KMU nicht wesentlich von denen großer Organisationen. Auch sie benötigen einen Schutz, der alle Systeme, Netze und Kommunikationskanäle umfasst, ganzheitlichen Schutz bietet und bei Sicherheitsvorfällen schnell und effizient reagiert. Alle diese Anforderungen mit internem Personal abzudecken, ist jedoch nur in den seltensten Fällen möglich. Die Zusammenarbeit mit Managed-Security-Service-Providern ist daher der beste Weg, größtmögliche IT-Sicherheit zu erreichen, ohne dass Kosten und Aufwand aus dem Ruder laufen. ■

Bild: AndreyPopov, BigStock

DELL Technologies

DELL EXPERT NETWORK
Das kostenlose Supportprogramm für IT-Berater und MSPs aus dem KMU-Segment in Deutschland

Das kostenlose Programm unterstützt IT-Berater und MSPs dabei, ihren Kunden aus dem KMU-Segment kosten- und zeitsparenden Support anzubieten.

Das Dell Expert Network bietet vier Hauptvorteile:

1. **DEDIZIERTER ACCOUNT MANAGER**

   Nach der Registrierung im Dell Expert Network werden Sie innerhalb von 3 Arbeitstagen von einem Account Manager kontaktiert, um die Teilnahme zu formalisieren. Dieser zentrale Ansprechpartner widmet sich Ihnen und den Bedürfnissen Ihrer Kunden, während er gleichzeitig die besten Deals und Werbeaktionen zur Verfügung stellt.

2. **SCHNELLER ZUGRIFF AUF SERVICE UND SUPPORT**

   Mit Dell TechDirect Tool sparen Sie wertvolle Zeit und können so Ihre Kunden schneller unterstützen, indem Sie den normalerweise erforderlichen Telefonanruf überspringen, wenn Sie Support benötigen. Mit dem TechDirect Tool können Sie selbst Tickets für den Kundensupport loggen und Ersatzteile versenden. Zudem erhalten Sie Zugriff auf das Live-Onlinereporting der Bestände der Kunden.

3. **DEN-PRÄMIEN**

   Sie erhalten 3 % von allen Einkäufen zurück, die Ihre Kunden aus dem KMU Segment bei Dell tätigen. Diese Prämien können Sie für zukünftige Käufe bei Dell nutzen.

4. **DELL FINANCIAL SERVICES FÜR MSP-SERVICES**

   Bieten Sie Ihren Kunden eine umfassende Lösung mit Dell Financial Services (DFS). Ihr dedizierter Account Manager unterstützt Sie dabei, mit den neusten DFS-Aktionen eine Zahlungslösung zusammenzustellen, die für Ihre Kleinunternehmerkunden geeignet ist.

Dell stellt für MSPs und IT-Berater, die Ihren Kleinunternehmerkunden die beste Beratung und den besten Service anbieten wollen, branchenführende End-to-End-Lösungen bereit. Und dank dem Dell Expert Network steht ihnen nun eine echte zentrale Anlaufstelle zur Verfügung.

DELL Technologies

Mehr Informationen finden Sie unter www.dell.de/expert-network

** Zahlungslösungen werden von Dell Financial Services L.L.C. oder seinen Partnern oder Bevollmächtigten („DFS“) für qualifizierte Kunden bereitgestellt und verarbeitet. Die Angebote sind in bestimmten Ländern möglicherweise nicht oder nur in abweichender Form verfügbar. Bei Verfügbarkeit können Angebote ohne vorherige Ankündigung geändert werden. Angebote unterliegen der Produktverfügbarkeit, geltendem Recht, einer Kreditgenehmigung, der von DFS bereitgestellten und akzeptierten Dokumentation sowie möglicherweise einer Mindesttransaktionsgröße. Die Angebote sind nicht für Privatkunden verfügbar. Dell EMC und das Dell EMC Logo sind Marken von Dell Inc. Möglicherweise gelten Einschränkungen und zusätzliche Anforderungen für Transaktionen mit Behörden oder öffentlichen Einrichtungen.

Bild: dolgachov, BigStock

Dell Expert Network: häufige Fragen & Antworten

Hier finden Sie Antworten auf die am häufigsten gestellten Fragen rund um das Dell Expert Network, das Partner-Support-Programm von Dell Technologies.

Was ist das Dell Expert Network?

Das „Dell Expert Network" ist ein Support- und Relationship Programm, entwickelt mit dem Ziel IT-Berater und IT-Dienstleister in der Zusammenarbeit mit ihren Kunden aus dem Small Business Segment zu unterstützen.

Wer kann teilnehmen?

Jeder IT-Berater / IT-Fachmann oder IT-Dienstleister, der für Kunden im Small Business Segment als Lösungs- oder Serviceanbieter tätig ist, mit Wohnsitz in Deutschland. Nicht teilnehmen können IT-Berater oder IT-Dienstleister, die bereits registrierte Wiederverkäufer sind oder Weiterverkauf als Kerngeschäft betreiben und davon abhängig sind sowie IT-Berater mit Wohnsitz außerhalb Deutschlands.

Warum sollte ich teilnehmen?

Sie profitieren von einem kostenlosen Support-Programm, mit dem Sie die Geschäftsbeziehungen zu Ihren Kunden ausbauen und entwickeln können. Ein dedizierter Account Manager unterstützt Sie dabei als Ihr Ansprechpartner bei Dell. Weiter profitieren Sie von vielen kostenlosen Vorteilen, sobald Ihre Registrierung geprüft und genehmigt ist.

Wie funktioniert das Prämienprogramm?

Für jede Ihrer Dell Produktempfehlungen an Ihre Kunden, die zu einem Auftrag bei Dell führen, der Ihre Dell Expert ID beinhaltet, erhalten Sie Prämien in Form von 3% vom Kaufbetrag. Prämien können bei einem Kauf aus der breiten Auswahl an Dell Produkten eingelöst werden.

Was ist die Dell Expert ID?

Dell Expert ID ist ein eindeutiges Kennzeichen, dass als Anerkennung für qualifizierte Einkäufe von Ihnen und Ihren kleinen Geschäftskunden dient.

Kann ich Prämien auch für meine eigenen Einkäufe oder nur für die meiner Kunden erhalten?

Ja. Sie werden mit Prämien auch für Ihre eigenen Einkäufe belohnt. Sie müssen dazu Ihre Dell Expert ID benutzen.

Sind meine Prämien auf andere IT-Berater, Familie oder Freunde im Dell Expert Network-Programm übertragbar?

Nein. Alle von einem IT-Berater gesammelten Prämien sind personengebunden, nicht übertragbar und dürfen nicht an andere Programmteilnehmer oder an Dritte vergeben werden.

Bild: dolgachov, BigStock

Erhalte ich beim Kauf über das Dell Expert Network-Programm Sonderpreise?

Durch eine direkte Beziehung zu Dell mittels der Teilnahme an dem Programm können für einen Kauf Sonderpreise gelten. Von Zeit zu Zeit gibt es exklusive Angebote für Mitglieder. „Weiterverkauf" wird bei diesem Programm nicht unterstützt.

Was passiert, wenn mein Kunde seine Bestellung zurückgibt oder storniert?

Ihr dedizierter Ansprechpartner wird Sie kontaktieren, um Sie darüber zu informieren. Bei einem Storno werden alle, aus dieser Bestellung erhaltenen Punkte, storniert. Geschäftskunden haben kein Rückgaberecht.

Können meine Mitarbeiter dem Dell Expert Network beitreten oder ist dieses Programm nur Geschäftsinhabern vorbehalten?

Ja, jeder IT-Berater oder IT-Dienstleister in Ihrem Team kann dem Programm beitreten. Sie müssen jedoch die Programmanforderungen erfüllen.

Was passiert, wenn mein Kunde vergisst, meine Dell Expert ID beim Kauf anzugeben?

Wir können Ihnen Prämien nur für Bestellungen, die mit Ihrer Dell Expert ID aufgegeben wurden, zuweisen.

Gibt es eine jährliche Mindestbestellmenge, um meine Mitgliedschaft zu behalten?

Es gibt keine Mindestbestellmenge, um Ihre kostenlose Mitgliedschaft aufrechtzuerhalten. Dell empfiehlt Mitgliedern jedoch, sich aktiv mit dem Dell Expert Network-Programm zu befassen und regelmäßig Empfehlungen abzugeben, um den Nutzen für sich zu maximieren.

Dell Expert Network

MSPs und IT-Beratern, die ihren Kleinunternehmerkunden beste Beratung und besten Service bieten wollen, stellt Dell branchenführende End-to-End-Lösungen zur Verfügung. Das „Dell Expert Network" ist dafür eine echte zentrale Anlaufstelle. Sind Sie IT-Berater oder IT-Dienstleister und wollen bei ihren Kunden keine Wünsche offenlassen? Dann werden Sie kostenlos Mitglied im Dell Support-Programm Dell Expert Network und profitieren Sie von dessen Vorteilen.

Mehr Informationen finden Sie unter
www.dell.de/expert-network