DELL Technologies

Sind Sie auf einen disruptiven Cyber-Incident vorbereitet?

Die mit Cyberangriffen verbundenen Risiken und Kosten nehmen immer weiter zu, wobei Ransomwareangriffe den Geschäftsbetrieb mit am stärksten schädigen können. Wenn der Betrieb über einen längeren Zeitraum – Wochen oder sogar Monate – ausgesetzt werden muss, kann dies für den langfristigen Erfolg des Unternehmens verheerend sein.

Die Wiederherstellung ist von entscheidender Bedeutung, doch die Rückkehr zum Normalbetrieb stellt eine erhebliche Herausforderung dar. Für das Wiederherstellen von Servern und enormen Mengen an Daten und Anwendungen, die schnellstmögliche Onlinestellung der kritischsten Anwendungen sowie die Erfüllung von Recovery Time Objectives (RTO) ist ein gewaltiger Aufwand vonnöten.

72 %

der Unternehmen benötigen externe Unterstützung, um sicherzustellen, dass sie alle IT-Sicherheits- und Risikoanforderungen abdecken.[5]

Kritische Hilfsmaßnahmen, um Sie wieder ins Geschäft zu bringen

Incident-Response- und Recovery-Services

Unser Team aus branchenzertifizierten Cybersicherheitsfachleuten arbeitet bei jedem Schritt mit Ihnen zusammen. Dank des weitreichenden globalen Netzwerks von Dell Technologies können wir schnell reagieren, um die Bedrohung zu eliminieren und den Geschäftsbetrieb schnell und mit so wenig Unterbrechungen wie möglich wiederherzustellen.

Cyberbedrohungen nehmen weiter zu und die Auswirkungen können verheerend sein.

Alle 11 Sekunden kommt es zu einem erfolgreichen Cyber- oder Ransomwareangriff[1]

16 Tage beträgt die durchschnittliche Ausfallzeit nach einem Ransomwareangriff[2]

75 % der Unternehmen werden bis 2025 einem oder mehreren Angriffen ausgesetzt sein[3]

Über 60 % der Unternehmen erlebten bereits, dass eine Sicherheitslücke ausgenutzt und Daten kompromittiert wurden[4]

Incident-Response- und Recovery-Services

Wir bei Dell Technologies Services können in puncto Wiederherstellung von Kundensystemen nach einem Cyber-Incident eine lange Erfolgsbilanz vorweisen.

Es ist ein Incident aufgetreten. Was nun?

Der Betrieb ist betroffen und es kann folgende Probleme geben:

- E-Mail funktioniert nicht.
- Kein Datenzugriff
- Malware
- Netzwerkausfall
- Active Directory funktioniert nicht.
- Transaktionen können nicht verarbeitet werden.
- Lösegeld wurde gefordert.

Hilfe anfordern

Hilfe anfordern

Unser Expertenteam kann Ihnen sofort behilflich sein. Kontaktieren Sie uns unter: Incident.Recovery@dell.com

Wiederherstellen

Team für Incident Response und Recovery (IRR)

Fachleute stehen Ihnen bei jedem Schritt zur Seite.

Vertrauen Sie den Fachleuten

Unser Team aus branchenzertifizierten Cybersicherheitsfachleuten bietet umfassendes Know-how und Best Practices für zahlreiche Aufgabenfelder.

In jeder Situation die notwendige Hilfe

Unsere Services sind auf Ihre Anforderungen abgestimmt, ganz egal, mit welcher Situation Sie konfrontiert sind oder was betroffen ist. Zunächst bewerten wir Ihre Lage und setzen dann genau die richtigen Ressourcen ein, um Sie bei der schnellen Wiederherstellung zu unterstützen.

Unsere Aufgaben

Ganz gleich, ob es gerade zu einem Angriff gekommen ist oder Sie bereits an der Wiederherstellung arbeiten und Hilfe benötigen, um schneller voranzukommen, unsere Fachleute stehen Ihnen zur Seite:

- Bewerten und Bereitstellen der richtigen Ressourcen
- Beseitigen der Bedrohung und Mindern von Sicherheitsrisiken
- Wiederherstellen von Business Applications auf den Zustand vor dem Incident
- Erneutes Bereitstellen von Workstations, damit MitarbeiterInnen wieder an die Arbeit zurückkehren können
- Kompetente Datenforensikservices
- Unterstützung bei der Verbesserung der Sicherheit

Hilfe anfordern

- Wir nehmen innerhalb von Minuten/Stunden mit Ihnen telefonischen Kontakt auf und unser Team ist in der Regel in weniger als 48 Stunden vor Ort
- Mehr als 100 Ressourcen in mehreren Arbeitsbereichen an mehreren Standorten und in mehreren Sprachen mit flexibler Anpassung nach Bedarf
- Branchenzertifizierte Cybersicherheitsexperten, die meisten m it mehr als 10 Jahren Erfahrung
- Fachwissen zu Infrastruktur- und Endgeräten von Dell und anderen Herstellern
- Wissen und Erfahrung in den Bereichen Edge, Cloud, Recht, Versicherung und mehr
- Globale Reichweite in mehr als 170 Ländern
- Innovative Zahlungslösungen, die Ihnen die Flexibilität geben, die Kosten für IT-Lösungen an die Technologienutzung und die Verfügbarkeit des Budgets anzupassen**

Wiederherstellen

- Beseitigung der Bedrohung
- Schnelle Rückkehr zum Normalbetrieb
- Verstärkung vorhandener IT-Kräfte aufgrund erhöhter Workloads
- Erneuter Aufbau einer besser geschützten Netzwerkumgebung
- Verbessern des Sicherheitsstatus durch Entwicklung und Implementierung einer Sicherheitsstrategie zur Vermeidung wiederholter Cyberangriffe
- Schulung und Austausch von Best Practices

Weitere Informationen finden Sie unter **Delltechnologies.com/incident-response-and-recovery**

** Zahlungslösungen für qualifizierte gewerbliche Kunden von Dell Financial Services (DFS) oder von Unternehmen der Dell Technologies-Gruppe und/oder von autorisierten Geschäftspartnern von Dell (zusammen mit DFS „Dell"). Angebote sind möglicherweise nicht verfügbar oder können je nach Land variieren. Angebote können ohne vorherige Ankündigung geändert werden und unterliegen der Verfügbarkeit, Berechtigung, Kreditgenehmigung und Ausführung von Dokumentationen, die von Dell oder den autorisierten Geschäftspartnern von Dell bereitgestellt werden und von diesen akzeptiert werden. In Spanien werden Lösungen von der Dell Bank International d.a.c Niederlassung Spanien und in der restlichen EU von Dell Bank International d.a.c bereitgestellt. Die Dell Bank International d.a.c. firmiert als Dell Financial Services und wird von der irischen Zentralbank reguliert. Die Logos von Dell Technologies, Dell EMC und Dell sind Marken von Dell Inc.

[1] Schätzung für 2021, Cybersecurity Ventures: https://cybersecurityventures.com
[2] Why Ransomware Costs Businesses Much More than Money, Forbes, 30. April 2021, https://www.forbes.com/sites/forbestechcouncil/2021/04/30/why-ransomware-costs-businesses-much-more-than-money/?sh=469c541a71c6
[3] Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware, Nik Simpson, Gartner, 6. Januar 2021, https://www.gartner.com/doc/reprints?id=1-258HHK51&ct=210217&st=sb
[4] Von Dell in Auftrag gegebenes Forrester Consulting Thought Leadership Paper: BIOS Security – The Next Frontier for Endpoint Protection, Juni 2019
[5] Eine im Auftrag von Dell Technologies durchgeführte Studie von Forrester Consulting, Dezember 2020.