Come difendersi dai Ransomware con la sicurezza datacentrica

Sia che muovano da un semplice smarrimento o sottrazione di credenziali sia che derivino da campagne di *phishing* mirate, **i *ransomware* restano protagonisti assoluti nel quadro del rischio cyber** a cui sono esposte aziende e infrastrutture, anche critiche: basti pensare agli aumentati attacchi diretti a strutture ospedaliere, dalle conseguenze talvolta fatali. Complici la pandemia – che ha imposto, per motivi di lavoro o studio a distanza, un'iperconnessione senza precedenti a utenti poco o per nulla formati alla sicurezza informatica – e la conseguente estensione delle superfici d'attacco, il relativo *trend* si è mostrato in costante crescita nell'ultimo biennio. E niente sembra indicare che sia destinato a invertirsi nel prossimo futuro.

In effetti, secondo la *Harvard Business Review*, nel 2020 si è assistito a un aumento del 150% negli attacchi di tipo *ransomware* (tendenza perfino peggiorata nel 2021) e a un incremento del 300% nelle cifre pagate a titolo di riscatto, con una perdita di 20 miliardi di dollari nel solo settore sanitario. E come conferma l'*ENISA Threat Landscape 2021*, gli attacchi non sono cresciuti solo in volume ma anche in sofisticazione. Ad esempio, nell'anno corrente, sembra che il 91% del *malware* abbia viaggiato su reti (apparentemente) "sicure".

Per questo Varonis, nata nel 2005 e pioniera nel campo della *data security*, offre procedure gratuite di ***Ransomware Preparedness Assessment*** alle aziende che vogliano irrobustire la propria strategia di cyberdifesa.

Tali percorsi mirano a individuare i punti deboli – anche ignoti – di un'organizzazione per proporre, in seguito, soluzioni personalizzate che permettano d'intervenire in modo efficace secondo tre linee operative: drastica riduzione (tramite il controllo e monitoraggio automatico degli accessi) della superficie d'attacco, rapida identificazione dei segnali di potenziali *ransomware* e, in caso l'incidente si verifichi, messa a disposizione dell'*Incident Response & Forensics* team per la rimessa in sicurezza dei sistemi.

Grazie a un approccio data-centrico e all'uso di modelli di rischio *behavior-based*, la ***Data Security Platform*** di Varonis permette di cogliere precocemente anomalie sospette nel comportamento di qualsiasi utente. Ad esempio, Varonis è in grado di rilevare un insolito "accumulo" di dati o l'uso improvviso (e spesso non previsto) della crittografia e, quindi, attivare una serie di risposte automatizzate a partire dal dato e verso l'esterno.

Come ricorda Yaki Faitelson, co-fondatore e CEO, *«la miglior difesa dagli attacchi di tipo ransomware parte dal far in modo che ciascuno abbia accesso soltanto ai dati di cui ha bisogno per fare il suo lavoro»*.

Questo approccio ha provato il proprio valore permettendo di identificare **minacce recentissime**, mostratesi capaci di sfuggire ai tracciamenti tradizionali. Come REvil o Darkside, operazioni globali di crimine informatico scoperte e neutralizzate nel 2020; ma solo dopo aver portato a segno migliaia di attacchi e totalizzato ingentissime somme in criptovalute a titolo di riscatto.

È evidente che in un ecosistema iperconnesso, popolato di minacce in costante espansione, solo una mappatura delle vulnerabilità e una robusta strategia di prevenzione e reazione possano consentire ad aziende e istituzioni di operare in sicurezza, prevenendo sia perdite economiche e sia i molteplici, sgradevoli effetti dei *data leaks*.

Moltissime imprese ed enti di altissimo profilo – dalla Coca-Cola alla NASA – si affidano a Varonis per tutelare i loro dati. Il 97% di questi clienti riporta che il *Data Risk Assessment* ha richiesto meno tempo di quanto si aspettassero; e il 93% conferma che non ha causato rallentamenti o interruzioni nel loro ambiente IT, coniugando azioni incisive con un minimo investimento di tempo. Un investimento destinato a dare i suoi frutti in futuro.

https://www.ictsecuritymagazine.com/notizie/come-difendersi-dai-ransomware-con-la-sicurezza-datacentrica/