Il fattore umano nella cyber security

Valori e strategie da costruire insieme

A cura di Nicola Sotira

GLOBAL CYBER SECURITY CENTER

FrancoAngeli

MANAGEMENT

TOOLS

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con

La versione completa dell'e-book (a pagamento) è leggibile con Adobe Digital Editions. Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta cliccando qui le nostre F.A.Q.

MANAGEMENT TOOLS

Visioni, esperienze, metodologie per potenziare competenze e capacità: proprie e dei collaboratori

---

Erede della storica collana *Formazione permanente* (che ha accompagnato per oltre quarant'anni la crescita della cultura di management in Italia), *Management Tools* offre a tutti i professional (e agli imprenditori) testi precisi, puntuali, agili e innovativi. Scritti appositamente da consulenti qualificati, i volumi affrontano tutte le aree e i temi di rilievo per valorizzare le competenze e indirizzare al successo le organizzazioni.

Il fattore umano nella cyber security

Valori e strategie da costruire insieme

A cura di Nicola Sotira

Prefazione di Massimiliano Cannata

FrancoAngeli

TOOLS

L'umanità ha da sempre barattato un po' di felicità
per un po' di sicurezza.
(Sigmund Freud)

Indice

Prefazione

di Massimiliano Cannata

La sicurezza è una delle grandi questioni del nostro tempo. IoT, *big data*, robot, macchine intelligenti costituiscono l'ecosistema digitale entro cui viviamo immersi. Sulle reti corre l'economia mondiale, gli interessi dei piccoli risparmiatori come il business dei più avanzati ed evoluti player che operano nei più svariati campi dell'industria moderna. Garantire la protezione delle infrastrutture materiali e immateriali, il rispetto della privacy, facendo sì che l'enorme flusso di dati e informazioni sensibili possano attraversare i binari digitali nel rispetto dei necessari standard di riservatezza, è un compito imprescindibile che chiama in causa le imprese, che si misurano quotidianamente con l'instabilità e le insidie dei mercati, e le istituzioni, il cui compito precipuo è quello di tutelare il benessere dei cittadini. Eventi drammatici ed eclatanti, basti pensare agli attentati terroristici che hanno avuto impatti devastanti sulla vita reale oltre che sull'immaginario di intere popolazioni, l'*escalation* fatta registrare nell'ultimo anno del cyber crime, la violazione delle banche dati e delle infrastrutture critiche, i ripetuti attacchi portati alle strutture sanitarie e a diversi partiti politici hanno messo sotto scacco, soprattutto negli ultimi tempi, i governi in molte aree del pianeta.

L'incidenza di pericolose attività criminali "spicciole", come le quotidiane campagne mirate a compiere truffe ed estorsioni realizzate tramite *phishing* e *ransomware*, le attività di cyber spionaggio e la "guerra delle informazioni" che si combatte a tutti i livelli, condizionando il libero esercizio della stampa e il diritto di cronaca, rendono il quadro ancora più complesso. Se, poi, si prova ad allargare lo sguardo alla condizione dei minori, oggetto di aggressioni odiose e atti di inaudita violenza, si può avere l'esatta misura della fragilità intrinseca all'universo digitale, una fragilità che fa da complemento alla potenza tecnologica che è il tratto

caratterizzante di quella "società del rischio", di cui Ulrich Beck ha offerto un insuperato ritratto.

Nel contesto mutante della "quarta rivoluzione", attraversato da luci e ombre, il cyberspazio è la prima frontiera da presidiare, che ci fa vedere quanto sia difficile trovare un equilibrio sostenibile tra la libertà che innerva e nutre la democrazia e la sicurezza, da cui dipende la sua stessa tenuta. Non vi sono più target "protetti", i sistemi di difesa che aziende e istituzioni devono mettere in atto, si focalizzano su due aspetti: il prepotente progresso scientifico e tecnologico che sta modificando i modi di concepire e praticare il lavoro, e l'aggiornamento costante dei saperi e delle professionalità che operano nell'ambito della cyber security, settore cui viene ormai riconosciuto un valore strategico, tanto da figurare ai primi posti nell'agenda di molti Stati nazionali, in uno scenario geo-politico in costante divenire.

Le imprese sono al centro di molteplici fenomenologie del cambiamento, investite da un compito sfidante: affinare osservazione critica, motivazione, lucidità, attitudine all'innovazione, rapidità di intervento. Anticipare le situazioni di crisi può, infatti, generare un vantaggio competitivo in contesti ambientali caotici, riguardanti strutture lontane dall'equilibrio, per cui risulta particolarmente difficile la previsione di quelle componenti che sono in grado di minare l'integrità di reti e sistemi. Sarebbe illusorio, di fronte alla complessità crescente, ipotizzare uno status di "sicurezza definitiva", circoscritta in un perimetro limitato e rigido; diventa, invece, di cruciale importanza l'investimento sulla qualità del fattore "umano", quale elemento determinante per mettere in campo interventi efficaci di prevenzione e di *governance* del rischio.

La sicurezza è un bisogno oltre che un'esigenza insita nella natura dell'uomo, in quanto tale richiede perciò, prima di tutto, l'adozione di soluzioni a "misura" di ogni singolo "attore" che si muove nell'impresa. I livelli di protezione del business non possono prescindere dalla qualità dei servizi all'utente/cliente, che deve rimanere al centro di ogni progetto di sviluppo economico-industriale. In quest'ottica appare sempre più evidente che le attività della cyber security, oltre a fondarsi su una puntuale azione di contrasto del crimine, possono contribuire a favorire il rispetto dei principi etici e della trasparenza, potranno contribuire a riaffermare il valore della responsabilità sociale nei territori seducenti dell'*infosociety*.

Questo manuale, curato della Fondazione Poste Italiane, prende le mosse dal contesto socio-tecnologico della contemporaneità segnato da instabilità e da continui mutamenti, per affrontare il nodo cruciale della *security awareness*, termine critico che presuppone: la pratica di linguag-

gi innovativi nel campo della formazione, un innalzamento dei livelli di attenzione rispetto alle tante minacce che corrono sui binari digitali, la pratica di una comunicazione semplice ed efficace, adatta a raggiungere target differenziati. Nel corso della trattazione vengono, in particolare, affrontate questioni metodologiche inerenti l'individuazione di competenze e strumenti idonei per l'attuazione di una *strategy awareness* di successo.

Quello che si avverte, scorrendo le pagine del volume, è la necessità di costruire un'"intelligenza collettiva", fatta di *expertise*, sensibilità, competenze. La società del rischio, cui si faceva riferimento prima, ha infatti bisogno di regole, di comportamenti, ma anche di strumenti e codici che consentono di far parlare mondi e saperi diversi. Per raggiungere questo obiettivo, spiegano molto bene gli autori, non basterà in futuro lavorare all'interno delle organizzazioni produttive, risultando utile un confronto costante con tutto ciò che avviene fuori dal circuito lavorativo. Diventerà sempre più importante la progettazione di momenti di incontro, seminari di approfondimento, giornate di studio, mostre tematiche, iniziative di coinvolgimento delle scuole e del mondo della ricerca (il libro si sofferma con dovizia di particolari sulle diverse tipologie di coinvolgimento ideate e praticate con successo in Poste Italiane), finalizzate all'implementazione di un modello avanzato di *security by design*. Molte le aree da presidiare: dalla posta elettronica, alle password, ai social network, strumenti straordinariamente delicati e importanti, che vanno utilizzati con consapevolezza, padronanza, accortezza.

L'originale concezione della **security awareness**, che si fa strada seguendo il percorso narrativo proposto dagli autori, proietta una diversa luce sul compito del *security manager* del futuro, che si muoverà sul terreno dell'interdipendenza e della complessità, toccando con mano la progressiva trasformazione del suo ruolo, destinato a evolvere da "sentinella" posta a presidio della tecnologia a responsabile di più team interdisciplinari, impegnati nella delicata missione di catalizzatori della crescita della cittadinanza digitale, categoria del diritto ancora inedita ma destinata a innestarsi in un orizzonte sociale e giuridico ancora tutto da esplorare.

Introduzione

di Nicola Sotira

Il termine *OnLife* è un neologismo coniato nel 2013 da Luciano Floridi per definire la nuova società digitale. Una parola che sta a indicare l'intreccio tra la nostra esperienza di vita digitale e fisica (online e offline). Un mondo con nuove regole con responsabilità liquide condivise fra strumenti e persone, dove è sempre più impercettibile la distinzione tra reale e virtuale. In questo scenario il rapporto con le tecnologie viene scandito dal cambiamento delle nostre abitudini, come rilevato dal rapporto del Censis[1], che sottolinea come un italiano su due controlla lo smartphone prima di prendere sonno e appena sveglio, mentre uno su quattro non esce di casa senza un power bank (una batteria di scorta). Numeri significativi che non devono stupirci, già nel 2018 i cellulari avevano superato quello dei televisori, e oggi più che mai questi oggetti sono la porta di ingresso al mondo digitale; oggetti che continuiamo, per abitudine, a chiamare soltanto telefoni. In particolare lo smartphone, come sottolineato anche dal rapporto di Ericsson 2019[2], è sempre più lo strumento che viene utilizzato per l'accesso ai servizi digitali. Queste stesse fonti rilevano che il numero delle Sim (le piccole schede presenti nel cellulare che lo fanno funzionare) è pari al 103% della popolazione mondiale. Ovvero più Sim che persone poiché molti oggetti sono oggi connessi, grazie alle Sim, direttamente alla rete; fenomeno che aumenterà a dismisura con l'avvento della nuova tecnologia 5G. OnLife è dunque la nuova dimensione che scandisce il passaggio dall'analogico al digitale, cambiando il mondo e anche la natura umana nella sua relazione con l'ambiente, costringendoci a una ridefinizione della nostra identità. Proprio per questo motivo oggi si

[1] *53° Rapporto sulla situazione sociale del Paese*, 2019, www.censis.it.

[2] *Ericsson Mobility Report*, June 2019, https://www.ericsson.com/en/mobility-report/reports.

parla di metamorfosi digitale e non più di trasformazione, questo poiché la metamorfosi è propria degli organismi viventi. La metamorfosi rappresenta il cambiamento di forma di un organismo, un fenomeno che affascina il genere umano da sempre, acquisendo significati filosofici profondi in relazione ad aspetti della natura umana. Il termine trasformazione è invece più adatto alle macchine, ai processi, mentre oggi parliamo di persone che utilizzano tecnologie complesse. Stiamo vivendo una metamorfosi digitale che sta cambiando le nostre abitudini e le nostre interfacce, un futuro digitale sul quale si interroga anche Shoshana Zuboff, docente della Harvard Business School e autrice del saggio *Il capitalismo della sorveglianza*[3]. Uno degli interrogativi con cui si apre il libro è: "Potremo chiamare casa il futuro digitale?", una domanda che resta aperta in uno scenario nel quale il mondo digitale prende il sopravvento e l'idea di un futuro prevedibile svanisce pian piano. Fondamentale diventa, in questo contesto, il tema della conoscenza sia per quanto concerne la formazione delle nuove generazioni sia per quanto concerne l'utilizzo degli strumenti digitali, sul delicato terreno della sicurezza.

L'accelerazione imposta dal digitale ha messo in evidenza come il problema della sicurezza cyber sia oggi uno dei problemi da affrontare per garantire una transizione di successo. Le istituzioni e le organizzazioni hanno una maggiore probabilità, oggi, di ricevere attacchi di *phishing* o *ransomware* e molti dei loro dipendenti e/o clienti non sanno nemmeno che cosa significhino queste due sigle. In un contesto dove l'accesso alle informazioni è illimitato, un numero preoccupante di dipendenti delle organizzazioni non è attrezzato per contrastare il crescente numero di attaccanti che prendono di mira i loro luoghi di lavoro ogni giorno, rappresentando pertanto l'anello debole del sistema, un paradigma che richiede una completa metamorfosi dell'utente e un approccio strutturato da chi offre servizi digitali. Nonostante le organizzazioni implementino tecnologie di sicurezza sempre più efficaci, insieme a processi e policy che migliorano il governo della sicurezza, tutto può essere compromesso da utenti scarsamente preparati, mettendo così a serio rischio l'organizzazione e tutti gli investimenti in materia di sicurezza.

Le campagne di sensibilizzazione o *security awareness* devono diventare, pertanto, una parte integrante dei programmi aziendali di sicurezza. L'insieme di queste azioni deve tendere principalmente a incrementare il livello di consapevolezza degli utenti, innalzando il livello di sicurezza dell'organizzazione e l'efficacia dei programmi di protezione dei dati

[3] Edizioni Luiss, Roma.

personali. Prima di cimentarsi con una campagna di sensibilizzazione è indispensabile assicurarsi che questa possa avere successo, questo significa anche definire i parametri che ci consentano di **misurarne i risultati**. Al fine di avviare la campagna in modo corretto sarà fondamentale capire lo stato attuale della sicurezza e individuare le aree che richiedono un miglioramento. Tutto questo dovrà essere documentato insieme alle metriche che si deciderà di utilizzare per determinare l'efficacia della campagna.

Altro fattore determinante da inserire nel vostro progetto di sensibilizzazione è la **motivazione**, in molte organizzazioni questi progetti formativi vengono percepiti come troppo impegnativi; questo è particolarmente sentito sui temi di cyber security dove si è portati a pensare che certe cautele possano ostacolare la produttività e l'efficienza. Per contrastare questa perdita motivazionale occorre rendere i programmi di sensibilizzazione più coinvolgenti per i partecipanti utilizzando tecniche di *gamification* e facendo largo uso di materiale multimediale come filmati, cartoon ecc. Bisogna precisare che occorre un'analisi attenta di quei complessi cognitivi e fattori emotivi che giocano un ruolo essenziale nel mantenimento di attenzione al programma. È importante comprendere le esigenze del proprio pubblico in modo da poterli motivare attingendo anche al loro senso di comunità. Da quest'analisi possono scaturire diverse leve come l'introduzione di piani di sviluppo o l'introduzione di un sistema di premi, in ogni caso, di qualunque natura possa essere la motivazione è necessario identificarla prima di avviare un programma di *awareness*. Su questo argomento non esiste, come facilmente intuibile, un approccio unico, il programma deve essere pensato "a misura" delle organizzazioni produttive e testato sulle risorse principali su cui fare leva: le persone.

Per cambiare le abitudini e i comportamenti in un'organizzazione è fondamentale il coinvolgimento del management, queste iniziative devono avere dunque il giusto **commitment dalla direzione** sia nel guidare l'iniziativa, prendendo visione della reportistica e delle azioni correttive, sia fungendo da esempio e motore del cambiamento. È evidente che il coinvolgimento e il supporto del management determineranno anche il livello di importanza che l'intero programma di formazione avrà agli occhi dei dipendenti. Determinante si rivelerà l'impegno del datore di lavoro sui temi della cyber security.

Fondamentale in queste campagne è la **misurazione delle conoscenze acquisite dai dipendenti**, a questo scopo è opportuno predisporre dei test che possano diventare fonte di competizione interna.

Va ricordato che è molto importante che gli esercizi proposti siano concretamente realizzabili, nel contempo sarebbe opportuno evitare di sotto-

porre a test di memoria i dipendenti su dettagli normativi, appare più utile focalizzarsi sugli obiettivi di lungo termine che inducano a migliorare la consapevolezza sui fattori di rischio e sulle azioni da mettere in campo per migliorare la *governance* della sicurezza. Per incidere sul comportamento e cambiarlo, le persone devono, infatti, capire il contenuto di quello che studiano per poterlo applicare al loro quotidiano nei loro rispettivi ruoli. Adattare il programma di sensibilizzazione all'organizzazione aziendale e alle esigenze del capitale umano contribuirà a favorire quel cambiamento culturale necessario, in cui la sicurezza diventa parte del quotidiano.

Il fattore tempo è fondamentale per tutte le organizzazioni, fattore che però viene spesso ignorato. Pertanto, la **tempistica del programma di sensibilizzazione** dovrà essere curata e progettata con attenzione. È consigliabile definire con rigore i tempi di rilascio e di pubblicazione del materiale sull'intranet o sulla piattaforma che avete scelto per l'erogazione dei contenuti. Nell'utilizzo delle campagne di *phishing* vale la stessa cosa: serve puntualità nell'individuazione dei tempi di apprendimento prima di avviare la campagna di simulazione.

Come già precisato, nel digitale siamo circondati e influenzati da diversi format comunicativi, questo succede di continuo sia navigando sul proprio smartphone, sia scansionando dei manifesti in metropolitana. Quando si progettano dei corsi e/o programmi di sensibilizzazione, molte organizzazioni si limitano a utilizzare un singolo canale, sovente con slide animate, quando in realtà bisognerebbe imparare a prendere in esame l'universo multimediale in tutte le diverse sfaccettature tecnologiche, comunicative e linguistiche.

Occorre tenere bene a mente che le campagne di comunicazione interna sono assimilabili alle iniziative di **marketing** in quanto presentano delle finalità pubblicitarie orientate a influenzare il comportamento dei target di riferimento. Utilizzando l'approccio sperimentato dal team di lavoro, che mi onoro di guidare, è possibile arricchire la campagna *awareness* di contenuti multimediali, che renderanno quest'ultima più divertente, più accattivante e sicuramente più efficace. Possiamo immaginare contenuti generati dagli stessi utenti con grande autonomia, come per esempio le illustrazioni utilizzate in questa pubblicazione, allo stesso modo si possono progettare campagne a fumetti, podcast e video-pillole. Va detto che il successo della campagna non può essere solamente basato sull'autovalutazione o la consapevolezza del personale, occorrerà infatti una **serie di dati opportunamente selezionati, che dimostrino un effettivo miglioramento della performance aziendale sul terreno della cyber security**. Queste metriche possono essere, per esempio, la riduzione di attacchi

malware o in alternativa un aumento nelle segnalazioni di e-mail sospette. Metriche che, una volta selezionate, devono essere monitorate per farne oggetto di opportuna reportistica da sottoporre ai vertici aziendali. Perché si possa registrare un successo nel tempo di questi programmi occorre che **siano ripetuti a intervalli regolari** aggiornando, quando risulta necessario, il contenuto e scegliendo nuovi media a supporto della formazione. Il consiglio che, sulla base dell'esperienza maturata, mi sento di dare è quello organizzare una campagna pianificando i suoi successivi rilasci, impegnandosi a costruire, insieme al progetto, un vero e proprio programma editoriale.

In conclusione si può affermare che un programma di formazione continua sulla consapevolezza della cyber security e sull'uso consapevole delle tecnologie digitali può garantire alle organizzazioni, e al Paese, quella resilienza necessaria per reggere alle sollecitazioni dell'universo digitale. Occorre non dimenticare che stiamo parlando di un modello di formazione continua, poiché gli strumenti di attacco evolvono e gli attaccanti troveranno sempre nuove metodologie per inserirsi nei sistemi: l'aggiornamento è perciò assolutamente imprescindibile se si vogliono ottenere risultati. Se si riesce ad applicare la giusta metodologia i vantaggi sono immediatamente visibili, l'aumento della resilienza organizzativa mitiga il rischio per la sicurezza riducendo l'errore umano e le inefficienze di processo. Vivere OnLife in modo consapevole è il primo passo per traguardare una metamorfosi digitale che dobbiamo far diventare sempre più a nostra misura.

In questo libro abbiamo raccolto la nostra esperienza e il nostro "approccio olistico" al tema della sicurezza. Nel corso della lettura si possono trovare esempi interessanti e le esperienze di un team che ha approcciato in maniera strutturata la formazione in tema cyber security, cercando di utilizzare al meglio tutti i canali che il digitale ci mette oggi a disposizione.

1 Aspetti psicologici e cognitivi: il valore dell'individuo per la cyber security

di Alessandra Rose

Il miglior minuto che si spende è quello investito nelle persone.
(Kenneth Blanchard)

1. Cyber security e necessità di *awareness*

Mentre gran parte dell'attenzione nell'ambiente della cyber security è rivolta ad attacchi diretti alla rete, la minaccia informatica più insidiosa per le organizzazioni è rappresentata da attacchi subdoli e persistenti che sfruttano sia l'ingenuità che l'inadeguata conoscenza degli addetti ai lavori.

Le nuove tecniche di manipolazione, come il *mind hacking*, fanno leva su fattori che, soprattutto quando presenti contemporaneamente, possono compromettere le capacità del processo decisionale in quanto diminuiscono la lucidità dell'utente, confondendolo.

Questo capitolo si occupa di spiegare come il fattore umano, attraverso gli aspetti emotivi e i fattori cognitivi, possa influenzare pratiche e comportamenti dell'individuo nel cyberspazio rendendolo vulnerabile e, seppur in maniera non intenzionale, una minaccia per l'organizzazione.

2. Vulnerabilità dell'utente: elementi psicologici

Per comprendere meglio l'esigenza di fare sensibilizzazione sulla cyber security, è necessario partire dalla differenza tra comunicazione online e comunicazione offline (c.d. *face to face* o F2F), dalle loro caratteristiche e dall'influenza che entrambe esercitano sul comportamento individuale e di gruppo (Christopherson, 2007). Semplificando, possiamo affermare che gli aspetti visivi, uditivi e sociali degli ambienti online e offline condizionano i comportamenti delle persone. Sappiamo, inoltre, che l'interazione sociale coinvolge diversi canali di comunicazione, tra cui quello verbale (che comprende tono e volume della voce), quello visivo (espressioni facciali,