Come evitare di essere la prossima vittima di un Ransomware

Date : 15 giugno 2017

Il ransomware è una delle forme di attacchi di sicurezza in assoluto più prevalenti e temute. Le organizzazioni sono spaventate dal ransomware perché è estremamente difficile da **individuare in anticipo**, difficile da fermare nella diffusione una volta che ha colpito e potenzialmente disastroso in termini di **distruzione dei dati**. A questo si aggiunge l'ignominia di dover pagare il riscatto ai criminali e una penale da parte delle autorità per la regolamentazione della protezione dei dati e il ransomware diventa una minaccia critica per le organizzazioni di tutti i tipi e dimensioni.

Il ransomware viene spesso introdotto in un'organizzazione tramite **email di phishing** ma può anche essere introdotto tramite exploit, unità USB e altri supporti contenenti malware. Funziona rapidamente. Per esempio, siamo a conoscenza di un'organizzazione in cui 30.000 file sono stati danneggiati in quattro minuti. Si estende da macchina a macchina attraverso la rete aziendale, influenza i dispositivi endpoint (PC, laptop) come i server e può anche diffondersi sui supporti di archiviazione sulla rete. Una volta che i file sono criptati è impossibile sbloccarli, qualche che sia lo scopo dell'operazione. La *best practice* suggerisce che affinché un'organizzazione possa prepararsi per questa tipologia di attacco, sia necessaria una **buona strategia di backup** da cui sia possibile ripristinare i dati. Ma i dati sono raramente archiviati in tempo reale, quindi un certo grado di perdita di dati è di solito inevitabile.

Le potenziali conseguenze del ransomware aumenteranno con l'**introduzione del GDPR** nel 2018. Una violazione dei dati personali che include la "distruzione illegale" dei dati potrebbe portare ad una multa fino al 2 percento del fatturato annuo globale. Questo rappresenta chiaramente un aumento significativo del rischio per le aziende, sia in termini di prospettiva finanziaria ma anche in termini di reputazione del marchio.

Che cosa possono fare le aziende per proteggersi dal ransomware? FireEye ritiene che ci siano **cinque aree** in cui le organizzazioni dovrebbero cercare di **minimizzare il rischio della minaccia**.

Il **primo approccio** è quello di **minimizzare la probabilità** che una campagna di phishing possa avere successo, educando gli utenti dell'importanza di conoscere la provenienza di

un’email o di un sito web. Diffondere la consapevolezza sulla pericolosità potenziale degli allegati di una email o di un sito web falso è utile, così come riportare comportamenti sospetti o sconosciuti ad un amministratore di security o ad un altro individuo esperto. Sebbene sia difficile eliminare del tutto le azioni di persone che cliccano su un URL malevolo, educare gli utenti a comportamenti corretti è un buon punto di partenza.

Il **secondo livello** di protezione è **implementare la tecnologia su gateway web e email** che effettuino la scansione per URL conosciuti e sospetti. Tali soluzioni sono utili per classificare contenuti legittimi da malware o siti sconosciuti ma sospetti.

Il **terzo livello** di difesa è avere la **tecnologia installata sull’endpoint**. Questo monitora il comportamento dei processi, rilevando attività sospette che indichino la presenza di ransomware. Per esempio, un processo che sta criptando in modo sequenziale i file è probabilmente un ransomware. Tuttavia è possibile che questo sia anche un processo legittimo utilizzato per la **protezione dei dati**. In questi casi, il processo può essere incluso in una whitelist. Altri approcci riguardano il controllo di autorizzazione ad eseguire un’applicazione, non permettendo l’avvio di applicazioni non presenti nella lista o presenti in una blacklist.

Il **quarto livello** è l’utilizzo di **soluzioni di network security** che possono rilevare il ransomware prima che venga eseguito e possono **mettere in quarantena** il processo sospetto o detonarlo in una sandbox. Altra tecnica permette di rilevare la probabilità di un processo ransomware dipendentemente dalla fonte di download o da altri attributi.

Infine, l’attività dei file sospetta sul server dovrebbe essere rilevata utilizzando tecnologie simili a quelle sugli endpoint. In aggiunta, i dati dei server sono tipicamente archiviati con frequenza giornaliera o superiore, in base alle procedure di data governance. Fino a che questo piano di backup comporta un’archiviazione inaccessibile al ransomware, rappresenta un contributo essenziale nella protezione dal ransomware.

Nessuno di questi approcci è particolarmente innovativo, ma è raro vederli tutti attivi in un’unica organizzazione. Le organizzazioni più mature hanno maggiori probabilità di aver implementato questo approccio a più livelli per una serie di attacchi, e quindi saranno meglio protette contro il ransomware.

A cura di: ***Duncan Brown,*** *Research Director, European Security Practice, at IDC and leads the firm’s security research program in Europe.*