Cyber Security Awareness White Paper

Investire sul Fattore Umano per garantire la Cyber Security

La *Cyber Security Awareness* o *Security Awareness* (da ora in poi CSA), si definisce come:

> la consapevolezza delle persone rispetto ai rischi di Cyber Security nell'interazione con le tecnologie digitali e in modo particolare con il Web.

Executive Summary

In un'organizzazione pubblica o privata, agire sulla *Cyber Security Awareness*, significa innalzare il livello di Cyber Security dell'intera organizzazione sia in termini di protezione dei dati aziendali critici sia in termini di tutela dei dati personali. Si tratta di un investimento che produce benefici per l'organizzazione, ma con ricadute che incidono anche sulla dimensione privata e sociale degli individui.

Questo tipo di investimento diventa sempre più urgente, in virtù della rapida crescita del Cyber Crime, che nel 2017 ha fatto registrare quello che tutti gli osservatori hanno definito un vero e proprio salto quantico del crimine informatico, che ha prodotto danni per oltre 500 miliardi di dollari, un "volume di affari" superiore a quello del crimine tradizionale.

Nell'analisi di questo scenario, emerge un dato preoccupante, ossia che la maggior parte delle violazioni può essere ricondotta al cosiddetto fattore umano: comportamenti inadeguati che hanno funzionato da "apri porta" rispetto alle strategie utilizzate dagli attaccanti. Oltre l'80% delle, violazioni è stata causata da errori commessi da individui che agiscono in modo inconsapevole rispetto alla qualità e alla quantità delle minacce Cyber.

Per agire in modo consapevole è necessario quindi acquisire gli elementi cognitivi che consentano di maturare attitudini e adeguare i comportamenti rispetto ai rischi del Cyber Spazio. All'interno di qualsiasi organizzazione pubblica o privata è quindi necessario fare in modo che il personale non-specialistico segua un percorso formativo che li porti a fare un uso sempre più consapevole delle tecnologie digitali, degli strumenti social e delle risorse presenti nel web.

Quando si fa un intervento di questa portata, che riguarda tutti i dipendenti di un'organizzazione, bisogna studiare un percorso formativo con delle caratteristiche precise: estremamente efficace, efficiente, e a basso impatto rispetto alla produttività dell'organizzazione.

Deve essere un percorso stimolante e coinvolgente, e non si deve limitare a fornire gli elementi teorici e nozionistici della materia, ma deve allenare alcune caratteristiche umane, come l'attenzione, la prontezza, la reattività, così da mettere l'individuo in condizione di reagire anche alle minacce sconosciute.

Cyber Guru è un progetto che ha come target il personale non-specialistico delle organizzazioni pubbliche e private. La finalità principale di questo progetto è quella di contribuire a ridurre il rischio Cyber, andando ad agire sul fattore umano attraverso modelli avanzati di formazione che siano in grado di sviluppare consapevolezza rispetto alle minacce.

E in questo contesto che è stata sviluppata la piattaforma Cyber Guru Enterprise, un sistema avanzato di Cyber Security Awareness Computer based training.

Cyber Guru Enterprise è una piattaforma sviluppata applicando le più moderne teorie educative e pedagogiche, nonché i più attuali e consolidati paradigmi di progettazione orientati a garantire la massima facilità di utilizzo da parte di un parco utenti estremamente eterogeneo.

La formazione è strutturata in 3 livelli formativi, dove ogni livello (annualità), corrisponde a un ciclo formativo completo e auto-consistente.

La qualità di Cyber Guru Enterprise è garantita da un processo di sviluppo e aggiornamento particolarmente efficace e attento al particolare. La necessità di rendere accessibile a tutti una formazione che riguarda argomentazioni che presentano un background di tipo tecnico e che fino a ieri rappresentavano un'esclusiva degli specialisti di Cyber Security, richiede la massima cura di ogni elemento del processo e il ricorso alle metodologie più avanzate dal punto di vista pedagogico ed educativo.

Sommario

Definizione

La CSA può essere definita come la consapevolezza delle persone rispetto ai rischi di Cyber Security nell'interazione con le tecnologie digitali e in modo particolare con il Web.

Agire sulla CSA e quindi sul livello di consapevolezza delle persone, attraverso processi di formazione e informazione significa contribuire a proteggere la persona e la sua dimensione sociale, diminuendo la sua esposizione al rischio di subire un attacco Cyber.

Quando per dimensione sociale di una persona si intende l'organizzazione pubblica o privata in cui questa opera, questo livello di consapevolezza assume ancora maggiore valore. In questo ambito, il comportamento inconsapevole di una persona nella sua interazione con la dimensione digitale può provocare rischi molto seri per l'esistenza stessa dell'organizzazione.

In questo caso, agire sulla CSA, significa innalzare il livello di Cyber Security dell'intera organizzazione sia in termini di protezione dei dati aziendali critici sia in termini di tutela dei dati personali e quindi anche rispetto a quanto previsto dalle normative sulla Privacy, non ultimo il nuovo regolamento europeo sulla tutela dei dati personali: GDPR.

Considerando che la dimensione personale e professionale degli individui si va sempre più sovrapponendo, spinta dagli attuali processi di trasformazione digitale e dalla centralità che strumenti come lo smartphone hanno assunto nella quotidianità delle persone, qualsiasi azione che vada ad agire sulla CSA dell'individuo produce benefici concreti sia a livello personale sia a livello professionale.

Il salto quantico del Cyber Crime

Il 2017 ha registrato per molti osservatori il cosiddetto "salto quantico" del Cyber Crime, una crescita senza precedenti delle attività criminali che hanno riguardato la dimensione digitale, con il definitivo sorpasso, in termini di volume di "affari", del Cyber Crime nei confronti del crimine tradizionale.

Nella simbologia moderna il "ragazzo con la felpa e il cappuccio" si pone in contrapposizione al "rapinatore con passamontagna e pistola", una simbologia che non aiuta a dimensionare l'aggressività e la pericolosità del crimine digitale. Se è pur vero che all'interno del Cyber Crime possiamo anche considerare il piccolo hacker, la realtà è che le grandi organizzazioni criminali si stanno riposizionando nella sfera digitale e che il livello di aggressività di queste organizzazioni aumenta continuamente. Non entriamo nelle considerazioni che riguardano la dimensione geopolitica del Cyber Crime, e quindi degli intrecci che si vanno creando tra le organizzazioni criminali e gli Stati nella gestione del Cyber Spazio, ma è comunque certo che il "ragazzo con la felpa e il cappuccio" è un'icona che ormai non rappresenta più il Cyber Crime.

Per dare una dimensione chiara del fenomeno e del suo sviluppo, possiamo fare ricorso a una grande quantità di ricerche disponibili nel Web, che convergono tutte rispetto a una crescita esponenziale della criminalità informatica, un trend di crescita di cui è difficile prevedere la fine.

Una visione autorevole è certamente quella rappresentata del rapporto 2018 pubblicato dal Clusit, l'Associazione Italiana per la Sicurezza Informatica, che certifica appunto questa sorta di "salto quantico" della criminalità Cyber, che nel 2017 ha prodotto danni stimati intorno ai 500 miliardi di dollari. Sempre secondo il rapporto, le attività criminali intese come truffe, estorsioni, furti di denaro e di dati personali hanno colpito quasi un miliardo di persone nel mondo, causando ai soli privati cittadini una perdita stimata intorno ai 180 miliardi di dollari. Numeri impressionanti, che si sono addirittura quintuplicati nel corso degli ultimi 6 anni (2011-2017). Sempre secondo questo rapporto, il 2017 è stato anche "l'anno del trionfo del Malware, degli attacchi industrializzati realizzati su scala planetaria contro bersagli multipli e della definitiva discesa in campo degli Stati come attori di minaccia".

Il rapporto Clusit, come tutte le altre ricerche fatte in materia, mostra come nel Cyber Spazio si consumi quotidianamente una "guerra sporca", tra chi attacca e chi tenta di difendersi, una guerra che per essere vinta richiede la "chiamata alle armi" non solo degli specialisti della sicurezza informatica, ma di tutti gli individui che agiscono come utenti delle tecnologie digitali.

Infatti, nell'analisi della rapida evoluzione del Cyber Crime, emerge un dato preoccupante rispetto alle violazioni subite dalle organizzazioni pubbliche e private: tutte le ricerche convergono nel riconoscere come fattore scatenante di gran parte di queste violazioni, il cosiddetto "fattore umano". All'interno di questa categoria concettuale, vengono considerati comportamenti inadeguati da parte di un qualsiasi componente dell'organizzazione, che di fatto hanno funzionato da "apri porta" rispetto alle strategie utilizzate dagli attaccanti. Le percentuali variano da ricerca e ricerca, ma tutte concordano sull'assegnare al fattore umano una percentuale superiore all'80%, evidenziando come sia il piccolo hacker sia le grandi organizzazioni criminali, abbiano messo gli individui e le loro debolezze al centro delle loro strategie di attacco.

Il fattore umano nella Cyber Security

A dispetto dei grandi investimenti effettuati in tecnologie di Cyber Security, il rischio Cyber delle organizzazioni pubbliche e private continua crescere. Per invertire questa tendenza è necessario investire in modo consistente sul fattore umano, soprattutto sul livello di consapevolezza delle persone. Un investimento che vada a chiudere il gap culturale che è stato generato dalla rapida trasformazione digitale: tutti i processi economici e sociali hanno subito pesanti trasformazioni, mentre le capacità umane non hanno avuto il tempo di evolvere, ma soprattutto di acculturarsi rispetto ai rischi associati a questo tipo di trasformazione.

Il problema non riguarda solo le "vecchie generazioni", che spesso hanno difficoltà anche ad interagire con le tecnologie digitali di ultima generazione, ma riguarda tutti. Le nuove generazioni, in modo particolare i cosiddetti "millenials" hanno infatti una naturale propensione all'uso delle tecnologie digitali, ma lo fanno spesso da "utenti inconsapevoli", perché nessuno si è preoccupato di trasferire loro gli strumenti cognitivi per riconoscere il rischio di diventare vittime di organizzazioni senza scrupoli che violando la loro privacy cercano di manipolarne i comportamenti e le scelte.

Lo scandalo Cambridge Analytica, scoppiato all'inizio del 2018, ha reso "popolare" un tema che è sul tappeto già da alcuni anni, e cioè la reale possibilità di una persona di mantenere il controllo sui propri dati personali nella dimensione social, un tema che è stato posto alla base

dell'evoluzione continua delle normative sulla privacy, fino ad approdare all'attuale regolamento europeo GDPR sulla tutela dei dati personali, che rivede il concetto stesso di privacy alla luce della trasformazione digitale. Un tema che potrà essere posto sotto controllo solo se tutti gli individui cominceranno ad agire in modo consapevole, tenendo conto dell'importanza di tutelare la sfera personale e quella sociale.

Per agire in modo consapevole è necessario acquisire gli elementi cognitivi che consentano di maturare attitudini e adeguare i comportamenti rispetto ai rischi del Cyber Spazio. Un processo continuo fatto non solo di conoscenza, ma anche di allenamento di alcune caratteristiche umane, come la prontezza e la reattività, ciò che gli anglosassoni sintetizzano con il termine *readyness*. Per aumentare la consapevolezza delle persone sono necessari processi formativi avanzati, basati su una metodologia di "formazione continua" e di "allenamento". Se è vero che le strategie di attacco evolvono costantemente, sul piano quantitativo e su quello qualitativo, allora è necessario, per chi deve proteggersi, mantenersi allo stesso livello di evoluzione del Cyber Crime, anzi possibilmente porsi un "passo in avanti" rispetto alla capacità di "identificare una minaccia", anche quando questa rientra nel novero delle minacce ancora sconosciute. E questo risultato lo si può ottenere solamente adeguando costantemente il proprio livello di conoscenza e mantenendo sempre vigile la propria attenzione rispetto ai fattori di rischio.

Il ruolo della formazione

Come conseguenza di tutto quello che è stato descritto in precedenza risulta ovvio che all'interno di un'organizzazione, pubblica o privata che sia, è necessario fare in modo che il personale non-specialistico, cioè coloro che non hanno competenze specifiche in ambito Cyber Security, segua un percorso formativo che li porti a 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 un atteggiamento estremamente difensivo, che, di fronte ad un'irrazionale percezione del rischio, produca comportamenti che incidano negativamente sulla produttività dell'individuo e dell'organizzazione.

Il profilo consapevole è quello che permette di ridurre i rischi usando una giusta combinazione di conoscenza ed esperienza, e che allo stesso tempo mantiene gli individui pienamente produttivi e non "bloccati" di fronte ad un'interpretazione irrazionale del pericolo.

Caratteristiche del percorso formativo

Per acquisire questo profilo consapevole è necessario un percorso formativo che contenga:

- una parte più orientata alla nozione, che produce il miglioramento della componente attitudinaria;
- una parte più orientata alla pratica, che produce il miglioramento del profilo comportamentale verso minacce più o meno conosciute.

Considerando la specificità della materia sarà necessario che questo percorso formativo sia:

- motivante, stimolando la persona a sentirsi coinvolta nel percorso formativo;
- a basso impatto, rispetto alla normale attività lavorativa;
- divulgativo, rifuggendo ogni forma di ortodossia tecnologica che provocherebbe un naturale rifiuto da parte del personale non specialistico.

Rispetto ai tradizionali piani di training, un piano di CSA ha delle caratteristiche di unicità derivanti dal fatto che impatta sull'intera popolazione aziendale. Dovrà quindi essere caratterizzato da unità formative brevi, auto-consistenti e ben distribuite nel tempo, prendendo spunto da metodologie di "on-going training", così da produrre un effettivo cambio di atteggiamento e di comportamento di fronte al rischio Cyber.

Le persone devono trasformarsi da potenziali "alleati inconsapevoli" di attività criminali, ad agenti consapevoli del sistema di Cyber Defence.

Facciamo alcune ulteriori considerazioni relativamente a un percorso formativo di CSA:

- abbiamo già detto che deve avere un basso impatto, al fine di contenere i costi indiretti, legati alla produttività dei dipendenti;
- per le stesse ragioni deve essere flessibile nella sua fruizione, al fine di limitare l'impatto operativo; pochi minuti a settimana da poter fare nei momenti ritenuti più opportuni;
- deve utilizzare un lessico semplice, divulgativo, finalizzato alla comprensione e quindi all'efficacia del processo di apprendimento, e non al rispetto di canoni di carattere tecnologico;
- deve essere distribuito nel tempo, con frequenti richiami di concetti già esposti, per favorire l'assimilazione e lo sviluppo delle attitudini e dei comportamenti;
- deve essere intuitivo e gradevole da fruire, con contenuti di carattere multimediale;
- deve includere forme di gioco e di competizione, che lo rendano coinvolgente anche rispetto al fattore tempo;
- deve includere forme di riconoscimento e valutazione dell'impegno profuso e del livello di apprendimento raggiunto;
- deve fornire benefici sia sul piano personale che sul piano professionale, considerando che un comportamento consapevole produce anche un incremento della sicurezza della persona, estensibile alla sua sfera familiare.

Modalità di erogazione

Dal punto di vista formativo si contrappongono normalmente due modalità di erogazione della formazione:

- la formazione d'aula
- la formazione su piattaforma di e-learning.

Entrambe presentano elementi di valutazione positivi e negativi, ma nel caso della CSA la tradizionale formazione d'aula presenta dei limiti macroscopici. Per prima cosa si tratta di una formazione molto "dispendiosa" e con un impatto organizzativo elevato, specialmente se si sommano complicazioni di carattere logistico (distribuzione su più sedi).

Ma il vero limite della formazione d'aula rispetto ai programmi di CSA è dato dalle caratteristiche proprie di questo tipo intervento formativo, molto concentrato nel tempo e che produce risultati effimeri, poco duraturi e che non lasciano molto spazio all'aggiornamento, che nel caso della CSA è invece una vera e propria necessità.

Il coinvolgimento è molto forte durante l'erogazione del corso e tende invece a dissiparsi con il passare del tempo. Nel caso della CSA, la formazione d'aula si presta più ad attività iniziali, di lancio e di informazione, che rispondono soprattutto ad obiettivi di comunicazione piuttosto che ad obiettivi di carattere formativo.

Le piattaforme di e-Learning, per loro natura hanno costi unitari contenuti, sono più agili e più facili da adottare. L'impatto sulla produttività e certamente più basso di quello generato dalla formazione d'aula e si adattano meglio ai ritmi produttivi delle diverse figure e dei diversi ruoli. Per questo sono soluzioni di più facile adozione.

Anche le piattaforme di e-Learning hanno i loro punti di debolezza che consistono in un basso livello di coinvolgimento, che comporta il rischio di un abbandono prematuro nel programma, oppure, nei casi di formazione obbligatoria, ad un abbassamento del livello di attenzione, con un decadimento dei processi di apprendimento.

Al fine di minimizzare questi rischi è quindi necessario che sia la piattaforma sia i contenuti formativi erogati, siano progettati secondo i dettami più avanzati della formazione aziendale. Per quanto riguarda la piattaforma sarà fondamentale la semplicità di fruizione e i criteri di interfaccia che devono essere realizzati secondo i più elevati standard di User Interface. La fruizione deve essere collegata a un processo di "gamification", perché il gioco è la forma più naturale di apprendimento. L'utente deve essere poi coinvolto in una competizione virtuosa, dove percepisca una missione collettiva che va oltre il mero apprendimento. Il concetto di appartenenza a un team serve a rafforzare le motivazioni individuali e a stimolare la partecipazione.

Anche i contenuti devono essere progettati per stimolare l'apprendimento e la partecipazione e non devono diventare un ostacolo al percorso formativo. Inoltre, l'utente deve percepire l'utilità dell'apprendimento e comprendere come i benefici ottenuti a fronte del suo impegno siano concreti, in grado di incidere sulla qualità della sua esperienza, in questo caso l'esperienza nell'interazione con le tecnologie digitali.

Rispetto alle modalità di erogazione, non ci sono dubbi che la CSA richieda l'adozione di una piattaforma di e-Learning, ma nello stesso tempo è indispensabile che si tratti di una piattaforma avanzata, con contenuti che rispondono a criteri formativi altrettanto avanzati.

Cyber Guru

Cyber Guru è un progetto che ha lo scopo di dare una risposta concreta a queste istanze di crescita del livello di consapevolezza, sviluppando un'intera linea di prodotti di Cyber Security che hanno come target il personale non-specialistico delle organizzazioni pubbliche e private.

La finalità principale di questo progetto è quella di contribuire a ridurre il rischio Cyber, andando ad agire sul fattore umano attraverso modelli avanzati di formazione che siano in grado di sviluppare consapevolezza rispetto alle minacce.

Si tratta di un progetto che punta quindi ad incidere in modo concreto ed efficace su attitudini e comportamenti, trasformando le persone da veicoli inconsapevoli del Cyber Crime, ad "agenti attivi" del sistema di Cyber Defence.

Cyber Guru Enterprise

In modo particolare focalizziamo l'attenzione su Cyber Guru Enterprise, un sistema avanzato di Cyber Security Awareness Computer based training, proposto quindi in modalità e-Learning, che fornisce gli elementi cognitivi fondamentali rispetto ai rischi e alle minacce Cyber all'interno di un percorso formativo che favorisce i processi di apprendimento.

Cyber Guru Enterprise è una piattaforma sviluppata completamente in Italia, applicando le più moderne teorie educative e pedagogiche, nonché i più attuali e consolidati paradigmi di progettazione orientati a garantire la massima facilità di utilizzo da parte di un parco utenti estremamente eterogeneo.

La formazione è strutturata in 3 livelli formativi, dove ogni livello (annualità), corrisponde a un ciclo formativo completo e auto-consistente.


Cyber Guru
Statistiche · Alessandro Bianchi
Cyber-Security-Awa...
Cyber Security Awaren...
Phishing
Attestato di partecipa...
Ciao Alessandro, riprendi il corso
Attestato - scarica pdf
Premi - vai alla sezione
E-LEARNING
CYBER SECURITY AWARENESS
Il fattore umano è un elemento decisivo nel successo di qualsiasi iniziativa e nella Cyber Security sono i comportamenti umani a fare la differenza. Aumentare la consapevolezza degli individui nell'interazione con le tecnologie digitali e con il web è la strada maestra per elevare il livello di Cyber Security degli individui e delle organizzazioni.
News
Cyberpedia
Tutorial
MODULO 01
PHISHING
Il Phishing è la più comune tecnica di attacco utilizzata dai criminali Cyber e utilizza la mail come principale veicolo di diffusione. Scopri come riuscire a riconoscere un attacco phishing, adottando le necessarie contromisure.
Cos'è il Phishing e come riconoscerlo
Test - Cos'è il Phishing e come riconoscerlo

12 moduli formativi

Ogni livello è strutturato in 12 moduli formativi, ognuno dei quali è dedicato ad uno specifico argomento, anche se sono frequenti i richiami tra un modulo e un altro. I moduli vengono abilitati con la frequenza di uno al mese, e il metodo di fruizione è rigidamente sequenziale. E quindi necessario completare la fruizione di un modulo, prima di passare al modulo successivo.

3 lezioni per modulo

Ogni modulo è formato da 3 brevi lezioni, ognuna delle quali è costituita da un contenuto video di pochi minuti e, come alternativa, da un documento pdf che riproduce gli stessi contenuti del video in un formato "rich text".

Le 3 lezioni all'interno di un modulo sono organizzate secondo questo schema:

- La prima lezione è quella della conoscenza di base; consente una presa di conoscenza dell'argomento, fornendo gli elementi cognitivi che consentono la comprensione del rischio.
- La seconda lezione è quella dell'approfondimento; consente di stimolare la "prontezza", creando le condizioni per riconoscere le minacce anche quando queste si presentano in forma insolita e sofisticata.
- La terza lezione è quella delle best practice; consente di acquisire "buone pratiche" di comportamento, stimolando la "reattività", e quindi la capacità di agire in modo consapevole.

Test di apprendimento

Per passare da una lezione all'altra è necessario superare un test di apprendimento, costituito da 4 domande a risposta multipla. La lezione è considerata superata quando si risponde correttamente ad almeno 3 domande su 4. Il test può essere ripetuto più di una volta e ai fini del percorso formativo viene sempre considerato il risultato migliore.

Documento di approfondimento

Coloro che vogliono approfondire la tematica specifica trattata nel modulo possono accedere al documento di approfondimento, che integra i contenuti "obbligatori" delle lezioni, con contenuti la cui fruizione è facoltativa rispetto al percorso formativo.

Medaglia

Il completamento del modulo si ottiene automaticamente con il superamento del terzo test di apprendimento, e quindi con l'attestazione del superamento della terza lezione. Qualora tutti e 3 i test di apprendimento siano stati completati con un livello di eccellenza, corrispondente a 4 risposte esatte sulle 4 domande proposte, a fine modulo al partecipante viene assegnata a una medaglia. La medaglia viene assegnata anche quando il livello di eccellenza viene ottenuto ripetendo un test più volte.

Test di valutazione e Coppa

Alla fine di 3 moduli formativi, e quindi di quello che viene definito un blocco formativo (o trimestre), viene proposto un test di valutazione di 5 domande a risposta multipla. I test di valutazione, a differenza di quelli di apprendimento, sono "one shoot" e quindi non possono essere ripetuti. Nel caso di un percorso eccellente, e quindi nel caso in cui il partecipante abbia ottenuto tutte le medaglie relative ai 3 moduli formativi che costituiscono il blocco, il test di valutazione diventa decisivo per conquistare una coppa. Per conquistare la coppa è necessario fornire 5 risposte esatte su 5 domande.

Classifica

Il percorso formativo permette di valorizzare una classifica individuale e un “medagliere”. La classifica individuale serve a valorizzare la classifica per team, che tratteremo più avanti.

Di seguito lo schema di punteggio applicato:

- 1 punto per ogni risposta esatta ottenuta nel test di apprendimento, a fine lezione (il superamento di una lezione comporta quindi il punteggio minimo di 3 punti e il punteggio massimo di 4 punti).
- La conquista di una medaglia comporta l'assegnazione di 15 punti (12 punti conquistati nelle risposte ai test delle 3 lezioni e un bonus di 3 punti),
- 1 punto per ogni risposta esatta ottenuta nel test di valutazione a fine blocco (massimo punteggio 5 punti).
- In caso di conquista della Coppa viene concesso un bonus di ulteriori 10 punti.

Per effetto di questo schema un partecipante che arriva a fine corso può produrre da un punteggio minimo di 108 punti a un punteggio massimo di 240 punti.

Organizzazione e competizione per team

Come già accennato in precedenza, Cyber Guru Enterprise prevede un’organizzazione per team, e quindi per unità organizzative. L’organizzazione per team è propedeutica all’attivazione di una competizione virtuosa tra i vari team, una sorta di campionato della “Cyber Security”.

Il percorso formativo di ogni partecipante, valorizzato attraverso lo schema di punteggio citato nel paragrafo precedente, contribuisce in forma aggregata a costituire una classifica dei team tenendo conto delle seguenti considerazioni:

- Il punteggio del team è mediato rispetto al numero dei suoi componenti, così che ogni team, indipendentemente dalla propria consistenza numerica, può competere con gli altri.
- E' possibile che una persona cambi team durante il percorso formativo (spostamenti organizzativi). In questo caso le sue prestazioni verranno ereditate dal nuovo team di appartenenza.

Team leader e supervisore

Oltre alla figura del partecipante, Cyber Guru Enterprise, prevede altre due figure:

- Il team leader, che è un partecipante che ha funzioni di coordinamento e di stimolo nei confronti del proprio team.
- Il supervisore, che è il responsabile del progetto formativo e che ha un’ampia visibilità rispetto all’andamento del progetto attraverso una serie di report statistici dedicati alla sua funzione e ai suoi obiettivi.

Statistiche e comunicazione

Cyber Guru Enterprise fornisce una serie di statistiche che consentono di mantenere un completo monitoraggio sull’efficacia del percorso formativo. Queste statistiche rappresentano un ulteriore stimolo ad una piena partecipazione, favorendo il coinvolgimento del partecipante, rispetto al team e all’organizzazione. Tra le varie informazioni fornite, il medagliere, ad esempio, è uno strumento che stimola l’emulazione positiva. Le statistiche sono diversificate a seconda del ruolo (utente, team leader e supervisore).

La piattaforma prevede efficaci strumenti di comunicazione che servono a stimolare la piena partecipazione. La sezione news consente ad esempio di evidenziare novità importanti che

riguardano sia l'evoluzione del percorso formativo sia l'evoluzione del contesto relativo alla Cyber Security.

Sono previste inoltre in automatico una serie di mail di "Student Caring", che consentono di evidenziare il percorso formativo del singolo individuo, paragonandolo a quello del proprio team e degli altri team in competizione.

Tutte le statistiche vengono fornite nel pieno rispetto della Privacy e della tutela dei dati personali. Ogni partecipante ha contezza dei propri indicatori, rapportati al team e all'organizzazione. Per il resto sia i partecipanti sia i team leader vedono solo dati aggregati, per team e per organizzazione. L'unica statistica personale visibile a tutti è il cosiddetto medagliere, che evidenzia solo i meriti di coloro che hanno profuso il massimo impegno.

Semplicità di fruizione

Per rendere ancora più semplice la fruizione della piattaforma esiste un'ampia sezione tutorial che descrive in maniera estremamente chiara ogni unità funzionale, ricorrendo a tecniche di video animazione.

La sezione Cyberpedia consente di approfondire il significato di concetti e termini tecnici che vengono utilizzati durante il corso. Come già riferito in precedenza, il corso usa un linguaggio estremamente divulgativo che rifugge ogni ortodossia tecnologica. In alcuni casi però è necessario ricorrere a concetti e termini più tecnici, che vengono "spiegati" all'interno della sezione Cyberpedia. In alcuni casi questa sezione serve a ritrovare una terminologia di tipo tecnico a un concetto che nei contenuti nel corso viene trattato in modo divulgativo.

Gamification

I test di apprendimento e di valutazione, le classifiche, individuali e di team, l'organizzazione in team, l'assegnazione di coppe e medaglie sono tutti elementi che contribuiscono a stimolare il gioco e la competizione virtuosa, rendendo il percorso formativo più coinvolgente.

Il processo di sviluppo

La qualità di Cyber Guru Enterprise è garantita da un processo di sviluppo e aggiornamento particolarmente efficace e attento al particolare. La necessità di rendere accessibile a tutti una formazione che riguarda argomentazioni che presentano un background di tipo tecnico e che fino a ieri rappresentavano un'esclusiva degli specialisti di Cyber Security, richiede la massima cura di ogni elemento del processo e il ricorso alle metodologie più avanzate dal punto di vista pedagogico ed educativo.

Piattaforma di erogazione

Prima di approfondire il processo, poniamo l'attenzione sulla piattaforma di erogazione, che è uno dei punti di forza della proposta Cyber Guru Enterprise.

La piattaforma di erogazione è basata sul framework di e-Learning Moodle, uno strumento didattico, con accesso ed utilizzo interamente dal web e che si basa su modelli responsive e quindi pienamente accessibili da qualsiasi dispositivo, inclusi i dispositivi mobili.

Moodle è il framework di e-learning più diffuso al mondo, in particolar modo nelle Istituzioni accademiche e scolastiche: oltre 1150 organizzazioni di vario genere e tipologia di 81 paesi del mondo hanno installato la piattaforma Moodle per gestire le attività di e-Learning; in Italia è utilizzata da moltissime organizzazioni e da gran parte delle istituzioni scolastiche ed universitarie.

User Interface

Per la realizzazione della piattaforma sono stati adottati i più attuali e consolidati paradigmi di progettazione orientati a garantire la massima facilità di utilizzo da parte di un parco utenti estremamente eterogeneo.

Le soluzioni di user experience introdotte (e validate su un apposito campione di utenti) hanno posto al centro l'obiettivo di supportare l'utente nell'avanzamento del proprio percorso formativo a partire da un impianto di fruizione verticale (modulo > lezione > test di verifica) pensato per minimizzare l'effort cognitivo e garantire un agevole approdo alla didattica; gli utenti possono quindi facilmente accedere ai contenuti loro proposti avanzando tra moduli e lezioni e, in un'ottica di continuità e semplicità, riprendere velocemente il percorso formativo eventualmente interrotto bypassando le informazioni a corredo dell'esperienza.

Sebbene la piattaforma proponga un modello di fruizione estremamente semplice, gli utenti hanno a disposizione dei videotutorial che li aiutano nella comprensione delle diverse meccaniche e funzionalità.

La piattaforma può inoltre giovarsi di un "linguaggio" visivo e interattivo che, incentrato su codici colore (semaforo: verde, giallo e rosso) e su comportamenti della pagina, comunica con l'utente con chiarezza e precisione, stabilendo un "dialogo" che riduce via via la quantità e affina la qualità dei messaggi man mano che l'utente si misura con il percorso formativo.

Per garantire continuità e coerenza alla didattica è stata sviluppata una piattaforma fruibile con comodità da tutti i dispositivi e le cui cromie, il cui corredo iconico e i cui *artwork* conferiscono infine freschezza e modernità alla *user interface*, agendo da ulteriori elementi di facilitazione nel percorso di comprensione e interazione con il contesto.

Il processo di sviluppo vero e proprio

Di seguito una descrizione delle principali fasi del processo di produzione dei contenuti della piattaforma Cyber Guru Enterprise:

- Definizione dei contenuti – è gestita dal Comitato tecnico-scientifico di Cyber Guru, l'entità che seleziona ed elabora i contenuti con un approccio specialistico. Questa entità propone e definisce gli argomenti e seleziona il materiale di base. E' formata da specialisti della Cyber Security con provata esperienza e in possesso di tutte le certificazioni.
- Trasformazione dei contenuti – è la parte del processo in cui i contenuti specialistici si trasformano in contenuti di carattere divulgativo, assumendo la forma dello schema con cui vengono strutturate le lezioni (conoscenza, approfondimento, best practice). Questa parte del processo è guidata da esperti di comunicazione che però hanno una provata esperienza nel settore IT e IT Security.
- Multimedialità – in questa fase, gestita da esperti della comunicazione multimediale, i contenuti subiscono un primo adattamento alle forme e ai linguaggi video.
- Formazione – in questa fase, gestita da esperti della formazione e condotta con la collaborazione incisiva del Dipartimento di Scienza della Formazione dell'Università di Roma Tre, i contenuti vengono ulteriormente adattati rispetto ai criteri più avanzati delle scienze pedagogiche ed educative, con lo scopo di renderli più efficaci, avendo come obiettivo il massimo coinvolgimento del partecipante. E' la fase in cui vengono strutturate anche le domande secondo lo schema di domanda a risposta multipla.
- Sceneggiatura – E' la prima fase della produzione video, in cui i contenuti prendono la forma di dialoghi e di indicazioni per la fase di post-produzione. Questa fase viene gestita con la collaborazione di esperti della produzione video e multimediale.
- Produzione Video – che include tutte le fasi di produzione e post-produzione, gestita da professionisti della produzione video e multimediale. Alla fine di questo processo i contenuti hanno assunto una forma definitiva e sono pronti per il processo di revisione.
- Revisione contenuti – in questa fase tutte le entità coinvolte nel processo verificano la qualità del processo di produzione dei contenuti e l'efficacia del risultato ottenuto. In questa fase si apportano le opportune modifiche e si procede al rilascio definitivo del modulo formativo.
- Rilascio – è la fase in cui i contenuti si strutturano definitivamente in lezioni, test, documenti di approfondimento, e quindi nel modulo formativo.

Il primo livello formativo

Di seguito la lista argomentata dei 12 moduli formativi che costituiscono il primo livello formativo. Benché ogni modulo sia auto-consistente, la sequenza con cui sono stati organizzati è stata studiata per produrre dei "naturali" richiami ad argomentazioni già affrontati in precedenza, rafforzando in questo modo il livello di apprendimento e memorizzazione dei contenuti.

PHISHING

Il PHISHING è la più comune tecnica di attacco utilizzata dai criminali Cyber e utilizza la mail come principale veicolo di diffusione, anche se si va estendendo velocemente ad altri canali, come i più popolari canali di messaggistica e i canali social. È particolarmente subdola perché basata su un inganno, con cui si cerca di indurre la potenziale vittima a compiere un'azione che consente al criminale di sferrare il suo attacco. Questo modulo formativo fornisce gli elementi cognitivi per riconoscere un attacco PHISHING e per adottare le necessarie contromisure.

PASSWORD

Uno dei pilastri della Cyber Security è rappresentato dalla PASSWORD la chiave di accesso a tutte quelle risorse informatiche a cui si deve garantire un accesso sicuro e riservato. La gestione delle proprie PASSWORD diventa quindi un elemento basilare delle strategie difensive, della persona e dell'organizzazione. Questo modulo formativo fornisce gli elementi cognitivi necessari ad una gestione sicura delle PASSWORD, mettendole al riparo da tentativi di violazione che potrebbero avere conseguenze disastrose.

SOCIAL MEDIA

I SOCIAL MEDIA rappresentano una nuova modalità di socializzazione basata sulle ampie possibilità che la tecnologia digitale mette oggi a disposizione. Sono anche fattori di rischio, dove si può arrivare a compromettere sia la privacy delle persone sia la sicurezza dei sistemi delle organizzazioni. Questo modulo fornisce gli elementi cognitivi per utilizzare in modo consapevole questi strumenti, proteggendo la persona e l'organizzazione dai rischi che la condivisione in rete di contenuti individuali e professionali può generare.

PRIVACY & GDPR

L'introduzione del nuovo regolamento europeo sulla protezione dei dati aumenta la sensibilità delle organizzazioni rispetto alla PRIVACY e alla protezione dei dati sensibili. Al di là dei ruoli specifici individuati proprio dal GDPR è importante che tutti i membri di un'organizzazione acquisiscano maggiore sensibilità rispetto alla protezione dei dati. Questo modulo fornisce gli elementi cognitivi per assumere un atteggiamento proattivo rispetto alla protezione dei dati, e per contribuire alla conformità dell'organizzazione rispetto alle nuove norme europee.

MOBILE DEVICE & APP

I DEVICE MOBILI, soprattutto Smartphone e Tablet, sono strumenti che diventano ogni giorno più critici e che rappresentano la massima espressione della rischiosa sovrapposizione tra dimensione personale e professionale. Questo modulo fornisce gli elementi cognitivi per utilizzare i dispositivi mobili, siano essi personali o professionali, in modo consapevole, abilitando buone pratiche che siano in grado di aumentare il livello di sicurezza e di protezione dei dati.

FAKE NEWS

Le FAKE NEWS, in italiano False Notizie, sono articoli redatti con informazioni inventate o semplicemente distorte, che hanno lo scopo di disinformare. Sono un fenomeno pericoloso, che se non controllato può avere ripercussioni negative sia per l'individuo sia per le organizzazioni. L'argomento viene spesso trattato dal punto di vista sociale e politico, ma ha anche una implicazione diretta con la Cyber Security. Questo modulo formativo fornisce gli elementi cognitivi necessari a riconoscere una Fake News, attivando alcuni processi di indagine che aiutano a sviluppare un atteggiamento corretto su qualsiasi informazione acquisita in rete.

MEMORIE USB

Le MEMORIE USB, e comunque tutte le memorie esterne, possono diventare un punto critico rispetto alla necessità di proteggere le informazioni riservate, ed è per questa ragione che sono spesso oggetto di specifiche policy. Questo modulo formativo fornisce gli elementi cognitivi per riconosce tutti i rischi associati alle memorie esterne, abilitando buone pratiche per evitare di incorrere in fenomeni di sottrazione di dati.

EMAIL SECURITY

La MAIL è uno strumento sempre più importante, che nella vita professionale assume un ruolo centrale e particolarmente critico. Attraverso le MAIL vengono scambiate informazioni sensibili e quindi l'aspetto della sicurezza non può essere sottovalutato. Questo modulo formativo fornisce gli elementi cognitivi per le mail e le informazioni in esse contenute.

MALWARE & RANSOMWARE

I MALWARE in generale e il RANSOMWARE in particolare hanno conquistato velocemente gli allori della cronaca, mettendo in evidenza tutta la loro pericolosità. Le persone devono comprendere che i software anti-virus non garantiscono la protezione totale rispetto a questi programmi maligni. Questo modulo formativo fornisce gli elementi cognitivi per ridurre il rischio di cadere vittima di questa particolare tipologia di software e per limitare le conseguenze negative in caso di violazione.

WEB BROWSING

La NAVIGAZIONE nel WEB presenta molti rischi e in quella che ormai sembra quasi un'attività scontata si presentano molti aspetti critici. Una buona conoscenza di alcune caratteristiche peculiari dei siti Web e dei browser può aiutare a ridurre notevolmente il livello di rischio. Questo modulo formativo fornisce gli elementi cognitivi su come navigare nel WEB in sicurezza.

CRITICAL SCENARIOS

Nell'interazione con il Cyber Spazio, esistono alcuni scenari critici: l'uso delle piattaforme Cloud, il viaggio di piacere o di affari, piuttosto che l'uso delle piattaforme di e-commerce, sia in ambito B2B che B2C. Sono scenari che risultano particolarmente esposti alla possibilità di subire attacchi da parte dei criminali Cyber, con rischi sia sul piano individuale che sul piano professionale. Questo modulo vuole fornire elementi essenziali di consapevolezza che aiutano a comprendere le minacce, spesso sottovalutate, che sono collegate a questi particolari scenari di utilizzo delle tecnologie digitali.

SOCIAL ENGINEERING

Il social engineering, o ingegneria sociale, è la madre di tutte le strategie di attacco Cyber. È una strategia che punta sull'inganno e sulla manipolazione psicologica per perseguire finalità truffaldine. Il nucleo di questa strategia è costituito dall'acquisizione di informazioni sulla vittima designata, per rendere più efficace l'attacco. Questo modulo fornisce elementi di consapevolezza sulle tecniche utilizzate dai Cyber Criminali, diventando di fatto la sintesi ideale di elementi già trattati nei moduli precedenti.