Gamification e cyber security

Introduzione

Oggi i dipendenti delle aziende sono diventati sempre più l'anello debole nella difesa contro gli attacchi informatici. La regola base del *buon senso* non può essere l'unico elemento di difesa contro tecniche di attacchi sempre più sofisticate. Inoltre gli attacchi provengono spesso da vere e proprie organizzazioni strutturate, di natura criminale o di natura governativa ostile, in grado di fare leva su grandi risorse economiche e tecnologiche. È per questo motivo che le aziende nell'ultimo decennio hanno iniziato, anche se non come ci si augurerebbe, ad investire risorse per assicurarsi che le *best practice* sulla sicurezza non vadano disattese e che nei loro dipendenti si crei una cultura più attenta alla sicurezza in generale. La sicurezza riguarda non solo la protezione delle informazioni aziendali, ma anche tutto ciò che, attraverso l'utilizzo delle tecnologie ICT, può essere esposto a rischi, ad esempio, la reputazione aziendale legata alla comunicazione tramite i canali dei social network.

Infatti, che si tratti di semplici errori innocenti o perché alcuni dei dipendenti possano essere presi di mira da parte di *social engineerer* perché sono la porta di accesso a informazioni sensibili, l'errore dei dipendenti facilmente facilita l'ingresso a *malware*, a tecniche di ingegneria sociale, al furto di informazioni. La cyber security quindi deve assolutamente diventare un processo e non una soluzione tecnologica.

Da quanto si sta osservando, emerge che un tema chiave per tutte le organizzazioni sta diventando quello di creare o rendere più efficace il processo di cyber security: come creare un meccanismo autonomo e continuo di *self-reinforcement* di team e dipendenti? Come assicurare nel tempo una costante

attenzione ai comportamenti e un aumento della consapevolezza sul tema sicurezza e sulla sua importanza?

Una risposta a questa esigenza la si può trovare – e sempre più la si sta trovando – nell'applicazione di tecniche di *gamification* al campo della sicurezza.

Elementi di gamification

La *gamification* è l'utilizzo di elementi, metodi derivati dai giochi e di tecniche di game design in contesti estranei ai giochi stessi.

Il termine *gamification* è un concetto giovane [1], cerca di rendere le numerose azioni spesso ritenute noiose (pagamento di tasse, file nei vari uffici) della vita quotidiana più accattivanti attraverso il gioco che per sua natura è un'azione volontaria fatta per avere piacere. La *gamification* cerca così di coinvolgere le persone a provare più passione e divertimento nelle attività di routine quotidiane attraverso gli stessi elementi del gioco.

Gli obiettivi della *gamification* cercano di modificare le abitudini degli utenti principalmente attraverso meccanismo di:

- Fedeltà;
- Reclutamento;
- risoluzione di problemi.

Il principio che si pone alla base della *gamification* è quello di utilizzare le dinamiche e meccaniche del gioco:

- punti;
- livelli;
- ricompense.

per stimolare una serie di istinti primari dell'essere umano come la competizione, lo status sociale, i compensi, il successo, l'affermazione all'interno di un gruppo. Ed è questo

principalmente il punto di forza della *gamification*.

Un prodotto “gamificato” fornisce obiettivi da raggiungere, livelli in cui progredire, competere con gli altri utenti, condividere i propri successi e guadagnare ricompense.

Oggi molti sono i siti web che cercano di creare community attraverso la *gamification*, quello mostrato in Figura 1 è un esempio molto valido di come il sito web del Sigaro Toscano® [2] utilizza i principi della *gamification*, facendo progredire l’utente all’interno del suo sito web alla ricerca di nuovi gusti, curiosità, abbinamenti e concedendo all’utente punti da accumulare per il migliorare il suo “status” all’interno della community stessa: si passa dal livello 1 “Gringo” al livello 2 “Trovatore” e così via, in un crescendo di gioco e soddisfazione finale dell’uso del sito web e del prodotto stesso. In Figura 2 invece stessa logica di *gamification* sui livelli e sulla possibilità di migliorare nello status della community sul forum di una comunità della penna stilografica [3] fountainpen.it ®.

Figura 1 – Gamification dei livelli sito web Sigaro Toscano®

Figura 2 – Gamification dei livelli nella community fountainpen.it ®

Gamification e cyber security

Attacchi di successo spesso coinvolgono processi aziendali poveri, mal strutturati e sfruttano le debolezze umane a cui quei processi fanno riferimento. Per ridurre il più possibile le possibilità di subire un attacco informatico la formazione dei dipendenti regolare, continua e continuativa deve passare da una sua visione di reazione a quella di prevenzione. Tecniche “didattiche” solamente didascaliche

orientate alla lezione frontale dei dipendenti si sono rivelate spesso inefficaci perché non sono abbastanza interessanti perché non riescono a catturare l'immaginazione dei dipendenti/discenti. Un modello di insegnamento laboratoriale orientato al *problem solving* si allontana dal semplice trasferimento di informazioni. L'incontro con modalità frontale è adatta a pochi, quelli che probabilmente si applicherebbero comunque, a prescindere dal corso, e anche senza il formatore. Le aziende quindi dovrebbero concentrare i loro sforzi e le loro risorse sull'educazione dei propri dipendenti sul come proteggere i propri dati personali, incoraggiando così i dipendenti a implementare ulteriori pratiche orientate alla sicurezza sul posto di lavoro, insegnamento laboratoriale e *problem solving* appunto.

La formazione dei dipendenti può assumere diverse forme, inclusa la crescente pratica di programmi educativi di "*cyber security*" "*gamifying*". La *gamification*, come già detto, è il processo di utilizzo della meccanica di gioco in un contesto non di gioco, sfruttando ciò che è più eccitante e applicandolo ad altri tipi di attività che potrebbero non essere così divertenti. Questi percorsi sono progettati con elementi di competizione e ricompensa.

Esistono due modi principali in cui i titolari di aziende possono utilizzare la *gamification* come strumento per affrontare la cyber security nella propria organizzazione: interessare i propri dipendenti nelle attività e incentivare i corretti comportanti con premi.

Rendere la formazione più eccitante e coinvolgente per i dipendenti

L'utilizzo della *gamification* può aiutare le aziende a migliorare la propria sicurezza informatica in molti modi, mostrando ai dipendenti come evitare gli attacchi informatici e l'apprendimento delle vulnerabilità nel software.

Negli USA una società di consulenza PwC insegna la sicurezza informatica attraverso il suo gioco di minacce [4]. I dirigenti competono l'uno contro l'altro nelle situazioni di sicurezza informatica del mondo reale, giocando come attaccanti o difensori. Gli attaccanti scelgono tattiche, metodi e abilità di attacco, mentre i difensori sviluppano strategie (di difesa) e investono nelle tecnologie e nel modo giusto per rispondere all'attacco. Il gioco offre ai dirigenti uno studio di come prepararsi e reagire alle minacce, di come deve essere ben preparata l'azienda e di ciò che deve possedere il team di cyber security per affrontare quotidianamente questo tipo di minacce.

In questo modo la *gamification* contribuirà a rendere il processo di formazione più interessante e coinvolgente per tutti i dipendenti, aumentando la consapevolezza dei dipendenti sulle pratiche di cyber security, incluso il modo corretto di affrontare gli attacchi.

Offrire incentivi e premi per incoraggiare i comportamenti desiderati

L'errore umano è responsabile nella maggior parte delle violazioni della sicurezza, con i dipendenti che si sentono pressati a completare il lavoro entro determinate scadenze e il più rapidamente possibile, il che può tradursi in una politica aziendale importante in materia di sicurezza.

Ad esempio, molte società propongono, attraverso simulazioni sul *phishing*, una formazione attiva per i propri dipendenti per una migliore gestione della sicurezza della posta elettronica. Questi test includono l'invio di e-mail di *phishing* per testare la risposta dei dipendenti e l'azione dello staff di cyber security.

La *gamification* consente alle aziende di premiare i dipendenti che seguono le procedure di sicurezza, che aderiscono alle corrette linee guida sulla sicurezza e che elevano un buon

comportamento aziendale. Questa fase di gratificazione può essere svolta in vari modi: dipendenti che ricevono un premio produzione, punti per avanzare di livello all'interno dell'azienda, oppure nel raggiungere traguardi specifici si possono ottenere ricompense materiali, come un buono regalo per sé e per la propria famiglia.

Questo sistema, inoltre, consente anche l'identificazione di coloro che mostrano un comportamento scorretto all'interno della *gamification* e può comportare la necessità per il dipendente di completare un'ulteriore fase di studio sulla sicurezza informatica. Riconoscere, gratificare, premiare i dipendenti quando fanno la cosa giusta porta a un comportamento positivo continuo, motivando i dipendenti a intraprendere pratiche sicure e creando un ambiente di lavoro più sicuro per il cyber criminale.

Al centro di qualsiasi attività di formazione dovrebbe trovarsi la consapevolezza della sicurezza, educazione i propri dipendenti ad un senso **condiviso** di responsabilità per i dati con cui lavorano e i dati che creano e utilizzano anche da casa. Tutto il processo di educazione e di sensibilizzazione alla sicurezza dovrebbe far parte di un processo a più ampio respiro, non una singola iniziativa in cui i dipendenti sono costretti a partecipare. Per creare questa cultura di sicurezza ed innestarla nei processi aziendali occorre una profonda radicalizzazione dell'educazione alla cultura della sicurezza. Di seguito alcuni degli elementi didattici e possibili soluzioni implementative, che possono veicolare atteggiamenti *proattivi* alla sicurezza.

- **L'abecedario base: A-B-C-D (Ammaestra, Breve, Conciso e Divertente).** La cultura dei social network pervade oramai tutti. Le email lunghe sono sempre ignorate. Articoli o scritti pieni zeppi di testo senza immagini tendono a stancare prima. Tenere corte e divertenti le proprie lezioni, e assicurarsi SEMPRE che

ci sia un approccio top-down. Infatti i dipendenti guardano ai loro leader. Se il leader non incarna una cultura cyber-sicura, perché dovrebbero farlo loro? L'obiettivo è educare i dipendenti alle *best practice*, non costringerli a essere esperti di sicurezza informatica. Divertente così tutti possono imparare e allo stesso tempo divertirsi e ridere.

- **Le tattiche intimidatorie non funzionano.** L'obiettivo aziendale dovrebbe essere quello di costruire una cultura della *cyber security awareness*, una consapevolezza sulla sicurezza cibernetica. Bisogna iniziare a pensare ad una strategia di marketing *gamification* con l'intento di persuadere e modificare il comportamento di un dipendente (migliorare i propri livelli, avere uno status migliore del collega…).
- **I video attirano maggiore attenzione.** Iniziare con alcuni piccoli video, piccoli concorsi simpatici sulla sicurezza per far capire a tutti che la sicurezza è una responsabilità condivisa.
- **Rinforzo e follow-up sono fondamentali.** L'allenamento è una costante; imparare da ciò che funziona ed eventualmente ricominciare dall'inizio. Riesaminare subito i dipendenti che si trovano di fronte ad un'email di *phishing* e controllare quanti di loro non riescono ancora a riconoscere un'email falsa. Incoraggiare l'aspetto comunicativo per segnalare un falso e richiamare i dipartimenti che potrebbero essere in ritardo nella loro preparazione. L'obiettivo non è quello di separare le persone, ma piuttosto creare una sana rivalità all'interno dell'unità organizzativa.

Gamification delle buone pratiche: uno scenario possibile

Come esemplificazione e puro esercizio intellettuale – la

gamification va progettata e costruita ad hoc per il contesto reale di applicazione e non vive di ricette predefinite – proviamo ad introdurre qui un esempio ipotetico di esperienza gamificata per un dipendente generico che chiameremo Luca.

Luca, dipendente di un'azienda che si occupa di import/export, arriva in ufficio e accede alla intranet aziendale. La password è scaduta così il sistema gli chiede di aggiornarla. Luca riempie la password avendo un feedback visivo che indica che la password che ha scelto è complessa e quindi molto sicura. Per questo motivo, Luca, riceve 50 punti sicurezza che vanno a sommarsi a quelli che il suo profilo ha già: gli mancano 100 punti sicurezza per passare dal livello 4 al livello 5. Il sistema, per aiutare Luca a memorizzare la password gli propone un mini gioco che consiste nell'inserire la password ripetute volte a sempre maggiore velocità. Luca completa il gioco arrivando a scrivere la password in meno di 3 secondi. Questa impresa gli vale altri 50 punti sicurezza. Luca così ha già scalato la classifica del suo ufficio, portandosi alla seconda posizione della classifica dei punti sicurezza del suo team. Il suo collega Paolo, che ha ricevuto la notifica dalla Intranet del nuovo punteggio di sicurezza di Luca, gli manda un messaggio per ricordargli che in cima alla classifica c'è ancora lui. Luca torna al suo lavoro e apre la posta. Leggendola scopre di aver ricevuto un'email e ne riconosce un possibile phishing. Al posto di cestinarla, Luca usa il pulsante di segnalazione di phishing: questo gli vale altri 100 punti e il raggiungimento del livello 5. Il sistema lo celebra con una piccola animazione e lo informa che potrà convertire i suoi punti sicurezza in un biglietto per un film al cinema convenzionato con la sua azienda o in una ricarica gratuita della chiavetta per la macchina del caffè. Il suo collega Paolo lo ricontatta e gli promette che si riprenderà la vetta della classifica al più presto: la sfida non è finita.

In questo piccolo esempio possiamo individuare che con un

sistema tipico dei giochi (punti e classifiche) abbiamo:

- premiato il comportamento virtuoso di creazione di una password sicura;
- ridotto che il rischio che una password complessa sia scritta su carta motivando il dipendente a memorizzarla (scrivendola più volte sotto la spinta di un gioco a tempo);
- segnalato un pericolo di *phishing* al reparto tecnico che altrimenti non avrebbe ricevuto la segnalazione;
- premiato il comportamento virtuoso di segnalazione di una minaccia secondo le policy dell'azienda;
- incentivato nei colleghi la volontà di applicare il comportamento virtuoso per rispondere a quello degli altri.

L'esempio è ovviamente molto generico e non esaustivo di tutte le possibilità che la *gamification* implica. Un esercizio – o forse meglio un gioco – che il lettore potrebbe fare è quello di espandere quanto proposto adattandolo alle policy di sicurezza presenti nella propria realtà aziendale per contestualizzare vantaggi e possibilità offerte da questi approcci.

Conclusione

Riguardo all'introduzione di metodologie di questo tipo in azienda, non va sottovalutata la complessità in termini organizzativi e di *know-how* specifico necessari. La volontà di introdurre la *gamification* va sostenuta da un chiaro *commitment* dirigenziale per garantirne il successo. Un supporto, in questi casi, può venire da consulenti specializzati sulla gamificazione dei processi e l'offerta crescente di programmi di formazione di cyber security proposte dalle aziende specializzate in cyber security [5]. In Figura 3 un esempio di piattaforma strutturata per creare competenze in cyber security nei dipendenti aziendali attraverso la *gamification*.

Figura 3 – Esempio di piattaforma di formazione dei dipendenti per la creazione di competenze di sicurezza informatica tramite gamification (fonte www.kaskersky.it).

L’eliminazione dei rischi informatici in qualsiasi azienda è un processo che deve avvenire passo dopo passo e, soprattutto, può essere gestito. Spostare la rotta dell’azienda verso una cultura di sicurezza attraverso il gioco e la *gamification* permetterà di continuare a essere sicuri nel tempo perché la consapevolezza di essere parte della sicurezza stessa permane nelle coscienze dei dipendenti molto più profondamente rispetto al *gaming* e al sorriso con cui è stata realizzata.

Sitografia (ultimo accesso 28 marzo 2018)

A cura di: **Michelangelo De Bonis**, **Matteo De Simone**

https://www.ictsecuritymagazine.com/articoli/gamification-e-cyber-security/