Milano, 3 ottobre 2022 - Una “guida” firmata Cisco per rendere Internet un posto più sicuro per tutti. Nello specifico 6 consigli utili, pubblicati in concomitanza con il mese della sicurezza, per far fronte agli attacchi di tipo ransomware messi in atto da organizzazioni criminali di vario tipo.

Il ransomware è un tipo di software dannoso (malware) che codifica i dati della vittima: per poter accedere di nuovo ai dati rubati viene chiesto un riscatto che può variare da poche centinaia sino a milioni di euro. Per non essere rintracciati, gli hacker chiedono molto spesso di essere pagati sotto forma di criptovalute. Una volta pagato il riscatto, l'aggressore invia una chiave di decrittazione che permette di ripristinare l'accesso ai dati.

Come funziona?

Gli attacchi di tipo ransomware avvengono attraverso quattro metodi principali:

- Il phishing via e-mail: comunicazioni fraudolente che sembrano provenire da una fonte attendibile.
- Il malvertising: annunci pubblicitari malevoli che, una volta cliccati, installano software malevolo sul device dell'utente.
- Il social engineering che induce l'utente a "fidarsi" dell'hacker a compiere azioni compromettenti.
- Gli exploit kit: un programma, o una parte di codice, progettato per trovare e sfruttare una falla di sicurezza o una vulnerabilità in un'applicazione o in un sistema informatico. Vengono utilizzate anche altre tecniche al fine di aumentare le possibilità di guadagno. Ad esempio, attraverso la compromissione dei sistemi di backup in modo che gli amministratori non possano utilizzarli per ripristinare i dati.

Come difendersi dal ransomware?

Il settore del ransomware è in continua evoluzione: tipologie di attacchi sempre più sofisticate, nuovi gruppi di criminali informatici e nuove tecnologie come, ad esempio, il Ransomware as a Service (RaaS), una vera e propria soluzione che permette anche a gruppi criminali senza particolari competenze informatiche di "affittare" il software malevolo e concentrarsi soltanto sulla scelta della vittima da colpire. Esistono però delle pratiche di cyber hygiene - come appunto quelle suggerite da Cisco - che permettono di evitare di essere colpiti. Vediamole.

La Guida Cisco: 6 consigli per tutti

- **Prevenire l'infiltrazione.** La maggior parte degli attacchi ransomware avviene tramite un allegato e-mail o un download dannoso. È possibile bloccare i siti web, le e-mail e gli allegati sospetti attraverso un approccio alla sicurezza a più livelli e un programma di condivisione dei file che sia sicuro e approvato dall'azienda.
- **Tenere sotto controllo le attività della rete aziendale.** È essenziale essere in grado di vedere ciò che accade all'interno della rete aziendale: soltanto così è possibile scoprire attività sospette e tentativi di attacco. L'unico modo è scegliere una soluzione per la sicurezza informatica che unisca in un unico luogo tutte le informazioni, l'analisi e la capacità di rispondere ad un attacco in modo rapido. È molto importante fare un inventario accurato e aggiornato delle risorse informatiche: le macchine più vecchie e dimenticate spesso forniscono una via d'accesso agli aggressori.
- **Conoscere il nemico attraverso la threat intelligence.** È fortemente consigliato tenersi informati sui rischi e sulle tattiche difensive più recenti, poter fare affidamento su un solido piano di risposta agli incidenti ed essere in grado di gestire le minacce impreviste. Cisco Talos è un team composto da 350 professionisti tra ricercatori, analisti, ingegneri, sviluppatori e linguisti che riescono a

controllare ogni giorno oltre 600 miliardi di email e a risolvere oltre 500 miliardi di richieste DNS al giorno, riuscendo a monitorare circa il 2% del traffico mondiale: una visibilità maggiore di qualsiasi altro fornitore di sicurezza al mondo.

- **Aggiornare con regolarità i software utilizzati.** Controllare e applicare sempre gli aggiornamenti più recenti. Gli hacker sono sempre alla ricerca di un software senza patch: utilizzare un software aggiornato è uno dei modi più efficaci per evitare un attacco.
- **Sfruttare il backup.** Eseguire sempre il backup dei dati in modo che possano essere recuperati in caso di emergenza. Archiviare i backup offline in modo che non possano essere trovati. Sviluppare un piano di ripristino dei dati che possa aiutare a ottenere un ripristino su larga scala garantendo la continuità aziendale.
- La maggior parte degli attacchi avviene a causa di un **errore umano**. Condividere le conoscenze sulla sicurezza informatica è un dovere di tutti: le aziende e i dipendenti devono avere familiarità con la sicurezza informatica e con il ransomware, essere informati sull'importanza della password, su come riconoscere un'e-mail di phishing e su cosa fare se ricevono una comunicazione sospetta.

I principali target

Secondo Cisco Talos, la più grande organizzazione privata di intelligence sulle minacce informatiche al mondo, i settori più bersagliati sono quelli delle Telecomunicazioni, Istruzione, Sanità e Pubblica Amministrazione: tutti settori in cui i dati sono numerosi, sensibili e qualitativamente molto importanti.

Conviene davvero pagare il riscatto?

Spesso si pensa che l'unica soluzione per ripristinare i dati sia pagare: ma è davvero la scelta giusta? Gli esperti di security e il governo stesso sconsigliano fortemente il pagamento. Prima di tutto per fermare il ciclo di attacco: un aggressore che riceve un pagamento sarà sicuramente più motivato a prendere di mira la stessa azienda, sapendo che molto probabilmente pagherà di nuovo. In secondo luogo, pagare non significa che i dati verranno ripristinati o che le informazioni sensibili non verranno divulgate ad altri criminali.

Il mese della sicurezza è una campagna mondiale il cui obiettivo è quello di informare, educare e responsabilizzare le persone sul tema della sicurezza informatica: un'opportunità per aiutare gli utenti e le aziende a conoscere i metodi più efficaci per proteggersi dai criminali informatici.