DELL Technologies

Le organizzazioni sono preparate a un incidente informatico che interrompe le attività?

I rischi e i costi associati agli attacchi informatici continuano ad aumentare e gli attacchi ransomware sono tra i più dannosi per le operazioni aziendali. L'impossibilità di svolgere le operazioni aziendali per un lungo periodo di tempo, settimane o addirittura mesi, può essere devastante per il successo a lungo termine dell'organizzazione.

Il ripristino è cruciale e il ritorno al funzionamento normale richiede sforzi notevoli. Ripristinare i server e le enormi quantità di dati e applicazioni, portare online le applicazioni più critiche il prima possibile e raggiungere i Recovery Time Objective (RTO) richiede un grande impegno.

72%

le aziende che affermano di aver bisogno di un aiuto esterno in grado di soddisfare tutte le esigenze relative a sicurezza e rischio IT.[5]

Assistenza cruciale per la prosecuzione delle attività

Servizi di Incident Response e ripristino

Il nostro team di esperti di sicurezza informatica certificati del settore collabora con i clienti in ogni fase del percorso. Grazie alla scalabilità della rete globale di Dell Technologies, possiamo rispondere rapidamente per eliminare le minacce e ripristinare le operazioni aziendali in modo rapido e con le minori interruzioni possibili.

Le minacce informatiche sono in costante aumento e gli effetti possono essere devastanti

Ogni 11 secondi un attacco informatico o ransomware va a buon fine[1]

16 giorni il downtime medio dopo un attacco ransomware[2]

75% le organizzazioni che dovranno affrontare uno o più attacchi entro il 2025[3]

Oltre 60% le aziende che hanno già subito una compromissione dei dati a causa di una vulnerabilità[4]

Servizi di Incident Response e ripristino

Dell Technologies Services vanta una comprovata esperienza nel ripristino delle attività di clienti interessati da un evento informatico

Si è verificato un incidente, qual è il passaggio successivo?

Le operazioni sono compromesse e i possibili effetti sono:

- L'e-mail è disattivata
- È impossibile accedere ai dati
- Malware
- La rete è inattiva
- Active Directory è inattivo
- È impossibile elaborare le transazioni
- È stato richiesto un riscatto

Assistenza

Il nostro team di esperti è in attesa di fornire una risposta immediata e tutto ciò che occorre fare è contattarci all'indirizzo: Incident.Recovery@dell.com

Ripristino

Team di Incident Response e ripristino (IRR)

Esperti al fianco del cliente in ogni fase del percorso

Affidarsi agli esperti

Il nostro team dedicato di esperti di sicurezza informatica certificati del settore offre notevoli competenze e best practice in diversi settori e ambiti di conoscenze

L'assistenza ideale, indipendentemente dalla situazione

I nostri servizi soddisfano ogni esigenza, indipendentemente dalla situazione affrontata o dal componente che ha subito attacchi. Prima valutiamo la situazione, poi attiviamo le risorse giuste per eseguire rapidamente il ripristino.

Cosa facciamo

Che si sia appena verificato un attacco o che il cliente abbia già intrapreso un'operazione di ripristino e abbia bisogno di aiuto per intervenire più rapidamente, i nostri esperti sono a disposizione per:

- Valutare e implementare le risorse giuste.
- Debellare le minacce e ridurre i rischi per la sicurezza.
- Ripristinare le applicazioni aziendali per riportarle alle operazioni preliminari all'incidente.
- Reinstallare le workstation per consentire ai dipendenti di tornare al lavoro.
- Erogare servizi forensi professionali per i dati.
- Contribuire a migliorare la sicurezza.

Assistenza

- Assistenza telefonica in pochi minuti/ore e intervento on-site di un team in meno di 48 ore.
- Scalabilità di oltre 100 risorse con più flussi di lavoro in varie posizioni e lingue, con flessibilità di adattamento in base alle esigenze.
- Assistenza da parte di esperti di sicurezza informatica certificati del settore con oltre 10 anni di esperienza.
- Messa a disposizione di competenze per l'infrastruttura e i dispositivi endpoint Dell e non Dell.
- Conoscenze ed esperienza in ambito edge, cloud, legale, assicurativo e altro ancora.
- Copertura globale in oltre 170 mercati.
- Utilizzo di soluzioni di pagamento innovative che consentono di allineare e scalare i costi delle soluzioni IT in base al consumo tecnologico e alla disponibilità di budget.**

Ripristino

- Rimozione dell'autore della minaccia.
- Ripristino rapido del funzionamento normale.
- Incremento del personale IT esistente a causa dell'aumento del carico di lavoro.
- Ricostruzione di un ambiente di rete rinforzato.
- Miglioramento del profilo di sicurezza sviluppando e implementando una strategia di sicurezza per prevenire i ripetuti attacchi informatici.
- Formazione e condivisione di best practice.

Per ulteriori informazioni, visita **Delltechnologies.com/incident-response-and-recovery**

** Soluzioni di pagamento fornite a clienti commerciali qualificati da Dell Financial Services (DFS) o tramite le società del gruppo Dell Technologies e/o tramite i partner commerciali autorizzati di Dell (insieme a DFS "Dell"). Le offerte potrebbero non essere disponibili o variare a seconda del Paese. Le offerte possono variare senza preavviso e sono soggette alla disponibilità dei prodotti, all'idoneità, all'approvazione del credito, alla presentazione della documentazione fornita e accettata da Dell o dai partner commerciali autorizzati di Dell. In Spagna, i servizi sono forniti dalla filiale Dell Bank International d.a.c. e nel resto dell'UE da Dell Bank International d.a.c. che opera con il nome di Dell Financial Services, regolamentata dalla Central Bank of Ireland. Dell Technologies, DellEMC e i loghi Dell sono marchi di Dell Inc.

[1] Stima per il 2021, Cybersecurity Venture: https://cybersecurityventures.com
[2] Why Ransomware Costs Businesses Much More than Money, Forbes, 30 aprile 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 More, Gartner, 6 gennaio 2021, https://www.gartner.com/doc/reprints?id=1-258HHK51&ct=210217&st=sb
[4] Documento sulla leadership di pensiero di Forrester Consulting, commissionato da Dell, BIOS Security – The Next Frontier for Endpoint Protection, giugno 2019
[5] Studio su commissione condotto da Forrester Consulting per conto di Dell Technologies, dicembre 2020

Settembre 2021-LC | Servizi di Incident Response e ripristino