Recovery nach Cyberangriffen

Stellen Sie den Betrieb nach einem Incident effektiv und effizient wieder her.

Eine umfassende Security-Recovery-Strategie deckt Folgendes ab:

Minderung der Auswirkungen eines Angriffs → Wiederherstellung der kompromittierten Services und Geräte → Wieder-aufnahme des Betriebs → Analyse des Incident und entsprechender Erkenntnisgewinn

Maßnahmen für eine verbesserte Cybersicherheit

1. **Eindämmung des Incident**
   Trennen Sie die betroffenen Systeme vom Netzwerk, deaktivieren Sie kompromittierte Konten und verhindern Sie weiteren Schaden.
2. **Wiederherstellung von Systemen/Geräten**
   Stellen Sie die kompromittierten Systeme wieder her, installieren Sie Software neu und wenden Sie Sicherheitspatches und Updates an.
3. **Daten-Recovery**
   Stellen Sie Daten mithilfe von Backups wieder her oder nutzen Sie spezielle Techniken zur Daten-Recovery, um verloren gegangene oder verschlüsselte Dateien wiederherzustellen.
4. **Forensische Analyse**
   Untersuchen Sie die Funktionsweise des Angriffs und die ausgenutzten Sicherheitslücken, um künftige Incidents zu verhindern.
5. **Bewertung der Incident Response**
   Bewerten Sie nach der Recovery den gesamten Prozess und suchen Sie nach Verbesserungsmöglichkeiten.
6. **Einsatz von KI/ML**
   Beschleunigen Sie die Recovery, indem Sie die betroffenen Systeme und Daten schnell ermitteln und den Prozess der Wiederherstellung mithilfe von Backups automatisieren.

Cyber Recovery ist Teamsache.

Dienstleistungen und Partnerschaften
Cybersicherheitspartner bieten Ihnen wertvolle Fachkenntnisse und Ressourcen:

- Forensische Analyse
- Ermittlung der Ursache von Sicherheitsverletzungen
- Maßnahmen zum Verhindern künftiger Incidents

Erfahren Sie mehr darüber, wie Sie eine umfassende Cybersicherheitsstrategie implementieren.

E-Book lesen →

DELL Technologies