DELL Technologies

Ransomware: Stärkung der Cybersicherheit und Resilienz mit Dell Technologies

Was ist Ransomware?

Ransomware ist eine Art bösartiger Software (Malware), die den Zugriff auf ein Computersystem oder Daten blockiert, bis ein Lösegeld gezahlt wird. Es handelt sich um eine der disruptivsten Arten von Cyberangriffen. 50 % der Unternehmen weltweit waren im letzten Jahr mindestens einmal von Ransomware betroffen und die durchschnittliche Ausfallzeit nach einem Ransomwareangriff beträgt drei Wochen, was zu erheblichen Betriebsunterbrechungen führt.

Wachsende Bedrohung durch Ransomware

Ransomware ist eine Art bösartiger Software (Malware), die den Zugriff auf ein Computersystem oder Daten blockiert, bis ein Lösegeld gezahlt wird. Es handelt sich um eine der disruptivsten Arten von Cyberangriffen. 50 % der Unternehmen weltweit waren im letzten Jahr mindestens einmal von Ransomware betroffen und die durchschnittliche Ausfallzeit nach einem Ransomwareangriff beträgt drei Wochen, was zu erheblichen Betriebsunterbrechungen führt.

So funktioniert Ransomware

Ransomware infiziert Unternehmen in der Regel, wenn eine Person auf einen bösartigen Link klickt, einen infizierten Anhang öffnet oder eine kompromittierte Website besucht. Sie dringt dann in Systeme ein, um Dateien zu verschlüsseln, sodass sie unlesbar werden. Im Ransonwareprogramm wird dann normalerweise eine Nachricht angezeigt, in der eine Zahlung (oft in Kryptowährung) im Austausch für einen Entschlüsselungsschlüssel gefordert wird. Wenn das Lösegeld nicht bezahlt wird, drohen AngreiferInnen möglicherweise damit, Daten zu löschen oder öffentlich weiterzugeben. Ein bekanntes Beispiel für einen Ransomwareangriff aus dem Jahr 2017 war der WannaCry-Angriff, der sich rasch weltweit ausbreitete, Krankenhäuser, Unternehmen und Regierungsbehörden traf und massive finanzielle Auswirkungen hatte. Die weltweiten wirtschaftlichen Auswirkungen des WannaCry-Virus beliefen sich laut Cyber Risk Management (CyRiM) und Lloyd's of London auf 4 bis 8 Mrd. USD, wobei innerhalb weniger Tage über 200.000 Systeme in 150 Ländern befallen waren.

Zwei der weltweit größten betroffenen Unternehmen waren FedEx, das aufgrund von Betriebsunterbrechungen und Aufräumarbeiten einen Verlust von 300 Mio. USD meldete, und Renault-Nissan, das die Produktion in mehreren Werken vorübergehend einstellen musste. Ransomwareangriffe sind mit zahlreichen versteckten Kosten verbunden, darunter:

- Ausfallzeiten und Produktivitätsverluste in Unternehmen
- Reputationsschäden
- Kosten für System-Recovery und -Patching
- Rechtliche und behördliche Geldstrafen

Unternehmen, die einem Ransomwareangriff ausgesetzt sind, sollten die folgenden Schritte unternehmen:

- Zahlen Sie nur dann, wenn dies unbedingt erforderlich ist – es gibt keine Garantie, dass die AngreiferInnen den Zugriff wiederherstellen.
- Führen Sie die Wiederherstellung von einem Backup durch, falls verfügbar.
- Melden Sie den Angriff den Behörden.
- Stärken Sie Abwehrmaßnahmen, um zukünftige Infektionen zu verhindern (z. B. Software auf dem neuesten Stand halten, MitarbeiterInnen schulen, Endpunktschutz nutzen).

© 2025 Dell Inc. oder deren Tochtergesellschaften.

Bekämpfung von Ransomwareangriffen mit Dell Technologies

Dell Technologies stattet Unternehmen mit umfassenden, zukunftsorientierten Tools aus, die dazu beitragen, Risiken im Zusammenhang mit Ransomware abzuwehren, bevor sie Schaden anrichten.

Verbesserte Endpunktsicherheit mit Dell Trusted-Devices

Endpunkte sind oft die primären Einstiegspunkte für Ransomwareangriffe, weshalb die Endpunktsicherheit zu einem kritischen Schwerpunktbereich wird. Dell Trusted-Devices verfügen über hardwareseitig integrierte Sicherheitsfunktionen, die Systeme schützen, ohne die Leistung zu beeinträchtigen. Lösungen wie Dell SafeBIOS und SafeID verstärken Endgeräte gegen unbefugten Zugriff, während Dell SafeData Daten verschlüsselt, um sensible Informationen auch außerhalb der Unternehmensfirewall zu schützen. Durch die direkte Integration von Sicherheit in Geräte sorgen Unternehmen für Schutz auf Hardwareebene, sodass AngreiferInnen weniger Chancen haben, Fuß zu fassen.

Proaktive Erkennung mit CrowdStrike

Ransomwareangriffe sind nicht unvermeidlich, wenn Unternehmen die richtigen Tools verwenden, um Bedrohungen in Echtzeit zu erkennen und darauf zu reagieren. CrowdStrike, das als Teil des Lösungsportfolios von Dell angeboten wird, bietet eine Plattform der nächsten Generation für den Endpunktschutz, die KI und Verhaltensanalysen nutzt. Diese Technologie erkennt und neutralisiert verdächtige Aktivitäten, bevor sie sich zu einem Angriff entwickeln. Durch die nahtlose Integration in die Dell Infrastruktur bietet CrowdStrike IT-Teams einen umfassenden Überblick über ihre gesamte Umgebung und ermöglicht so eine sofortige und effektive Reaktion auf Bedrohungen.

Umfassende Data Protection mit Dell PowerProtect

Dell PowerProtect-Lösungen sind das Rückgrat der Ransomwareresilienz. Diese erweiterten Data-Protection-Tools wurden entwickelt, um Unternehmensdaten sowohl vor internen als auch externen Bedrohungen zu schützen. Funktionen wie unveränderliche Backups stellen sicher, dass Ihre Daten nicht durch Ransomware geändert, gelöscht oder verschlüsselt werden können. So wird selbst bei ausgeklügelten Angriffen ein zuverlässiges Sicherheitsnetz bereitgestellt. Dell PowerProtect Cyber Recovery Vault isoliert beispielsweise kritische Daten mithilfe von Air-Gap-Technologie aus dem Netzwerk und stellt sicher, dass sie auch bei komplexesten Sicherheitsverletzungen unberührt bleiben. Mit der automatisierten Erkennung von Anomalien und intelligenten Workflows können Unternehmen bösartige Aktivitäten frühzeitig erkennen und reagieren, bevor sich Ransomware ausbreitet.

Fortschrittliche Netzwerksicherheit und Mikrosegmentierung mit Dell PowerSwitch-Netzwerklösungen und SmartFabric OS

Stärkt die Abwehr von Zero-Day-Angriffen durch erweiterte Netzwerksegmentierung, strenge Zugriffskontrollen und Echtzeitanalysen des Datenverkehrs in Ihrer gesamten Infrastruktur.

Recovery nach Maß mit Dell Data Protection-Services

Dell weiß, dass Prävention zwar wichtig ist, die Recovery jedoch ein ebenso bedeutender Aspekt der Ransomwarebereitschaft ist. Dell Data Protection-Services umfassen nicht nur automatisierte Backup- und Recovery-Lösungen, sondern auch fachkundige Beratung, um sicherzustellen, dass Unternehmen die Recovery schnell durchführen und Ausfallzeiten minimieren können. Services wie Remotedatenwiederherstellung und Incident Response stellen sicher, dass Unternehmen in Krisenzeiten die Unterstützung erhalten, die sie benötigen. Diese umfassende Herangehensweise sichert die Datenintegrität und reduziert die Wiederherstellungszeiten, was Betriebsunterbrechungen verhindert.

Dies sind nur einige Beispiele aus dem Dell Portfolio an Lösungen, die bei bösartigen Insiderbedrohungen helfen können.

Stärke durch Partnerschaften

Der kollaborative Ansatz von Dell erweitert den Schutz über die reine Technologie von Dell hinaus. Durch Partnerschaften mit führenden Cybersicherheitsunternehmen wie CrowdStrike und Secureworks bietet Dell ein Ökosystem integrierter Lösungen, die alle möglichen Angriffsvektoren abdecken. Zusammen stellen diese Lösungen eine End-to-End-Sicherheitsabdeckung bereit, sodass Unternehmen mehrschichtige Abwehrmaßnahmen entwickeln können, die auf ihre einzigartigen Risikoprofile zugeschnitten sind.

Gründe für Dell

Dell Technologies ist mehr als nur ein Technologieanbieter – das Unternehmen ist ein zuverlässiger Partner im Kampf gegen Ransomware. Durch die Kombination von Innovationen, Fachwissen und dem Engagement, Unternehmen zu unterstützen, stattet Dell Unternehmen mit den Tools und der Zuversicht aus, die sie benötigen, um neu aufkommende Bedrohungen abzuwehren. Unabhängig davon, ob es darum geht, Endpunkte zu sichern, kritische Daten zu schützen oder eine schnelle Wiederherstellung zu ermöglichen – die Produkte und Services von Dell sorgen dafür, dass die operative Kontinuität gewährleistet ist und Sie sich in Ruhe auf Ihre Arbeit konzentrieren können.

© 2025 Dell Inc. oder deren Tochtergesellschaften.

Zusammen für eine ausfallsichere Zukunft

Ransomwareangriffe entwickeln sich weiter, aber mit Dell Technologies können Unternehmen einen Schritt voraus bleiben. Durch die Nutzung fortschrittlicher Hardware, Software und Services können Unternehmen ein Cybersicherheits-Framework aufbauen, das resilient, anpassbar und zuverlässig ist. Schützen Sie Ihre Daten, Ihren Betrieb und Ihr Unternehmen noch heute mit den umfassenden Dell Lösungen gegen Ransomware.

Um die Ausfallsicherheit Ihres Unternehmens sicherzustellen, ist es wichtig, die aktuelle Bedrohungslandschaft zu verstehen und über neue Bedrohungen auf dem Laufenden zu bleiben. Die CybersicherheitsexpertInnen von Dell Technologies überwachen ständig neue Angriffsvektoren (wie nennen wir das?) und arbeiten daran, proaktiv potenzielle Sicherheitslücken in unseren Produkten und Services zu beheben. So können wir Ihnen den neuesten Schutz vor sich ständig weiterentwickelnden Ransomwarebedrohungen bieten.

Unternehmen müssen nicht nur auf dem Laufenden bleiben, sondern auch einen mehrschichtigen Sicherheitsansatz einführen. Das bedeutet die Bereitstellung einer Reihe von Sicherheitsmaßnahmen wie Firewalls, Anti-Malware-Software, Systeme zur Erkennung von Angriffen und Datenbackups. Durch die Diversifizierung Ihrer Abwehrstrategien können Sie die Auswirkungen eines Angriffs minimieren und sicherstellen, dass Ihr Unternehmen auch bei einem erfolgreichen Ransomwareversuch betriebsbereit bleibt.

Ebenso wichtig ist es, Ihre Sicherheitsmaßnahmen regelmäßig zu testen und auf dem neuesten Stand zu halten (sowohl Patches für Ihre Systeme als auch Aktualisierung Ihrer Richtlinien). HackerInnen finden ständig neue Möglichkeiten, herkömmliche Sicherheitsmaßnahmen zu umgehen. Daher ist es wichtig, dass Unternehmen immer einen Schritt voraus sind, indem sie ihre Abwehrmaßnahmen regelmäßig testen und nach Bedarf aktualisieren. Dazu gehören regelmäßige Sicherheitslückenbewertungen, Penetrationstests und das Patchmanagement.

Ein weiterer wichtiger Aspekt beim Schutz Ihres Unternehmens vor Ransomware ist die Schulung Ihrer MitarbeiterInnen zu Best Practices für Cybersicherheit. Viele Ransomwareangriffe werden mithilfe von Social-Engineering-Taktiken wie Phishing-E-Mails oder bösartige Links durchgeführt. Indem Sie Ihre MitarbeiterInnen darüber informieren, wie sie diese Bedrohungen erkennen und vermeiden, können Sie die Wahrscheinlichkeit eines erfolgreichen Angriffs erheblich reduzieren.

Darüber hinaus kann ein Disaster-Recovery-Plan die Auswirkungen eines Ransomwareangriffs erheblich abmildern. Dieser Plan sollte regelmäßige Backups wichtiger Daten und Systeme sowie eine klare Vorgehensweise für die Reaktion auf einen Angriff und die Wiederherstellung umfassen.

Zusätzlich zu diesen proaktiven Maßnahmen ist es auch wichtig, über einen guten Incident-Response-Plan zu verfügen. Dazu gehören klar definierte Rollen und Verantwortlichkeiten für den Umgang mit einem Ransomwareangriff sowie Kommunikationsprotokolle für die Benachrichtigung von StakeholderInnen und die Eindämmung von Schäden.

Schließlich sollten Sie sich stets über die neuesten Trends und Entwicklungen bei Ransomwareangriffen informieren, um potenziellen Bedrohungen einen Schritt voraus zu bleiben. Durch regelmäßiges Lesen von Branchenberichten und Neuigkeiten von SicherheitsexpertInnen können Sie proaktiv neue Sicherheitsmaßnahmen implementieren, um Ihr Unternehmen zu schützen.

Denken Sie daran, dass kein Unternehmen immun gegen Ransomwareangriffe ist, aber mit den richtigen Strategien und Tools können Sie das Risiko und die Auswirkungen solcher Angriffe minimieren. Durch einen proaktiven Cybersicherheitsansatz schützen Sie nicht nur Ihr Unternehmen, sondern schaffen auch Vertrauen bei Ihren Kunden und StakeholderInnen.

Erfahren Sie, wie Sie einige der größten Herausforderungen von heute im Bereich der Cybersicherheit bewältigen können: **Dell.com/SecuritySolutions.**

Weitere Informationen zu den Lösungen von Dell

Kontakt zu Dell Technologies ExpertInnen

Weitere Ressourcen anzeigen

Kommen Sie ins Gespräch über #HashTag

© 2025 Dell Inc. oder deren Tochtergesellschaften. Alle Rechte vorbehalten. Dell und andere Marken sind Marken von Dell Inc. oder deren Tochtergesellschaften. Alle anderen Marken können Marken ihrer jeweiligen Inhaber sein.

DELL Technologies