ARTICOLO DI ELEARNINGNEWS

Year 6 - number 197 Wednesday 6 april 2022

E-learning e cybersecurity: competenze da trasferire

Nella progettazione di un format per corsi in modalità eLearning, occorre tener conto di almeno tre competenze da somministrare agli utenti. Scopriamo quali sono

Una delle principali richieste da parte dei clienti, soprattutto grandi organizzazioni, è quella di identificare i principali **rischi connessi all'utilizzo dei device aziendali**.L'identificazione dei rischi è, sempre più spesso, connessa alla policy aziendale per la sicurezza ma, secondo la mia esperienza, è possibile strutturare un format basandosi su regole fondamentali che potrai poi adattare al caso specifico.

In questo articolo, tuttavia, non indagheremo tutte le possibili competenze da trasferire ai discenti di corsi in modalità eLearning sulla sicurezza informatica ma, in modo analitico e strutturato, definiremo l'impostazione di un format partendo da alcuni argomenti che, in passato, mi è capitato di affrontare con alcuni clienti.

Un ottimo e immediato corso online per la formazione alla cybersecurity dei dipendenti aziendali è sicuramente **Cyber Security - Tutela dei dati e delle informazioni aziendali - 1 ora**.

La protezione dei device

Converrai con me che ogni aspetto della sicurezza informatica meriterebbe un articolo dedicato. Tuttavia, come anticipato, la realizzazione di un format per corsi in modalità eLearning prevede, necessariamente, l'identificazione di un topic, ovvero di un argomento, di partenza.

Ho così selezionato uno dei topic più richiesti dalle aziende con cui ho lavorato: la protezione dei device.

Nella progettazione di un format per corsi in modalità eLearning dovrai così tener conto di almeno tre competenze da somministrare agli utenti di un corso: **creazione di password complesse**, **contrasto al phishing (difesa dalle frodi online)**, **installazione di un antivirus**.

Già dalla prima struttura della sinossi di un corso in modalità eLearning sarà necessario identificare le informazioni *costanti* e quelle *variabili*: prendiamo in analisi la prima delle competenze e identifichiamo quali saranno le variabili formative da offrire al nostro cliente.

Creazione di password complesse

Utilizzare una password è diventato ormai un'abitudine quotidiana, sia che si tratti di accedere alla posta elettronica o che sia necessario acquistare un prodotto online. Per questo motivo le **password robuste** sono un elemento essenziale per la nostra protezione: se un malintenzionato riuscisse ad ottenere una delle tue password potrebbe infatti prendere possesso della tua identità, trasferire del denaro e avere accesso alle tue informazioni personali.

Ovviamente ci sono alcuni **accorgimenti che è bene adottare per migliorare la sicurezza delle password** in modo da proteggere account, dispositivi fisici e operazioni online.

Sono queste le **costanti** da valutare nella creazione di corsi in modalità eLearning, le famose **best practice** o, in italiano, buone pratiche che ogni persona dovrebbe adottare quando si tratta di sicurezza informatica.

Inseriamo qui una lista generica, ma la tua potrebbe avere molte più voci:

- Impiegare una password differente per ogni account che si possiede. Meglio non utilizzare la stessa password ovunque: se un hacker dovesse scoprirla, la proverà su tutti i siti Web ai quali potreste essere registrati per carpire quante più

informazioni possibili.
- Utilizzare password complesse, mai banali: scegliere una parola facile da indovinare come il tuo nome o cognome non è una buona idea.
- Scegliere password di dimensioni giuste, almeno 14 caratteri e con un certo livello di complessità con caratteri speciali e maiuscoli.

Queste possono essere le nostre costanti nella struttura di un format per la sicurezza informatica aziendali. Tuttavia, per policy interna o, semplicemente, per una valutazione di mercato, potrebbero esserci degli elementi *variabili* da inserire all'interno dei vostri corsi corsi in modalità eLearning.

Ecco un esempio:

Password lunghe e complesse possono essere difficili da ricordare e, se l'utente dispone di molti account, sarebbe impossibile ricordarsi di tutte. Per questo motivo esistono molti password manager sia gratuiti che a pagamento, che forniscono inoltre indicazioni sul livello di robustezza delle password degli account;

La creazione di un corso in modalità eLearning, in questo caso, necessità di un adeguamento alle condizioni di utilizzo dei device aziendali: è possibile installare software di terze parti? È disponibile un catalogo software che possiamo citare all'interno del corso? Quali sono gli utenti più colpiti da questo tipo di errore? È necessario riportare un tutorial per l'installazione?

Tutte queste variabili possono fare *gioco-forza* non soltanto sulla ricchezza di informazioni di corsi in modalità eLearning ma possono fare la differenza sull'offerta da inviare al cliente: maggiori saranno le possibilità di essere aderenti alle loro esigenze e di customizzare il prodotto su una base solida, maggiore successo di mercato potrà avere il tuo prodotto.

Possiamo così passare al secondo argomento.

Difendersi dalle frodi online

La posta elettronica e le app di messaggistica sono i principali strumenti con cui comunichiamo sia in ambito familiare che aziendale: è uno dei modi in cui le aziende forniscono i loro servizi online e, soprattutto, comunicano eventuali richieste fiscali.

Per questo motivo, questi strumenti sono tra i più attaccati dai malintenzionati e, ovviamente, le tecniche di difesa dal phishing, questo il nome di questo particolare attacco, sono tra gli argomenti più richiesti.

Leggi anche " **Quali sono gli 8 attacchi più comuni all'impianto di cybersecurity aziendale?**" e " **Cybersecurity aziendale: i dati sugli attacchi**".

Cadere vittima di questi attacchi provoca il furto di informazioni sensibili o la compromissione dei vostri dispositivi, computer o smartphone, attraverso l'installazione di software chiamati malware.

Capirai perciò la delicatezza di un argomento del genere e la necessità da parte delle aziende di dotarsi di scudi non soltanto informatici ma **informativi e formativi**.

Anche in questo caso esistono delle linee guida generali o, **best practice** da adottare, in ogni caso:

- allegati e link contenuti in tutte le email e messaggi sui social vanno letti con attenzione; se si nutrono dei sospetti è necessario verificare il mittente e capire se il collegamento è reale.
- Prestare attenzione agli allegati, soprattutto a quelli che non attendete: fatture, ricevute di acquisti online e richieste di danaro-
- Utilizzare un software antivirus sempre aggiornato per rilevare eventuali virus all'interno della email
- Diffidare dalle email che richiedono di aggiornare l'antivirus e richiedono clic

E così via.

Anche in questo caso è necessario verificare cosa inserire all'interno di un format e cosa va offerto al cliente come una variabile da adeguare alla policy aziendale.

Il cliente potrebbe avere già a disposizione una suite di sicurezza installata sulle email aziendali che filtra questo genere di richieste e le inserisce direttamente nella cartella di posta indesiderata. Allo stesso modo, cosa che mi capita con alcuni clienti, potrebbe essere attivo un servizio interno di segnalazione di difformità che, con una certa tempestività è in grado di sciogliere ogni dubbio sull'argomento: basta fare una telefonata o inviare una mail con uno screenshot della mail incriminata e attendere una risposta.

Ancora una volta il consiglio è quello di dotarsi di uno schema di gestione delle integrazioni: potrebbe essere utile offrire al cliente un pacchetto base di best practice per poi integrare altre informazioni sulle quali personalizzare il contenuto.

Molto spesso, per adeguare le richieste del cliente al budget, può essere utile avere già a disposizione contenuti informativi che vengono proposti *unicamente in licenza.*

Questi contenuti sulla sicurezza informatica non saranno contenuti ad uso esclusivo del cliente ma potranno essere formattati per un utilizzo generale e contrattualizzati per un utilizzo annuale o, se si vorrà, lifetime ma senza diritto di autorialità.

Questa scelta ti consentirà di ridurre l'effort di realizzazione dei contenuti, almeno quelli testuali, e di proporre un'offerta più bassa rispetto alla concorrenza con una rapida scalabilità e industrializzazione dei tuoi corsi in modalità eLearning.

Possiamo così passare al nostro terzo argomento, forse quello più soggetto ad una certa *variabilità del contenuto*.

Installazione antivirus

I nostri smartphone, i nostri tablet e, soprattutto, i nostri PC vengono acquistati per gli usi più disparati: utili per inviare comunicazioni, per compilare fogli di lavoro, li utilizziamo per ascoltare musica, accedere al conto in banca o per postare le foto delle nostre vacanze al mare.

Per questo motivo è impossibile pensare che i dati in essi presenti non possano far gola a tanti malintenzionati che potrebbero, abbastanza semplicemente, riuscire ad appropriarsi di informazioni sensibili.

Per evitare questo pericolo, esistono alcune buone pratiche che ogni persona o lavoratore dovrebbe attuare per garantire la sicurezza dei propri device.

- Inserire una password robusta in caso di smarrimento o furto del computer, in questo modo non potrà essere a completa disposizione di un malintenzionato
- Prestare attenzione alle app installate su smartphone e tablet, ma soprattutto su PC. Scaricare software in modo illegale potrebbe portare al download di software malevolo come virus e malware.
- Evitare di utilizzare chiavi usb senza controllarle
- Evitare di accedere a wi-fi pubbliche

E così via.

Anche in questo caso esistono delle buone pratiche che possono dipendere direttamente dalla policy interna di un'azienda che potrebbe stringere partnership con un fornitore per l'installazione di un determinato software anti-virus che protegge tutti i device aziendali.

Un anti-virus effettua una scansione dello smartphone, del tablet o del personal computer alla ricerca di malware conosciuti: nel caso in cui un file risulti infetto lo stesso sarà eliminato per neutralizzare la minaccia.

Capirai comunque che non tutti i clienti hanno dimestichezza con questo genere di soluzioni e potrebbero scegliere di affidarti il compito di illustrare le potenzialità di un software anti-virus generico.

In quel caso è necessario prepararsi al meglio: introdurre nel format un pacchetto di funzionalità comuni alla maggior parte dei software anti-virus in commercio e non scendere nel dettaglio.

I criminali informatici sviluppano, in ogni caso, nuove e sempre più sofisticate soluzioni in grado di evitare i tentativi di individuazione, per cui i produttori di anti-virus provvedono ad aggiornarli costantemente con nuove caratteristiche.

Chiedi al tuo cliente di illustrarti casi studio, eventuali incidenti già accaduti e fai partire da quell'evento la tua originalissima proposta di instructional design. Riuscirai, in questo modo, a proporre un concetto di formazione unico, partendo da argomenti più generici.

Puoi iniziare a progettare corsi in modalità eLearning un po' più specifici, come quelli animati, partendo da un format che hai già creato in precedenza.

Quale sarà la tua prossima produzione?