ARTICOLO DI ELEARNINGNEWS

Year 5 - number 170 Wednesday 1 september 2021

Cyber risk: la difensiva delle imprese

Le nuove sfide per la sicurezza informatica delle imprese sono state portate dal lavoro a distanza e la crescita della digitalizzazione

I nostri dispositivi informatici (privati e aziendali) contengono una enorme quantità di dati, molto interessanti per i **cyber criminali**.

Abbiamo visto che difendersi dagli attacchi informatici è possibile e dipende soprattutto dalla **formazione**, anche in **eLearning**.

Nel corso degli ultimi anni, il **lavoro a distanza** e le comunicazioni via **videoconferenza** hanno portato alla luce nuove criticità per le imprese per difendere efficacemente la sicurezza informatica.

I cyber attacchi non riguardano solo le grandi imprese, anzi. Circa il 50% degli attacchi informatici è diretto verso le PMI, con un costo medio per attacco di quasi 200.000 euro.

Quali sono gli 8 attacchi più comuni all'impianto di cybersecurity aziendale?

1. Advanced Persistent Threat (APT)

APT è una minaccia portata avanti in maniera invisibile e per periodi di tempo molto estesi su una rete o un computer, con l'obiettivo di carpire informazioni riservate o di rendere inutilizzabili alcuni servizi dell'entità attaccata. Molto spesso si tratta di cyberspionaggio ed è attuato da entità statuali. Infatti, gli hacker che utilizzano ATP agiscono spesso per motivazioni politico-economiche.
Se lo stesso livello di attenzione da parte dei criminali informatici fosse rivolto contro un'azienda potrebbe rivelarsi devastante.

2. Phishing

E' la più comune truffa informatica, effettuata inviando un'e-mail con il logo e l'indirizzo email contraffatto (per esempio, di un istituto di credito o di una società di commercio elettronico), in cui si invita il destinatario a compiere una determinata azione, per esempio fornire dati riservati (numero di carta di credito, password di accesso al servizio di home banking, ecc.) o cliccare un link che in realtà rimanda ad un sito malevolo; motivando tale richiesta con ragioni di ordine tecnico. Una volta completata l'azione, l'hacker può accedere a sistemi informatici e raccogliere informazioni personali o aziendali.

3. Denial of Service (DoS)

Il DoS indica un malfunzionamento del sito web dovuto ad un attacco informatico in cui si fanno esaurire deliberatamente le risorse del sistema informatico stesso attraverso due metodi:

- Dati creati su misura: questo metodo consiste nell'inviare a un sistema dati specifici capaci di causare un errore all'interno dello stesso, impedendone il funzionamento.
- Inondazioni: questo metodo comporta il sovraccarico di un sistema per rallentarlo in modo che quest'ultimo non sia più in grado di funzionare.
  Il risultato è inevitabilmente il down time del sito web e conseguente perdita di profitti.

4. Attacchi dall'interno

Gli attacchi dall'interno, sempre più preoccupanti, vedono protagonista un utente che abbia le credenziali per accedere al sistema informatico aziendale (dipendenti, collaboratori esterni).

5. Malware

Il termine malware definisce qualsiasi programma informatico scaricato su un pc all'insaputa dell'utente e usato per causare gravi danni o macchiarsi di violazioni dei dati. Il malware è spesso utilizzato su dispositivi aziendali e privati, ma è anche comunemente usato come forma di spionaggio internazionale a livello governativo.

6. Attacchi alle password

Gli attacchi alle password, noti anche come brute force attacks, sono attacchi in cui un hacker inserisce diverse combinazioni di password nel tentativo di accedere a una rete. Ciò avviene spesso con l'ausilio di sistemi automatizzati.

7. Ransomware

Il ransomware è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom) da pagare per rimuovere la limitazione. Purtroppo, il pagamento non sempre si traduce nella restituzione dell'account.

8. Man-In-The-Middle (MITM)

Un attacco man-in-the-middle avviene quando un elemento terzo intercetta una comunicazione tra due parti. Questa terza parte ottiene l'accesso alla comunicazione, ascoltando o monitorando l'attività, ottenendo l'accesso a qualsiasi informazione condivisa, incluse le credenziali di accesso, le informazioni personali o altro ancora.

Risk management: nuove sfide

Secondo il VIII Osservatorio sulla diffusione del **risk management nelle medie imprese** realizzato da Cineas in collaborazione con Mediobanca, l'emergenza sanitaria che ha colpito l'Italia e il resto del mondo negli ultimi mesi non apparteneva all'orizzonte dei rischi mappati e potenziali, ma non impedirà ad oltre la metà delle imprese interrogate (54,7%) di mantenere gli investimenti programmati. Come detto, invece, il lavoro da remoto e l'avanzamento della digitalizzazione aziendale hanno aperto per tutte le aziende nuove sfide sul fronte della sicurezza che richiedono lo sviluppo di strategie e piani dedicati in ottica di cybersecurity e protezione dei dati sensibili. L'indagine, che ha coinvolto un campione di 339 aziende, evidenzia come, oggi, le imprese intravedono minacce soprattutto in due aree: in primis gli infortuni sul lavoro, ma anche il cyber risk corollario della dipendenza sempre maggiore dalle tecnologie.

Inoltre, "in relazione allo sviluppo del lavoro a distanza, esiste un rischio di perdita di competenze applicate. Serve migliorare lo smart management, la gestione delle persone in remoto, per assicurare la coesione dei team, supportare emotivamente i collaboratori, formarli più intensamente, chiarire ancora meglio gli obiettivi attesi e le tappe per realizzarli" dichiara Massimo Michaud, Presidente di Cineas.