AGENZIA STAMPA QUOTIDIANA NAZIONALE
Prima Pagina News

Primo Piano - *Samuele Zaniboni: “Alcune operazioni fondamentali da mettere in pratica per evitare un attacco ransomware”*

Roma - 06 ago 2021 (Prima Pagina News) **Cosa fare oggi per minimizzare l'impatto di un eventuale attacco ransomware? Ce lo spiega Samuele Zaniboni, Presales Engineer Manager di Eset Italia.**

Purtroppo, nonostante il continuo impegno da parte dei gruppi di cybersicurezza nel contrastare le bande di criminali, gli attacchi ransomware di successo che vengono lanciati in ogni parte del mondo, fanno ancora notizia. Basti pensare all’attacco subito dalla Regione Lazio nella notte tra il 31 luglio e l’1 agosto, che ha compromesso i sistemi informatici della regione, compreso il portale di registrazione per le vaccinazioni COVID-19.Un attacco che ha portato come risultato, al momento noto, la cifratura di file nel data center regionale, generando problemi anche sulla rete informatica istituzionale, sul quale stanno investigando Polizia Postale, Europol e persino l’FBI.Non sono solo le grandi aziende nel mirino: le bande che organizzano attacchi ransomware colpiscono anche le piccole imprese che potrebbero non avere i mezzi adeguati per difendersi dagli attacchi. Se la nostra azienda viene colpita, o se vogliamo essere pronti a ogni evenienza, ecco cinque misure da adottare per evitare danni in futuro. 1. Disporre di backup Molte aziende colpite da ransomware scoprono che i loro backup non sono efficaci o mancano dei dati chiave. Questo è emerso, ad esempio, nell'attacco di Colonial Pipeline, dove il riscatto è stato pagato subito per timore di ritardi nel ripristino dei dati di backup. La beffa è stata che, dopo il pagamento, l’azienda ha scoperto che lo strumento di decrittazione era così lento che hanno dovuto ripristinare comunque i dati dai backup, sostenendo inutilmente il costo del riscatto. Serve poi ricordare che, nella concitazione iniziale, bisogna sempre mantenere fiducia nei nostri strumenti di archiviazione. Se non abbiamo una strategia di backup, suggeriamo di consultare il testo Backup Basics che può servire come punto di partenza, così come l’introduzione sui tipi di backup e i cinque errori da evitare durante il backup.2. Sapere come ripristinare i backup Non basta prevedere un sistema di backup, solo dopo aver effettuato il ripristino dei file possiamo avere la certezza che funzioni davvero. Quando è il momento del crash-cart nel bel mezzo di un incidente, è già troppo tardi per mettersi alla ricerca di cosa rallenta il ripristino del backup. È quindi opportuno creare più copie con tecnologie diverse. In questo modo, se una mostra dei problemi, non resteremo comunque bloccati. Questa strategia è utile anche nel caso in cui si cancellino o sovrascrivano accidentalmente i file, ma è fondamentale nel disaster recovery. Gli hard disk sono molto più economici dei nostri dati critici, quindi non bisogna aver paura di comprarne uno in più. 3. Assicurarsi che i backup funzionino in cloud Se è vero che è comodo fare il backup in cloud, sappiamo che il ripristino dei dati può essere estremamente lento, specialmente per i grandi volumi di dati. Un conto è recuperare una lista di contatti, un altro è il ripristino di tutti i backup delle unità aziendali. Inoltre, gli stessi provider di servizi cloud

hanno problemi di sicurezza e possono essere soggetti a violazioni, quindi occorre verificare quali siano le loro policy di sicurezza.Per i dati sensibili, alcune organizzazioni non ricorrono mai al cloud, proprio per proteggere i dati dagli attacchi. Per questo livello di sicurezza, spesso nemmeno i supporti di backup sono collegati alla rete e restano conservati fisicamente presso la sede aziendale in modo sicuro. 4. Essere pronti per il recupero Effettuare un'esercitazione di disaster recovery in tutta l'azienda può essere complicato. Tuttavia, limitando l'esercitazione a una singola divisione potrebbe essere una simulazione praticabile. Nel farla scopriremo quasi sicuramente problematiche da risolvere che potranno essere analizzate con calma e non con la forte pressione che si presenta nel bel mezzo di un attacco. Queste esercitazioni forniscono importanti informazioni ai vertici delle aziende che possono intervenire affinché in caso di attacco non vi siano problemi nel backup e nel ripristino dei dati. È possibile evitare i backup secondo il paradosso di Schrödinger, effettuando test periodici con un ripristino, idealmente su computer diversi in modo da poter verificare che i preziosi dati aziendali non siano andati persi. Come già detto, il momento migliore per testare un backup è prima che se ne abbia realmente bisogno per un'emergenza.5. Definire un piano strategico Pianificare una strategia in caso di un attacco e di una richiesta di riscatto è senz'altro opportuno. Per esempio, ingaggeremo un negoziatore, o abbiamo un team addestrato per la verifica delle richieste degli aggressori? Decisioni come questa sono difficili da prendere lucidamente nell'emergenza di un attacco attivo, quindi diventa essenziale delineare disposizioni operative preventive.Samuele Zaniboni

(Prima Pagina News) Venerdì 06 Agosto 2021

Verbalia Comunicazione S.r.l. Società Editrice di PRIMA PAGINA NEWS
Registrazione Tribunale di Roma 06/2006 - P.I. 09476541009
Iscrizione Registro degli Operatori di Comunicazione n. 21446

Sede legale : Via Costantino Morin, 45 00195 Roma
Redazione Tel. 06-45200399 r.a. - Fax 06-23310577
E-mail: redazione@primapaginanews.it