Cyber security awareness: per 7Layers sono fondamentali consapevolezza e formazione

La formazione in ambito cyber security è ormai un tema imprescindibile per le aziende poiché in grado di mitigare i rischi e proteggere il business trasformando i dipendenti da anello debole a strumento di difesa. Oltre l'80% degli incidenti di sicurezza deriva dal **fattore umano**, è fondamentale quindi, tramite un efficace programma di security awareness, portare maggiore consapevolezza del rischio in azienda non solo nei semplici dipendenti ma anche in manager e dirigenti. I più alti livelli di governance sono infatti bersagli più sensibili poiché detengono informazioni aziendali critiche come documenti riservati, segreti industriali etc. Inoltre, in molti casi, saranno proprio i dirigenti a far rispettare le politiche aziendali, sviluppare le risorse umane e garantire che ciascun dipendente sia adeguatamente formato e preparato.

Un tempo la sicurezza informatica era appannaggio di addetti ai lavori, mentre per i semplici utenti era sufficiente avere installato un buon antivirus sul proprio dispositivo. Oggi non è più così: man mano che le tecnologie sono diventate più diffuse e complesse e gli attacchi informatici più sofisticati, è diventato fondamentale sensibilizzare tutti verso l'assunzione di comportamenti corretti, specie in ambito lavorativo.

Secondo **Sergio Dornelles**, Chief BDO & Public Affairs di 7Layers *"Bisogna crescere da un punto di vista culturale e questo lavoro parte dalle aziende, ma deve arrivare a tutti i cittadini. Ci sono più attori che devono stare insieme: il governo del Paese, gli enti per la sicurezza nazionale,*

l'industria delle telecomunicazioni, i fornitori di servizi, gli OTT, gli enti regolatori per la sicurezza, ecc. Ma tutto questo non è sufficiente se non mettiamo al centro le persone, la loro consapevolezza e la loro formazione. Per fortuna stiamo notando una crescita costante degli investimenti e della spesa da parte delle aziende nel campo dell'awareness".

A seguito di una repentina digitalizzazione, avvenuta come risposta alla pandemia e non sempre pianificata nei suoi molteplici aspetti, stiamo assistendo ad un notevole incremento degli attacchi informatici che appaiono cresciuti sia nella quantità che nella severità, intesa come grado d'impatto sull'obiettivo.

Tra le motivazioni spicca il **cybercrime**, riscontrato dietro oltre l'80% degli attacchi, seguito a lunga distanza da attività di *Espionage* e *Information Warfare*. Per quanto riguarda il profilo dell'attaccante, oggi si vede la predominanza di gruppi strutturati e organizzati, specie in settori "specializzati" come quello (in crescita) rappresentato dal *Financial Cybercrime.*

L'onnipresenza del digitale nelle attività e nelle comunicazioni quotidiane comporta numerosi rischi dei quali, come società, soltanto di recente iniziamo ad assumere consapevolezza. Se l'uso di dispositivi interconnessi per lavorare, svagarsi o mantenere contatti con familiari e amici agevola enormemente le nostre vite professionali e sociali, il panorama delle minacce informatiche – dai più banali tentativi di frodi online alle sofisticate campagne di cyber attacco rivolte a obiettivi istituzionali o aziendali – appare in preoccupante espansione, rendendo necessarie attività mirate e costanti allo scopo di proteggere dati e *asset* sensibili di vario tipo, nonché la privacy e la sicurezza delle persone.

Purtroppo il mercato del lavoro non riesce a rispondere ad una così diffusa richiesta di sicurezza e lamenta un gap di oltre il 50% relativo al reclutamento di candidati adatti a

ricoprire ruoli in ambito cybersecurity sottolineando così l'importanza e il valore della formazione specifica in tale settore.

Per poterci difendere è innanzitutto necessario sapere cosa rischiamo: in questo senso, il noto adagio *"conosci il tuo nemico"* non è mai stato così attuale. Vediamo, di seguito, quali sono e in cosa consistono le forme di *cyber menace* ad oggi maggiormente diffuse.

DoS / DDoS: tecniche note per minacce persistenti

Si tratta di una forma di cyber attacco piuttosto datato che prevede un accesso massiccio e automatizzato, di solito tramite *botnet*, a una rete o servizio al fine di saturarlo, portandolo al "collasso" per il troppo traffico. Gli attacchi di tipo (*Distributed)* ***Denial of Service*** presentano il vantaggio di essere piuttosto economici e di fornire una perfetta base per successive richieste estorsive volte al ripristino dei sistemi colpiti.

Ransomware: dati "in ostaggio" e misure di prevenzione

Tra le più diffuse tecniche di attacco informatico e ormai al centro di un giro d'affari miliardario, il ***Ransomware*** è un tipo di **Malware** in grado di crittografare dati o file inerenti una persona, azienda o istituzione bloccandogli l'accesso al dispositivo infetto per poi esigere dalla vittima un pagamento (solitamente in criptovalute) finalizzato alla rimozione di tale limitazione. La più tradizionale – ma sempre efficace – forma di difesa da questo software malevolo consiste nel realizzare diverse copie di backup, almeno tre, su storage differenti e con cadenze regolari. Per garantire la business continuity il backup deve essere a sua volta protetto e isolato in modo da risultare inaccessibile ai cybercriminali.

Phishing e Smishing: comunicazioni pericolose

Tutti scambiamo ogni giorno enormi quantità di informazioni, anche sensibili, tramite email o messaggi telefonici. Le tecniche di ***Phishing*** e ***Smishing*** si inseriscono in tali flussi comunicativi per indurre l'utente a installare sul proprio dispositivo – cliccando su link ingannevoli, facendo download di allegati non verificati o condividendo incautamente una password – del *malware* che sarà in seguito utilizzato per l'attacco vero e proprio. Volendo prevenire questa comune quanto deleteria tipologia di attacchi, è necessario investire sul duplice fronte delle risorse tecnologiche (non solo antispam) e della formazione rivolta agli utenti.

Malvertising: il fronte di rischio che passa dall'*advertising*

Essendo abituati al costante "bombardamento" promozionale su siti, app o piattaforme online, rischiamo di non saper più distinguere l'ADV autentico da quello strumentale; il ***Malvertising*** sfrutta questa confusione, utilizzando falsi annunci o inserendo codice malevolo all'interno di contenuti pubblicitari reali per utilizzarli come vettori di intrusione. Analogamente, lo ***Scareware*** ricorre a messaggi pop-up che segnalano inesistenti problemi o anomalie per spingere ad aprire il link da cui muoverà l'attacco. L'utilizzo di *ad-blocker* può mitigare l'esposizione a queste tipologie di minacce; che tuttavia, per sfuggirvi, assumono forme via via più sottili e sofisticate.

Va ricordato che tutte queste attività malevole, come anche i "classici" attacchi BEC (*Business email compromise*) sono frequentemente condotte attraverso strumenti di ***Social Engineering***; ovvero impiegando tattiche multidisciplinari che inducono una persona, sfruttandone abitudini o disattenzioni, ad "aprire un varco" attraverso cui sarà materialmente

veicolato l’attacco. Ancora una volta, su un piano di prevenzione, l’educazione alla *cyber-awareness* degli utenti appare la sola misura realmente efficace.

Ma oltre alle attività di ***Threat assessment***, necessarie per aver chiare le minacce a cui siamo esposti, è fondamentale conoscere a fondo i punti deboli delle proprie infrastrutture e degli strumenti utilizzati; anche e soprattutto per poter anticipare e prevenire i temutissimi ***Zero-Day***, che sfruttano vulnerabilità sconosciute sino al momento dell’attacco stesso.

Ecco perché l’adozione di strumenti e procedure per la gestione degli incidenti, che includano la periodica formazione di tutte le persone coinvolte insieme a regolari attività di ***Penetration Testing,*** per mettere concretamente alla prova i nostri sistemi e la nostra comunità di utenti, devono co-esistere in una strategia di ***Cybersecurity Awareness*** integrata ed efficace.

A cura della Redazione

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/cyber-security-awareness-per-7layers-sono-fondamentali-consapevolezza-e-formazione/