economiaepolitica
Rivista online di critica della politica economica
Economia e Politica
Rivista online ISSN: 2281-5260
https://www.economiaepolitica.it

Cybersecurity e vulnerabilità del fattore umano

Di Valentina de Vito,Ester Macrì,Anna Pettini,Giuliano Resce

Cybersicurezza | *A dispetto dei luoghi comuni, cyber attacchi e furti di dati colpiscono molto anche i più giovani e i più istruiti. L'intervento pubblico è sempre più necessario.*

Il ***Global Risks Report 2018*** indica che i cyber attacchi e i furti di dati occupano rispettivamente il terzo ed il quarto posto nella classifica 2018 sui rischi globali in termini di probabilità, dopo gli eventi climatici estremi ed i disastri naturali.[1] Un recente sondaggio ha stimato che circa 978 milioni di persone sono state colpite dalla criminalità informatica nel 2017.[2] Per dare un'idea della dimensione delle perdite economiche, il ***CEO*** e fondatore della società russa di cyber sicurezza Kaspersky Lab, Eugene Kaspersky, ha commentato che ogni anno il crimine informatico costa al mondo l'equivalente di "tredici volte la spesa globale per le missioni spaziali",[3] una cifra che si aggira intorno ai 600 miliardi di dollari (0,8% del PIL mondiale), stando alle stime pubblicate nel febbraio 2018 da McAfee e il Center for Strategic and International Studies.

La rapida evoluzione delle tecnologie ha avuto un profondo impatto sulla società e sull'economia: accanto al miglioramento della produttività delle imprese e alla creazione di nuova occupazione - in 27 Paesi europei tra il 1999 e 2010 la digitalizzazione ha prodotto 11,6 milioni di posti di lavoro aggiuntivi[4] -, la dipendenza dalle ICTs, per la quasi totalità delle attività nelle economie avanzate, ha anche esposto le attività produttive a crescenti minacce cibernetiche.

La cyber-sicurezza è un argomento complesso e la sua comprensione richiede conoscenze e competenze provenienti da varie discipline. Sebbene, chiaramente, le misure tecniche siano un elemento fondamentale, la cyber-sicurezza sta ponendo sfide tanto di natura tecnica quanto non tecnica.[5] I problemi relativi alla cyber-sicurezza sorgono a causa dell'inevitabile presenza di vulnerabilità nelle tecnologie, dell'esistenza di attori malevoli pronti ad approfittarne e della scarsa consapevolezza delle ripercussioni e dei rischi in cui si incorre attraverso quei comportamenti che prevalentemente, ma non unicamente, derivano da una conoscenza solo superficiale dei dispositivi che usiamo.

Si tratta dunque di una questione che riguarda ormai ugualmente singoli individui, realtà aziendali, ma anche gli Stati nel loro intero poiché le minacce informatiche minano le identità delle persone, la tenuta economica delle aziende e la tenuta democratica dei Paesi,[6] come ha dimostrato in modo eclatante il recente caso della società Cambridge Analytica. [7]

Guardando al volume di produzione giuridica, anche internazionale, e alla mole di organismi predisposti alla sicurezza dei cittadini e delle imprese, [8] pare oggi ovvio che i decision-makers, sia di ambito pubblico che privato, abbiano presente l'importanza della sicurezza cibernetica. Lo stesso non può dirsi per i cittadini che, a livello individuale, mostrano una cultura digitale

largamente insufficiente. Per il singolo individuo, cybersicurezza vuol dire sicurezza dei propri dati personali, ma anche difendersi dalle notizie false che proliferano sul *web*, che diviene una delle variabili che indicano il grado di esposizione al rischio informatico. Dai risultati di uno studio recente pubblicato su *Social Science* sulla diffusione di notizie vere e false in rete, [9] emerge infatti che lo strumento cibernetico tende a favorire la viralità delle informazioni false. Alla luce di ciò, è quindi imprescindibile sviluppare consapevolezza, capacità e strumenti per tutelare la nostra presenza nello spazio cibernetico.

La ricerca sta rivolgendo crescente attenzione al ruolo che il fattore umano gioca nella sicurezza cibernetica, in particolar modo laddove le tecnologie preposte hanno fallito nel proteggere le aziende dai cyber attacchi.[10] E' infatti la composizione di fattori organizzativi, ambientali e comportamentali che determina la misura in cui i lavoratori aderiscono alle pratiche di cyber sicurezza (Herath e Rao 2009b). Alcuni studi hanno esplorato il modo in cui i diversi tratti della personalità possono impattare sull'adozione o meno di procedure di cyber sicurezza,[11] o la discrepanza tra le intenzioni di comportamento ed il comportamento effettivo, che va a minare la possibilità di predire condotte conformi (Shropshire *et al.* 2015). La ricerca sta quindi rivolgendo alcuni sforzi in una direzione sempre più necessaria ma, tuttavia, non ancora debitamente esplorata.

Nel solco della ricerca sui comportamenti individuali ad uso delle pratiche di cybersicurezza, ci siamo chiesti se esista una correlazione tra le fonti di informazione di cui le persone fanno uso ed il sussistere di comportamenti digitali che le rendano più vulnerabili. L'atteggiamento più comune, nella generalità degli individui, è prestare fiducia alle informazioni generate nell'ambiente a loro contiguo (definito "pregiudizio della verità" da Bond & DePaulo, 2006). Questo, si è detto in passato, consente alle persone di gestire efficacemente la grande quantità di informazioni ricevute ogni giorno (Gilbert, 1991) al fine di evitare di dover svolgere valutazioni sistematiche per giudicare la legittimità ed affidabilità di ciascuna informazione ricevuta. Nello spazio cibernetico, la propensione alla fiducia varia in base alle conoscenze o convinzioni individuali sui potenziali rischi della comunicazione in rete e della tecnologia in generale (Corritore, Kracher, e Wiedenbeck, 2003; Wang e Emurian, 2005), ma in generale l'uso della rete si presta a dare agli utenti una percezione di anonimato che li induce a rivelare maggiori informazioni di sé rispetto a quante ne rivelerebbero *face to face* (Joinson e Paine, 2007).

Per questo motivo si è scelto di osservare attraverso quali piattaforme si informassero gli intervistati, ed il grado di fiducia da essi accordato alle diverse testate. Al contempo, sono stati sondati il livello di conoscenza dei più comuni crimini informatici ed il comportamento digitale dei partecipanti. In particolare, è stato rilevato di quali cyber crimini fossero state vittime gli intervistati al fine di testare il grado di vulnerabilità effettiva. La vulnerabilità potenziale è stata, invece, controllata sulla base delle risposte ai quesiti su variabili quali la frequenza nell'aggiornamento delle password dei più comuni servizi *online* (posta elettronica, *home-banking,*…), l'utilizzo delle *app* più diffuse, la motivazione soggiacente al *download* delle *app*, la scelta dell'utilizzo del *social login*, la disponibilità a fornire la propria posizione nell'utilizzo di dispositivi dotati di GPS o di *app* per le quali il GPS è richiesto, la scelta del sistema operativo e del *browser* utilizzati con maggior frequenza. Infine, è stato esaminato anche livello di conoscenza della cybersicurezza a livello macro.

2. I dati

La ricerca è stata condotta tramite un questionario standardizzato costruito *ad hoc* per l'indagine, utilizzando il *web* come canale di somministrazione[12]. Nello specifico, il questionario è stato somministrato ai partecipanti tramite ***Facebook***, in quanto si tratta del *social network* più diffuso in Italia. [13]

Dato l'argomento di indagine, la ricerca non poteva che essere condotta *online*, in modo da andare ad intercettare gli utenti privilegiati del web e quindi più interessati al tema. Per il campionamento si è quindi proceduto utilizzando un metodo non probabilistico, detto "di convenienza", proprio perché prevede la selezione del campione in base a criteri di comodità. Se, da un lato, un campione estrapolato con questo metodo è ben diverso dai canoni classici dell'inferenza statistica, dall'altro è quello che permette di intercettare al meglio la popolazione di riferimento dell'indagine, cioè persone che utilizzano internet con frequenza e sono attive sui Social Network. Visto che la tematica dell'indagine è proprio un fenomeno che ha strettamente a che fare con la rete, la *web survey* appariva l'unica strada percorribile e perfettamente in linea con l'obiettivo della ricerca. La rilevazione *web* ha avuto inizio il 21 febbraio 2018 e si è conclusa entro quasi un mese dal suo avvio, il 18 marzo 2018, con un totale di 1139 questionari compilati per intero.

2.1 I partecipanti all'indagine

Il campione ottenuto dall'indagine si è configurato come segue. Sul totale di 1139 partecipanti provenienti da tutto il territorio italiano, il 48,6% dei rispondenti è di genere maschile (n = 554) ed il 51,4% è di genere femminile (n = 585). La maggior parte dei rispondenti, ossia il 41,44%, appartiene alla fascia di età 18-24, il 21,33% alla fascia 25-29 ed il 12,20% alla fascia 30-34. Infine, un quarto dei rispondenti dichiara di avere più di 35 anni.

Rispetto al titolo di studio, quasi la metà (49,78%) degli intervistati si dichiara in possesso di un diploma di istruzione superiore. Una numerosità così corposa in questo intervallo è dovuta al fatto che la maggior parte del campione appartiene alla fascia di età 18 – 24 e dunque da persone ancora troppo giovani, nella maggior parte dei casi, per aver ottenuto un titolo di studio più elevato della licenza superiore. Si fa presente, inoltre, che il test è stato somministrato anche ad una classe di circa 60 studenti al primo anno di Università e il principale canale di diffusione è stato proprio il network universitario. Pertanto, si può presupporre che il questionario abbia raggiunto molte persone attualmente iscritte ad un corso di laurea triennale.

Rispettivamente il 15,89% ed il 17,38% sono quelli in possesso di laurea triennale e di laurea magistrale. Più di un decimo del campione possiede un titolo post-laurea e solo il 6,15% è in possesso di licenza media. I dati relativi all'occupazione mostrano che quasi la metà del campione è costituito da studenti. Infatti, la percentuale cumulata di studenti e studenti-lavoratori è del 49,43%. Il 38,28% degli intervistati ha un'occupazione full-time o, in minor misura, part-time. La restante parte del campione ha dichiarato di essere disoccupata, in cerca di occupazione, NEET, casalinga/o o altro.

3. Analisi dei dati

L’analisi statistica condotta per studiare l’associazione tra la vulnerabilità informatica (relativa e assoluta) e la fiducia accordata in diversa fonti di informazione quotidiana, misura l’*outcome* mediante due variabili dicotomiche:

1. Vulnerabilità Potenziale: (1) l’intervistato ha avuto almeno un comportamento potenzialmente a rischio, (0) altrimenti;
2. Vulnerabilità Effettiva: (1) essere stato oggetto di almeno un attacco e (0) altrimenti.

L’associazione tra la fiducia accordata alle diverse testate giornalistiche e la vulnerabilità potenziale e effettiva è studiata mediante delle regressioni logistiche multivariate. Al fine di mantenere solo le variabili significative nel modello finale, si procede mediante *backward stepwise selection.* Nei risultati si mostrano le determinanti della probabilità di avere una vulnerabilità potenziale e/o effettiva mediante *adjusted Odds Ratios* (aOR) con un intervallo di confidenza del 95%. In epidemiologia l'OR è la misura dell'associazione tra due fattori, per esempio tra un fattore di rischio e una malattia. Il calcolo dell'OR è dato dal confronto tra le frequenze di comparsa dell'evento nei soggetti esposti e le frequenze di comparsa dell'evento nei soggetti non esposti al fattore di rischio in studio. In questi termini, in questa analisi trattiamo la disposizione a dare fiducia a una serie di fonti informative come un fattore di rischio (o un fattore protettivo) per la vulnerabilità potenziale e effettiva. aOR =1 indica assenza di associazione tra esposizione ed evento di interesse, aOR>1 indica associazione positiva, aOR