Security Awareness

Un efficace programma di Awareness sulla Sicurezza come strumento per l'incremento della sicurezza aziendale ed elemento abilitante per il successo di nuovi servizi on line

Garibaldi Conte

Information & Cyber Security Advisor

Membro del Comitato Tecnico – Scientifico del Clusit

gconte@clusit.it

Roma 7 giugno 2018

PREMESSA E OBIETTIVO

- Le statistiche mettono in evidenza che circa il **90%dei programmi malware** si installa a causa di **errori umani** effettuato da utenti fondamentalmente inconsapevoli. Questo dato conferma che le persone sono l'anello più debole per la sicurezza dei sistemi e delle reti
- Di conseguenza, si può affermare che le **persone sono il fattore chiave** per realizzare un **efficace sistema di sicurezza in azienda** aumentando la loro **Consapevolezza** (Awareness in inglese) sui potenziali pericoli, rischi e minacce che afferiscono ai sistemi e alle informazioni che utilizzano durante le loro attività lavorative.
- L'intervento illustra come un **efficace Programma di Awareness sulla Sicurezza** può aumentare la consapevolezza delle persone sulla Sicurezza delle Informazioni creando un **circolo virtuoso** il quale, partendo da attività di Formazione, che forniscono le necessarie informazioni sulla sicurezza, permette alle persone di comprenderle e rifletterle nelle quotidiane attività lavorative.
- La consapevolezza della sicurezza è fondamentale anche per il **successo dei nuovi servizi on line**, siano essi pubblici o privati. Un **uso sicuro e consapevole** di tali di tali servizi da parte dei loro fruitori ne determina automaticamente il successo. Viceversa, un servizio percepito dagli utenti come non sicuro e pericoloso, genera un **clima di insicurezza e diffidenza** nei suoi utilizzatori portando gli stessi ad abbandonare il servizio decretandone così il fallimento.

SECURITY AWARENESS : DEFINIZIONE

Con il termine Security Awareness si intende l'insieme delle azioni mirate a far crescere la consapevolezza dell'utente in merito a tutti gli aspetti di sicurezza (al fine di assicurare i requisiti di riservatezza, integrità e disponibilità dei dati) connessi al trattamento delle informazioni aziendali siano esse in formato elettronico che cartaceo.

- I concetti chiave che ruotano intorno al termine «Security Awareness» sono :
  - Consapevolezza
  - Persone
  - Sicurezza

Awareness is not training. The purpose of awareness presentations is simply to focus attention on security and understand why security is important. Awareness presentation are intended to allow individuals to recognize IT security concerns and respond accordingly. (NIST Special Publication 800-16)

SECURITY AWARENESS : GLI ERRORI PIU' COMUNI

- Tra gli errori più comuni che si commettono negli attuali Programmi di Security Awareness si evidenziano:
  - Le attività di formazione sono frammentarie, non coordinate e non si sostengono a vicenda
  - Le attività di formazione sono guidate più dalla necessità di conformarsi ad adempimenti normativi, nazionali e non, piuttosto che a rafforzare il livello di sicurezza dell'azienda
  - Le attività di formazione sono rivolte solo a specifiche categorie di persone, soprattutto in ambito IT e sicurezza IT, e non coprono tutta l'azienda
  - Le attività di formazione sono le stesse per tutti i segmenti di lavoratori e sono le stesse anno dopo anno
  - Non è stato stanziato un budget specifico per la formazione in ambito sicurezza
  - Formazione tradizionale con sessioni in aula e/o di e-learning
  - La Formazione è basata sull'illustrazione delle regole di sicurezza presenti in azienda senza evidenziare i pericoli, i rischi e le minacce che le regole cercano di contrastare

La Security Awareness è a tutti gli effetti una misura di sicurezza e come tale va correttamente implementata e mantenuta

LO SVLUPPO DI UN PROGRAMMA DI SECURITY AWARENESS

- Un Programma di Security Awareness può essere sviluppato in 5 fasi:
  - Analisi del contesto (detto anche Security Assessment)
  - Progettazione del Programma
  - Esecuzione del Programma
  - Misurazione dei risultati
  - Miglioramento del Programma

ANALISI DEL CONTESTO

- Il principale obiettivo dell'analisi di contesto è quello di analizzare il contesto aziendale nel quale verrà erogato il Programma di Awareness al fine di:
  - Identificare le principali caratteristiche dell'audience
  - Il loro livello di «conoscenza» e «consapevolezza» rispetto alle tematiche di security
  - Lo stato, in termini di completezza, dell'impianto documentale in ambito ICT Security

ANALISI DEL CONTESTO – CARATTERISTICHE DELL'AUDIENCE

- L'identificazione delle caratteristiche dell'audience ha la principale finalità di aumentare l'efficacia del programma attraverso la definizione di modalità di erogazione del programma «personalizzate» per le persone/gruppi cui il programma è diretto.
- Tali informazioni, generalmente reperibili presso la funzione HR della società, possono essere, a titolo esemplificativo, le seguenti:
  - Età (per fasce di età)
  - Grado di scolarità (diploma, laura breve, laurea magistrale,…)
  - Inquadramento inquadramentale (impiegato, quadro, dirigente,…)
  - Inquadramento organizzativo (Funzione Aziendale di appartenenza) e responsabilità in azienda
  - Turnover (neoassunti, veterani, persone che hanno cambiato lavoro,…)

- Dipendenti
- Impiegati di front-office
- IT Staff
- Security Staff
- Amministratori di Sistema
- Personale Esterno
- Management
- Executive Management
- ….

I Gruppi Target per il Programma di Awareness possono essere definiti utilizzando criteri di omogeneità delle mansioni, uniformità delle competenze, stesse forme di comunicazione, le «necessità» rispetto alla tematica di Sicurezza Informatica.

ANALISI DEL CONTESTO – ASSESSMENT LIVELLO DI SICUREZZA

- Altro step importante dell'analisi del contesto è la valutazione del livello di «conoscenza» e «consapevolezza» rispetto alle tematiche di security dell'audience del programma
- Esistono due metodi largamente utilizzati che possono essere usati separatamente oppure in contemporanea:
  - Un questionario on line da sottoporre a tutta l'audience de programma o a un campione di essa, purché questo sia significativo sia dal punto di vista dimensionale che come rappresentatività dei gruppi identificati
  - Simulazione di Social Engeneering sia attraverso Phishing inviato a tutti i componenti dell'audience del programma che Spear Phishing inviato a specifici utenti/gruppi target.

Gli utenti sono invitati a compilare un **questionario on line** composto da un numero limitato di domande (circa 25-30 domande) che hanno la principale finalità di valutare la **vita digitale** degli utenti e il **livello di responsabilità** verso la **sicurezza delle informazioni**

A titolo esemplificativo, ma non esaustivo:

- **Phishing**: Invio massivo a tutti gli utenti attestati sul dominio della Società di una **mail di phishing «standard»** che li invita a cliccare su un link. La mail contiene diversi indizi che consentirebbero agli utenti di intercettarla come fake mail.
- **Spear Phishing**: Invio a tutti dipendenti di una **mail da un'utente interno** all'azienda che li invita a cliccare su diversi link che rimandano ad un sito civetta attestato sul dominio della società. Una volta arrivati sul sito civetta si richiede di inserire la propria utenza e password di dominio. La mail contiene un oggetto plausibile (es. Trasparenza Privacy, Piano Ferie,..) proveniente da un indirizzo plausibile (es. azienda.info invece che azienda.it), ma vengono lasciati dentro la mail dei segni che è un possibile phishing.

ANALISI DEL CONTESTO – IMPIANTO DOCUMENTALE DI SICUREZZA

- Altro aspetto fondamentale per la riuscita di un Programma di Security Awareness è l'esistenza in azienda di un impianto documentale in ambito sicurezza completo, esaustivo e non ambiguo.
- In particolare, devono essere state definite le cosiddette norme comporta-mentali (es. utilizzo dei dispositivi mobili, l'utilizzo di Internet in azienda, l'uso della posta elettronica aziendale, le password policy, l'utilizzo dei social,…) che rappresentano l'oggetto principale sulle quali deve essere raggiunta la massima conoscenza e consapevolezza

LA PROGETTAZIONE DI UN PROGRAMMA DI SECURITY AWARENESS: LE FASI

- La Progettazione di un Programma di Security Awareness può essere strutturata nelle seguenti fasi:
  - La **sponsorizzazione del Top Management** per avere un adeguato supporto al Programma
  - **Definizione del Team di Progetto** che deve comprendere le figure considerate essenziali per il successo del Programma (es. in ambito formazione, comunicazione, IT, Risk Management,..) integrato da consulenti esterni esperti della tematica
  - **Definizione degli obiettivi** sulla base dei risultati dell'analisi del contesto, ed in particolare dell'assessment sul livello di sicurezza, per poter identificare il punto di partenza e di arrivo del programma.
  - **Identificazione dei gruppi target** sulla base delle informazioni raccolte durante l'analisi di contesto e comprensione delle necessità educative per ogni gruppo target per colmare le carenze identificate durane l'assessment.
  - **Definizione degli indicatori di prestazioni (KPI),** con relativi obiettivi (KPO), per misurare i risultati raggiunti sia in termini di apprendimento che di livello di consapevolezza.
  - **Definizione Budget e Costi del Programma**

LA PROGETTAZIONE DI UN PROGRAMMA DI SECURITY AWARENESS: IL SUPPORTO DEL TOP MANAGEMENT

- Il supporto del TOP Management è una componente essenziale per il successo del Programma di Awareness ed è quindi essenziale convincere il Top Management dei benefici che un Programma di Awareness sulla Sicurezza induce e perché la sicurezza deve essere considerata una priorità dell'azienda.
- Un buon strumento per ottenere la sponsorizzazione del Top Management potrebbe essere la preparazione di un Business Case sul Programma di Awareness con la valutazione del **ROSI** (Return Of Security Investment) associato al programma.
- Per poter calcolare il ROSI è necessario disporre di dati storici sulle violazioni/incidenti di sicurezza e stimare di quanto il programma di awareness potrebbe ridurne i numero agendo sul comportamento dei dipendenti.
- Il ROSI è basato sulla valutazione dell'Esposizione al Rischio la quale, in base alle modalità di calcolo utilizzate, può variare notevolmente. Per ottenere dei valori consistenti, la metodologia di calcolo dovrebbe bilanciare misurazioni quantitative dei fattori di costo direttamente associabili agli incidenti di sicurezza (costi di sostituzione, costi di configurazione, costi di ripristino,..) con misurazioni qualitative e conservative dei costi indiretti associati agli incidenti d sicurezza (perdita di produttività, di perdita di proprietà intellettuale di perdita di dati dei clienti,….).

ESECUZIONE DEL PROGRAMMA DI AWARENESS : I MATERIALI

- Un Programma di Awareness efficace dovrà utilizzare una vasta gamma di materiali partendo da quelli disponibili in Azienda e integrandoli con materiali di pubblico dominio disponibili su Internet e materiali pubblicati da Enti Governativi nazionali e non. Tra questi si evidenziano:
  - Policy e Standard di Sicurezza
  - Normative e Best Practice di settore
  - Linee guida e Procedure di Sicurezza
  - Statistiche e news di incidenti di sicurezza, sia interni che esterne (es. notizie di stampa)
  - Informazioni sui rischi di sicurezza sia esistenti che emergenti
  - Informazioni sui Controlli di Sicurezza necessari per mitigare i rischi di sicurezza
  - Casi di Studio reali e/o realistici

ESECUZIONE DEL PROGRAMMA DI AWARENESS : I METODI

- Le forme di comunicazione che saranno scelte per i messaggi di sicurezza dovranno essere innovative e creative per poter aumentare la probabilità di recepimento del messaggio da parte di chi ascolta.
- Bisogna pertanto combinare mezzi di comunicazione tradizionali (formazione in aula, newletter, poster,..) a metodi più moderni (e-learning, new via mail, pop-up sui terminali,…) e innovativi (seminari interattivi di sicurezza, simulazioni di incidenti, giochi a premi, …). Tra i principali metodi si evidenziano:
  - **Sito interno dedicato alla Sicurezza** che costituisce il punto di riferimento per tutto il programma. Il sito sarà costantemente aggiornato con tutte le informazioni sul programma e costituirà la principale fonte dove acquisire tutto il materiale disponibile sulla sicurezza (policy, procedure, linee guida, …)
  - **Materiale di awareness** composto da newsletters, opuscoli, brochure, avvisi di sicurezza, etc, che potrà essere spedito via mail o stampato
  - **Formazione in aula** che costituisce il metodo migliore per la trasmissione della conoscenza
  - **Eventi di sicurezza** che hanno lo scopo di far avvicinare le persone agli argomenti delle sicurezza con modalità ricreative e divertenti per far arrivare il messaggio in maniera più diretta
  - **Gadget promozionali** (tappetini per mouse, penne, segnalibri, tazze,…) per supportare il ricordo dell'attività d Security Awareness effettuata. Sui gadget può essere riportato un breve messaggio di sicurezza

ESECUZIONE DEL PROGRAMMA DI AWARENESS : LA COMUNICAZIONE

- Identificazione di un Logo ed un Motto che colleghi insieme tutte le diverse iniziative del Programma di Awareness. Queste tecnica, molto utilizzata nel marketing, rafforza l'obiettivo del programma e permette di creare una cultura della sicurezza in grado di raggiungere tutta l'audience del programma radicandosi velocemente nell'Azienda

- Per catturare l'attenzione dell'audience è necessario diversificare i mezzi di comunicazione in modo da raggiungere il maggior numero di persone e nel contempo cercare di «visualizzare» i concetti per renderli più facilmente «comprensibili» dai discenti. È stato dimostrato che utilizzare immagini/video divertenti e conditi con un po' di umorismo, permette di avere una maggiore attenzione da parte dei discenti e un maggior recepimento del messaggio inviato

IL MONITORAGGIO DEL PROGRAMMA : INDICATORI PER VALUTAZIONE DEI RISULTATI DEL PROGRAMMA

- La definizione di Indicatori di prestazioni di un Programma di Security Awareness ha due obiettivi primari:
  - Contribuire alla gestione del programma identificando **azioni di miglioramento** del Programma
  - **Valutare i miglioramenti** indotti dal Programma per «giustificare» gli investimenti effettuati
- I principali elementi da misurare sono:
  - **Diffusione del programma** : verifica del rispetto della pianificazione e del budget del Programma. Utilizzo di classiche tecniche di PM quali piani progetto, Stati Avanzamento Lavori periodici, executive report,…
  - **Diffusione del Messaggio** : oltre alla percentuale di partecipazione dell'audience per la quale si prevede la copertura completa, è importante comprendere il recepimento del programma nelle sue finalità e approcci attraverso l'utilizzo di commenti di feedback e sondaggi erogabili anche on line.
  - **Efficacia del Programma** : è il risultato più importante da raggiungere, ma è anche quello più difficile da misurare. Gli indicatori di efficacia sono relativi alla riduzione degli incidenti di sicurezza e, in genere, tutti i tipi di risparmio dovuti al miglioramento del comportamento degli utilizzatori. Le tecniche di misurazione sono varie e possono includere simulazioni di attacchi (es. phishing), l'utilizzo di questionari ad hoc, il numero di segnalazioni di sicurezza pervenute all'help desk,…..

SERVIZI ON LINE E SECURITY AWARENESS : LE PECULIARITA'

- Generalmente la **popolazione** cui è diretto un servizio on line è **molto vasta e «presunta»**, nel senso che può variare per età, livello culturale, maturità tecnologica e livello di consapevolezza della sicurezza. Per tale ragione, le tecniche di Awareness dovranno essere adattate a più segmenti di utilizzatori cercando di catturare quelli predominanti.
- Non è possibile utilizzare **tecniche di misurazioni** del livello di sicurezza **invasive** quali «simulazioni di attacchi di phishing», ma si dovranno rafforzare i presidi di monitoraggio delle segnalazioni che pervengono dagli utilizzatori (rafforzamento degli Help Desk e dei canali di comunicazione) al fine di intercettare/anticipare fenomeni che impattano sulla sicurezza e apportare le necessarie azioni correttive.
- I **servizi di alerting** sono uno degli strumenti di maggiore efficacia nell'ambito della Security Awareness dei servizi on line in quanto permettono all'utilizzatore di prendere coscienza di un eventuale pericolo e agire di conseguenza modificando il suo comportamento
- Le modalità di interazione tra il fornitore del servizio e i suoi utilizzatori deve tenere conto della **tecnologia utilizzata** e delle modalità con cui **l'utilizzatore la usa**.

Nelle tavole che seguono si riportano degli esempi di come si possono integrare tecniche di Security Awareness nei servizi on line per segmenti specifici di utilizzatori

SERVIZI ON LINE E SECURITY AWARENESS : GLI IMMIGRATI DIGITALI

- Gli Immigrati Digitali sono persone nate senza tecnologia e che si sono avvicinati ad essa soprattutto per necessità. Il loro approccio verso la tecnologia è alquanto esitante, se non proprio diffidente. Tendono ad assumere atteggiamenti standardizzati e a delegare ad altri, a volte anche in maniera impropria (es. dispositivi di firma digitale lasciati ai propri commercialisti)
- Tendenzialmente non usano molti servizi on line, se non quando sono obbligati, e la loro consapevolezza verso gli aspetti di privacy e di sicurezza informatica non è elevatissima.

- Gli Immigrati sono comunque mediamente più recettivi delle altre categorie di utilizzatori e quindi, un programma classico di awareness può sortire risultati buoni perché gli Immigrati Digitali tendono a standardizzare i propri comportamenti e quindi accettano di buon grado le cosiddette “Istruzioni per l’uso”.
- I servizi di alerting sono utilissimi perché rafforzano il loro senso di sicurezza e diventano una discriminante nella scelta del provider del servizio

SERVIZI ON LINE E SECURITY AWARENESS : I MILLENNIALS

- I Millennials (nati negli anni ‘80 e detti anche Nativi Digitali Spuri) sono generalmente studenti universitari o giovani lavoratori, navigano tantissimo in Internet, utilizzano la posta elettronica e usano sempre più il cellulare per inviare sms, foto e video. Per loro la tecnologia è un bisogno e, con l’avvento dei social, anche il luogo dove comunicare e organizzare la propria vita. Sono grandi utilizzatori di servizi on line.
- Essendo nati con il PC, hanno un approccio molto intuitivo verso la tecnologia e non percepiscono i pericoli presenti su Internet fintanto che non incappano in un qualche problema di sicurezza. Rispetto alla Privacy e alla Sicurezza informatica adottano un approccio molto semplificato poiché credono che la tecnologia li protegga in maniera adeguata.

- Un piano di awareness classico basato su una costante informativa sugli aspetti di sicurezza e privacy non è sufficiente per tale tipologia di utilizzatori perché rischierebbe di essere sottovalutato, se non ignorato. Risulta più efficace l’attivazione di servizi di notifica ed alerting che consentono di mantenere sempre alta la loro attenzione.
- A titolo esemplificativo, come avviene oggi per i grandi player presenti in Intenet (Google, Facebook, …), l’invio di una comunicazione che qualcuno è acceduto al proprio account da un altro apparato, è un messaggio che i Millennials comprendono perfettamente e che li mette in grado di attivare le opportune contromisure. Analogamente, è molto utile “costringere” i Nativi Digitali Spuri a confermare periodicamente le impostazioni della privacy e di sicurezza attive sui servizi utilizzati.

SERVIZI ON LINE E SECURITY AWARENESS : I NATIVI DIGITALI

- Con il termine Nativi Digitali si identificano prevalentemente i bambini e gli adolescenti che sono nati dopo il 2000 e vissuti con i nuovi apparati digitali. Hanno un'esperienza diretta con la tecnologia e con Internet sempre più precoce (videogiochi, Smartphone, tablet, MP3,…). e sono perennemente connessi in Internet.
- Utilizzano prevalentemente tecnologia "chiusa" e proprietaria, e sono abituati ad interagire con i servizi che la rete gli offre utilizzando icone separate per ognuno di essi (le famose APP). i Nativi Digitali hanno un bassissimo livello di consapevolezza sia degli aspetti legati alla privacy che alla scurezza informatica
- Non mandano più mail né fanno telefonate; comunicano prevalentemente attraverso messaggi inviati con Facebook e Whatsapp nella logica del "sempre connesso". Hanno verso la tecnologia un atteggiamento compulsivo con una bassissima conoscenza sia della rete che dei pericoli in essa presenti.
- I Nativi Digitali hanno un bassissimo livello di consapevolezza sia degli aspetti legati alla privacy che alla sicurezza informatica

- Gli spunti interessati che si possono trarre per integrare iniziative di security awareness nei servizi diretti ai Nativi Digitali sono i seguenti:
  - I servizi on line dovranno evolvere necessariamente verso logiche di fruizione ad icona stile APP. In questa configurazione, gli aspetti di sicurezza e di privacy dovranno essere cablati nelle APP e dovranno garantire il necessario livello di sicurezza in maniera automatica (ad esempio utilizzando delle configurazioni standard non modificabili);
  - Come per i Millennials, anche in questo caso il mezzo migliore per mantenere alta l'attenzione degli utilizzatori sulla sicurezza è l'attivazione di servizi di notifica e alerting (preferibilmente attraverso pop-up e servizi quale WhatsUp), così come la periodica conferma delle impostazioni di privacy e di sicurezza.

SECURITY AWARENESS E LE NORMATIVE

- Come detto all'inizio di questa presentazione, la Security Awareness è a tutti gli effetti una misura di sicurezza e come tale va correttamene implementata e mantenuta.
- Tale concetto era già stato metabolizzato degli Standard di riferimento nell'ambito della Sicurezza Informatica che hanno da tempo inserito tra le misure di mitigazione attività di Security Awareness. Ricordiamo tra i principali l'ISO 27001, il Cobit 5, il NIST, lo standard PCI/DSS, le Linee Guida ENISA e così via
- Egli ultimi tempi, anche le Autorità nazionali ed internazionale hanno compreso l'importanza della security awareness e la stanno inserendo come adempimento obbligatorio nelle principali normative che si stanno emettendo in questi tempi in mbiti nei quali la Sicurezza Informatica è rilevante. A titolo esemplificativo e non esaustivo, ricordiamo:
  - Le linee guida EBA sulla sicurezza dei pagamenti via Internet (ora parte integrante della Circolare 285/13 emessa da banca d'Italia)
  - Le linee guida EBA sulle misure di sicurezza in ambito PSD2
  - La legge sulla privacy italiana D.lgs 196/03
  - Il Nuovo Regolamento Europeo sulla Privacy (GDPR)
  - La Direttiva Europe sulla sicurezza delle reti (NIS)

GRAZIE PER L'ATTENZIONE

Garibaldi Conte
Information Security Consultant
Membro del Comitato Tecnico – Scientifico del Clusit
gconte@clusit.it