DELL Technologies

Lezioni da un attacco ransomware

alla Universitat Autònoma de Barcelona

Gonçal Badenes
CIO della Universitat Autònoma de Barcelona.
Intervista condensata ed editata per maggiore chiarezza.

Azione rapida, trasparenza e un rinnovato impegno per l'aggiornamento della sicurezza informatica hanno caratterizzato la risposta dell'Università a un attacco ransomware.

Sameer Shah, Dell Technologies Cybersecurity Marketing, ha parlato dell'incidente con il CIO Gonçal Badenes.

Shah: Abbiamo parlato della necessità di aiutare le organizzazioni a migliorare progressivamente la loro maturità in termini di sicurezza informatica. Voi avete subito un attacco informatico qualche tempo fa. Prima di addentrarci nei dettagli di questo attacco, potrebbe parlarci un po' dell'Università e del suo ambiente IT?

Badenes: L'Universitat Autònoma de Barcelona è una delle principali università della Spagna. L'IT supervisiona tutti i servizi necessari per far funzionare l'università.

Subito prima dell'attacco avevamo stilato un piano completo per migliorare la nostra strategia di sicurezza informatica. Avevamo implementato l'autenticazione a più fattori (MFA), ma non su tutti i servizi e gli utenti. Tutti gli studenti e il personale IT erano già dotati di autenticazione a più fattori, tuttavia solo limitatamente alla piattaforma Microsoft 365. Gli altri servizi non erano protetti. La mancanza di MFA universale è stata importante, come vedremo più avanti.

Quando si è verificato l'attacco e di che tipo è stato?

Si è trattato di un attacco ransomware che si è verificato durante un weekend lungo, come accade solitamente. Intorno alle quattro del mattino ho ricevuto una chiamata dal mio team, che mi avvisava che alcuni servizi stavano andando giù come tessere di domino. Hanno dato l'allarme e abbiamo immediatamente riunito il team di risposta che avevamo previsto per questi casi.

Come sapevate che si trattava di un attacco ransomware? C'è stata una richiesta di riscatto?

Erano presenti note di riscatto sui sistemi interessati. Ma gli hacker hanno eseguito anche un attacco di minore entità, eseguendo uno script per crittografare i computer che erano online nel fine settimana. L'impatto di quest'ultimo è stato limitato e, probabilmente, il suo scopo principale era quello di garantire che anche il personale e gli studenti scoprissero l'attacco, non solo il team IT.

C'è stato qualche momento in cui la vostra organizzazione ha preso in considerazione il pagamento del riscatto?

No.

Per quale motivo?

Non potevamo farlo per una questione di etica. Fortunatamente avevamo dei backup già pronti, due copie in due diversi centri dati sul campus e una terza su nastro al di fuori del perimetro dell'organizzazione.

E per essere chiari, questi backup non erano un data vault, giusto?

No, non in quel momento. Non avevamo un vault. Era una priorità futura, inserita nella roadmap. Ma a quel punto, naturalmente, è diventata una priorità assoluta [dopo l'attacco].

Le comunicazioni possono essere cruciali in queste situazioni. Sembra che voi abbiate fronteggiato l'attacco comunicando in maniera chiara e trasparente, anche con i media?

Sì, fin dal primo giorno. Dovevamo essere perfettamente trasparenti e il più possibile aperti nello spiegare l'accaduto. Ci stavamo assicurando che altre persone potessero prepararsi e imparare dalla nostra esperienza. Secondo me, qualcuno della stampa ha letto la nota di riscatto e ha contattato gli autori dell'attacco, perché noi non lo abbiamo mai fatto. Il gruppo degli autori dell'attacco si è identificato come il gruppo PISA (Protect Your System, Amigo).

Molte volte le organizzazioni preferiscono la segretezza per evitare di esporre i loro punti deboli o le loro tattiche di correzione. Questo aspetto non vi preoccupava?

Queste sono preoccupazioni validissime. Ma sono abbastanza certo che tutti noi sappiamo di essere vulnerabili. Quando cerchiamo di mettere in sicurezza la nostra casa, sappiamo che anche se acquistiamo la porta migliore esistente, se i ladri lo vogliono davvero, troveranno un modo per aprirla o escogiteranno un altro modo per entrare. È esattamente lo stesso.

Non c'è da vergognarsi se siamo stati attaccati e se avevamo delle vulnerabilità. Il fatto che noi avessimo una roadmap molto chiara per la protezione ma siamo stati comunque colpiti è un dettaglio importante da condividere con le persone. Anche se avessimo delle protezioni ottime, avremmo comunque delle vulnerabilità passibili di essere attaccate. Adottando ulteriori misure, ci si può trovare in una posizione decisamente più forte.

Cosa avete fatto nell'immediato per iniziare ad affrontare il problema?

Abbiamo spento la rete, tutti i suoi sistemi. Abbiamo contattato la polizia e l'agenzia regionale per la protezione dei dati, che sono cose che bisogna fare per legge. E poi abbiamo fatto partire immediatamente due squadre: una per l'analisi forense e un'altra per il ripristino. Abbiamo chiamato Dell, che ci ha attribuito immediatamente la massima priorità e ci ha assegnato un team davvero straordinario che ha lavorato senza sosta al nostro caso. Sono riusciti a ripristinare completamente tutti i dati sul secondo dominio di dati.

Quindi le analisi forensi sono iniziate durante il processo di ripristino?

Per alcuni dei processi di ripristino, abbiamo dovuto attendere un po'. Per questo direi che sono partite prima le analisi forensi. Tutto è stato messo in quarantena perché occorreva capire cosa fosse successo. Abbiamo dovuto assemblare un altro sistema per iniziare a rimettere a posto le cose. Abbiamo deciso che, anche se ci avessimo messo un po' più di tempo, tutti i sistemi che sarebbero tornati online avrebbero dovuto soddisfare i più elevati standard di sicurezza.

"Credo che la cosa più importante da considerare sia che esiste un'altissima probabilità che tutti, prima o poi, subiamo un attacco informatico e, pertanto, dobbiamo tenere pronto un piano dettagliato di mitigazione e di ripristino".

Lei accennava al fatto che l'autenticazione MFA era solo su Microsoft 365, il che, in parte, è ciò che ha consentito l'attacco. Quindi ora l'MFA è presente su tutta la linea?

Il vettore di attacco era un utente con credenziali compromesse che si trovava in un team che aveva già l'autenticazione multifattore su Microsoft. Quando gli autori dell'attacco hanno tentato di accedere alla posta elettronica e hanno visto che non riuscivano a causa dell'autenticazione MFA, hanno continuato a cercare. E hanno scoperto che avevamo una VPN che non era protetta da MFA. Una volta ottenuto l'accesso tramite VPN, hanno potuto iniziare a ispezionare la rete.

In una rete molto grande come la nostra, hanno trovato un sistema che aveva una vulnerabilità e hanno iniziato i movimenti laterali. Per cui adesso, una volta iniziato il ripristino dei sistemi, abbiamo deciso che niente sarebbe tornato online finché non fosse stato protetto con l'autenticazione multifattore.

Se ci fosse UN consiglio chiave o UNA raccomandazione per evitare un attacco ransomware, quale sarebbe?

È molto difficile dare un unico consiglio, ma ritengo che la cosa più importante da considerare sia che esiste un'altissima probabilità che tutti, prima o poi, subiamo un attacco informatico e, pertanto, dobbiamo tenere pronto un piano dettagliato di mitigazione e di ripristino.

Per esempio, è molto importante avere a portata di mano i contatti dei partner chiave per l'analisi forense e il ripristino, disporre di una mappa dettagliata e prioritaria dei servizi con una tempistica di ripristino e una strategia ben allineata con le principali business unit, compresa la comunicazione (sia interna che esterna). E, naturalmente, è importantissimo tenere gli utenti sempre informati e addestrati sulle tecniche utilizzate dagli autori degli attacchi.

Lei ritiene che il rafforzamento della capacità di sicurezza informatica all'università abbia aumentato la fiducia nel proseguire la vostra missione e nel fare tutte le cose straordinarie che state facendo?

Assolutamente. Prima dell'attacco, una percezione comune era che qualsiasi nuova misura volta a proteggere il sistema fosse ricevuta con molte domande e preoccupazioni circa l'effettiva necessità di tali misure. Il fatto è che la protezione è assolutamente necessaria, perché altrimenti rischi di mettere in pericolo la tua intera azienda. E, naturalmente, alcune persone credono ancora che queste misure ostacolino il loro lavoro. La maggior parte, però ritiene che i sistemi sono protetti molto meglio.

Grazie. La sua schiettezza e trasparenza sono utili a tutti coloro che lavorano d'anticipo per migliorare la loro maturità in termini di sicurezza informatica.