DELL Technologies

Cybersicherheit und Ausfallsicherheit stärken

Der Reifegrad der Cybersicherheit ist ein strategischer Hebel für jedes moderne Unternehmen

Die heutige Cyberbedrohungslandschaft ist dynamischer und unerbittlicher als je zuvor, wobei KI-gesteuerte Angriffe an Häufigkeit, Geschwindigkeit und Raffinesse zunehmen. Unternehmen können sich nicht mehr auf Patchwork-Abwehrmaßnahmen oder inkrementelle Updates verlassen.

Als Führungskraft müssen Sie so arbeiten, als ob eine Sicherheitsverletzung unvermeidbar ist oder gar unmittelbar bevorsteht. Bei Dell Technologies helfen wir unseren Kunden dabei, ihre Sicherheitsreife zu erhöhen, also das Maß an Vertrauen zu steigern, mit dem sie ihr Geschäft trotz Cyberrisiken betreiben können. Dafür verfolgen wir einen umfassenden, mehrschichtigen Ansatz für Cybersicherheit und Resilienz, der sich auf drei wichtige Praxisbereiche stützt.

Unternehmen müssen über Funktionen für Folgendes verfügen:

- **Verkleinerung der Angriffsfläche**
- **Erkennung von und Reaktion auf Cyberbedrohungen**
- **Wiederherstellung der Systeme nach einem Cyberangriff**

Effektive Cybersicherheit beginnt mit einer ehrlichen und realistischen Bewertung Ihres aktuellen Sicherheitsstatus und -reifegrads. Indem Sie sich ein klares Bild davon machen, können Sie die richtigen Verbesserungen priorisieren und in eine sicherere Zukunft investieren.

Reduzierung der Angriffsfläche

Die Angriffsfläche eines Unternehmens ist dynamisch und entwickelt sich schnell weiter, wobei KI neue Angriffsvektoren einführt. Zusammen mit Remote-Arbeit und Legacy-Systemen erweitern sie die Angriffsfläche und schaffen mehr Einstiegspunkte für Bedrohungsakteure. Daher ist die Verringerung der Angriffsfläche eine strategische Notwendigkeit, um Risiken zu reduzieren, Compliance-Verpflichtungen zu erfüllen, die Resilienz des Unternehmens zu schützen und grundlegendes Vertrauen aufzubauen.

Cybersicherheit und Ausfallsicherheit stärken

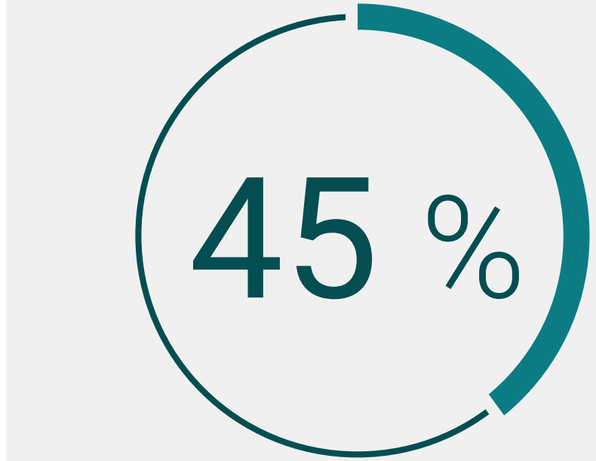
Die Reduzierung der Angriffsfläche trägt dazu bei, das Gesamtrisiko zu senken, indem die Einstiegspunkte minimiert werden, die AngreiferInnen ausnutzen können. Dies stärkt Ihren Sicherheitsreifegrad und optimiert die Compliance-Bemühungen. Das Ergebnis ist eine höhere Ausfallsicherheit, niedrigere Kosten durch die Vermeidung von Vorfällen und die Möglichkeit, schneller zu agieren, Innovationen freier zu entwickeln und selbstbewusst neue Märkte zu erschließen, da Sicherheit von Anfang an integriert ist. Das beginnt mit der Einführung von Zero-Trust-Prinzipien – nie vertrauen, immer überprüfen – und der Durchsetzung der geringsten Berechtigungen für NutzerInnen, Geräte und Anwendungen.

Wir bei Dell Technologies setzen auf die Mentalität der „integrierten Sicherheit". Cybersicherheit ist in alles integriert, was wir tun, angefangen bei unserer sicheren globalen Lieferkette bis hin zu integrierten Schutzmaßnahmen in unseren Kernprodukten. Diese Schutzmaßnahmen beginnen auf Hardwareebene, um sicherzustellen, dass Geräte gestartet werden und nur vertrauenswürdige Software ausführen. Wir richten unsere Lösungen auf Zero-Trust-Prinzipien aus und helfen Ihnen, Sicherheitslücken zu beseitigen, bevor AngreiferInnen sie ausnutzen können. Unsere weltweit sichersten kommerziellen KI-PCs[1] bieten beispielsweise grundlegende Schutzmaßnahmen für den modernen Arbeitsplatz.

Durch die Reduzierung der Angriffsfläche wird Ihre Sicherheitsreife erhöht, da Unsicherheiten beseitigt werden – weniger Unbekannte, weniger Einstiegspunkte und weniger Überraschungen.

Wichtige Kundenergebnisse:

- **Schwachstellen minimieren:** Indem Sie Endpunkte, Infrastruktur und Anwendungen proaktiv absichern, können Sie die Möglichkeiten für AngreiferInnen drastisch reduzieren.
- **Vereinfachtes Sicherheitsmanagement:** Weniger gefährdete Ressourcen bedeuten weniger notwendige Kontrollen im Management, was zu einem optimierten und effizienteren Sicherheitsstatus führt.
- **Stärkere Grundlage für Innovationen:** Mit vertrauenswürdigen Endpunkten und geschützten Daten können Sie neue Technologien wie KI und Edge Computing zuverlässigerer einführen.



Unternehmen, die sich auf die Reduzierung ihrer Angriffsfläche konzentrieren, erreichen beim Management externer Risiken eine Reduzierung des Risikos von Cybersicherheitsverletzungen um 45 %.[2]

Cyberbedrohungen erkennen und darauf reagieren

Im Bereich der Cybersicherheit gehen Geschwindigkeit und Intelligenz Hand in Hand. Durch effektive Erkennung und Reaktion können Sie Bedrohungen schnell identifizieren und eindämmen, wodurch die Verweilzeit reduziert und der Schaden eines Angriffs begrenzt wird. Das Ergebnis sind niedrigere Kosten, weniger Ausfallzeiten und eine größere Betriebssicherheit, sodass Ihr Unternehmen auch unter ständiger Bedrohung sicher arbeiten kann.

Cybersicherheit und Ausfallsicherheit stärken

Viele Unternehmen haben jedoch mit eingeschränkter Transparenz in hybriden Umgebungen und einer überwältigenden Menge an Warnmeldungen zu kämpfen. AngreiferInnen verweilen jetzt durchschnittlich 11 Tage in Netzwerken, bevor sie erkannt werden. Um dem entgegenzuwirken, benötigen Sie Echtzeittransparenz über Endpunkte, Netzwerke und Systeme hinweg durch kontinuierliches Monitoring, Threat Intelligence und Automatisierung.

Die richtigen Sicherheitspartner stellen spezialisierte Fachkompetenz in den Bereichen Threat Intelligence und Incident Response bereit. Dell kombiniert erweiterte Analysen, KI-/ML-gesteuerte Bedrohungserkennung und Managed Services rund um die Uhr mit einer sicheren Hardwaregrundlage, um Bedrohungen zu identifizieren und einzudämmen, bevor sie Unterbrechungen verursachen. Optionale Services wie unsere MDR (Managed Detection and Response) bieten Sicherheitsfachwissen, um die Transparenz zu erweitern und schnell auf Bedrohungen reagieren und diese beheben zu können.

Starke Erkennungs- und Reaktionsfunktionen erhöhen Ihren Sicherheitsreifegrad, indem sie die Verweildauer verkürzen und Teams das Vertrauen geben, dass sie bei auftretenden Bedrohungen entschlossen handeln können.

Wichtige Kundenergebnisse:

- **Schnellere Erkennung und kürzere Verweildauer:** Managed Detection and Response (MDR) kann die durchschnittliche Zeit für die Erkennung und Reaktion um 25 bis 49 % reduzieren und die Wahrscheinlichkeit verringern, dass ein Angriff schwerwiegender wird.
- **Verringerte operative Belastung:** Durch die Zusammenarbeit mit Experten für die proaktive Bedrohungssuche und kontinuierliches Monitoring wird die Belastung für interne Teams reduziert, sodass sie sich auf strategische Aufgaben konzentrieren können.
- **Verbesserte Ausfallsicherheit:** Ausgereifte Erkennungs- und Reaktionsfunktionen führen zu weniger Sicherheitsvorfällen und tragen dazu bei, höhere Kosten im Zusammenhang mit Sicherheitsverletzungen zu vermeiden.

4,44Mio.$

Die durchschnittlichen Kosten eines Datenverstoßes werden 2025 voraussichtlich 4,44 Mio. $ betragen.[3]

Wiederherstellung nach einem Cyberangriff

Tritt der Worst Case ein, ist das primäre Ziel eine schnellstmögliche Rückkehr zum Normalbetrieb mit minimalen Unterbrechungen. Die Wiederherstellung nach einem Cyberangriff sorgt dafür, dass Sie saubere Daten und die Systeme schnell wiederherstellen können, wodurch Reputationsschäden reduziert werden und Sie sich darauf verlassen können, dass Ihre Recovery zuverlässig und frei von erneuter Infektion ist.

Cybersicherheit und Ausfallsicherheit stärken

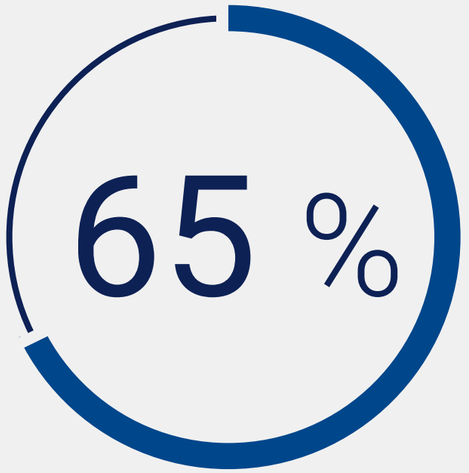
Auch wenn Sie die bestmöglichen Verteidigungsmaßnahmen ergreifen, müssen Sie so planen, als wäre ein Angriff unvermeidlich. Es ist von entscheidender Bedeutung, über einen vollständigen Recovery-Plan und die entsprechenden Fähigkeiten zu verfügen. Dazu gehören die Pflege sauberer, unveränderlicher Backups kritischer Daten in einem isolierten Recovery-Vault und die Verwendung von Reinraumumgebungen, um zu überprüfen, ob wiederhergestellte Systeme frei von Malware sind, bevor sie wieder online geschaltet werden.

Dell integriert Wiederherstellungsfunktionen in seine Produktangebote – und die Wiederherstellung des normalen Geschäftsbetriebs hat bei Vorfällen oberste Priorität. Lösungen wie unser PowerProtect Cyber Recovery Vault isolieren und schützen saubere Kopien kritischer Daten für eine schnelle Recovery, begrenzen Verluste und nehmen Ransomware-AngreiferInnen ihren Einfluss. Diese Architektur hilft Ihnen, kritische Workloads schnell wieder online zu schalten, sodass Sie sich sicher fühlen können.

Bei der Wiederherstellung wird die Sicherheitsreife oft am intensivsten getestet – wenn das Vertrauen davon abhängt, wie schnell und reibungslos das Unternehmen wieder zum normalen Betrieb zurückkehren kann.

Wichtige Kundenergebnisse:

- **Weniger geschäftliche Auswirkungen:** Unternehmen mit einem gut einstudierten Incident-Response-Plan können die Kosten für Sicherheitsverletzungen um ca. 61 % senken.
- **Schnellere Wiederaufnahme des Betriebs:** Die Priorisierung einer schnellen Wiederaufnahme des Geschäftsbetriebs, nicht nur der Entfernung von Bedrohungen, trägt dazu bei, den Betrieb mit minimalen Unterbrechungen und Kosten wiederherzustellen.
- **Verbesserte Datenintegrität: Die** Isolierung kritischer Daten, die Verwendung unveränderlicher Kopien und die Validierung der Integrität vor einer Wiederherstellung stärken das Vertrauen in den Recovery-Prozess.



der Unternehmen gaben zu, dass sie Schwierigkeiten dabei hatten, nach einem Cyberangriff zum Normalbetrieb zurückzukehren und gleichzeitig ihre Service Level Agreements einzuhalten.[4]

Ihre Sicherheitsreife durch strategische Partnerschaften stärken

Erfahrene Partner sind unerlässlich, um die sich schnell wandelnde und komplexe Cybersicherheitslandschaft von heute zu bewältigen. Cyberbedrohungen werden immer ausgefeilter und häufiger, sodass es für ein einzelnes Unternehmen fast unmöglich ist, das Fachwissen, die Ressourcen und die Technologie aufrechtzuerhalten, die erforderlich sind, um einen Schritt voraus zu bleiben. Durch die Zusammenarbeit mit führenden Sicherheitsanbietern wie Dell erhalten Unternehmen Zugang zu spezialisierten Kompetenzen, hochmodernen Technologien und einem Netzwerk vertrauenswürdiger Partner. Diese Partnerschaften bieten die Unterstützung und das Fachwissen, das erforderlich ist, um Bedrohungen effektiv zu erkennen, zu verhindern und darauf zu reagieren, sodass Unternehmen in einer sich ständig weiterentwickelnden digitalen Umgebung geschützt bleiben.

Mit dem richtigen Ansatz in diesen drei Praxisbereichen steigern Unternehmen ihre Sicherheitsreife und bauen Vertrauen auf, um trotz ständigem Druck durch Cyberbedrohungen zu agieren, innovativ zu sein und zu wachsen. Dell vereint eine vertrauenswürdige Infrastruktur, einen vertrauenswürdigen Arbeitsplatz, erweiterte Services und ein Partnernetzwerk, damit Ihr Unternehmen sicher, anpassungsfähig, resilient und damit bereit für die Zukunft bleibt.

Infos zu Sicherheitslösungen

DELL Technologies

Häufig gestellte Fragen

1. Warum sollte Cybersicherheit für mein Unternehmen oberste Priorität haben?
Cybersicherheit ist mehr als nur Schutz. Sie ist die Grundlage, auf der ein Unternehmen Innovationen entwickeln und wachsen kann, während es sich in der gefährlichen Cybersicherheitslandschaft behauptet. Bei einem starken Sicherheitsstatus geht es nicht nur um Abwehr, sondern auch um Unterstützung. Unternehmen mit ausgereiften Cybersicherheitsrahmen können schneller agieren, freier innovativ sein und selbstbewusst neue Märkte erschließen. Sie sind besser gerüstet, um behördliche Änderungen, Kundenanforderungen und Wettbewerbsdruck zu bewältigen.

2. Wie können wir die Notwendigkeit strenger Sicherheitsvorkehrungen mit der Freiheit zur Innovation in Einklang bringen?
Sie sollten sich nicht zwischen Sicherheit und Innovation entscheiden müssen. Wir glauben, dass solide Sicherheitfunktionen Innovationen ermöglichen. Wenn Sie über „Sicherheit per Design" als Grundlage verfügen, bei der Sicherheit von Anfang an in Ihre Geräte, Infrastruktur und Daten integriert ist, können Ihre Teams neue Technologien wie KI und Edge-Computing zuverlässig einführen.

3. Warum ist die Sicherheit der Lieferkette so wichtig?
Echte Sicherheit beginnt lange bevor der Netzschalter gedrückt wird. Mit zunehmender digitaler Nutzung steigt auch Ihre Präsenz – und Vertrauen wird zu Ihrer ersten Verteidigungslinie. Jedes Glied in der Lieferkette muss geschützt werden, da eine einzige kompromittierte Komponente selbst die fortschrittlichste Software untergraben kann. Aus diesem Grund schaffen wir Sicherheit von Grund auf und schützen jeden Schritt von der Produktion bis zur Bereitstellung. Von der Fertigung bis zur Lieferung – Ihre Technologie wird vertrauenswürdig, verifiziert und für zuverlässige Leistung entwickelt geliefert.

4. Wie unterstützt Dell mein Unternehmen bei der Wiederherstellung nach einem Cyberangriff?
Die Minimierung von Ausfallzeiten und Störungen ist entscheidend, wenn Vorfälle auftreten. Die Vorbereitung ist entscheidend. Unser PowerProtect Cyber Recovery Vault isoliert eine saubere, unveränderliche Kopie Ihrer kritischsten Daten, die sicher von Ihrer primären Umgebung getrennt sind. Bei einem Vorfall können Sie die Betriebsfähigkeit schnell und zuverlässig wiederherstellen, ohne Kompromisse einzugehen und ohne Lösegeld zu zahlen.
Dell bietet eine Vielzahl von Produkten und Services, die Sie bei der Implementierung einer umfassenden Recovery-Strategie unterstützen. Das Spektrum reicht von Beratungsleistungen zur Erstellung eines Recovery- und Schulungsplans bis hin zu Data Protection-Funktionen, die kritische Daten sicherstellen können. Dell verfolgt einen menschen- und technologieorientierten Ansatz und sorgt dafür, dass sowohl MitarbeiterInnen als auch Technologie zusammenarbeiten, um eine schnelle Recovery zu ermöglichen.

5. Kann Dell bei der Erkennung von Bedrohungen in Echtzeit helfen?
Auf jeden Fall. Geschwindigkeit ist alles, wenn es darum geht, eine Cyberbedrohung zu stoppen. Wir kombinieren integrierte Sicherheitsfunktionen mit erweiterten Services wie Managed Detection and Response (MDR), um Ihre Umgebung rund um die Uhr zu überwachen. Durch KI-/ML-gestützte Erkenntnisse und menschliches Fachwissen helfen wir Ihnen, Anomalien und potenzielle Bedrohungen sofort zu erkennen, sodass Sie auf Probleme reagieren und diese eindämmen können, bevor sie sich auf Ihr Unternehmen auswirken.

Quellen

[1] Basierend auf einer internen Analyse von Dell, Oktober 2024 (Intel) und März 2025 (AMD). Gilt für PCs mit Intel und AMD-Prozessoren. Nicht alle Funktionen sind bei allen PCs verfügbar. Einige Funktionen müssen zusätzlich erworben werden. Intel basierte PCs validiert von Principled Technologies, Juli 2025
Infografik zur Anatomie eines vertrauenswürdigen Geräts

[2] Forrester Consulting, „The Total Economic Impact™ of BitSight: Cost Savings and Business Benefits Enabled by BitSight", Oktober 2024.

[3] IBM und Ponemon Institute, „Cost of a Data Breach Report 2025: The AI Oversight Gap", 2025.

[4] Dell Technologies, „Steigerung der Cybersicherheit: Technologieinfrastruktur ist der Herzschlag jedes modernen Unternehmens", Februar 2025.

Informationen über Dell Technologies

Dell Technologies (NYSE: DELL) unterstützt Unternehmen und Privatpersonen dabei, ihre digitale Zukunft zu gestalten und Arbeitsplätze sowie private Lebensbereiche zu transformieren. Das Unternehmen bietet das branchenweit umfangreichste und innovativste Technologie- und Serviceportfolio für das KI-Zeitalter.

Mehr unter Dell.com