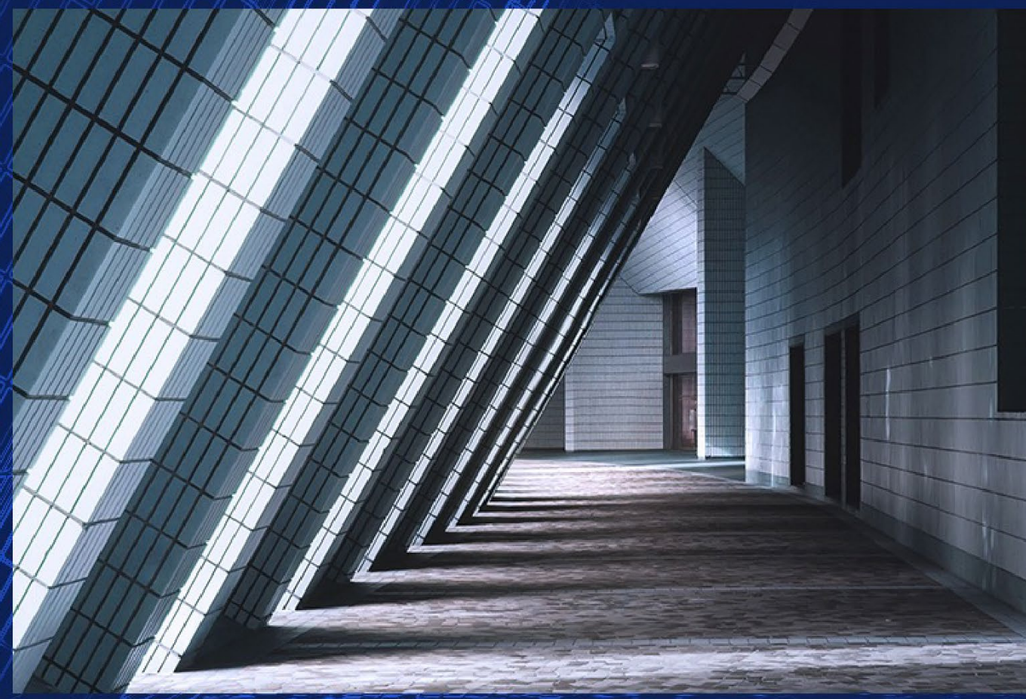
DELL Technologies



Höhere Cybersicherheit

Technologieinfrastruktur ist der Herzschlag jedes modernen Unternehmens

Sicherheit und Resilienz sind entscheidend dafür, dass diese wichtigen Organe ununterbrochen funktionieren. Viele Unternehmen können jedoch nur schwer mit fortschreitenden Bedrohungen Schritt halten. Unserer aktuellen Studie zufolge erkennen 93 % der Unternehmen, dass ihre Sicherheitsstrategien verbessert werden müssen.

Die Frage ist nicht mehr, ob Ihr Unternehmen mit einer Cyberbedrohung konfrontiert wird, sondern wann und wie. Als Führungskraft müssen Sie so arbeiten, als ob eine Sicherheitsverletzung unvermeidbar ist oder gar unmittelbar bevorsteht. Gleichzeitig müssen Sie sicherstellen, dass Sicherheitsrisiken die Innovationsfähigkeit Ihres Unternehmens nicht beeinträchtigen. Laut unserer Studie haben 79 % der Befragten Schwierigkeiten, Sicherheit und Innovation in Einklang zu bringen.

Immer ausgefeiltere Cyberbedrohungen und die rasante Verbreitung von Technologien wie künstlicher Intelligenz (KI) machen eine proaktive Sicherheitseinstellung wichtiger denn je. Der Weg in die Zukunft besteht aus drei wichtigen Sicherheitsschwerpunkten. Unternehmen müssen über robuste Funktionen für Folgendes verfügen:

- **Verkleinerung der Angriffsfläche,**
- **Erkennung von und Reaktion auf Cyberbedrohungen,**
- **Recovery nach einem Cyberangriff.**

93 %

der Unternehmen erkennen, dass ihre Sicherheitsstrategien verbessert werden müssen.

Reduzierung der Angriffsfläche

Die Angriffsfläche eines Unternehmens ist sehr dynamisch und entwickelt sich schnell weiter. In den letzten zehn Jahren ist die Angriffsfläche des Unternehmens um rund 1000 % gewachsen, was die zunehmende Sicherheitskomplexität moderner digitaler Umgebungen widerspiegelt.

Jeder neue technologische Fortschritt führt zu potenziellen Sicherheitslücken. Generative KI (GenAI) birgt beispielsweise neue Risiken in Bezug auf Datengefährdung, Ergebnismanipulation, Offenlegung sensibler Informationen und Prompt-Injection mit sich. Die Liste ist endlos. Sicherheitsherausforderungen gehen auch über KI-Implementierungen hinaus. Tatsächlich befürchten 67 % der Führungskräfte, dass neue Innovationen ihre Angriffsfläche vergrößern werden.

Die Reduzierung dieser Angriffsfläche erfordert einen mehrschichtigen Ansatz. Zunächst müssen grundlegende Praktiken wie gründliche Penetrationstests und Vulnerability Assessments angewendet werden, um potenzielle Sicherheitslücken, die sofortige Aufmerksamkeit erfordern, zu identifizieren und zu schließen. Weitere vorbeugende Maßnahmen sind eine umfassende Netzwerksegmentierung, die Isolierung kritischer Daten, die Durchsetzung strenger Zugriffskontrollen und die regelmäßige Aktualisierung und das Patchen von Systemen und Anwendungen.

Da Cybersicherheit ein fortlaufender Prozess und keine begrenzte Aktivität ist, müssen die anfänglichen Penetrationstests und Sicherheitslückenbewertungen regelmäßig durchgeführt werden, da sich sowohl das Unternehmen als auch die Bedrohungslandschaft kontinuierlich weiterentwickeln.

Wir bei Dell Technologies setzen auf die Mentalität der „integrierten Sicherheit“. Dabei sind vor allem unsere sichere Lieferkette sowie Zero-Trust-Prinzipien wie Identitätszugriffsmanagement durch Multifaktor-Authentifizierung (MFA) und rollenbasierte Zugriffskontrolle (RBAC) zu nennen, die in unseren Kernprodukten enthalten sind. Als Beispiel für die Leistungsfähigkeit dieser Funktionen bietet Dell die sichersten KI-PCs.

85 %

der Führungskräfte stimmen zu, dass ihre Lieferketten für ihren Sicherheitsstatus von entscheidender Bedeutung sind.

54 % der Unternehmen implementieren GenAI oder planen dies für die nächsten 12 Monate.

56 % der IT-EntscheidungsträgerInnen (ITDMs) sind besorgt über GenAI-Risiken.

32 % der ITDMs glauben, dass GenAI das Potenzial zur Verbesserung der Sicherheit hat.

Erkennung von und Reaktion auf Cyberbedrohungen

Im Bereich der Cyberabwehr gehen Geschwindigkeit und Intelligenz Hand in Hand. Unternehmen müssen daran arbeiten, potenzielle Sicherheitsvorfälle und bösartige Aktivitäten in den frühesten Phasen einer Sicherheitsverletzung aktiv zu identifizieren und zu beheben.

Dazu sind Technologien zur Bedrohungserkennung, die auf KI- und maschinellem Lernen basieren, zwingend erforderlich. Diese Systeme überwachen den Netzwerkverkehr, die Datenmuster und das Nutzerverhalten in Echtzeit und nutzen KI, um mögliche Sicherheitsbedrohungen zu erkennen.

Die richtigen Sicherheitspartner können außerdem spezialisierte Fachkompetenz in den Bereichen Threat Intelligence und Incident Response bereitstellen. Bei Dell bauen wir Sicherheit direkt in unsere PCs und Infrastrukturprodukte ein. Optionale Services wie MDR (Managed Detection and Response) helfen dabei, Bedrohungen zu identifizieren und darauf zu reagieren.

80 %

der Unternehmen geben zu, dass ihre Fähigkeiten zur Erkennung von und Reaktion auf Cyberbedrohungen verbesserungswürdig sind.

Wiederherstellung nach einem Cyberangriff

Tritt der Worst Case ein, sollte das primäre Ziel eine schnellstmögliche Rückkehr zum Normalzustand mit minimalen Unterbrechungen sein. In unserer aktuellen Umfrage gaben jedoch 64 % der Unternehmen zu, dass sie Schwierigkeiten hätten, nach einem Cyberangriff zum Normalbetrieb zurückzukehren und gleichzeitig ihre SLAs (Service Level Agreements) einzuhalten.

Auch wenn Sie die bestmögliche Abwehr aufbauen müssen, sollten Sie planen, als wäre ein Angriff unvermeidbar. Daher sind ein Recovery-Planung und -Funktionen von entscheidender Bedeutung. Dazu gehören die Aufrechterhaltung sicherer Backups kritischer Daten und Systeme sowie unveränderlicher, isolierter und/oder sicherer externer Storage mit Verschlüsselung. Außerdem müssen klare Incident-Response-Protokolle erstellt werden, in denen die Rollen und Verantwortlichkeiten aller Parteien ab dem Zeitpunkt des Angriffs beschreiben und Kanäle für eine nahtlose Koordination zwischen internen Teams und Partnern identifiziert werden. Schließlich müssen Recovery-Verfahren regelmäßig getestet werden, einschließlich der Simulation verschiedener Angriffsszenarien, um die Bereitschaft sicherzustellen.

Dell integriert Recovery-Funktionen in seine Produktangebote – und die Wiederherstellung des normalen Geschäftsbetriebs hat bei Incidents oberste Priorität. Lösungen wie unsere PowerEdge Server mit ASR (Automated System Recovery), PowerStore- und PowerMax-Systeme mit erweiterter Snapshot-Funktion für unveränderlichen Storage und PowerProtect Cyber Recovery Vault sorgen dafür, dass Ihre erfolgskritischen Daten intakt bleiben.

65 %

der Unternehmen gaben zu, dass sie Schwierigkeiten hätten, nach einem Cyberangriff zum Normalbetrieb zurückzukehren und gleichzeitig ihre Service Level Agreements einzuhalten.

Stärken Sie Ihren Sicherheitsstatus durch strategische Partnerschaften

Der Reifegrad von Cybersicherheit und Resilienz ist ein ständiger Prozess, der anhaltende Wachsamkeit und Weiterentwicklung erfordert. Durch die Aufrechterhaltung eines starken Sicherheits- und Resilienzstatus können Unternehmen ihre Risiken deutlich reduzieren, finanzielle Verluste minimieren, die Betriebseffizienz verbessern und mehr Vertrauen bei ihren Kunden aufbauen.

Erfahrene Partner können Sie in diesem dynamischen Umfeld unterstützen. In Zusammenarbeit mit Dell profitieren Sie von spezialisierten Fähigkeiten und Kenntnissen, die in Ihrem Unternehmen intern möglicherweise nicht verfügbar sind, z. B. Analysen neu auftretender Risiken und fortschrittlicher Angriffstechniken sowie aktuelle Sicherheitsstrategien und Best Practices.

Mit dem richtigen Ansatz zur Reduzierung der Angriffsflächen, zur Erkennung und Reaktion auf Bedrohungen und zur Wiederherstellung nach Incidents können Unternehmen die erforderliche Resilienz aufbauen, um im heutigen digitalen Zeitalter erfolgreich zu sein – und Innovationen entwickeln, um die Herausforderungen von morgen sorgenfrei zu meistern.

Weitere Informationen zu Sicherheitslösungen von Dell

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

Alle Datenpunkte in diesem eBook stammen aus einer im Februar 2025 durchgeführten Umfrage von Dell Technologies unter 750 Geschäfts- und IT-EntscheidungsträgerInnen aus den USA, dem Vereinigten Königreich, Deutschland, Frankreich und Japan und gelten für alle Segmente.
Die vollständigen Ergebnisse finden Sie hier.