ATTACCHI CYBER

LA CONSAPEVOLEZZA NON È PIÙ UN OPTIONAL

ATTACCHI CYBER
LA CONSAPEVOLEZZA NON È PIÙ UN OPTIONAL

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 a un errore umano, ha tolto definitivamente ogni dubbio rispetto a quale sia l'anello debole della catena difensiva di ogni organizzazione.

IL TREND DEGLI ATTACCHI CYBER È IN CONTINUO E RAPIDISSIMO AUMENTO.

LA CYBERSECURITY È UN PROBLEMA TRASVERSALE CHE RIGUARDA TUTTO IL SISTEMA PAESE E CHE COLPISCE INDIFFERENTEMENTE INDIVIDUI E ORGANIZZAZIONI DI OGNI GENERE

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. Se si parte dal 2020 analizzando i vari rapporti 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 fanno leva principalmente sul fattore umano.
Un'ulteriore conferma del fatto che la stragrande maggioranza degli attacchi Cyber ha una matrice umana, riconducibile a un'azione non corretta da parte di un utente.

L'ingresso nello scenario economico e sociale della pandemia da Coronavirus non ha fatto altro che acuire questa situazione, facendo impennare il numero degli attacchi. In questi ultimi anni, 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** è **ricca** 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, "non siamo appetibili per un hacker", è stato smentito dai fatti.

Si tratta di una vera e propria **guerra cyber**. 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** e **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 fatti in quest'area, spesso insufficienti, 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

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.

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 E LE SUE TRAPPOLE

SUMMARY

Possiamo dire che il 2021 ha strutturato lo sconvolgimento sociale ed economico innescato dalla pandemia, nell'anno precedente, trasformandolo in una situazione di allarme cronico su tutti i fronti.
La trasformazione digitale forzata avvenuta nel 2020 e gestita in **modalità emergenziale** è diventata **realtà consolidata** con cui la collettività deve fare i conti, nel bene e nel male. Una delle conseguenze più evidenti è stata la crescita degli attacchi Cyber, che ha cavalcato l'onda dell'anno precedente continuando a sfruttare le vulnerabilità di carattere psicologico e anche il gap tra il processo accelerato di digitalizzazione e la consapevolezza degli utenti rispetto alle minacce Cyber, che ancora non è affatto colmato.

QUESTI ULTIMI DUE ANNI CHE ABBIAMO VISSUTO SARANNO SENZ'ALTRO RICORDATI SUI LIBRI DI STORIA COME GLI ANNI DELLA **PANDEMIA DA COVID 19** E DI TUTTE LE TRASFORMAZIONI EPOCALI CHE LA COLLETTIVITÀ HA VISSUTO IN SEGUITO A QUESTO EVENTO.

AI PRIMI POSTI TRA QUESTE C'È IL **RIPOSIZIONAMENTO** DELLA **NOSTRA VITA** SUL WEB. SE PRIMA DEL COVID SOLO UNA PARTE DI ESSA SI CONFRONTAVA QUOTIDIANAMENTE CON LA RETE, OGGI SI PUÒ DIRE CHE IL WEB GESTISCE LA MAGGIOR PARTE DELLE NOSTRE GIORNATE.

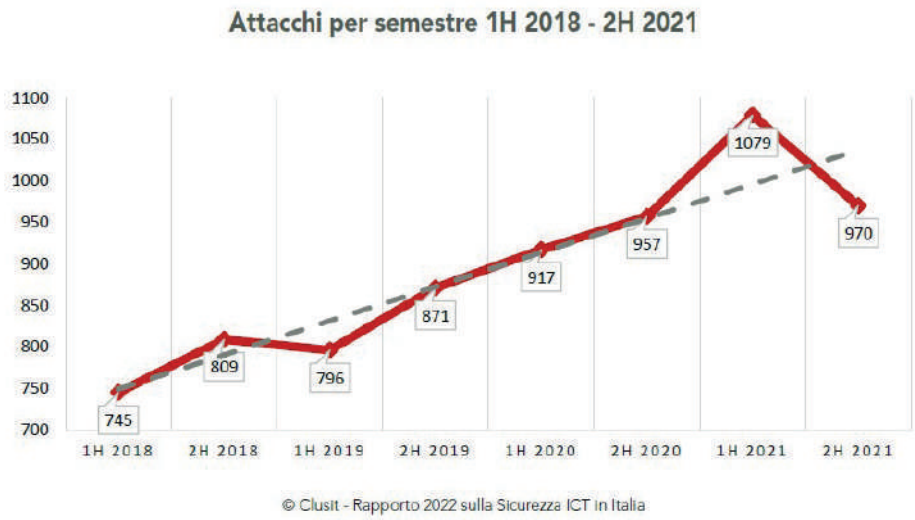
Dal lavoro, alla scuola, alle relazioni, allo shopping, all'informazione. Insomma, dal web in tutte le sue declinazioni oggi non si può più prescindere. Questo ha comportato un'occasione molto ghiotta per tutti coloro che fanno della **truffa informatica** il loro mestiere e così gli **attacchi hacker** sono diventati una **realtà molto diffusa** e altrettanto pericolosa.

Tanto da essere definiti "**l'arma più pericolosa del mondo**" da **JP Morgan** in occasione del suo International Council che si è svolto nel dicembre scorso, ed essere identificati come "la maggiore minaccia per la stabilità finanziaria, insieme al cambiamento climatico", da Christine Lagarde, alla conferenza annuale dell'European Systemic Risk Board (ESRB). Affermazioni che destano grande allarme e che purtroppo sono confermate dai dati.

Secondo il **Rapporto Clusit 2022** sulla **Sicurezza informatica**, negli ultimi 4 anni la media mensile di attacchi gravi a livello globale è passata da 130 a 171, con una conseguente drammatica crescita delle perdite che sono passate da 1 trilione di dollari nel 2020 a 6 trilioni nel 2021, con un tasso di peggioramento annuale a 2 cifre e un valore pari a 4 volte il PIL italiano.

Un'escalation dovuta principalmente al **massivo utilizzo** dello **smart working** che, da emergenziale, è diventato in molte situazioni una nuova modalità lavorativa, ma anche all'adozione sempre più frequente della didattica a distanza e di metodi di formazione online e, non ultimo, al ricorso 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, secondo i dati del rapporto di Salesforce Shopping Index, relativi al primo trimestre 2021, ha visto un **aumento globale del 58%** su base annua contro il 17% del primo trimestre 2020.



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.

Con l'Italia che fa da protagonista, registrando un'impennata del 78% che la posiziona al primo posto in Europa e al quarto nel mondo, dopo Canada, Olanda e Regno Unito. Un **salto tecnologico** carpiato che senz'altro ha rappresentato e rappresenta una grande opportunità sulla strada dell'innovazione ma che, di contro, può riservare atterraggi bruschi se non traumatici.

Il punto è che tutto questo 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. Un'assenza di consapevolezza delle minacce provenienti dal mondo digitale, che non è stata ancora colmata e che continua quindi a fornire grandi opportunità alle organizzazioni criminali Cyber.

1.2 **GLI ATTACCHI CYBER:** LE "CREPE" PSICOLOGICHE E TECNOLOGICHE

SUMMARY

La **situazione peculiare** generata dalla **pandemia** è all'origine della **crescita** degli **attacchi Cyber** iniziata nel 2020 e proseguita irrobustendosi nel 2021. Da questo punto di vista bisogna tenere conto sia delle **vulnerabilità** di **carattere tecnologico**, collegate allo smart working, all'aumento di tutte le attività online e all'utilizzo di nuovi strumenti digitali come i QR code, sia di quelle di **carattere psicologico**, collegate ai **continui stati** di **emergenza** e alla condizione di distanziamento sociale. Due importanti "crepe" nelle quali la criminalità si è facilmente infilata portando 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**.

Un trend già pesantemente registrato nel 2020 e che nel 2021 ha visto un forte aumento. Il rapporto Clusit, presentato a inizio anno, parla di casi gravi in aumento e di un'Europa sempre più al centro degli attacchi dei Cyber criminali: un + 22% rispetto a un 16% del 2020 e all'11% del 2019.

All'aumento quantitativo si somma quello qualitativo perché i **danni** sono molto più **seri** per le **aziende colpite**. In generale nel quadriennio 2018-2021 il numero di attacchi gravi analizzati dal Clusit segna un aumento del 32% e tra le categorie più colpite c'è proprio il settore governativo (15%) seguito da ICT e multiple targets.

Secondo i dati sulla **gravità degli attacchi**, quelli di livello critico hanno rappresentato il 32%, di livello alto il 47%, di livello medio il 19% e di livello basso solo il 2%.
Sul dato complessivo, dunque, la gravità critica e alta degli attacchi ha toccato l'80%, mentre l'anno prima era del 56%.

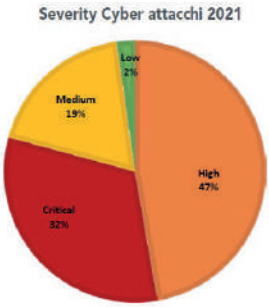
Inoltre un recente studio prodotto da IBM security, **Cost of a Data Breach Report 2021**, ha evidenziato come gli attacchi alla sicurezza informatica abbiano portato, nell'anno che si è appena concluso, ai costi più alti mai associati alle violazioni dei dati nei 17 anni di storia del rapporto, con una media di 4,24 milioni di dollari per ogni incidente. Insomma, se il trend dovesse continuare così le prospettive non sarebbero certo rosee.

I PRINCIPALI **DRIVER** DELL'ACCELERAZIONE DEGLI **ATTACCHI CYBER** SONO SEMPRE ANCORATI ALLE TRASFORMAZIONI INDOTTE DALLA PANDEMIA. UNO DI TIPO **PSICOLOGICO** CONNESSO CON L'EFFETTO SULLA PSICHE UMANA DELLA SITUAZIONE DI EMERGENZA, L'ALTRO DI TIPO **TECNOLOGICO** RICONDUCIBILE AL RICORSO MASSIVO A FORME DI TELELAVORO E AL MAGGIORE UTILIZZO DELLA RETE PER LE ATTIVITÀ QUOTIDIANE.

Il **livello piscologico** 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, difficoltà enfatizzata anche a causa delle avanzate tecniche di costruzione delle **Fake News**.

Facendo leva su questi stati ansiosi molto più diffusi nella popolazione rispetto al periodo pre-covid, si sono moltiplicate le **campagne** di **phishing** che hanno avuto come oggetto i temi del Covid in tutte le sue declinazioni: le diverse varianti del virus, il Green Pass e tutte le informazioni, spesso allarmistiche, che hanno ruotato intorno alla pandemia.

L'utente si è poi trovato maggiormente isolato e più propenso a perdere i suoi abituali punti di riferimento all'interno dell'azienda o 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 sono stati e sono ancora 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.



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

LA CONDIVISIONE DEI DISPOSITIVI, DELLA RETE, MA ANCHE L'AGIRE INCONSAPEVOLE A CAUSA DI FENOMENI INDOTTI DALLA DISTRAZIONE, DIVENTANO ELEMENTI CHE GIOCANO A VANTAGGIO DELLA CRIMINALITÀ.

Considerato che l'**anello debole** è sempre il **comportamento umano**, in una situazione di allarme sanitario generalizzato l'attenzione ai giusti comportamenti da tenere online è stata penalizzata, spalancando così le porte ai **criminali informatici** che, da raffinati conoscitori della psiche umana, **si infilano** proprio nelle **crepe** delle **emozioni**.

A tutto questo si è aggiunto il **livello 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.
Anche in questo caso è comunque il fattore umano a preoccupare maggiormente perché il gap che esiste tra la **velocità** del **processo** di **trasformazione digitale** e quella di **adeguamento** delle **persone** a questa nuova dimensione socioeconomica rimane, ancora oggi, a tutto vantaggio del crimine informatico.

Basti pensare ai **rischi emersi** con l'aumento massiccio dell'utilizzo dei **QR Code**, sempre più frequentemente utilizzati per risolvere problemi correlati alle restrizioni pandemiche o per fornire servizi più innovativi ed efficaci.

Uno strumento che, come tutta la tecnologia, può facilitare molto la vita di tutti giorni ma che va però "maneggiato" con cura perché può **nascondere pericolose insidie**, come **malware** o **siti fraudolenti**. Il fatto che la maggioranza degli utenti sia poco informata sui risvolti opachi dei QR code, e degli strumenti digitali in generale, offre facilmente il fianco agli hacker sempre in cerca di nuove strade per accedere al loro crimine preferito.

1.3 **LA GUERRA:** NON SOLO AL FRONTE MA ANCHE NEL CYBER SPAZIO

SUMMARY

A complicare questa situazione già di per sé drammatica si è aggiunta, all'inizio di quest'anno, anche la **guerra** in **Ucraina**, che ha aperto **ulteriori scenari** sul fronte della **sicurezza informatica**. Accanto alla guerra tradizionale, quella fatta con le armi che sparano, si sta combattendo infatti un'altra **guerra**, quella **cibernetica**, fatta con un altro genere di armi e che ha delle forti ricadute a livello globale. Ma gli effetti non sono ancora quantificabili e probabilmente si vedranno tra qualche mese, forse anni.

Secondo i **monitoraggi** di **CheckPoint**, gli attacchi al settore governativo e a quello militare dall'inizio delle ostilità sono già cresciuti su base mondiale del 21%.
Un indubbio segnale di quanto il conflitto russo-ucraino sia a tutti gli effetti un conflitto globale e non solo confinato nello spazio geografico dei due paesi protagonisti.

In questo scenario nessun paese europeo può certo stare tranquillo, viste le molte **voci istituzionali** che hanno recentemente lanciato un **grido di allarme** sulla vulnerabilità informatica dei loro paesi indicando la guerra cibernetica come uno dei maggiori rischi che può vederci coinvolti.

I casi di attacchi hacker che sfruttano i **timori** della **guerra** in corso sono sempre più frequenti. Le prime nel mirino degli hacker sono state le aziende manifatturiere europee, rimaste vittime di questa guerra e prese di mira da una campagna di mail phishing con oggetto "**Supplier Survey: Effect of supply chain from the Ucraine/Russia conflict**". Nella mail, gli hacker, sotto mentite spoglie, hanno sollecitato i destinatari a compilare un form in allegato, ovviamente contenente un malware, per segnalare eventuali ritardi e piani di back up.

Un terreno fertile che sfrutta i timori provocati dalla guerra e i pesanti impatti di approvvigionamento. Per non parlare delle varie ondate di spam e phishing, nelle quali i **criminali informatici** spacciandosi per **agenzie umanitarie** o i**stituzioni ucraine**, hanno fatto circolare in Europa e negli Usa campagne di beneficienza e di raccolta fondi, con l'unico obiettivo di rubare denaro.

Ma questi pochi esempi di cui abbiamo parlato non sono certo esaustivi di una situazione dinamica e in continuo movimento che potrebbe portare a sconvolgimenti dello scenario geopolitico, finanziario, degli equilibri economici, cosa che avrà sicuramente conseguenze sulla sicurezza informatica ma i cui effetti probabilmente si vedranno tra qualche mese, forse anni.

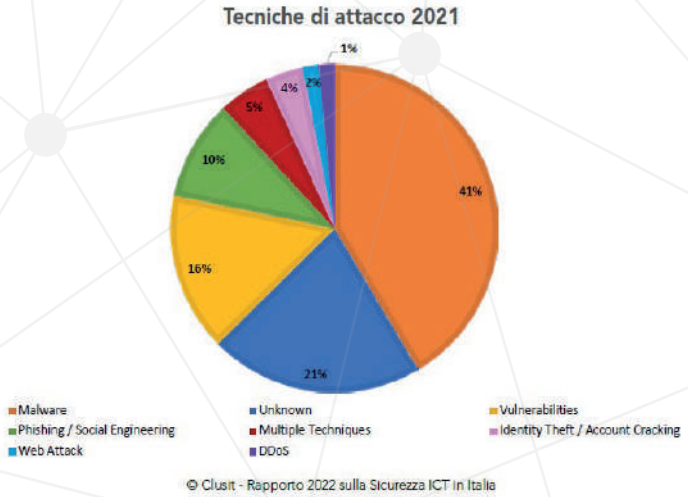
L'**AGENZIA** PER LA **CYBERSICUREZZA NAZIONALE** IN ITALIA HA RINCARATO LA DOSE AVVISANDO LE AZIENDE DELL'**URGENZA** DI "PROCEDERE A UN'ANALISI DEL RISCHIO DERIVANTE DALLE **SOLUZIONI** DI **SICUREZZA INFORMATICA** UTILIZZATE E DI CONSIDERARE L'ATTUAZIONE DI OPPORTUNE STRATEGIE DI DIVERSIFICAZIONE PER QUANTO RIGUARDA, IN PARTICOLARE: ANTIVIRUS, WEB APPLICATION, FIREWALL, PROTEZIONE DELLA POSTA ELETTRONICA, PROTEZIONE DEI SERVIZI CLOUD, SERVIZI DI SICUREZZA GESTITI".

1.4 **OLTRE IL PHISHING E I MALWARE**

SUMMARY

Se la maggior parte dei riflettori continua a essere puntata sui fenomeni Malware e ovviamente Phishing, abbiamo già detto come siano letteralmente esplose nell'ultimo anno tutte le altre forme di attacco legate alla varietà di "crepe", o vulnerabilità, in cui i criminali riescono a infilarsi per recare danni o estorcere dati o denaro a privati e aziende. Tra queste occupa un posto d'onore senz'altro quella legata all'**intelligenza artificiale** e all'**IoT** (**internet of things**), **Internet delle cose**.

QUELLO CHE EMERGE ANALIZZANDO LE NUOVE MODALITÀ DI ATTACCO NEL 2021, È CHE I **CRIMINALI CYBER** SONO SEMPRE PIÙ **SOFISTICATI** E IN GRADO DI FARE RETE CON LA CRIMINALITÀ ORGANIZZATA. DI CONSEGUENZA LE **MINACCE** SI SONO FATTE SEMPRE PIÙ **SUBDOLE** E DIFFICILI DA INDIVIDUARE E SEMPRE PIÙ FOCALIZZATE NELLO SFRUTTARE TUTTI I PUNTI DI INGRESSO RITENUTI PIÙ DEBOLI, INCLUSI GLI INDIVIDUI.



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

Nel **rapporto Clusit 2021** emerge che più della metà degli obiettivi colpiti sono stati vittime di malware e delle loro vulnerabilità. In sostanza i criminali Cyber hanno fatto principalmente affidamento sull'**efficacia** dei **Malware**, prodotti ormai industrialmente a costi sempre più bassi, e sullo sfruttamento di qualunque anello debole in grado di rappresentare un'opportunità per i loro scopi.

In quest'ottica, il **rapido sviluppo** delle **tecnologie digitali** e delle applicazioni che utilizzano l'intelligenza artificiale, indubbiamente un'importante opportunità per tutta l'umanità, non può passare inosservata. Se infatti fino a pochi anni fa avessimo visto il nostro migliore amico parlare con il frigorifero, avremmo pensato di chiamare un medico o di consigliargli un lungo periodo di vacanza, mentre oggi ci sembra già la cosa più normale del mondo. Sì, perché le nostre azioni quotidiane sono sempre più avvinghiate a strumenti di intelligenza artificiale che sostituiscono l'uomo non solo nelle azioni ma anche nel pensiero. Tanto che a volte è difficile capire dove finisce l'una e comincia l'altro.

SMART CITY, SMART BUILDING, SMART OFFICE, SMART HOME, SMART DEVICE, SMART WEARABLES, IL FUTURO DELL'UMANITÀ OCCIDENTALE SEMBRA ORMAI AVVIATO IN MODO IRREVERSIBILE VERSO IL MASSIMO RENDIMENTO CON IL MINIMO SFORZO.

Parliamo di una rivoluzione che riguarda le persone nella loro dimensione individuale ma anche in quella professionale. Infatti, l'adozione di sistemi IoT è in continua crescita anche nelle organizzazioni, in particolare nell'automazione degli edifici, nel settore automobilistico e nell'assistenza sanitaria.

Si tratta di un **processo** in **continua evoluzione** che apre la strada a un'infinità di applicazioni possibili e che, soprattutto quando la rete 5g sarà capillarmente diffusa, gestirà la nostra vita nella maggior parte dei suoi aspetti. Una prospettiva per molti affascinante ma che comporta anche grandi rischi.

Senza entrare nel merito delle implicazioni che tutto questo può avere sul funzionamento della nostra mente, va indubbiamente sottolineato il **rischio** della **sicurezza** che è **proporzionale** all'**utilizzo** della connessione internet. Anche perché i dispositivi smart sono spesso, soprattutto se paragonati ai computer e agli smartphone, molto meno evoluti dal punto di vista delle difese tecnologiche e potrebbero essere usati come una sorta di cavallo di Troia per infiltrarsi nelle reti. Insomma, le prede perfette per i Cyber criminali.

Negli ultimi cinque anni, infatti, gli **attacchi informatici** legati all'IoT sono **aumentati** di ben **70 volte** proprio perché la maggior parte (il 76% circa) dei vari strumenti comunicano con la rete su canali non cifrati, diventando così oggetto di vulnerabiltà che fanno la gioia degli hacker.

BASTI PENSARE CHE QUESTI SISTEMI DI INTELLIGENZA ARTIFICIALE SONO SPESSO INTEGRATI CON SISTEMI DI E-COMMERCE E DI CONSEGUENZA CON MEZZI DI PAGAMENTO, COME CARTE DI CREDITO O PORTAFOGLI DIGITALI. UN'OPPORTUNITÀ DAVVERO GHIOTTA PER I TRUFFATORI A CACCIA DI PROFITTO.

Secondo uno studio condotto da **Kaspersky**, l'89% dei proprietari di dispositivi IoT esprime perplessità circa la loro sicurezza in rete. Fra le preoccupazioni più diffuse c'è quella di essere **spiati** dai **Cyber-criminali** attraverso **telecamere** e **microfoni**, oppure di ricevere una richiesta di riscatto a seguito del blocco di uno dei dispositivi, oppure quella di infettare l'intera rete domestica.

Preoccupazioni assolutamente fondate sia per gli ambienti di vita sia per quelli di lavoro, anche perché la diffusione dell'IoT vede una crescita irreversibile.
Secondo alcuni analisti entro il 2025 si prevede la presenza di oltre 30 miliardi di connessioni IoT a livello globale. Con questi numeri ogni persona e ogni lavoratore avrà mediamente a disposizione 4 dispositivi interconnessi. La conoscenza degli strumenti per difendersi da questi rischi è dunque di primaria importanza

LA CONSAPEVOLEZZA E LA GIUSTA FORMAZIONE SUI RISCHI DIGITALI RIMANGONO LE DUE ARMI PIÙ EFFICACI.

1.5 **NELLA NUOVA ERA DIGITALE LA SICUREZZA NON È UN OPTIONAL**

SUMMARY

Ormai è diventato evidente che la vita "com'era prima", di cui molti hanno nostalgia, forse non tornerà più e gli effetti che la pandemia ha provocato diventeranno strutturali. La fiducia che esprimevamo lo scorso anno sulla fine dell'emergenza probabilmente deve essere ridimensionata. Ci siamo infatti resi conto che l'**emergenza** in tutte le sue forme sta diventando la **nuova normalità** e che dovremo **adattarci** più **velocemente** possibile alle trasformazioni sociali e lavorative che la crisi sanitaria ci ha imposto. 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**.

LO **SMART WORKING** STA ASSUMENDO UNA **CONNOTAZIONE STRUTTURALE**, COSÌ COME IL COMMERCIO ELETTRONICO, LA DIDATTICA A DISTANZA E LE VARIE PIATTAFORME FORMATIVE, I SERVIZI AL CITTADINO DA PARTE DELLA PUBBLICA AMMINISTRAZIONE E DELLE SOCIETÀ CHE EROGANO SERVIZI DI PUBBLICA UTILITÀ.

SE DA UN LATO LA **TRASFORMAZIONE DIGITALE** RAPPRESENTA UNA GRANDE **OPPORTUNITÀ** DI **INNOVAZIONE** E **MODERNIZZAZIONE**, DALL'ALTRO QUESTO SIGNIFICA INEVITABILMENTE FARE I CONTI CON UN **AUMENTO** DEI **RISCHI** PER LA **SICUREZZA**.

A peggiorare le cose c'è il fatto che le nuove modalità di attacco, come abbiamo visto, sono sempre più sofisticate, l'ingegneria sociale sempre più raffinata e spesso i Cyber criminali non agiscono più in modo autonomo ma fanno rete con altri loro "colleghi" o addirittura con la criminalità organizzata, provocando effetti molto dannosi, soprattutto per le aziende.

Insomma, se il futuro della nostra vita e del business non potrà prescindere dal digitale, questo significa che la **gestione** dei **dati**, il loro **corretto utilizzo** e la loro **protezione** saranno sempre più al centro di qualsiasi investimento aziendale.

Un trend che per fortuna è stato recepito dall'**Europa** e che si è tradotto in un impegno a sostenere gli **Stati membri** nel loro passaggio alla **digitalizzazione**. In questo scenario è importante essere consapevoli che non tutti i paesi nella comunità europea hanno lo stesso livello di digitalizzazione, come riscontrabile dall'edizione 2021 dell'indice di digitalizzazione dell'economia e della società (Desi).

Nei paesi con un minor livello di digitalizzazione quello che emerge è che la popolazione tra i 16 e i 74 anni possiede competenze digitali di base e solo il 22% ha competenze digitali superiori a quelle di base.

Secondo il rapporto, l'Italia, tra i paesi in Europa con un basso livello di digitalizzazione, "deve far fronte a notevoli carenze nelle competenze digitali di base e avanzate che rischiano di tradursi nell'esclusione digitale di una parte significativa della popolazione nonché di limitare la capacità di innovazione delle imprese".

Determinanti saranno dunque le scelte attuate per la migliore collocazione dei 48,1 miliardi che nel caso specifico il governo italiano ha deciso di destinare a questo settore attraverso il **PNRR**, nel quale la **Cyber security** occupa un posto centrale e strategico.

Anche perché fino ad ora gli studi pubblicati sul tema della transizione digitale indicano che l'evoluzione del trattamento dei dati e della loro sicurezza sarà la carta vincente per la ripresa economica. Insomma, l'innovazione digitale, oltre a essere molto attraente, è imprescindibile per il business del futuro ma con il suo sviluppo cresce anche il suo lato oscuro, ovvero il rischio di attacchi cyber.

La strada per proteggersi è solo una: un'adeguata formazione aziendale che consenta a tutti i dipendenti di arrivare preparati all'appuntamento con la nuova digitalizzazione evitando fallaci e irreversibili click.

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 gli ultimi due anni ci hanno 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.

PERTANTO, NELLA SCELTA DEL PERCORSO DI CYBER SECURITY AWARENESS, LE ORGANIZZAZIONI DOVRANNO TENERE CONTO DI ALCUNE VARIABILI FONDAMENTALI COME L'EFFICACIA, LE METODOLOGIE DIDATTICHE UTILIZZATE, LE TECNICHE DI COINVOLGIMENTO UTILIZZATE, L'AGGIORNAMENTO CONTINUO SULLE TECNICHE DI ATTACCO, L'ADATTABILITÀ DEI PERCORSI AI DIVERSI LIVELLI DI CONSAPEVOLEZZA, E NON ULTIMO I LINGUAGGI MULTIMEDIALI UTILIZZATI.

2. LA FORMAZIONE
2.1 UNA MISURA DI SICUREZZA NECESSARIA

SUMMARY
Tutte le organizzazioni che vogliono trarre vantaggio da questo processo di 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 cresce ed evolve costantemente. Siamo di fronte a una sfida asimmetrica che vede gli attaccanti in una posizione di indubbio vantaggio. Per riportare simmetria in questa sfida è necessario appunto fare leva 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?**". Negli anni passati abbiamo vissuto tutto ciò con una certa "leggerezza": 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 tutti e che colpisce indifferentemente individui e organizzazioni di ogni genere.

Una **sfida asimmetrica** che vede gli attaccanti in una posizione di indubbio vantaggio, anche perché, la prima linea di difesa è costituita da persone "inermi" che non hanno la consapevolezza delle minacce e delle contromisure necessarie. In alcuni casi, gli utenti subiscono attacchi senza neanche rendersene conto. 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.

NEGLI ANNI LE ORGANIZZAZIONI SI SONO PREOCCUPATE SOPRATTUTTO DI SVILUPPARE CAPACITÀ DIFENSIVE A LIVELLO TECNOLOGICO, E QUESTE DIFESE SONO INDUBBIAMENTE AUMENTATE.

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 sfida sia sbilanciata a favore degli attaccanti.

Per poter riportare la simmetria in questa sfida, 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 difensive umane, come la **percezione** del **pericolo** e la **prontezza**.

Un processo che, se da una parte va considerato come 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. Bisogna anche considerare la necessità di guidare l'**apprendimento cognitivo** in modo appropriato, senza sovraccaricare il sistema cognitivo del discente che, non lo dimentichiamo, è una persona estremamente impegnata e può dedicare alla formazione solo alcune "scampoli" della sua attenzione.

NELLA CYBERSECURITY, IL FATTORE UMANO GIOCA UN RUOLO DECISIVO!

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 condiviso 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 NELL'ETERNA SFIDA 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.

2.3 **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 conoscenza, 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 DIDATTICO, 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, perché oggi queste due dimensioni tendono spesso a sovrapporsi.

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;

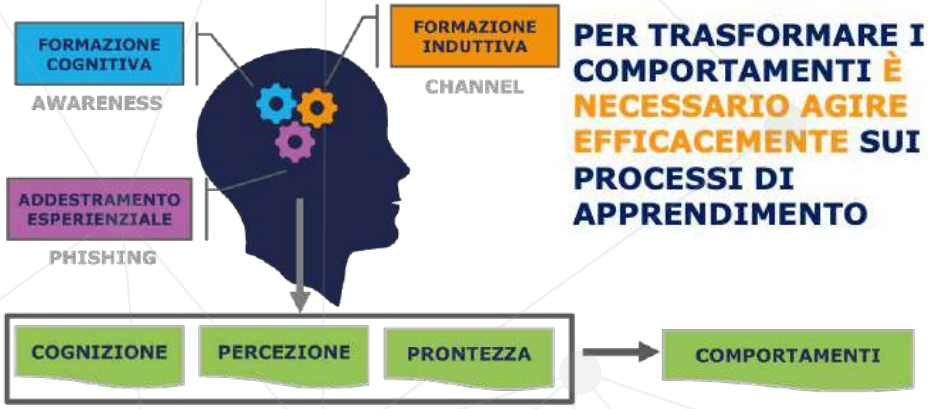
- LA CYBER SECURITY AWARENESS RIGUARDA ESCLUSIVAMENTE LA DIMENSIONE PROFESSIONALE DELL'INDIVIDUO E QUINDI IL SUO RUOLO ALL'INTERNO DELL'ORGANIZZAZIONE;

- 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 didattico, ad altri di carattere esperienziale e induttivo, si ottiene un significativo mix in grado di agire positivamente sulla conoscenza, sulla percezione del pericolo e sulla prontezza, condizionando attitudini e comportamenti.

Se è abbastanza facile immaginare una **formazione didattica**, 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.

2.4 **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 cognitivo, 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 compatibile con le proprie attività e con la necessità di non sovraccaricare il sistema cognitivo) per prevenire quello che già oggi è il rischio più importante per la loro sicurezza individuale, e di riflesso, per la sicurezza dell'intera organizzazione.

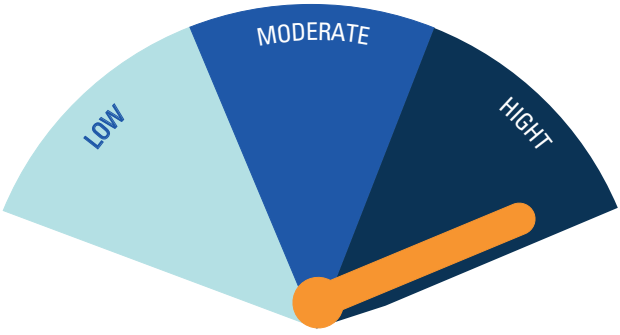
È QUINDI FONDAMENTALE CHE VENGA ACQUISITA UNA REALE CONSAPEVOLEZZA DEL LIVELLO DI RISCHIO. PERCHÉ IL RISCHIO CYBER PUÒ, DA UNA PARTE TRASFORMARE LA VITA DI UN INDIVIDUO IN UN VERO E PROPRIO INCUBO, E DALL'ALTRA METTERE ADDIRITTURA IN DISCUSSIONE LA SOPRAVVIVENZA STESSA DELL'ORGANIZZAZIONE.

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 a partire dal 2020, hanno di fatto dimostrato che per affrontare problematiche di questo tipo esiste esclusivamente l'opzione della formazione a distanza, in tutte le sue varie forme.

Per tornare alle due domande precedenti, 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 didattico, 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 tipo cognitivo.

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.

2.5 **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 ispirate ai principi dell'apprendimento multimediale 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 EQUILIBRATO.

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.

2.7 **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**

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:

FORMAZIONE DIDATTICA

APPRENDIMENTO ESPERIENZIALE

FORMAZIONE INDUTTIVA

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:

CONOSCENZA
AZIONE RAZIONALE

PERCEZIONE
AZIONE ISTINTUALE

PRONTEZZA
AZIONE IMMEDIATA

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.

3.3 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.

3.4 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.**

l 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.


Cyber
Guru
WWW.CYBERGURU.IT