So schützen Sie Geschäfts- und Kundendaten vor Cyberkriminellen

8 Cybersicherheitsstrategien für kleine und mittlere Unternehmen.

Dieser E-Guide

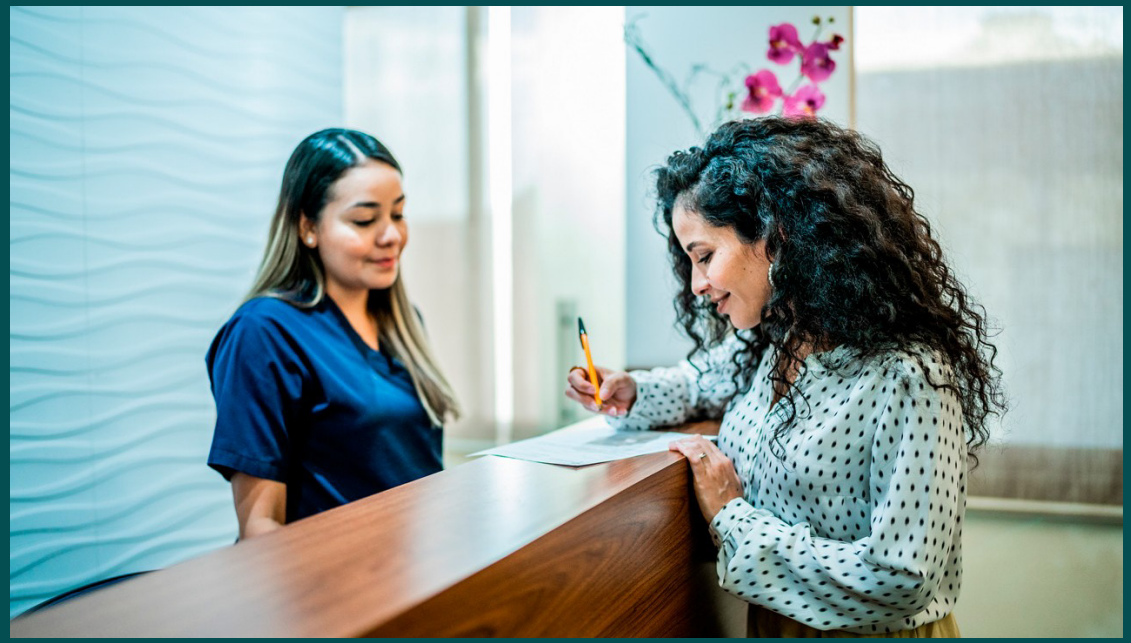
Als vertrauenswürdiger IT- und Sicherheitspartner für Unternehmen jeder Größe versteht Dell Technologies die alltäglichen Cybersicherheitsherausforderungen kleiner und mittlerer Unternehmen (KMUs). In diesem E-Guide stellen wir acht intelligente Strategien vor, mit denen Sie Ihre Geschäfts- und Kundendaten vor Cyberbedrohungen schützen können.

Inhaltsverzeichnis

Einführung

Wir alle haben die Schlagzeilen gesehen: Cyberangriffe passieren immer häufiger und treffen Unternehmen jeder Größe. Für kleine und mittelständische Unternehmen (KMU) ist Cybersicherheit nicht nur ein „wünschenswertes“ Element, sondern ein unverzichtbarer Bestandteil ihrer Sicherheitsstrategie. Cyberkriminelle nehmen oft kleine und mittlere Unternehmen ins Visier, weil sie glauben, dass es einfacher ist, dort einzudringen. Unternehmen verfügen oft über dedizierte IT- und Sicherheitsteams und –Ressourcen, KMUs jedoch möglicherweise nicht. Tatsächlich zeigen Untersuchungen, dass 35 % der kleinen Unternehmen weltweit der Ansicht sind, dass ihre Ausfallsicherheit bei Cyberangriffen unzureichend ist. Das sind siebenmal mehr als noch 2022! Ein einziger Fehler – ein PC ohne die neuesten Sicherheitspatches, ungeschützte sensible Informationen, ein unbedachter Klick auf eine Phishing-E-Mail – kann ein Unternehmen mit einer Vielzahl von Problemen konfrontieren, von finanziellen Rückschlägen bis hin zu verlorenen Daten und einem erschütterten Vertrauen der Kunden.

Die gute Nachricht: Einige proaktive Schritte können schon viel bewirken. Der Schutz Ihrer Geschäfts- und Kundendaten hilft Ihnen, zuversichtlich, wettbewerbsfähig und für die Zukunft gerüstet zu bleiben. ►



Cyberangreifer-InnenInnen 101

Bevor wir uns damit befassen, *wie* Sie sich schützen, ist es wichtig, die Denkweise der AngreiferInnen selbst zu kennen. AngreiferInnen gehen strategisch vor: Sie suchen nach einfachen Einstiegspunkten wie ungepatchten PCs, schwachen Kennwörtern und ungesicherten Netzwerken. Sie studieren häufig das Nutzerverhalten, identifizieren Zielgruppen und nutzen übersehene Sicherheitslücken aus. Durch die Kenntnis ihrer Taktiken können KMUs Abwehrmaßnahmen besser priorisieren, verdächtige Aktivitäten frühzeitig erkennen und eine Sicherheitsstrategie entwickeln, die proaktiv und nicht reaktiv ist. ►

Wer sind die AngreiferInnen?

AngreiferInnen können gewöhnliche Kriminelle sein, also HackerInnen mit böswilliger Absicht, aber auch ganze Staaten. Einige AngreiferInnen können leicht zu erkennen sein, zum Beispiel an schlecht geschriebenen E-Mails oder Texten. Einige verfügen über ausreichend finanzielle Mittel und können sehr ausgefeilte Angriffe starten.

Warum greifen sie an?

Geld ist ein wichtiger Motivator. Die globale Cyberkriminalität nimmt jedes Jahr weiter zu, wobei Experten prognostizieren, dass die jährlichen Kosten im Jahr 2025 auf 10,5 Billionen USD steigen werden. Natürlich ist die mögliche Beute aus einem erfolgreichen Angriff zu verlockend, um ignoriert zu werden.

Wie schlagen AngreiferInnen zu?

Cyberkriminelle sind unerbittlich – und sie werden intelligenter, da KI zur Verfügung steht. Hier sind einige Methoden, die sie verwenden:

- Angriffe auf „Endpunkte“ wie PCs sind ein wachsendes Problem. In Endpoint Security Market Insights, Forrester Research, Inc., März 2025, erläutert das Unternehmen „Endpunkte … gehören zu den primären Zielen externer Angriffe auf Unternehmen, die in den letzten 12 Monaten eine Sicherheitsverletzung erlebt haben“.
- Auch Identitätsangriffe nehmen zu. Phishing bleibt eine der größten Bedrohungen. Es ist nach wie vor eine der häufigsten Angriffsmethoden, die oft zum Diebstahl von Zugangsdaten und zur Verbreitung von Malware eingesetzt wird.
- Netzwerkangriffe wie Ransomware verursachen weiterhin Chaos und Schäden. Jüngste Untersuchungen zeigen, dass kleine Unternehmen stärker betroffen waren als große, wobei 88 % der Sicherheitsverletzungen mit Ransomware in Verbindung standen.

Kurz gesagt: Cyberangriffe zahlen sich aus. Bei einem erfolgreichen Ransomwareangriff erbeuten Cyberkriminelle im Durchschnitt 2 Millionen USD. Deswegen ist die Beharrlichkeit Teil ihrer Strategie – und deswegen sollte der Schutz Teil Ihrer Strategie sein.

Erhebliche Cybersicherheitsrisiken für KMUs

Gefährdung von Geräten

Gefährdung von Identitäten

Gefährdung von Netzwerken

So bleiben Sie sicher | 8 intelligente Strategien

1 Wissen, was geschützt werden muss

AngreiferInnen haben es auf sensible Kunden- und Mitarbeiterdaten abgesehen. Aber was Sie nicht kennen, können Sie auch nicht schützen. Machen Sie eine Bestandsaufnahme aller IT-Ressourcen und -Daten Ihres Unternehmens. Wo werden die Daten gespeichert? Wer hat Zugriff? Welche Geräte befinden sich in Ihrem Netzwerk? Ergreifen Sie mit diesen Informationen Maßnahmen. Stellen Sie sicher, dass Daten sicher gespeichert werden, und beschränken Sie den Zugriff auf vertrauliche Informationen. Das Wissen um Ihre Daten ist ein erster wichtiger Schritt zum Schutz der Daten. ►

2 Zusammenarbeit mit sicheren Lieferanten

Denken Sie an die Geschichte des Trojanischen Pferdes. Die Griechen versteckten Soldaten in einem scheinbar harmlosen Geschenk, das die Trojaner in ihre befestigte Stadt brachten. Einmal in der Stadt, konnten die Soldaten angreifen. Cyberkriminelle von heute wenden ähnliche Taktiken an, indem sie sich über vertrauenswürdige Anbieter, Softwareupdates oder Hardware einschleichen. KMUs sind oft auf viele verschiedene Lieferanten angewiesen, was sie anfällig macht, wenn einer davon kompromittiert wird. Aus diesem Grund sind z. B. die Überprüfung von Anbietern, die Überwachung der Softwareintegrität und die Transparenz der Versanddetails für eine starke Cybersicherheitsstrategie unerlässlich. ►

3 Arbeiten Sie auf PCs mit integrierter Sicherheit

Jeder PC ist ein potenzieller Einstiegspunkt für Cyberkriminelle. Integrierte Sicherheitsfunktionen wie Hardwareschutz, sicherer Start und Identitätsschutz tragen dazu bei, Bedrohungen sofort abzuwehren. Sichere PCs vereinfachen das IT-Management und bieten eine stärkere Verteidigung gegen Malware, Phishing und unbefugten Zugriff. Bedenken Sie auch, dass AngreiferInnen nicht immer aus der Ferne zuschlagen. Ein unbeaufsichtigter PC in einem öffentlichen oder gemeinsam genutzten Raum kann physisch von anderen BesucherInnen oder einer Person, die sich als MitarbeiterIn oder als Mitglied des Wartungspersonals ausgibt, zugänglich gemacht und kompromittiert werden. Angesichts begrenzter Ressourcen und wachsender Risiken – sowohl physisch als auch digital – ist integrierte Sicherheit heute ein Muss. ►

4 Halten Sie PCs auf dem neuesten Stand

Cyberkriminelle nutzen häufig bekannte Fehler in veralteten Systemen aus, so als ob sie durch eine offene Tür schleichen. Das Ignorieren von PC-Warnmeldungen und das Verschieben von Updates können Sie anfällig machen. Softwareupdates und -patches sind wie das Verriegeln dieser Tür. Sie beheben Fehler und Sicherheitslücken, die AngreiferInnen nutzen könnten. Regelmäßige Patches und Updates beheben diese Sicherheitslücken und tragen so zum Schutz Ihrer Geschäfts- und Kundendaten bei. Für KMUs ist dies ein einfacher Schritt, der große Probleme verhindern kann. ►

5 Finden Sie Probleme und beheben Sie sie schnell

Nur weil Sie über sichere PCs verfügen und diese sorgfältig auf dem neuesten Stand halten, bedeutet das nicht, dass diese nicht anfällig für Cyberkriminalität sind. AngreiferInnen können bei einem einzigen Gerät dutzende Angriffsversuche starten. Sie können mehrere Phishings per E-Mail oder per Text senden. Dies erhöht die Wahrscheinlichkeit, dass sie erfolgreich sind und Zugriff auf sensible Daten erhalten. Deshalb ist es wichtig, dass Sie einen Überblick über alle Unternehmens-PCs, Ihr Netzwerk und alle Cloud-Umgebungen haben, in denen Sie arbeiten. Hier kann eine Softwareschicht helfen, sodass Sie alles im Blick haben und vor allem schnell reagieren können, wenn Sie verdächtige Aktivitäten bemerken. ►

6 Verwenden Sie sichere Kennwörter und aktivieren Sie MFA

Verwenden Sie immer noch „123456“ oder „Passwort“? Nicht nur Sie … aber das ist sehr riskant. Gestohlene Zugangsdaten verursachen viele Sicherheitsverletzungen. Starke Passwörter sind unerlässlich für eine erste Verteidigungslinie. Dennoch finden hartnäckige AngreiferInnen Wege, um sie zu umgehen. Aus diesem Grund ist die Multifaktor-Authentifizierung (MFA) wichtig. Sie fügt eine zweite Schicht hinzu, sodass die Wahrscheinlichkeit, dass Sie gehackt werden, um 99 % geringer ist.

Legen Sie zuerst sichere Kennwörter fest.

Kombinieren Sie sie dann mit einer zweiten Methode zur Identitätsüberprüfung, z. B. Fingerabdruck-Lesegeräte, Smartcards oder NFC. Für einen noch stärkeren Schutz sollten Sie die Nutzeranmeldedaten in sicherer Hardware speichern, die für Malware, die diese Daten stehlen will, unzugänglich ist. ►

7 Schulen Sie MitarbeiterInnen und testen Sie ihre Fähigkeiten

Sie sind immer nur so sicher wie „das schwächste Glied in der Kette“. Leider ist menschliches Versagen weiterhin eine Hauptursache für Sicherheitsverletzungen. Dieser Fehler kann von der Verschiebung kritischer PC-Updates bis hin zur versehentlichen Offenlegung sensibler Daten bei der Wiederverwendung von Kennwörtern reichen. Cyberkriminelle verlassen sich auf menschliche Fehler und fahrlässiges Verhalten, um in Ihrem Unternehmen einen Fuß in die Tür zu bekommen. Aus diesem Grund sind Schulungen zur Cybersicherheit von entscheidender Bedeutung. Diese helfen MitarbeiterInnen, Bedrohungen zu erkennen und sichere Praktiken zu befolgen. Führen Sie regelmäßig Schulungen durch und testen Sie deren Fähigkeiten. Können sie ein Phishing erkennen? Reagieren sie angemessen? Warum bzw. warum nicht? Intensivieren Sie die Schulungen und decken Sie Lücken auf, bevor es zu spät ist. Wenn Sie MitarbeiterInnen mit ausreichend Kenntnissen versorgen, werden sie zu einer starken ersten Verteidigungslinie. ►

8

Haben Sie einen Plan für den Fall einer Sicherheitsverletzung

Planen Sie immer für das Worst-Case-Szenario. Es steht zu viel auf dem Spiel. Jede Sekunde zählt, wenn Sie Opfer eines Angriffs wurden. Wenn Sie dann einen Incident-Response-Plan haben, weiß Ihr Team genau, was im Fall der Fälle zu tun ist. Von der Erkennung der Sicherheitsverletzung über die Eindämmung des Schadens bis hin zur sicheren Wiederherstellung: Eine Reaktionsstrategie sorgt für weniger Ausfallzeiten und eine schnellere Rückkehr zum Geschäftsbetrieb. Starke Cybersicherheit bedeutet, proaktiv zu sein und auf jedes Problem vorbereitet zu sein. ►

Wichtigste Erkenntnisse

Die Modernisierung des Arbeitsplatzes ist für viele Unternehmen oberste Priorität, da sie generative KI (GenAI) nutzen, um die Produktivität zu steigern und die Mitarbeitererfahrung zu verbessern. Und während aktuelle Untersuchungen zeigen, dass 77 % der KMUs sagen, dass KI/GenAI ein wichtiger Teil ihrer Geschäftsstrategie ist, gibt die Mehrheit an, dass sie befürchten, dass neue Innovationen ihre Angriffsfläche erhöhen werden. Diese Sorge ist durchaus berechtigt.

Mit der zunehmenden Verbreitung von AI PCs und dem Ende des Supports für Windows 10 **gab es noch nie einen besseren Zeitpunkt für ein Upgrade.** Profitieren Sie von Leistungs- und Sicherheitsvorteilen mit den neuesten AI PCs. ►

Zusammenfassung der 8 Best Practices und was Dell für Sie tun kann

1 **Wissen, was geschützt werden muss.**
Dell Services kann Ihnen helfen, eine Bestandsaufnahme Ihrer IT-Ressourcen, Netzwerke und Daten zu erstellen.

2 **Zusammenarbeit mit sicheren Lieferanten.**
Die Lieferkettenkontrollen von Dell mindern das Risiko von Manipulationen. Sicheres PC-Design minimiert das Risiko von Schwachstellen.

3 **Arbeiten Sie auf PCs mit integrierter Sicherheit.**
Dell PCs sind ohne zusätzliche Kosten mit integrierter Sicherheit ausgestattet.

4 **Halten Sie PCs auf dem neuesten Stand.**
Dell schützt PCs mit zeitnahen Patches. Benötigen Sie Hilfe? Probieren Sie eine Schwachstellenanalyse mit Dell Security Services aus.

5 **Finden Sie Probleme und beheben Sie sie schnell.**
Nutzen Sie die Dell Partner-Software, um verdächtige Aktivitäten über PCs, Netzwerke und die Cloud hinweg zu überwachen.

6 **Verwenden Sie sichere Passwörter. Aktivieren Sie das MFA.**
Gehen Sie einen Schritt weiter mit Dell SafeID, einem hardwarebasierten System zur sicheren Speicherung von Zugangsdaten.

7 **Schulen Sie MitarbeiterInnen und testen Sie ihre Fähigkeiten.**
Wenden Sie sich an Dell Services, um Schulungen zum Sicherheitsbewusstsein Ihrer MitarbeiterInnen zu organisieren.

8 **Haben Sie einen Plan für den Fall einer Sicherheitsverletzung.** *Die Incident Response & Recovery von Dell kann helfen.*

Bereit zur Aktualisierung? Erfahren Sie, welche PCs für Ihr Unternehmen geeignet sind

Finden Sie AI PCs, die die Sicherheitsziele Ihres Unternehmens erfüllen.
Dell bietet mehrere Optionen.

Bekämpfen Sie Geräte-, Identitäts- und Netzwerkangriffe mit sicheren AI PCs. Bleiben Sie geschützt und konzentrieren Sie sich auf Ihren Alltag. ►

--

1 Eine PC-Funktion kann zwar innerhalb einer Produktlinie verfügbar sein, es ist jedoch nicht gewährleistet, dass sie auf jeder Plattform verfügbar ist.

2 „Die sichersten AI PCs“: Basierend auf einer internen Analyse von Dell, März 2025. Gilt für PCs mit AMD-Prozessoren. Nicht alle Funktionen sind bei allen PCs verfügbar. Einige Funktionen müssen zusätzlich erworben werden.

3 Authentifizierung über ein Fingerabdruck-Lesegerät mit Zugangsdaten, die sicher im TPM gespeichert sind.

4 Authentifizierung über ein Fingerabdruck-Lesegerät, eine Smartcard oder NFC mit Zugangsdaten, die sicher im einzigartigen ControlVault von Dell gespeichert sind.

5 Einige Angebote sind nur nach Volumen verfügbar und erfordern eine Mindestanzahl an Lizenzen. FedRAMP-autorisierte Optionen sind verfügbar.

			AM SICHERSTEN[2]
Verfügbare Sicherheit[1]	**Dell und Dell Plus**	**Dell Pro Essential**	**Dell Pro und Pro Max**
Sicherheit der Lieferkette	●	●	●
Verbesserte Sicherheit in der Lieferkette			●
Privacy Shutter	●	●	●
Vorrichtung für Sicherheitsschloss	●	●	●
Fingerabdruck-Lesegerät	●	●	●
TPM 2.0	●	●	●
Schutz von Zugangsdaten[3]			●
Verbesserter Schutz von Zugangsdaten[4]			●
PC-Sicherheitshinweise			●
Softwareupdates und -patches	●	●	●
PC-Verwaltung			●
Für KI optimierter Chip	●	●	●
Für Sicherheit optimierter Chip			●
Virenschutz der nächsten Generation (NGAV)[5]	●	●	●
NGAV plus Software zur Erkennung von PC-, Netzwerk- und Cloud-Bedrohungen[5]			●
Software für automatische Fehlerkorrektur, Geolokalisierung und Ausfallsicherheit für PCs			●
Erweiterter PC-Support	●	●	●

Ihr nächster Schritt

Aktualisieren Sie Ihre PCs.

Der Support für Windows 10 endet im Oktober, sodass viele KMUs mit veralteten, nicht unterstützten PCs konfrontiert sind.

Führen Sie ein Upgrade auf sichere Dell AI PCs mit AMD Ryzen AI PRO-Prozessoren durch.

Richten Sie eine Softwareebene ein.

Halten Sie AngreiferInnen mit mehreren Abwehrebenen fern.

Fügen Sie neuen und bestehenden PCs Softwareschutz hinzu.

Benötigen Sie Hilfe beim Sicherheitsmanagement?

Sicherheitsabläufe, die Sie benötigen, von Dell CybersicherheitsexpertInnen.

Erkunden Sie die Managed Security Services.

Führen Sie ein Upgrade auf die neuesten Dell AI PCs mit AMD Ryzen AI PRO-Prozessoren durch.

Weitere Informationen:

Schreiben Sie uns eine E-Mail an Global.Security.Sales@Dell.com

Weitere Informationen: Dell.com/Endpoint-Security

Folgen Sie uns: LinkedIn @DellTechnologies | X @DellTech

Informationen über Dell Technologies

Angesichts begrenzter Ressourcen müssen KMUs beim Schutz von Geschäftsinformationen und Kundendaten proaktiv vorgehen. Investitionen in Cybersicherheit sind unerlässlich, um die Geschäftskontinuität sicherzustellen, den Ruf zu schützen und das Vertrauen der KundInnen zu stärken. Sie sind damit ein intelligenter und notwendiger Bestandteil der Führung eines modernen Unternehmens.

Von der Risikominderung bei Ransomware-Angriffen über die Aufdeckung verdächtiger Aktivitäten bis hin zur Reaktion auf Echtzeit-Bedrohungen: Dell unterstützt Sie bei der Erstellung einer Sicherheitsstrategie und der Implementierung von Sicherheitslösungen, die den aktuellen und zukünftigen Anforderungen Ihres Unternehmens gerecht werden.