Cyber Security Awareness: il fattore umano e la sfida “post-pandemica”

www.cyberguru.it

Cyber Guru

INDICE

Gli effetti devastanti della pandemia sulle vulnerabilità umane, e la necessità di investire sul fattore umano per aumentare la resistenza dell'organizzazione agli attacchi Cyber.

EXECUTIVE SUMMARY

La crescita esponenziale degli attacchi Cyber andati a buon fine nei confronti di individui e organizzazioni, la cui causa originaria si può far risalire ad un errore umano, ha tolto definitivamente ogni dubbio rispetto a quale sia l'anello debole della catena difensiva di ogni organizzazione.

Il fattore umano, reso ancora più vulnerabile dall'effetto pandemico, è oggi il vettore primario utilizzato dalla criminalità informatica per insinuarsi all'interno delle organizzazioni, con strategie offensive che si fanno sempre più sofisticate. Sono proprio gli utenti, con i loro comportamenti non adeguati alla complessità della sfida, ad aprire inconsapevolmente la porta agli attaccanti.

Il trend era già molto evidente prima della pandemia. Analizzando i vari rapporti 2020 che riguardano lo stato della Cybersecurity, sia a livello italiano sia a livello globale, il quadro che emerge è che la crescita degli attacchi Cyber sembra inarrestabile, e che tra le varie tecniche di attacco utilizzate, quelle caratterizzate da una maggiore crescita, emergono soprattutto quelle che fanno leva sul fattore umano. Un'ulteriore conferma che la stragrande maggioranza degli attacchi Cyber ha una matrice umana, riconducibile ad un'azione non corretta da parte di un utente.

L'ingresso sullo scenario economico e sociale della pandemia da Coronavirus non ha fatto altro che acuire questa situazione, facendo impennare il numero degli attacchi. L'azione dei criminali Cyber si è concentrata sempre di più sugli individui, che di fronte al fenomeno pandemico e alle sue principali conseguenze, come il massiccio ricorso allo smart working, si sono rilevati molto più vulnerabili di quanto forse le organizzazioni avessero potuto immaginare.

La cronaca si è quindi riempita di attacchi Cyber andati a buon fine, che hanno colpito organizzazioni di tutti i settori e di tutte le dimensioni. Brand prestigiosi e altri meno conosciuti, hanno visto le proprie attività produttive bloccate e la propria reputazione compromessa. Anche il vecchio ritornello spesso citato da molte PMI, "noi non siamo appetibili per un hacker", è stato smentito dai fatti.

La Cybersecurity è un problema trasversale che riguarda tutto il sistema Paese e che colpisce indifferentemente individui e organizzazioni di ogni genere

Si tratta di una guerra asimmetrica che vede gli attaccanti in una posizione di indubbio vantaggio, soprattutto perché la prima linea di difesa è costituita da civili inermi che, nella maggior parte dei casi, non hanno neanche la percezione di essere attaccati. In questi ultimi anni le capacità di difesa a livello tecnologico sono indubbiamente aumentate, ma l'efficacia di questi investimenti viene costantemente vanificata, in virtù della teoria dell'anello debole, per cui la "forza complessiva di una catena è determinata dal suo anello più debole". Quando l'anello debole, come in questo caso, è rappresentato dagli utenti che interagiscono con le tecnologie digitali e con la rete Internet, risulta evidente che gli investimenti tecnologici non sono più sufficienti a fermare gli attacchi.

L'unico modo per ricreare una simmetria tra attaccanti e difensori, è quello di investire sulla "prima linea di difesa", ossia sugli utenti digitali. È necessario che ogni organizzazione predisponga programmi efficaci ed innovativi di Cyber Security Awareness. La guerra però potrà essere vinta solo se questi investimenti dimostreranno tutta la loro efficacia sul piano formativo, con programmi in grado di incidere concretamente sui comportamenti umani.

Negli ultimi anni gli investimenti, spesso insufficienti, fatti in quest'area sono stati guidati più dall'esigenza di raggiungere un grado minimo di conformità alle normative, che da quella di raggiungere obiettivi efficaci di protezione dagli attacchi Cyber. Del resto, tutte le principali normative e i framework che fanno espliciti riferimenti alla sicurezza informatica (es. GDPR, NIST, Direttiva NIS, AGID […]), hanno evidenziato la questione della formazione degli utenti finali, lasciando però un ampio spazio di interpretazione alle organizzazioni nel determinare cosa fosse necessario per raggiungere la conformità a queste prescrizioni. Uno spazio così ampio che le iniziative realizzate si sono rilevate sicuramente funzionali rispetto all'esigenza di risultare conformi alle normative, ma assolutamente inefficaci rispetto all'obiettivo reale: aumentare la protezione degli individui e delle organizzazioni dal rischio Cyber.

Possiamo pertanto dare per assodato che:

- il rischio Cyber è tra i più importanti rischi di business a cui andranno incontro le organizzazioni, da qui ai prossimi anni,
- gli attacchi Cyber fanno sempre più leva sulla componente umana, il vero anello debole della catena difensiva,
- il trend degli attacchi Cyber è in continuo aumento.

Per queste ragioni diventa quindi fondamentale avviare dei programmi di Cyber Security Awareness efficaci e innovativi, in grado di incidere sui comportamenti umani e trasformare gli utenti nella prima linea di difesa delle organizzazioni.

Questa è fin dall'inizio la specifica missione di Cyber Guru: realizzare una piattaforma di Cyber Security Awareness in grado di aiutare concretamente i propri clienti nel rafforzare l'anello più debole della catena di Cybersecurity.

La piattaforma Cyber Guru è stata realizzata e costantemente implementata, utilizzando le tecnologie, i processi di produzione e le metodologie pedagogiche più avanzate per garantire il massimo coinvolgimento degli utenti e il raggiungimento dell'obiettivo principale di un programma di Security Awareness: la protezione dai rischi Cyber.

1. Lo scenario

1.1 La trasformazione digitale

SUMMARY: il 2020 ha provocato uno sconvolgimento sociale ed economico innescato dalla pandemia da Coronavirus, una situazione che ha generato una trasformazione digitale forzata e soprattutto gestita in modalità emergenziale. Ma il 2020 verrà anche ricordato per la crescita degli attacchi Cyber, che hanno soprattutto sfruttato le maggiori vulnerabilità di carattere psicologico e anche il gap esistente tra il processo di digitalizzazione forzata e la consapevolezza degli utenti rispetto alle minacce Cyber.

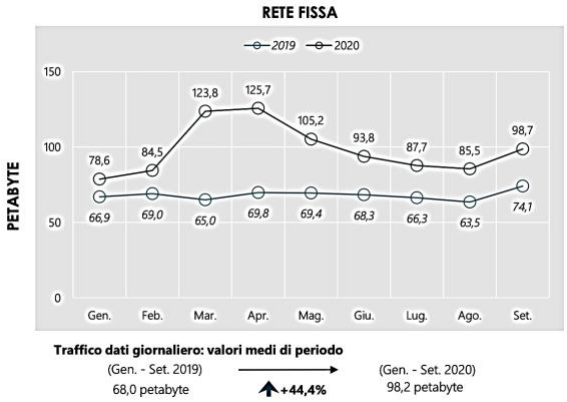
Il 2020 passerà certamente alla storia per la pandemia da Covid-19, ma verrà anche ricordato per il proliferare di attacchi Cyber in grado di colpire, sia sul piano simbolico che su quello fattuale, organizzazioni di tutti i tipi: brand più o meno famosi, istituzioni pubbliche, e, purtroppo, anche enti di ricerca e istituzioni sanitarie coinvolte in prima fila nella lotta contro il virus.

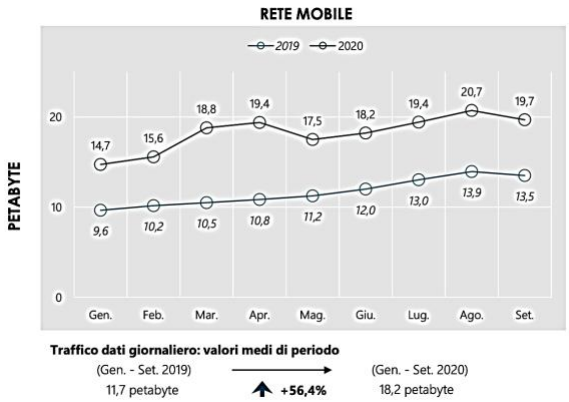
Molti di questi attacchi hanno preso spunto dallo sconvolgimento sociale ed economico innescato dagli effetti della pandemia. Uno degli effetti principali è stato sicuramente il forte impulso verso una spontanea trasformazione digitale della società, che si è trovata a far ricorso, in molti casi, a processi e modalità di carattere emergenziale.

Basti pensare al massivo utilizzo dello smart working, diventato in breve tempo indispensabile per dare una risposta veloce e continuativa alle attività lavorative, e rispondere alle nuove regole sociali e pandemiche. La trasformazione digitale è stata evidente anche nell'utilizzo massivo della didattica a distanza, nella crescita dell'e-commerce, nel ricorso sempre più frequente a piattaforme di social collaboration e di intrattenimento digitale.

Un segno indiscutibile di questa rapida trasformazione è anche riscontrabile nella crescita degli acquisti online, che, in Italia, si va attestando in questo anno sulla quota record di 22,7 miliardi di euro, con una crescita del 26% (4,7 miliardi) rispetto al 2019, l'incremento più alto di sempre.[i] Questa crescita è stata influenzata anche dall'aumento dei nuovi "clienti" che si sono avvicinati al commercio online per necessità, un target sicuramente interessante per chi voglia lucrare in modo più o meno lecito, facendo leva sulla loro inesperienza. Ricordiamo che nel commercio online entrano in gioco metodi di pagamento come le carte di credito, i cui dati sono particolarmente appetibili per i criminali Cyber.

A conferma della maggiore digitalizzazione della società non possiamo non evidenziare anche il consistente aumento dell'uso di banda. Nei primi mesi della pandemia molti operatori di servizi di rete hanno registrato aumenti così importanti, da far temere scenari apocalittici sulla tenuta di Internet. Secondo i dati dell'Osservatorio delle Comunicazioni, nel periodo gennaio-settembre 2020, il traffico dati giornaliero in Italia è aumentato, rispetto al corrispettivo periodo del 2019, del 44% sulla rete fissa e del 56,4% sulla rete mobile.[ii] Gli aumenti sono rimasti costanti anche nel periodo estivo, dopo la fase del lockdown, facendo pensare a un consolidamento strutturale di questo fenomeno, al di là degli effetti a breve termine indotti dalla pandemia e dal distanziamento sociale.





Un uso così "spinto" della sfera digitale, che rappresenta comunque una grande opportunità sulla strada dell'innovazione, è avvenuto senza una corrispettiva crescita della cultura digitale, e quindi senza una vera capacità da parte degli utenti di poter fruire delle tecnologie digitali e della rete Internet in modo sicuro. In assenza di una reale consapevolezza delle minacce del mondo digitale, questa trasformazione forzata ha fornito delle grandi opportunità alle organizzazioni criminali Cyber. Perché per un criminale Cyber, a differenza della maggior parte degli utenti, operare in smart working rappresenta la normalità e non l'eccezione.

1. Lo scenario

1.2 Gli attacchi Cyber: situazione Ante-Covid

SUMMARY: tutti i dati raccolti, confermano come già nel 2019, e quindi prima dell'esplosione della pandemia, gli attacchi Cyber rappresentassero una vera e propria emergenza, e come la leva principale utilizzata dalle organizzazioni fossero i comportamenti degli utenti, il cosiddetto fattore umano. I dati confermano anche l'uso di strategie multi-obiettivo messe in atto dalla criminalità Cyber, e quindi l'estrema trasversalità di un fenomeno che riguarda individui e organizzazioni, in questo ultimo caso di qualsiasi tipo e dimensione.

La situazione Ante-Covid risultava già molto preoccupante: il rapporto Clusit, il principale rapporto sullo stato della Sicurezza ICT italiana evidenziava per il 2019 lo stesso trend di crescita registrato per gli attacchi Cyber degli anni precedenti, raggiungendo per la categoria di attacchi classificati come gravi un +7,6% rispetto al 2018, e un +48% rispetto al 2014[iii].

Nel rapporto pubblicato dall'Enisa, l'Agenzia dell'Unione Europea per la Cybersecurity, si trovano riferimenti espliciti a conferma del trend di crescita degli attacchi in termini quantitativi, e in termini di capacità distruttiva[iv].

Dalle varie analisi disponibili, appare altresì evidente come, già nel 2019, la maggior parte delle strategie utilizzate dai criminali Cyber per effettuare un attacco, abbia avuto come obiettivo primario il fattore umano, ossia il comportamento non corretto dell'utente.

I criminali Cyber fanno leva sulle vulnerabilità dell'individuo per aprire una breccia all'interno del sistema difensivo delle organizzazioni. In questo quadro, l'individuo non solo diventa inconsapevole alleato di una strategia che mira al "bersaglio grosso", ma rischia di essere lui stesso vittima di questa strategia multi-obiettivo.

Nel Rapporto Clusit 2020 emerge come la tecnica di attacco con il maggiore incremento rispetto al 2018, e che ha prodotto gli effetti più gravi, è quella classificata come Phishing/Social Engineering, con un +58%. Altre due tecniche di attacco, i Malware (la più diffusa in termini assoluti) con un +24%, e l'Account Cracking con un +54%, sono comunque facilmente riconducibili a debolezze del fattore umano.

CYBERPEDIA

Il Phishing è una tecnica di attacco basata sull'inganno dove il vettore di attacco utilizzato è una mail dal contenuto ingannevole. Forme similari di attacco, vengono veicolate anche attraverso sistemi di messaggistica (SMS, Whatsapp, […]).

Il Social Engineering è l'insieme delle tecniche di attacco, tra cui il Phishing, che hanno l'obiettivo di ingannare l'utente grazie a forme di manipolazione psicologica. Il punto di forza di questa strategia manipolatoria è la conoscenza del target.

I Malware (Virus, per la comune terminologia) sono software malevoli che servono ad "infettare" i dispositivi di un utente o di un'organizzazione, con finalità fraudolente. Nella maggior parte dei casi, i Malware vengono distribuiti attraverso tecniche di Phishing.

Per Account Cracking si intende la violazione di un account (es. Account di Posta) con finalità fraudolente. Per ottenere questo risultato, il criminale Cyber fa spesso ricorso a vulnerabilità nel sistema di gestione delle credenziali di accesso, in modo particolare delle password.

1. Lo scenario

1.3 Gli attacchi Cyber: situazione Post-Covid

SUMMARY: la situazione peculiare generata dalla pandemia è all'origine della crescita degli attacchi Cyber registrata nel 2020. Da questo punto di vista bisogna tenere conto sia delle vulnerabilità di carattere tecnologico, collegate allo smart working, sia di quelle di carattere psicologico, collegate allo stato di emergenza e alla condizione di distanziamento sociale. La superficie di attacco a disposizione della criminalità è sicuramente aumentata, e questa opportunità è stata usata per portare a segno attacchi che hanno avuto un effetto dirompente su molte organizzazioni. La cronaca è stata saturata da casi emblematici relativi a organizzazioni di ogni tipo e ogni dimensione, che hanno visto venire meno la propria capacità di operare per periodi più o meno lunghi, con tutte le conseguenze, economiche e di immagine, che un fermo di questo tipo può comportare.

La pandemia da Covid-19 ha avuto un effetto dirompente non solo sul piano economico e sociale, ma anche sull'accelerazione degli attacchi Cyber classificati come gravi.

Tutto questo si è tradotto in una rapida crescita delle criticità. Lo smart working è diventato al contempo un'opportunità e un rischio: un'opportunità perché ha consentito di imprimere una svolta nei processi di trasformazione e innovazione digitale, un rischio perché il mondo digitale è diventato ancora più appetibile alle organizzazioni criminali di ogni tipo, con obiettivi che appartengono sia alla sfera economica sia a quella geopolitica.

Due i principali driver dell'accelerazione degli attacchi Cyber:

- il primo direttamente connesso con l'effetto pandemico sulla psiche umana, che ha generato stati di ansia e paura tipici delle emergenze, con la perdita dei tradizionali punti di riferimento, la ricerca ossessiva di notizie e informazioni e la difficoltà di discernere tra le informazioni vere e false;
- il secondo riconducibile al ricorso massivo ed emergenziale a forme di telelavoro, che sono state tutte classificate, anche in modo improprio, con il termine smart working.

Il rischio nell'epoca Post-Covid si è quindi caratterizzato per l'aumento della cosiddetta superficie d'attacco a disposizione dei criminali, che hanno potuto avvantaggiarsi di vulnerabilità di carattere sia tecnologico, sia psicologico:

- Tecnologico - lo smart working si basa su un'architettura complessa che fa spesso uso dei dispositivi privati dell'utente, meno sicuri per definizione e dotati di configurazioni hardware e software che non sono sotto il totale controllo dei dipartimenti IT-SEC.
- Psicologico: l'utente nella sua dimensione abitativa è maggiormente isolato, e quindi, per l'effetto del distanziamento sociale, tende a perdere i suoi abituali punti di riferimento all'interno dell'organizzazione, difficili da ritrovare con il solo utilizzo degli strumenti di social collaboration. Inoltre, nel contesto specifico generato dalla pandemia, spesso gli spazi casalinghi vengono condivisi con altri familiari che operano con le stesse modalità, sia per ragioni di carattere professionale sia per ragioni di carattere didattico, creando in questo modo condizioni critiche dal punto di vista della sicurezza informatica. La condivisione dei dispositivi, della rete, e anche fenomeni indotti dalla distrazione, diventano elementi che giocano a vantaggio della criminalità.

Sembra ormai evidente che il fenomeno dello smart working sia destinato a sopravvivere in forma strutturale, anche oltre la pandemia.

Se è vero che molte criticità evidenziate nella fase emergenziale sono già state affrontate, e lo saranno ancora di più in futuro, resta comunque uno scenario critico con una superficie di attacco molto estesa che va oltre i perimetri convenzionali delle organizzazioni.

Quello che preoccupa di più non sono tanto le vulnerabilità di carattere tecnologico, quanto quelle di carattere umano, perché il gap che esiste tra la velocità del processo di trasformazione digitale e quella del processo di adeguamento delle persone a questa nuova dimensione socioeconomica, diventa sempre più ampio. In una nota di aggiornamento del proprio rapporto, lo stesso Clusit definisce il primo semestre del 2020 come il "semestre nero" della Cyber Security, con un incremento degli attacchi "noti" (quelli di domino pubblico) del 7% rispetto allo stesso periodo dell'anno precedente.

Lo stesso rapporto evidenzia sia l'effetto pandemia, visto che il 14% degli attacchi registrati è stato a tema Covid, sia la matrice umana, con il 61% dei casi realizzati attraverso campagne di Phishing e Social Engineering[v].

Questo dato è confermato anche dal report sullo scenario Cyber prodotto da F-Secure. Il report dettaglia l'incremento di e-mail a tema Covid-19, evidenziando come il tasso di diffusione si sia alzato decisamente durante i mesi di marzo, aprile e maggio e sia proseguito anche successivamente, anche se con tassi più bassi[vi].

Il risultato di tutto quello che abbiamo visto è stato l'aumento impressionante di attacchi Cyber durante il 2020, che hanno finito per colpire, anche in modo serio, tantissime organizzazioni, sia del settore privato sia del settore pubblico. Hanno fatto scalpore gli attacchi Ransomware che hanno bloccato l'operatività di Brand famosi, e anche i numerosi attacchi subiti da istituzioni della sanità e della ricerca, tra cui quelle in prima linea nella lotta alla pandemia.

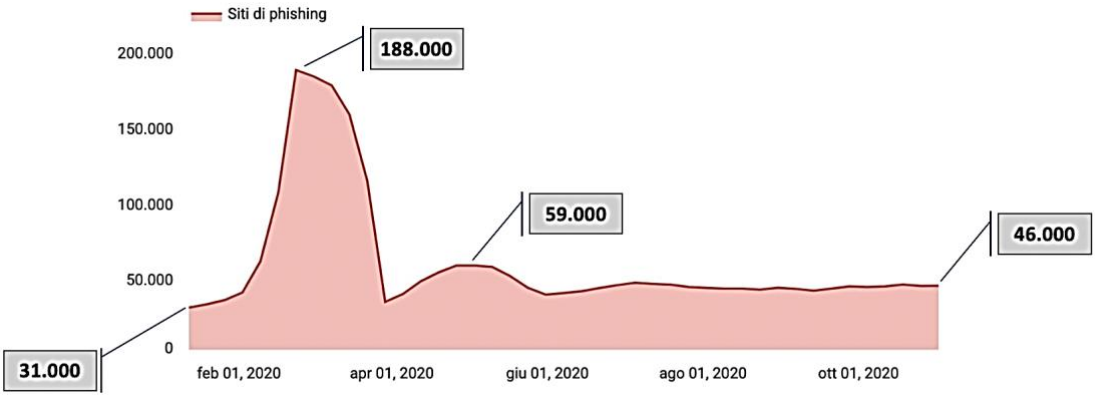
SUMMARY: tra le tecniche di attacco utilizzate dai Criminali Cyber, il Phishing è certamente la più utilizzata. Durante la pandemia si è registrato un aumento significativo di e-mail di Phishing, soprattutto a tema Covid. Gli hacker hanno saputo sfruttare in modo tempestivo, il cambiamento intervenuto nella sensibilità degli utenti e la particolare situazione emotiva generata dalla pandemia e dal distanziamento sociale.

Sicuramente nel 2020 il fenomeno Phishing è emerso in maniera particolare, con un aumento vertiginoso delle e-mail che hanno sfruttato il tema Covid, ma anche tutti i temi "caldi" del periodo, come il già citato smart working.

Le e-mail a tema Covid hanno fatto uso principalmente di due metodi di contagio: il classico allegato contenente malware e i collegamenti ipertestuali verso siti malevoli.

Nella top-ten mondiale di e-mail a tema Covid-19 con allegato, troviamo una mail circolata in Italia con oggetto: "Coronavirus – Informazioni importanti su precauzioni". La e-mail aveva come mittente apparente l'Organizzazione Mondiale della Sanità e invitava a cliccare su un file Word contenente le tanto attese informazioni sulle precauzioni da prendere. Questa e-mail è risultata particolarmente "aggressiva" nella prima fase della pandemia, anche a causa della spasmodica ricerca di informazioni sui comportamenti da adottare.

Quello che emerge con estrema chiarezza è la crescita impressionante avvenuta a cavallo di marzo e aprile del numero di siti Phishing. La reportistica di Google Navigazione Sicura ha censito un passaggio repentino da circa 30.000 siti Phishing individuati, a circa 188.000 nel momento peggiore, per poi attestarsi a oltre 40.000 alla fine del periodo di picco pandemico[vii].



Il cambiamento intervenuto nella sensibilità e nella vulnerabilità del fattore umano è stato registrato anche dalla nostra piattaforma di addestramento anti-phishing (Cyber Guru Phishing), che nei mesi di picco ha evidenziato due fenomeni:

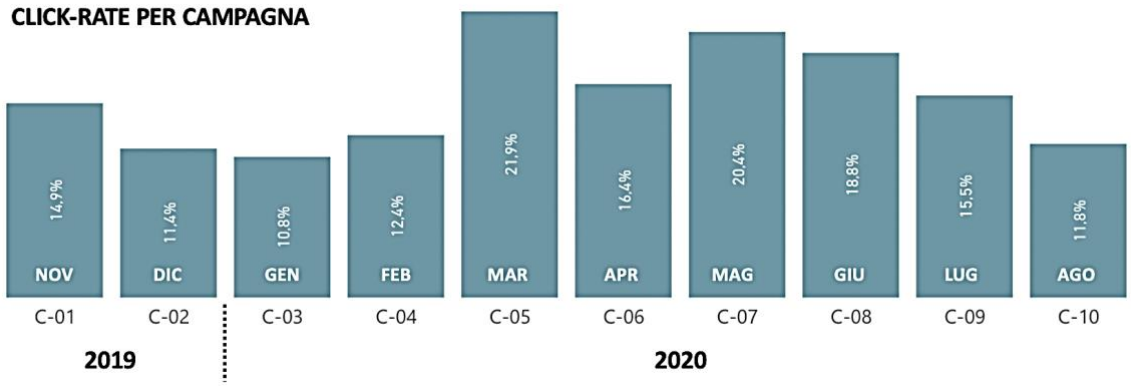
- un rimbalzo generalizzato del Click-Rate, più contenuto nelle aziende maggiormente "addestrate", ma comunque presente, a dimostrazione di una maggiore tendenza a cliccare;
- un cambio delle sensibilità rispetto all'oggetto e al contenuto delle e-mail.

CYBERPEDIA

Il Click-Rate è il cosiddetto tasso di Click e quindi il rapporto tra numero di Click e numero di attacchi ricevuti.

Ricordiamo per maggiore chiarezza che un Click effettuato su una mail di Phishing può provocare conseguenze serie. Una piattaforma che si occupa di effettuare attacchi simulati, come Cyber Guru Phishing, misura il Click-Rate come rapporto tra il numero di Click e il numero di attacchi simulati inviati.

Per quanto riguarda il "rimbalzo" del Click-Rate, si può osservare il grafico preso a campione da una delle tante organizzazioni che utilizzano questi programmi di addestramento anti-phishing.



Come si può vedere dall'immagine, un'organizzazione che aveva intrapreso il percorso di addestramento anti-phishing a partire da novembre del 2019 e che aveva già visto una significativa riduzione del Click-Rate, invece di proseguire nel suo trend al ribasso, come accade normalmente per questo tipo di addestramento, ha subito un rimbalzo per effetto dell'emergenza, a partire da febbraio 2020, che ha poi riassorbito solo a partire dal mese di agosto 2020.

Per quanto riguarda invece il cambio di sensibilità, la piattaforma ha registrato una variazione sostanziale dei Click-Rate in base all'oggetto e al contenuto del template di attacco. Tanto per esemplificare, le e-mail apparentemente provenienti dalle funzioni di Direzione o di HR hanno ottenuto un Click-Rate molto elevato, così come quelle che avevano un oggetto riferibile a scadenze fiscali, a informazioni sulle misure di prevenzione sanitaria oppure a notifiche di servizi in Cloud.

Prendiamo ad esempio questa e-mail di simulazione phishing. Il contenuto è molto scarno e anche un po' subdolo, con un oggetto che genera aspettativa, ma praticamente senza un vero contenuto.

Vantaggi per i dipendenti

Nuove disposizioni per i dipendenti aziendali

A: Maurizio [redacted]

Se non puoi visualizzare correttamente questo messaggio clicca qui

Questa e-mail, prima dell'emergenza pandemica, era considerata di bassa pericolosità, con percentuali medie di Click-Rate molto basse. Con l'avvento del Covid-19, l'oggetto "nuove disposizioni per i dipendenti" ha toccato evidentemente una corda scoperta proprio in un momento di attesa spasmodica di nuove disposizioni.

1. Lo scenario

1.5 Non solo Phishing

SUMMARY: il Phishing rappresenta una vera emergenza su cui si sta focalizzando la massima attenzione da parte delle organizzazioni. Ma sarebbe un errore pensare che tra le minacce Cyber correlate con il fattore umano ci sia solo il Phishing. Durante la pandemia sono state molte le aree critiche della sfera digitale, che hanno mostrato importanti vulnerabilità, dovute anche alla peculiare situazione di isolamento in cui le persone si sono venute a trovare. Tra queste aree particolarmente critiche, e pertanto interessanti per il Cybercrime, ci sono ad esempio le videoconferenze e lo streaming video, il cui uso si è fatto sempre più frequente.

È chiaro che in questo momento l'attenzione massima è nei confronti del fenomeno Phishing, che nello scenario attuale sembra un fiume che abbia rotto il proprio argine, creando una vera e propria alluvione, impossibile da arrestare con i sistemi tradizionali. Nessuno può quindi permettersi il lusso di restare ad osservare il fenomeno, in attesa che passi.

È fondamentale però comprendere che tra le minacce Cyber, correlate con il fattore umano, non esiste solo il Phishing. Spesso il Phishing rappresenta solo l'innesco di una sequenza di attacchi che chiama ripetutamente in causa l'utente e i suoi comportamenti.

L'uso ibrido dei dispositivi, la gestione delle credenziali, il ricorso frequente a servizi di video streaming e di giochi online, il download indiscriminato di APP e altri tool digitali, l'aumento volumetrico degli acquisti online, l'accesso a servizi in cloud, la diffusione dei sistemi di videoconferenza anche in ambito privato, sono tutti fenomeni che contribuiscono a una rapida crescita del rischio Cyber e che si sono decisamente accentuati durante la pandemia.

In questo particolare periodo abbiamo conosciuto anche altri fenomeni, come ad esempio quello degli "Aperizoom", un modo di sfruttare la tecnologia per riproporre "a distanza" gli eventi e le occasioni di incontro sociale.

Questo tipo di situazioni ha contribuito alla rapida diffusione di strumenti di social collaboration, che consentono lo svolgimento di video-riunioni di ogni tipo, e il cui uso si è diffuso in tutti gli ambiti della vita sociale.

Basti pensare che il solo Zoom, la vera star di questo settore, ha avuto nel primo semestre del 2020, un tasso di quasi 170 mila download al giorno. Il boom di Zoom ha trovato addirittura la costruzione di un neologismo "Zoombooming", a cui ne ha fatto riscontro un altro, stavolta con connotazione negativa: Zoomboombing, che identifica la pratica adottata da alcuni hacker di infiltrarsi nelle video-riunioni allo scopo di disturbare la riunione oppure con l'intento di veicolare Malware verso i partecipanti.

Il successo di Zoom ha inoltre indotto gli hacker a registrare un numero elevato di siti civetta, con i quali attirare gli utenti che erano alla ricerca dell'APP ufficiale da scaricare e utilizzare.

Un altro fenomeno indubbiamente rilevante è stato quello dello streaming video.

Del resto, cosa c'è di meglio di un buon film per ingannare il tempo in un periodo in cui cinema e ristoranti sono chiusi?

Ecco, che accanto ai classici canali commerciali di streaming video, si sono diffusi molti canali alternativi che consentivano il download o la riproduzione di film e serie video. Oltre a sottolineare che si tratta di un fenomeno che in molti casi può comportare conseguenze sul piano legale, l'uso di video scaricati o riprodotti da fonti non sicure può aprire facilmente la strada a Malware di vario tipo tra cui i famigerati Ransomware.

CYBERPEDIA

Il Ransomware è un particolare tipo di Malware che tende a crittografare i dati del dispositivo infettato, rendendoli indisponibili. Il Ransomware serve per sottoporre la vittima ad un ricatto, con tanto di riscatto ("ransom" in inglese vuol dire appunto "riscatto"): se vuoi ricevere la chiave per de-crittografare i dati, devi contattare una determinata organizzazione e pagare un riscatto in moneta virtuale (Bitcoin)

Il Ransomware è una forma di attacco che viene usata sia in ambito professionale, con il blocco di grandi sistemi elaborativi, sia in ambito più strettamente privato, con il blocco di dispositivi digitali, come personal computer o smartphone.

1. Lo scenario

1.6 Oltre la pandemia

SUMMARY: siamo tutti in trepidante attesa che i risultati delle intense attività di ricerca in campo medico ci portino al definitivo superamento della pandemia Covid-19 e a un ritorno graduale alla normalità. Siamo altresì convinti, e tutti i dati lo confermano, che la pandemia abbia segnato uno spartiacque decisivo rispetto alla trasformazione digitale della società, con effetti strutturali e incontrovertibili. Per questa ragione è necessario agire con decisione sul fattore umano, il vero anello debole del sistema difensivo, con programmi formativi efficaci di Cyber Security Awareness, una misura ormai ineludibile per la sicurezza degli individui e delle organizzazioni.

Siamo tutti fiduciosi che nel 2021 l'emergenza pandemica verrà definitivamente superata. Siamo altresì convinti che il Covid abbia fornito un'accelerazione dei processi di trasformazione digitale, i cui effetti saranno strutturali e incontrovertibili. Tra questi lo smart working, che assumerà una connotazione strutturale, ma anche il commercio elettronico, che continuerà la sua crescita nelle abitudini di acquisto, e i servizi al cittadino da parte della pubblica amministrazione e delle società che erogano servizi di pubblica utilità. La trasformazione digitale, pur rappresentando una grande opportunità di innovazione e modernizzazione, dovrà inevitabilmente fare i conti con un aumento dei rischi per la sicurezza.

Per questo è necessario agire con decisione sul fattore umano, il vero anello debole del sistema difensivo. L'azione sul fattore umano e di conseguenza i programmi formativi di Cyber Security Awareness, vanno considerati come una misura di sicurezza necessaria.

Molte organizzazioni nel tempo hanno attivato questi programmi con l'unico obiettivo di dimostrare la conformità alle varie normative che prevedono, nei loro standard, la formazione del personale; in molti casi questo ha significato una scarsa attenzione alla vera efficacia dei percorsi formativi. Ma il 2020 ci ha dimostrato in maniera inequivocabile che questo atteggiamento è perdente, e che in futuro dovremo preoccuparci soprattutto della loro efficacia. I programmi dovranno essere in grado di trasformare concretamente gli atteggiamenti e i comportamenti degli utenti di fronte alla minaccia Cyber.

2. La formazione

2.1 Una misura di sicurezza necessaria

SUMMARY: tutte le organizzazioni che vogliono sopravvivere a questa trasformazione digitale ormai inarrestabile, devono investire sul fattore umano, con programmi formativi avanzati ed efficaci, in grado di trasformare concretamente i comportamenti degli utenti, adeguandoli al livello della minaccia che evolve costantemente. Siamo di fronte a una guerra asimmetrica che vede gli attaccanti in una posizione di indubbio vantaggio. Per riportare simmetria in questa guerra è necessario agire sul fattore umano, che, nella Cybersecurity, gioca un ruolo decisivo.

Lo sviluppo della società digitale, con i suoi rischi, costringe tutte le organizzazioni ad investire in modo consistente sul fattore umano, soprattutto sul livello di consapevolezza delle persone. Un investimento divenuto necessario per colmare quel gap culturale che gli effetti pandemici e la rapida trasformazione digitale hanno acuito.

Il problema non riguarda solo le persone meno abituate all'utilizzo delle tecnologie digitali, ma anche le nuove generazioni e i cosiddetti "millennials". Le nuove generazioni, pur avendo una naturale propensione all'uso delle tecnologie, assumono molto spesso una postura digitale assimilabile a quella di "utenti inconsapevoli", senza la capacità di riconoscere i rischi Cyber che ci sono dietro le loro azioni.

Siamo stati abituati in questi anni a pensare alla Cybersecurity come ad un tema tecnologico, che riguardava solo una nicchia di specialisti. L'idea di fondo è che da qualche parte, nella nostra organizzazione, c'è sempre qualcuno che si occupa della sicurezza Cyber e che questo sia più che sufficiente. Di fronte ad un attacco Cyber, siamo portati a pensare che il problema sia soltanto correlato con la competenza di quel team di specialisti.

Inoltre, la Cybersecurity è sempre stata percepita come un qualcosa che riguardava esclusivamente la dimensione professionale della nostra esistenza. Nulla che ci riguardasse direttamente. Il pregiudizio è stato sempre lo stesso: "*Perché un hacker dovrebbe essere interessato a me come individuo?*". In questi anni abbiamo vissuto tutto ciò come un problema di percezione generale. Una convinzione che ha riguardato non solo il comportamento degli utenti, ma anche, e questo è ancora più preoccupante, quello delle funzioni manageriali.

Oggi è chiaro che la Cybersecurity è invece un problema trasversale che riguarda tutto il sistema Paese e che colpisce indifferentemente individui e organizzazioni di ogni genere. Una guerra asimmetrica che vede gli attaccanti in una posizione di indubbio vantaggio, anche perché, la prima linea di difesa è costituita da civili "inermi" che non hanno la consapevolezza delle minacce e delle contromisure necessarie. In molti casi, gli utenti subiscono attacchi senza neanche rendersene conto.

Negli anni le organizzazioni si sono preoccupate soprattutto di sviluppare capacità difensive a livello tecnologico, e queste difese sono indubbiamente aumentate.

Seguendo la teoria dell'anello debole, per cui la forza complessiva di una catena è determinata dal suo anello più debole, possiamo affermare che l'efficacia di questi investimenti viene oggi estremamente ridimensionata dalla debolezza del fattore umano.

La presenza in campo di un anello così vulnerabile, come quello rappresentato dagli utenti che interagiscono con le tecnologie digitali e con la rete Internet, ci restituisce il senso di quanto questa guerra sia sbilanciata a favore degli attaccanti.

Per poter riportare la simmetria in questa guerra, il cui esito è altrimenti già segnato, è necessario che gli utenti acquisiscano consapevolezza, per poi, di conseguenza, maturare attitudini e adeguare i propri comportamenti rispetto ai rischi Cyber. Un processo continuo fatto non solo di acquisizione di conoscenze teoriche, ma anche di allenamento di alcune caratteristiche umane, come la percezione del pericolo e la prontezza.

Un processo che, se da una parte va considerato una misura di sicurezza necessaria, dall'altra va progettato e governato secondo i criteri tipici della formazione orientata allo sviluppo delle risorse umane.

Per aumentare la consapevolezza delle persone sono necessari programmi formativi avanzati, basati su metodologie innovative di formazione continua, allenamento e coinvolgimento. Piattaforme formative in grado di minimizzare l'impatto sulle funzioni di gestione della formazione e della Cybersecurity.

Solo in questo modo sarà possibile mantenere il passo con l'evoluzione costante delle strategie di attacco, che si fanno sempre più sofisticate, e soprattutto si dimostrano in grado di adattarsi alla mutazione costante degli scenari.

Nella Cybersecurity, il fattore umano gioca un ruolo decisivo!

2. La formazione

2.2 Il ruolo della formazione

SUMMARY: l'unico modo di rafforzare le capacità difensive delle organizzazioni nei confronti della criminalità Cyber, consiste in un investimento significativo e costante sulla "prima linea di difesa", ossia sulle persone. Sarà quindi necessario coinvolgere tutta la forza lavoro in un percorso formativo che consenta a tutti di fare un uso sempre più consapevole delle tecnologie digitali, degli strumenti social e delle risorse presenti nel web. Un percorso di crescita che consenta di acquisire un livello di conoscenza condivisa e che stimoli alcune caratteristiche difensive umane come l'attenzione, la prontezza e la reattività.

Proviamo ad immaginare una città medioevale fortificata che si prepara a resistere ad un assedio.

Pensate ad un manipolo di soldati impegnati a rafforzare incessantemente le difese perimetrali della città, mentre la maggior parte degli abitanti continua ad entrare ed uscire dalle fortificazioni lasciando aperte le porte, e tra loro, alcuni scavano addirittura dei tunnel dall'interno verso l'esterno, per garantirsi delle vie di accesso privilegiate verso alcune zone della campagna circostante.

Sembra assurdo solo immaginarlo, perché gli abitanti di una città medioevale erano perfettamente consapevoli del rischio individuale e collettivo che un comportamento del genere avrebbe prodotto.

A meno che non si trattasse di un cospiratore al soldo del nemico, nessun cittadino avrebbe mai neanche pensato di indebolire il sistema difensivo della propria città con un comportamento "a rischio".

Invece, nella realtà digitale, comportamenti di questo tipo sono comuni, e avvengono in un clima di totale inconsapevolezza, senza una reale percezione del livello di rischio determinato da questi comportamenti.

Da questo quadro emerge la certezza che l'unico modo di ricreare una simmetria nella guerra tra attaccanti e difensori, consiste in un investimento significativo e costante sulla prima linea di difesa, ossia sulle persone, gli utenti delle tecnologie digitali.

Abbiamo già evidenziato come la matrice umana possa essere riscontrata nella maggior parte degli attacchi, anche quelli apparentemente più tecnologici. I vettori di innesco più comuni possono essere fatti risalire ad errori comportamentali da parte degli utenti che riguardano:

- la gestione dei dispositivi digitali;
- l'interazione con la messaggistica, a partire dalla posta elettronica;
- l'uso delle credenziali di accesso e, in modo particolare, delle password;
- la scarsa attenzione data al valore della privacy e delle informazioni critiche;
- l'atteggiamento con cui si naviga nella rete Internet e con cui si approcciano le risorse del Web.

Per contrastare efficacemente i rischi Cyber, ogni organizzazione, pubblica o privata, dovrà coinvolgere tutta la forza lavoro, indipendentemente dal ruolo svolto e dalle competenze, in un percorso formativo che consenta a tutti di fare un uso sempre più consapevole delle tecnologie digitali, degli strumenti social e delle risorse presenti nel web.

Un percorso di crescita che consenta di acquisire un livello di conoscenza condivisa e che stimoli alcune caratteristiche difensive umane come l'attenzione, la prontezza e la reattività. La consapevolezza del rischio porta a reagire in modo più appropriato di fronte ai pericoli conosciuti, ma anche ad avere un corretto atteggiamento difensivo di fronte a potenziali minacce non ancora conosciute, un atteggiamento che nel mondo Cyber è assolutamente necessario per la rapida evoluzione delle tecniche di attacco.

La consapevolezza è necessaria anche per evitare che un atteggiamento estremamente difensivo di fronte ad un'irrazionale percezione del rischio, produca comportamenti che incidano negativamente sulla produttività dell'individuo e dell'organizzazione. Anche nella città medioevali era necessario uscire dalle fortificazioni per coltivare la terra o per svolgere attività di carattere commerciale.

2. La formazione

2.3 Metodologia efficace

SUMMARY: un programma formativo che si pone l'obiettivo di trasformare i comportamenti individuali deve basarsi su una metodologia efficace, che evidenzi risultati tangibili sui processi di apprendimento. Una metodologia che non sia esclusivamente focalizzata sull'aspetto nozionistico, ma che sia in grado di integrare nel processo formativo anche percorsi di carattere esperienziale e induttivo. Questo mix di componenti consentirà di sviluppare non solo la cognizione, ma anche la percezione del rischio e la prontezza, creando una generazione di utenti consapevoli, in grado di interagire correttamente nella sfera digitale, sia nella loro dimensione individuale sia nella loro dimensione professionale.

Un programma formativo di Cyber Security Awareness deve avere alla base una metodologia efficace, orientata ad un risultato particolarmente sfidante come quello di trasformare i comportamenti umani. Il raggiungimento di questo risultato è strettamente collegato con la capacità di agire altrettanto efficacemente sui processi di apprendimento, sia su quelli di carattere più strettamente cognitivo, sia su quelli legati all'atteggiamento di fondo nei confronti della Cybersecurity, entrambi necessari per produrre un cambiamento duraturo nel comportamento.

La formazione deve contribuire a sviluppare la corretta percezione del rischio Cyber, riallineando la sfera razionale a quella emotiva, perché oggi nella maggior parte dei casi la dimensione oggettiva e quella soggettiva non sono equilibrate. Da parte degli utenti digitali c'è in generale una profonda sottovalutazione del rischio Cyber, o all'opposto, proprio per la mancanza di una corretta comprensione del fenomeno, si possono generare atteggiamenti di blocco nei confronti degli incontrovertibili processi di trasformazione digitale.

Un utente consapevole è un utente che ha una chiara comprensione delle minacce della rete e una corretta percezione del rischio Cyber, e che ha quindi maturato una postura digitale adeguata.

Un utente consapevole è anche quello che riesce a comprendere come il tema della consapevolezza riguardi sia la sua dimensione privata, sia la sua dimensione professionale, e a maturare la capacità di mantenere il più possibile queste due dimensioni distinte nei limiti del possibile, perché oggi queste due dimensioni tendono spesso a sovrapporsi inevitabilmente.

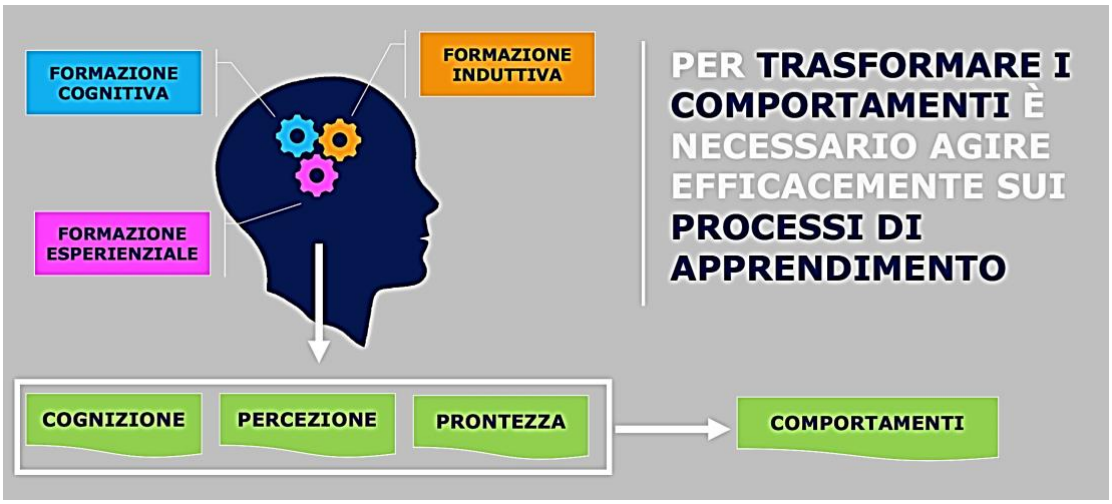
Una metodologia efficace deve evitare gli errori che negli anni passati hanno impedito alle iniziative di Cyber Security Awareness di generare il necessario clima di coinvolgimento, una condizione primaria per raggiungere risultati tangibili sulla strada della riduzione del rischio. Errori spesso insiti nei metodi di formazione tradizionale e che in questo specifico contesto, trattandosi di una materia immaginata come particolarmente ostica, possono assumere una maggiore rilevanza.

Tra le errate percezioni quelle più diffuse sul tema della Cyber Security Awareness sono:

- la Cyber Security Awareness è una disciplina tecnica che ha l'ambizione illusoria di trasformare gli utenti in specialisti del settore o in una sorta di moderni Sherlock Holmes in grado di effettuare sofisticate investigazioni;
- la Cyber Security Awareness riguarda esclusivamente la dimensione professionale dell'individuo e quindi il suo ruolo all'interno dell'organizzazione;

- la Cyber Security Awareness ha lo scopo esclusivo di cautelare l'organizzazione di fronte a processi di audit collegati ad oscure normative, e ha un coinvolgimento impositivo;
- la Cyber Security Awareness è una formazione imposta che non produce risultati utili, per l'individuo e per l'organizzazione;
- la Cyber Security Awareness tratta argomentazioni teoriche che non trovano alcun riscontro pratico nella dimensione privata e professionale dell'individuo.

La Cyber Security Awareness è invece di fatto una disciplina trasversale, di carattere divulgativo, che consente di sviluppare la competenza necessaria per agire in modo sicuro nella sfera digitale, sia in quella privata, tutelando sé stessi e il proprio network sociale, sia in quella professionale, tutelando il proprio ruolo e le proprie responsabilità aziendali, la propria organizzazione e l'intero ecosistema di cui l'organizzazione fa parte (clienti, fornitori, partner […]).



Per ottenere risultati concreti, i programmi di Cyber Security Awareness non possono limitarsi a fornire nozioni, ma devono articolarsi in percorsi di carattere esperienziale ed induttivo, seguendo approcci "learning by doing" e "learning by example".

Unendo approcci formativi di carattere nozionistico, ad altri di carattere esperienziale e induttivo, si ottiene un significativo mix in grado di agire positivamente sulla cognizione, sulla percezione del pericolo e sulla prontezza, condizionando attitudini e comportamenti.

Se è abbastanza facile immaginare una formazione nozionistica, è più difficile pensare a una formazione esperienziale e induttiva. Nel caso dell'apprendimento esperienziale, l'utente dovrà sperimentare situazioni tipiche di attacco, come avviene nel caso dell'attacco Phishing, diventando il target di simulazioni in grado di riprodurre l'esperienza reale. Nel caso della formazione induttiva dovrà essere condotto all'interno di situazioni reali, attraverso una narrazione efficace che produca un processo di identificazione, al punto da sentire la minaccia più concreta di quanto non sia abituato a fare.

2. La formazione

2.4 Formazione continua

SUMMARY: viste le caratteristiche e il contesto specifico della tematica, un programma formativo, per essere efficace, deve svilupparsi secondo un modello di formazione continua, che potremmo metaforicamente definire di tipo "omeopatico", caratterizzato quindi da micro-interventi, diluiti nel tempo. Una formazione in grado di agire non solo a livello nozionistico, ma anche a livello percettivo, permettendo quindi all'utente di sviluppare una vera e propria attitudine nel riconoscere le minacce della dimensione digitale, un po' come avviene rispetto alle minacce della vita reale.

Nell'attuale contesto storico, un programma di Cyber Security Awareness, per poter essere efficace, deve svilupparsi secondo un modello di formazione continua, che si mantenga in linea con il processo di trasformazione digitale e di evoluzione degli attacchi Cyber, che procede senza soluzione di continuità.

Per poter sostenere un modello di formazione continua, senza chiaramente incidere negativamente sulla produttività del singolo individuo e sui team di lavoro, sarà fondamentale procedere con micro-interventi, organizzati secondo una cadenza periodica regolare.

Il principio base è che le organizzazioni devono abituare la propria forza lavoro ad investire regolarmente una quota parte del proprio tempo, seppur minima e compatibile con le proprie attività, per prevenire quello che già oggi (e a maggior ragione nel futuro) è il rischio più importante per la loro sicurezza individuale, e di riflesso, per la sicurezza dell'intera organizzazione.

È quindi fondamentale che venga acquisita una reale consapevolezza del livello di rischio. Perché lo stesso rischio può, da una parte trasformare la vita di un individuo in un vero e proprio incubo, e dall'altra mettere addirittura in discussione la sopravvivenza stessa dell'organizzazione.

La Cybersecurity oggi non è più un tema di carattere tecnologico, ma è un serio problema di business, e quindi anche il rischio Cyber deve essere interpretato in modo diverso rispetto agli anni passati.

Ma qual è la relazione tra formazione continua e formazione efficace?

Perché un modello di formazione continua dovrebbe essere più efficace di un modello di formazione caratterizzata da approcci più "concentrati", più intensi, e quindi più semplici da organizzare, gestire e monitorare?

Prima di rispondere a questa domanda è necessario fare una premessa: in questo approfondimento non viene presa in considerazione la formazione in aula, perché considerata meno efficace in ambito professionale, e perché gli eventi accaduti nel 2020, hanno di fatto dimostrato che per affrontare problematiche di questo tipo esiste solo l'opzione della formazione a distanza, in tutte le sue varie forme.

Per tornare alle due domande di prima, è fondamentale sottolineare nuovamente qual è l'obiettivo reale e concreto della formazione in ambito di Cyber Security Awareness: generare consapevolezza rispetto alle minacce Cyber per trasformare i comportamenti di tutti gli individui, in special modo di quelli che non hanno alcuna conoscenza o specializzazione in ambito Cyber, da sempre considerato come un ambito tecnologico.

Per trasformare i comportamenti degli utenti digitali, rendendoli adeguati al livello attuale e futuro delle minacce, non è sufficiente agire con un modello nozionistico, ma è necessario incidere anche dal punto di vista percettivo.

L'utente deve maturare una vera e propria attitudine nel riconoscere i pericoli, sviluppando un discreto livello di resilienza, affinché questa sorta di istinto riesca a adattarsi costantemente alle continue evoluzioni delle strategie di attacco.

A livello digitale dobbiamo quindi aiutare gli utenti a sviluppare quel livello di percezione del pericolo, che nella vita di tutti giorni ci salva dalle tante minacce che ci circondano.

Per queste ragioni, una formazione intensiva e concentrata non può che generare un effetto effimero, con un'efficacia concreta solo nell'immediato, ma che per sua natura tende a disperdersi inevitabilmente nel tempo.

Utilizzare invece un approccio di carattere "omeopatico", con piccoli interventi diluiti nel tempo, permette di mantenere la dimensione percettiva ad un livello adeguato, e permette di aggiornare anche la dimensione nozionistica, mantenendola sempre in linea con gli sviluppi della tematica.

Poiché le minacce Cyber mutano costantemente, assumendo forme sempre più sofisticate, che le differenziano dalla loro forma originale, è fondamentale continuare ad instillare nelle persone piccole dosi di "vaccino", per renderle immuni a tutte le loro molteplici forme.

Ma qual è una quota di tempo accettabile da dedicare a questo tipo di formazione?

Qual è quel punto di equilibrio tra risultato ottenuto e impatto prodotto?

L'esperienza maturata ci ha dimostrato come un'occupazione di tempo che va dai 20 ai 30 minuti al mese, con una modularità che consente di suddividere questo impegno in sessioni formative autoconsistenti che non superano i 10 minuti, è compatibile con ogni tipo di esigenza lavorativa, azzerando qualsiasi potenziale blocco dovuto ad un sovraccarico di attività.

Molti corsi intensivi e concentrati, come quello sulla sicurezza del lavoro (legge 81/2008) o i corsi connessi con l'introduzione del GDPR (Regolamento Generale sulla Protezione dei Dati), hanno prodotto negli anni una sorta di rifiuto da parte di tutti i dipendenti: un errore da evitare assolutamente.

Nel prossimo paragrafo vedremo come un modello di formazione continua, seppur a basso impatto sulla forza lavoro, deve comunque essere sostenuto da tecniche di coinvolgimento dell'utente, che deve sentirsi motivato a partecipare per la qualità dei contenuti ricevuti e per i benefici ricavati.

2. La formazione

2.5 Coinvolgimento formativo

SUMMARY: un corso efficace deve essere estremamente coinvolgente e quindi non percepito secondo una mera logica "impositiva". Il coinvolgimento dipende fortemente dai linguaggi e dai formati, ma anche dalla capacità di trasmettere il beneficio di carattere individuale che il partecipante ottiene, una sorta di significativo cashback rispetto al suo impegno. Questo non significa che una formazione di questo tipo non possa essere classificata come obbligatoria, ma l'eventuale obbligatorietà non dovrà mai essere utilizzata come alternativa da sostituire all'utilizzo di efficaci criteri di "engagement".

Un programma che vuole essere efficace deve essere coinvolgente nei confronti del partecipante, e sviluppare in lui un sufficiente livello di "engagement".

Per coinvolgere l'utente su una tematica apparentemente "ostica", ritenuta erroneamente un'esclusiva del personale specialistico, bisogna superare l'istintivo pregiudizio di chi, non essendo un tecnico, non riesce a percepirne la motivazione.

La prima cosa di cui tenere conto è il linguaggio e le forme espressive che vengono utilizzate.

Siamo abituati a concepire la formazione aziendale come un qualcosa che debba essere caratterizzato da "pesantezza" dei contenuti e delle forme espressive. Basandoci sui canoni della formazione tradizionale correremmo il rischio, su una tematica il cui oggetto sono le minacce Cyber e le conseguenze che queste possono generare, di sconfinare nell'allarmismo e nel tecnicismo, e indurre una situazione di rifiuto.

Per raggiungere l'obiettivo della Cyber Security Awareness, il linguaggio utilizzato deve essere perciò altamente divulgativo, comprensibile da parte di tutti. Un linguaggio che spieghi con chiarezza che non si tratta di una materia di carattere tecnico, ma di una materia che riguarda la vita di tutti i giorni e di ogni persona che ha un'interazione con la sfera digitale.

Ogni effetto barriera preventivo deve crollare fin dall'inizio, lasciando il posto ad una chiara percezione dell'utilità dell'intervento formativo e della possibilità di poterne fruire pienamente, indipendentemente dalle proprie competenze.

Le forme espressive devono inevitabilmente essere multimediali e caratterizzate da grande interattività. L'aspetto moderno e accattivante non dovrà mai essere "appesantito" da un uso eccessivo delle animazioni, che devono mantenersi in equilibrio con l'elemento umano. La funzione di coaching continuerà quindi ad essere interpretata dall'elemento umano per favorire il processo di identificazione basato sul canone insegnante/allievo.

La Cyber Security Awareness è un investimento sul fattore umano, e questa connotazione deve trovare riscontro anche nel programma formativo.

L'interattività assume una concreta rilevanza nella logica di un'alternanza continua tra brevi contenuti formativi e test di apprendimento, che servono a rafforzare la comprensione del contenuto, seguendo la logica dell'esonero universitario, piuttosto che la logica dell'esamone finale.

Un’altra forma di coinvolgimento è legata al beneficio che si ottiene da una formazione, da ciò che possiamo definire la “leva individuale”. È fondamentale che il partecipante comprenda sin dalle prime lezione che il beneficio primario della Cyber Security Awareness è rivolto all’individuo e al suo network sociale, prima ancora che alla sua organizzazione. Questa convinzione mitigherà il carattere di imposizione della formazione stessa e l’idea che venga richiesta solo per cautelare l’organizzazione da possibili conseguenze.

Solo percependo questo tipo di beneficio il coinvolgimento sarà totale, e lo stimolo a mantenere aggiornato il proprio livello di consapevolezza sugli attacchi Cyber sarà automatico. Questo senso di coinvolgimento spontaneo sarà ulteriormente percepito se il processo di identificazione verrà rafforzato dal continuo riferimento a casi e situazioni reali, in cui è facile riconoscersi.

Spesso, quando si avvia un percorso di questo tipo, la domanda che più frequentemente ci viene fatta dai responsabili interni è se questa formazione debba essere classificata come obbligatoria o se si debba soprattutto puntare sul coinvolgimento delle persone. Onestamente non c’è una risposta univoca a questa domanda, perché ogni organizzazione ha le sue dinamiche. È indubbio che il massimo dell’efficacia lo si ottenga combinando queste due tipologie di leve: quella dell’obbligatorietà e quella del coinvolgimento.

Se è vero che l’obbligatorietà di un programma formativo potrebbe essere percepita negativamente come imposizione, è altresì vero, e l’esperienza acquisita lo conferma, che la mancanza di obbligatorietà potrebbe essere letta come sinonimo di “poco importante”. Per questo il massimo dell’efficacia lo si ottiene quando obbligatorietà e coinvolgimento convivono in modo sinergico.

2. La formazione

2.6 Gamification

SUMMARY: il gioco è forse il più potente tra gli elementi che generano coinvolgimento nella formazione aziendale. Forme di gamification individuale, con il rilascio di riconoscimenti virtuali, e di gruppo, con lo sviluppo di una competizione virtuosa tra team diversi, rafforzano i processi di apprendimento e agiscono positivamente anche sul gioco di squadra.

Che il gioco sia uno strumento che facilita i processi di apprendimento è cosa nota e risaputa da tempo, così come esiste un'evidenza per cui le tecniche di gamification applicate alla formazione aziendale aumentano l'efficacia della formazione stessa, agendo positivamente sia sulla partecipazione da un punto di vista quantitativo sia dal punto di vista qualitativo. Questo è valido a maggior ragione quando parliamo di formazione a distanza.

Le tecniche di gamification, aggiungendo elementi motivazionali, rafforzano il livello di coinvolgimento rispetto al percorso formativo, che come abbiamo visto rappresenta un passaggio fondamentale per ottenere un risultato efficace.

La gamification può agire a livello individuale, grazie ad elementi di gratificazione virtuali, come l'acquisizione di badge, medaglie, coppe, […], che segnano tutti i passaggi importanti del percorso formativo e premiano l'impegno del partecipante. La gamification può agire anche a livello di gruppo, facendo in questo modo leva sul senso di appartenenza e sul gioco di squadra.

Appartenere ad una squadra, e in questo senso attivare il meccanismo di competizione virtuosa con altre squadre, genera livelli elevati di coinvolgimento e una maggiore capacità di sviluppare processi pervasivi di comunicazione interna.

Le tecniche di gamification, e quindi la capacità di convertire il livello di fruizione del percorso formativo in punteggio, aiutano sia i partecipanti sia i supervisori a comprendere immediatamente i progressi raggiunti nell'apprendimento, e fornisce elementi concreti per effettuare una valutazione dei risultati.

2. La formazione

2.7 Commitment

SUMMARY: il livello di commitment all'interno dell'organizzazione, e l'attenzione del top management sono fattori decisivi, specialmente rispetto a un'iniziativa che si caratterizza per la sua trasversalità e per la criticità del tema trattato.

Nell'ambito della formazione aziendale, l'efficacia viene chiaramente favorita anche dal livello di commitment e di coinvolgimento delle strutture aziendali. L'attenzione del top management su un'iniziativa così trasversale diventa un fattore critico di successo dell'iniziativa stessa.

Abbiamo già evidenziato come il rischio Cyber sia di fatto un rischio di Business al pari di altri, ed è quindi ovvio che ridurre la minaccia di questo rischio deve essere un obiettivo dell'intera organizzazione e non un'esclusiva dei dipartimenti IT/SEC.

Il coinvolgimento delle strutture di HR, della Comunicazione Interna, con l'attivazione di tutti i canali di comunicazione, come ad esempio la rete Intranet, diventa fondamentale per favorire il successo dell'iniziativa e per portarla avanti nel tempo.

L'esperienza ha dimostrato che quando il commitment si spinge al cosiddetto livello-C, tutte le barriere che frenano la partecipazione e il coinvolgimento vengono abbattute e l'efficacia della formazione aumenta decisamente.

3. Cyber Guru

3.1 La piattaforma di Security Awareness

SUMMARY: Cyber Guru è la prima linea di soluzioni di Cyber Security Awareness progettata per aumentare il livello di sicurezza degli individui e delle organizzazioni. Una piattaforma in grado di agire efficacemente sul fattore umano grazie ad un'innovativa metodologia che migliora i processi di apprendimento.

La piattaforma Cyber Guru, progettata in Italia, si basa su metodologie di formazione che sono il frutto di un lavoro multidisciplinare, che si è avvantaggiato nel tempo anche della collaborazione del Dipartimento di Scienze della Formazione dell'Università di Roma Tre.

Tutte le soluzioni della piattaforma Cyber Guru consentono di raggiungere due principali obiettivi:

- aumentare la consapevolezza degli individui rispetto ai rischi che si corrono nell'interazione con le tecnologie digitali e con il Web;
- trasformare i comportamenti degli individui, per renderli adeguati alle necessità di protezione delle organizzazioni e alle sfide imposte dall'evoluzione del crimine informatico.

Per raggiungere questi obiettivi, la progettazione e lo sviluppo delle piattaforme hanno seguito precise linee metodologiche, che tengono conto della necessità di agire efficacemente sui processi di apprendimento.

La metodologia si articola su 3 livelli di formazione:

Inoltre, la metodologia, che è alla base di Cyber Guru, tiene conto di altri due aspetti determinanti:

- un processo di formazione continua, costituito da micro-interventi effettuati con costanza e regolarità;
- il coinvolgimento dell'utente in questo processo, rendendo chiaro all'utente stesso che l'obiettivo primario del processo è la sua protezione, come individuo inserito in un contesto sociale sempre più interconnesso.

Tutto questo serve a sviluppare, costantemente e progressivamente tre caratteristiche che influenzano i comportamenti umani quando le persone sono sotto minaccia, generando l'attitudine a reagire in modo corretto per proteggere sé stessi e la propria organizzazione:

3. Cyber Guru

3.2 Cyber Guru Awareness

SUMMARY: Cyber Guru Awareness è un innovativo sistema integrato di e-learning che consente di coinvolgere tutta l'organizzazione in un percorso di formazione basato su una metodologia di formazione continua e sull'applicazione di tecniche di gaming all'intero percorso formativo.

Cyber Guru Awareness è progettato per coinvolgere tutta l'organizzazione in un percorso di apprendimento educativo e stimolante, che si caratterizza per il suo approccio "a rilascio costante e graduale" e per alcune peculiari caratteristiche:

- moduli formativi auto-consistenti ad attivazione mensile;
- impegno settimanale minimo, compatibile con qualsiasi funzione;
- micro-lezioni video in formato multimediale;
- utilizzo di attori professionisti con funzioni di coach;
- linguaggio altamente divulgativo;
- approccio interattivo con continua alternanza tra micro-lezioni e test;
- test di valutazione a risposta multipla;
- metodologia di gamification, con organizzazione in team;
- piattaforma multilingua;
- contenuti aggiuntivi e costantemente attualizzati.

Il percorso formativo di Cyber Guru Awareness è costituito da moduli formativi auto-consistenti, ognuno dedicato ad uno specifico argomento, con attivazione mensile, a copertura di un periodo di 12/24/36 mesi.

Ogni modulo è a sua volta costituito da 3 brevi lezioni video di 5 minuti ciascuna, ognuna collegata ad un test di apprendimento con domande a risposta multipla.

La video lezione, con l'attore coach, rappresenta l'elemento chiave del percorso formativo che consente, insieme alla gamification, di coinvolgere attivamente l'utente in questo percorso.

I meccanismi di gamification sono strutturati per creare il massimo livello di coinvolgimento sia dell'individuo sia dell'organizzazione, favorendo l'attivazione di processi di comunicazione interna, anche in una logica di "team building".

La gamification è strutturata:

- in forma individuale, con l'assegnazione di medaglie e coppe virtuali che premiano la partecipazione dell'utente, anche dal punto di vista qualitativo;
- in forma aggregata, con un'organizzazione in team che consente di generare una competizione virtuosa tra team diversi, un meccanismo particolarmente motivante che fa leva sulle logiche di appartenenza.

Cyber Guru Awareness, al fine di aumentare il coinvolgimento dell'utente, senza gravare su chi governa la formazione, rende disponibile una funzione automatica di Student Caring, che si occupa di stimolare la partecipazione, attraverso notifiche puntuali.

3. Cyber Guru

3.3 Cyber Guru Phishing

SUMMARY: Cyber Guru Phishing è un'innovativa piattaforma di addestramento anti-phishing, basata su una metodologia di apprendimento esperienziale. L'obiettivo di Cyber Guru Phishing è di massimizzare l'efficacia formativa rispetto al rischio Phishing: percezione del pericolo, prontezza nel reagire all'attacco, cognizione della minaccia.

Cyber Guru Phishing è stato progettato per addestrare la forza lavoro a resistere agli attacchi Phishing, attraverso campagne di attacchi simulati, che vengono personalizzati sulla base del profilo comportamentale del singolo utente, grazie ad un processo automatico e adattivo, guidato dall'uso di tecniche di Intelligenza Artificiale.

Grazie al suo approccio adattivo, Cyber Guru Phishing può essere considerato un vero e proprio "personal trainer" in funzione anti-phishing.

Le campagne di simulazione riproducono l'esperienza reale e le strategie di attacco adottate dai criminali Cyber. Gli algoritmi di apprendimento usati dalla piattaforma sono in grado di selezionare i template di attacco, sulla base di un criterio di massima efficacia formativa.

Ad ogni campagna, il motore adattivo sceglie i nuovi template sulla base del profilo utente, aumentando, per esempio, il livello di difficoltà degli attacchi, per gli utenti classificati come "forti".

La piattaforma segue il seguente schema di funzionamento:

1. Ad ogni campagna la piattaforma seleziona automaticamente i template di attacco e li rende disponibili per l'approvazione.
2. La piattaforma distribuisce gli attacchi secondo uno schema personalizzato e con un meccanismo che evita il fenomeno del passaparola.
3. Ogni persona che cade nell'inganno, viene esposta a un training specializzato rispetto all'attacco subito, rafforzando il metodo dell'apprendimento esperienziale.
4. Gli effetti di ogni campagna consentono di valorizzare gli indicatori di rischio monitorati dalla piattaforma, determinando la preparazione e la distribuzione della campagna successiva.
5. Oltre alla classificazione degli utenti in "deboli", "intermedi" e "forti", la piattaforma consente di valorizzare anche la categoria definita dei "defender", ossia di coloro che, oltre a non cadere nell'inganno, riconoscono l'attacco e lo segnalano.
6. Tutti gli indicatori vanno ad alimentare in tempo reale la funzione di reportistica, fruibile attraverso una dashboard avanzata. La reportistica non si limita ad esporre il click-rate di una campagna, ma rende disponibili report e indicatori che esprimono una chiara mappa del rischio e la reale efficacia del percorso intrapreso.

L'apprendimento esperienziale, realizzato attraverso Cyber Guru Phishing, si dimostra particolarmente efficace nell'abbattimento del rischio Phishing, aumentando costantemente il livello di resistenza agli attacchi Cyber dell'intera organizzazione e riducendo con altrettanta regolarità, il numero di utenti classificati come "deboli".

Questa metodologia di apprendimento è supportata dalle caratteristiche della piattaforma, in modo particolare dal suo livello di automazione, che riduce al minimo l'impatto sui team di Cybersecurity.

3. Cyber Guru

3.4 Cyber Guru Channel

SUMMARY: Cyber Guru Channel è un percorso di formazione video basato su una metodologia induttiva, realizzato con tecniche di produzione avanzata, tipiche delle serie TV , e con uno storytelling coinvolgente, ideato per immergere l'utente all'interno di situazioni reali che riproducono le conseguenze di un attacco Cyber generato da un comportamento umano errato.

La metodologia induttiva implementata da Cyber Guru Channel si basa sull'immersione dell'utente all'interno di una situazione reale e su un processo di auto-identificazione con la minaccia Cyber, che assume una forma concreta e quindi possibile. L'utente assume consapevolezza non attraverso una nozione, ma attraverso una narrazione, la quale agisce, prima, sulla percezione del pericolo, e successivamente, sull'elemento nozionistico. L'elemento nozionistico viene "indotto" dalla narrazione stessa, e rafforzato dal materiale di approfondimento messo a disposizione dell'utente.

I video della piattaforma di Cyber Guru Channel sono realizzati con tecniche di produzione avanzata e con uno storytelling particolarmente coinvolgente.

In questo particolare percorso di formazione, in cui la chiave di comprensione è data dal coinvolgimento in una storia, l'utente viene ulteriormente supportato dalla disponibilità, all'interno della piattaforma, del necessario materiale di approfondimento, che fornisce i supporti teorici per aumentare il proprio livello di consapevolezza sulla minaccia posta al centro della storia.

Cyber Guru Channel prevede:

- più formati video con storytelling diversi;
- documentazione di approfondimento per ogni episodio;
- integrazione con il meccanismo di gamification;
- funzioni di Student Caring, per motivare la partecipazione;
- reportistica sul livello di fruizione.

Il livello di engagement generato da Cyber Guru Channel è molto elevato e quindi di fatto diventa un traino per altri percorsi formativi finalizzati alla Cyber Security Awareness e per attività di comunicazione interna volte alla diffusione della cultura della Cybersecurity nell'organizzazione.

I video formativi, integrati nella piattaforma Cyber Guru, sono arricchiti di tutte le componenti di access control, engagement e monitoring, proprie della piattaforma.

4. Bibliografia

Fonti utilizzate per la realizzazione del White Paper:

[i] Fonte: Osservatorio e-commerce della School of Management del Politecnico di Milano, insieme a Netcomm – Convegno eCommerce B2C: la chiave per ripartire.

[i] Fonte: AgCom – Osservatorio sulle comunicazioni – Monitoraggio Covid-19 n. 2/2020

[i] Fonte: Rapporto Clusit 2020 sulla sicurezza ICT – Associazione Italiana per la Sicurezza Informatica – edizione 2020

[i] ENISA Threat Landscape – The year in review – January 2019-Aprile 2020 – *pag.8 [...] the continuous increasing trend in the advanced adversary capabilities of threat actors [..]*

[i] Fonte: Rapporto Clusit 2020 sulla sicurezza ICT – Associazione Italiana per la Sicurezza Informatica – aggiornamento ottobre 2020

[i] Fonte: F-Secure - Attack Landscape H1 2020

[i] Fonte: Google Navigazione Sicura

Sulle teorie della guerra asimmetrica abbiamo citato liberamente alcuni concetti espressi in vari interventi dal Prof. Alessandro Curioni, docente dell'Università del Sacro Cuore di Milano e fondatore di Di. Gi. Academy.

www.cyberguru.it

Cyber Security Awareness: il fattore umano e la sfida “post-pandemica”

Cyber Guru

contatti@cyberguru.it