Sicurezza informatica: buoni propositi e sfide culturali per il 2021



Ci apprestiamo a chiudere l’anno 2020 che ha visto le organizzazioni costrette ad operare in condizioni di emergenza determinata dal manifestarsi dello scenario pandemico.

L’esperienza maturata e l’attenzione agli errori passati dovranno generare nel 2021 proposte per superare alcuni vecchi comportamenti in tema di gestione della sicurezza informatica.

Il cambiamento richiede importanti sfide culturali, alcune delle quali andremo di seguito ad analizzare.

Gestione di un problema VERSUS Rinvio dell’intervento fino alla crisi

Troppo spesso le organizzazioni rinviano la gestione di problematiche manifeste fino all’inevitabile aggravarsi del fatto rilevato che può comportare, ad esempio, un attacco cyber o un disservizio al cliente.

Esempi classici di mancate azioni riguardano il rifiuto a spegnere un server per una corretta applicazione di patch, piuttosto che la scelta di continuare a lavorare utilizzando hardware e software obsoleti per risparmiare budget.

Questo atteggiamento operativo e culturale comporta una operatività malata con conseguenze negative per l’immagine dell’organizzazione.

È necessario, quindi, che i rischi derivanti dal rinvio degli interventi e le possibili conseguenze siano condivisi con il Top Management in modo tale da supportarlo nel processo

decisionale.

Sicurezza come supporto al Business VERSUS Sicurezza come limite al Business

Da sempre la sicurezza è vista come il principale freno all'innovazione e alle attività di business. Tale visione deve cambiare.

La sicurezza oggi gioca un ruolo fondamentale nel business; essa è la chiave del vantaggio competitivo, conquistando la fiducia dei clienti e proteggendo il nome dell'azienda.

Il Chief Information Security Officer (CISO) di oggi non deve solo essere esperto di tecnologia ma deve sostenere l'Head of Business per una sicurezza allineata e di supporto alle necessità del mercato.

La sicurezza non deve rappresentare solo una difesa dell'organizzazione da attacchi ed imprevisti ma deve essere sempre più un elemento facilitatore di decisioni che bilanciano la necessità di protezione ed una efficiente gestione delle attività.

A sua volta, il responsabile del business deve rispondere anche del livello di sicurezza dei servizi offerti sul mercato.

Investimenti VERSUS Contenimento di risorse

La pandemia ha visto molte aziende investire in sistemi IT, ad esempio fornendo computer portali per favorire lo smart working ai dipendenti o potenziando la network per garantire a tutto il personale il lavoro da remoto.

L'aumento degli attacchi informatici, specie durante la pandemia, ha evidenziato che la sicurezza non va mai in

vacanza. Sono stati identificate lacune e punti di miglioramento che devono essere affrontati e risolti principalmente aumentando gli investimenti in modo da fronteggiare scenari di attacchi sempre più sofisticati.

Assunzione di rischio VERSUS Ignorare il rischio

Gestire la sicurezza non significa solo adottare le azioni necessarie per l'eliminazione di tutti i rischi.

Il processo di governance prevede l'identificazione dei rischi e la loro analisi con relativa misurazione. Nel caso non sia possibile implementare le azioni necessarie alla loro cancellazione o nel caso tal azioni siano possibili solo nel medio o lungo termine allora la soluzione da adottare è una mitigazione ed accettazione del rischio.

Fondamentale, infatti, è la conoscenza del rischio e delle possibili conseguenze da parte del top management. Al management si richiede, quindi, non di ignorare i rischi ma di comprenderli e di assumersi la relativa responsabilità.

L'accettazione del rischio deve ovviamente prevedere una data di scadenza ed un piano di mitigazione e/o eliminazione del rischio entro il termine stabilito.

Awareness continua VERSUS Formazione una tantum

Come ormai è noto con sicurezza informatica si intende una materia molto ampia ed in continua evoluzione. L'ultimo buon proposito sta nel riconoscere che la cybersecurity è in continua evoluzione e per questo necessita che il personale sia continuamente formato e sensibilizzato.

Non solo le aziende devono pianificare budget per investimenti hardware, software, di network o infrastrutturali ma anche di

training ed awareness.

Naturalmente tutto il personale riveste un ruolo fondamentale per quanto concerne la sicurezza dell’organizzazione in quanto coinvolto direttamente nell’uso di strumenti informatici e piattaforme che interagiscono fra loro.

Un attacco informatico banale spesso si insinua nella posta elettronica utilizzata da tutto il personale. Per questo motivo, è importante fornire a tutto il personale gli strumenti per affrontare le minacce derivanti dalla loro attività, riconoscerle e se possibile evitarle.

In conclusione, molte saranno le sfide che le organizzazioni dovranno affrontare nel corso del 2021 ma sicuramente investire su dipendenti formati e sensibilizzati sulle vulnerabilità delle organizzazioni sarà il presupposto necessario per la crescita futura delle stesse.

Articolo a cura di **Lisa Da Re**

https://www.ictsecuritymagazine.com/articoli/sicurezza-informatica-buoni-propositi-e-sfide-culturali-per-il-2021/