DELL Technologies

Miglioramento delle misure di sicurezza senza i costi aggiuntivi associati all'aumento dell'organico

Per rafforzare in modo significativo la propria sicurezza informatica, una grande contea nel sud-ovest degli Stati Uniti ha adottato la soluzione Dell Managed Detection and Response.

Profilo del cliente

Contea degli Stati Uniti

Pubblica amministrazione | Stati Uniti

"Sapevamo di dover migliorare il nostro profilo di sicurezza. Con Dell Managed Detection and Response ci siamo riusciti senza aumentare l'organico."

Responsabile dei sistemi informatici
Grande contea nel sud-ovest degli Stati Uniti

Esigenze aziendali

Con il rapido aumento degli attacchi ransomware e di altre minacce informatiche contro le pubbliche amministrazioni e gli enti governativi locali, una grande contea in crescita nel sud-ovest degli Stati Uniti aveva necessità di rafforzare il proprio profilo di sicurezza e migliorare la propria capacità di rilevamento e risposta alle minacce senza i costi e l'impegno necessari per assumere e formare ulteriori specialisti della sicurezza.

Risultati di business

- Miglioramento del profilo di sicurezza della contea senza aumentare l'organico.
- Completamento delle conoscenze, delle competenze e della scalabilità del team IT.
- Monitoraggio e risposta alle minacce 24x7 non più in carico al personale.
- Semplificazione del processo di rilevamento e correzione rapida di una violazione del server.
- Possibilità di contare su specialisti qualificati in tutta facilità.

Soluzioni in sintesi

- Managed Detection and Response

L'organizzazione oggetto di questo caso di studio è una grande contea in rapida crescita nel sud-ovest degli Stati Uniti che serve centinaia di migliaia di residenti ed è nota per le numerose imprese che hanno sede sul suo territorio, dalle più innovative società nel settore medicale e biotech alle aziende manifatturiere e agricole.

Negli ultimi anni, le minacce alla sicurezza informatica contro la pubblica amministrazione sono aumentate drasticamente. Negli Stati Uniti, nel corso del 2020 sono stati effettuati 79 attacchi ransomware contro enti governativi a tutti i livelli, con costi per il downtime e il ripristino pari a circa 19 miliardi di dollari.[1]

Dopo un'esperienza negativa con la soluzione offerta da un altro fornitore, questa contea ha scelto Dell Managed Detection and Response con software di analisi della sicurezza Secureworks® Taegis™ XDR, un servizio end-to-end gestito 24x7 che monitora, rileva e analizza le minacce nell'intero ambiente IT della contea stessa, rispondendo in modo efficace.

"Sapevamo di dover migliorare il nostro profilo di sicurezza. Con Dell Managed Detection and Response ci siamo riusciti senza aumentare l'organico", ha dichiarato il responsabile dei sistemi informatici.

Due funzionalità chiave combinate tra loro

La soluzione riunisce i due componenti più importanti alla base di un elevato profilo di sicurezza:

- L'esperienza degli analisti della sicurezza di Dell Technologies, che completano il team della contea formato unicamente da un analista della sicurezza, da un System Administrator e da un ingegnere.

- Le numerose funzioni di Secureworks Taegis XDR, una piattaforma cloud-native per l'analisi della sicurezza progettata per rilevare le minacce più avanzate. Questa soluzione consente agli analisti MDR di collaborare con il personale della contea per l'esecuzione delle opportune verifiche in minor tempo, aiutando anche i tecnici a intraprendere le azioni più appropriate per mitigare l'impatto.

"Quando abbiamo avuto bisogno, gli specialisti di Dell Technologies si sono subito prodigati lavorando assiduamente per una settimana o dieci giorni. Sapevamo di essere in buone mani."

Responsabile dei sistemi informatici
Grande contea nel sud-ovest degli Stati Uniti

[1] Bischoff, Paul, "Ransomware attacks on US government organizations cost $18.9bn in 2020" Comparitech, 17 marzo 2021. https://www.comparitech.com/blog/information-security/government-ransomware-attacks/

"Ci hanno aiutato a installare i software agent su tutti i server e sulle singole workstation, interrompendo i servizi, arrestando i PC o bloccando un account con appositi trigger. È stato inoltre impostato l'invio di notifiche in caso di rilevamento di una minaccia", ha dichiarato il responsabile dei servizi informatici. "Nei 90 giorni impiegati per implementare l'intera soluzione, gli specialisti di Dell Technologies ci hanno fornito preziosi consigli, dando priorità alle azioni necessarie".

Mitigazione rapida di un tentativo di violazione

La soluzione include fino a 40 ore di assistenza a trimestre per rispondere efficacemente alle minacce e porvi rimedio anche nelle situazioni più complesse, nonché altre 40 ore all'anno per analizzare le attività ed eseguire il ripristino in seguito a gravi incidenti di sicurezza, quando richiesto.

"Ci siamo convinti che questa soluzione fosse quella giusta nel momento in cui abbiamo avuto un vero e proprio tentativo di violazione", ha aggiunto il responsabile dei servizi informatici. "Un gruppo di hacker ha individuato una vulnerabilità nel server di posta elettronica di Microsoft Exchange. Dopo essere stati informati da Microsoft e dall'agenzia nazionale per la sicurezza informatica, abbiamo scoperto che uno dei nostri tre server era stato danneggiato. Il team di Dell Technologies ha condotto tutte le verifiche necessarie per accertare la violazione e ci ha aiutati a ripristinare il server".

"Il mio consiglio per i CIO delle altre contee? Adottare una soluzione di sicurezza di livello enterprise come Dell Managed Detection and Response anziché le soluzioni offerte dai vendor di software antivirus. Quando abbiamo avuto bisogno, gli specialisti di Dell Technologies si sono subito prodigati lavorando assiduamente per una settimana o dieci giorni. Sapevamo di essere in buone mani. Tra i nostri team si è creata una sinergia perfetta e c'è stata un'ottima collaborazione".