

News - 11/12/2024

Awareness & Training: Consapevolezza e Formazione per ridurre il rischio Cyber

In collaborazione con Digital Innovation Hub Piemonte e Valle D'Aosta



Da oggi, grazie alla collaborazione con il **Digital Innovation Hub Piemonte e Valle D'Aosta** il nostro sito si arricchisce con una selezione delle notizie e articoli sui temi della digitalizzazione delle imprese. L'obiettivo è offrirvi contenuti sempre aggiornati e di alta qualità. Oggi vi proponiamo un interessante articolo intitolato **"Awareness & Training: Consapevolezza e Formazione per ridurre il rischio Cyber"**, scritto da Michelangelo Polizzi, Digital Transformation Manager presso DIHP. Ecco tutti i dettagli:

Awareness & Training: Consapevolezza e Formazione per ridurre il rischio Cyber

Una delle aree di analisi del Cyber Assessment, valuta la consapevolezza e la formazione delle persone coinvolte in azienda, relativamente alla Cyber Security. La **Consapevolezza** e la **Formazione** sono il punto di partenza per ridurre il rischio degli attacchi informatici alla propria Azienda; quindi, esiste una correlazione diretta tra la Consapevolezza, la Formazione e il Rischio Informatico. Inoltre, uno degli aspetti fondamentali è di non fare l'errore di pensare che la Consapevolezza sia a solo appannaggio del personale IT, ma bensì per avere buoni risultati deve essere estesa a tutto il personale aziendale.

Che cos'è l'Awareness & Training?

Prima di spiegare che cos'è, bisogna sapere che viene stimato che l'**Errore Umano** in più del 90% dei casi è la causa primaria della riuscita di un attacco informatico, e conseguente violazione di un sistema. Di conseguenza, lo scopo principale dell'Awareness Training, è la mitigazione di questo aspetto in modo da ridurre il rischio, e con la formazione, portare **l'Organizzazione da una postura critica ad una più sicura**.

Il **security awareness training** (formazione sulla consapevolezza della sicurezza), in termini generali, consiste nell'assicurarsi che le persone comprendano e seguano determinate pratiche per contribuire a garantire la sicurezza di un'organizzazione. La Formazione ha un ruolo fondamentale nel **ridurre al minimo le gravi minacce alla cybersecurity** poste agli utenti finali dagli attacchi di phishing e dall'ingegneria sociale. Gli argomenti chiave della formazione comprendono: la protezione delle password e la gestione, la privacy, la sicurezza delle email e del phishing, la sicurezza del web/internet e la sicurezza fisica dell'ufficio.

L'obiettivo, i metodi e l'efficacia della formazione sulla sicurezza hanno subito cambiamenti significativi nel corso degli anni. Nel 2004, la maggior parte dei programmi era guidata dall'esigenza di conformità, ovvero di soddisfare semplicemente i requisiti normativi. Oggi, l'attenzione si è spostata sulla formazione alla consapevolezza della cybersecurity come mezzo per gestire e mitigare il rischio organizzativo.

Il circolo virtuoso della cyber security

Sicuramente il primo passo da fare è eseguire un **Cyber Security Assessment (CSA)**, ed in questo caso il **Digital Innovation Hub Piemonte** vi può supportare. Mettendo in condizione le PMI di comprendere la propria postura rispetto al **Livello di**

Maturità Minimo Richiesta, che verrà definito durante l'Assessment, in funzione dell'attività svolta dall'azienda e dalla tipologia dei dati gestiti. Avere una fotografia dell'“**AS IS**”, ovvero del sistema azienda è fondamentale per prendere consapevolezza della situazione in cui ci si trova e disegnare un percorso di formazione che vada realmente a colmare i gaps individuati.

Fino a qualche anno fa, termini come:

- Phishing
- Smishing
- Vishing
- Ransomware / Cryptolocking
- DDos
- Malware / Spyware
- Trojan

Erano dei termini ignoti o conosciuti per lo più dagli addetti al settore IT, oggi fanno parte della nostra vita quotidiana, e non solo aziendale, e dobbiamo conoscerli bene, perché possono diventare l'inizio di un'esperienza assolutamente negativa, a dir poco.

Quindi la prima reale protezione è: **Conoscerli per Evitarli**.

Quindi aumentare la consapevolezza e formare la maggior parte delle persone.

Il ruolo della Formazione sui rischi correlati alla cyber security

Il **Digital Innovation Hub Piemonte** può sostenere le PMI, che hanno effettuato l'assessment, con dei programmi di Formazione, che possono essere anche finanziati fino al 100%, in funzione della tipologia, nonché dimensione dell'azienda beneficiaria.

Durante tutti gli assessments che ad oggi abbiamo effettuato, troviamo un'importante **carenza di informazione/formazione**, sui rischi correlati alla Cyber Security, non per quanto riguarda chiaramente il personale IT, che normalmente è consapevole, ma relativamente alla popolazione aziendale che ha un computer aziendale, connesso in rete e spesso portatile. Altro punto di debolezza è che le attività necessarie, vengono svolte per prassi, ma siamo carenti sulla parte di **formalizzazione**.

La cosa fondamentale, come già detto, per l'Awareness and Training, è non fare l'errore di pensarlo solo ed esclusivamente per gli addetti ai lavori (personale IT), ma deve coinvolgere tutto il personale, per cambiare la cultura aziendale e mitigare il rischio di attacchi.

Bisogna entrare in un giro virtuoso: ovvero, dopo aver fatto un primo **Assessment**, proseguire con la **Formazione** (Educate) consigliata è fondamentale per **Potenziare** (Reinforce) l'Organizzazione e poi **Misurare** (Measure) i miglioramenti. Svolgere un percorso di questo tipo è un ottimo modo per prepararsi a **Penetration Tests o Vulnerability Tests**.

L'anello debole della catena della cyber security

Per ultimo ma non ultimo, bisogna considerare che tutte le aziende sono clienti e/o fornitori, quindi facendo parte di una catena di fornitura, potreste essere “**l'Anello Debole della Catena**” e diventare, nonostante tutto, la via di accesso per l'attacco informatico, ad un vostro cliente o fornitore.

È quindi fondamentale avere la **Consapevolezza** che proteggersi, non è solo un requisito per la propria Impresa, ma è una necessità nei confronti dei propri Fornitori e Clienti. Oggi è a nostra discrezione, ma a breve potrebbe diventare un obbligo per poter sviluppare, produrre e vendere il nostro prodotto o servizio.

Il DIHP e la partecipazione di Unione Industriale Biellese

Il **Digital Innovation Hub Piemonte e Valle D'Aosta (DIHP)** è un "centro di trasferimento tecnologico" creato per supportare la trasformazione digitale delle imprese delle due regioni, in particolare le PMI, e la Pubblica Amministrazione. L'obiettivo è aumentare la consapevolezza e la comprensione delle sfide digitali, guidando le aziende nell'elaborazione dei loro piani di digitalizzazione e fornendo servizi di mentoring e supporto. Collaborano con università, centri di ricerca e aziende leader per promuovere l'innovazione tecnologica. L' **Unione Industriale Biellese** partecipa al DIHP offrendo supporto alle aziende locali per avviare strategie di digitalizzazione, accedere a finanziamenti e migliorare la loro maturità digitale attraverso valutazioni e consulenze specializzate.

Scopri di più: [DIHP](#)