Consapevolezza dei rischi, cultura della sicurezza e valore dell'esperienza: riflessioni psicosociali per gli scenari futuri

Isabella Corradini

Nella preparazione alla gestione delle emergenze, esercitazioni e simulazioni costituiscono strumenti fondamentali per valutare i piani redatti, la reazione degli attori coinvolti e le attività di coordinamento necessarie. Per quanto tali interventi ripropongano una situazione il più vicino possibile alla realtà, solo l'esperienza diretta della situazione reale è in grado di far emergere in modo tangibile le fragilità, così come i punti di forza, di quanto preventivamente definito. Partendo da questo presupposto, nel paper si discute di come la situazione emergenziale prodotta dal Covid-19, pur nella sua drammaticità, debba essere interpretata come "lesson learned" *anche per il tema della sicurezza nel mondo digitale, evidenziando come il ruolo delle persone – il* fattore umano *– possa fare la differenza nella gestione di situazioni critiche e nella prevenzione. Inoltre, prendendo spunto dal dibattito scientifico sulla cybersecurity e tenendo conto che il digitale è ormai parte integrante delle nostre vite ed è in grado di incidere anche sulla nostra salute, ci si interroga sulla possibilità che la cybersecurity debba essere interpretata come un "bene pubblico". In tal senso, il pieno coinvolgimento dei cittadini – attraverso efficaci piani di informazione e sensibilizzazione – costituisce una necessità irrinunciabile per affrontare in un'ottica sistemica gli scenari futuri sempre più digitali.*

Trasformazione digitale e rischio cyber

Uno degli aspetti più discussi durante la pandemia ha riguardato il ruolo delle tecnologie digitali grazie alle quali, in una fase così critica, è stato possibile assicurare la continuità operativa in settori cruciali – ad esempio quello dell'istruzione – e, più in generale, di tutte quelle attività lavorative realizzabili anche da remoto. Si è così avanzata l'ipotesi che le necessità del momento abbiano accelerato il processo di digitalizzazione di cui si parla ormai da diversi anni. D'altro canto, a livello europeo ed internazionale il tema del digitale rappresenta una priorità per la crescita economica, e non solo, di qualsiasi Paese. Più che di accelerazione della trasformazione digitale, che comunque

richiede piani strategici a medio e lungo termine[1], l'esperienza del lockdown ha probabilmente fatto emergere una maggiore consapevolezza riguardo l'importanza delle tecnologie digitali, considerato che anche molte interazioni sociali si sono trasferite dalla dimensione fisica a quella online. Sono così cresciute le opportunità di apprendimento e il ricorso a moderni approcci organizzativi, come quello del lavoro agile, il cui quadro normativo è regolato dalla Legge 22 maggio 2017, n. 81. Se da un lato però è cresciuto l'uso di tecnologie e di piattaforme digitali da parte di tutti, dall'altro si sono create le condizioni per una maggiore esposizione al rischio cyber. In proposito, il World Economic Forum (WEF) ha allertato sul fatto che la maggiore dipendenza dagli strumenti digitali e la paura dettata dalla situazione emergenziale costituiscono un terreno fertile per l'aumento di cyber attacchi che sfruttano le debolezze umane per penetrare nei sistemi di difesa: è, infatti, più probabile che le persone tendano a commettere errori in una situazione di crisi, soprattutto se prolungata[2]. Considerando che nel prossimo futuro si sfrutteranno sempre più tecnologie digitali intelligenti, le preoccupazioni riguardo alla cybersecurity sono più che giustificate. Si rende tuttavia necessario un cambio di approccio e l'adozione di un *pensiero critico* perché le misure messe in campo per contrastare la minaccia informatica ad oggi non sembrano sortire gli effetti sperati, tanto che cyber attacchi e violazioni di dati sono ormai all'ordine del giorno, raggiungendo in taluni casi elevati livelli di sofisticazione.

Dall'esperienza della pandemia alla cybersecurity: la centralità del fattore umano

La gestione di qualsiasi pandemia richiede necessariamente il coinvolgimento della popolazione. Risultati efficaci si ottengono se c'è una collaborazione attiva delle persone che si adoperano nel seguire i dettami e le regole per far fronte alle criticità. Anche per la gestione del Covid-19 il fattore umano è stato considerato da tutti fondamentale. Il comportamento messo in atto dagli individui, infatti, nel seguire (o non seguire) le regole per prevenire il contagio – dall'uso della mascherina al distanziamento fisico – è quello che ha fatto la differenza (e continua a farlo), in positivo o in negativo. La tutela della propria salute e di quella dei propri cari ha rappresentato un fattore motivazionale potente:

[1] Si veda, ad esempio, il Piano Triennale per l'informatica nella Pubblica Amministrazione https://www.agid.gov.it/it/agenzia/strategia-quadro-normativo/piano-triennale

[2] WEF, Why cybersecurity matters more than ever during the coronavirus pandemic https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/

l'elevato rischio di contagio e l'incertezza del decorso, in molti casi purtroppo senza positiva risoluzione, hanno innescato nelle persone la paura per la propria vita. Inoltre, le campagne informative istituzionali sulle misure di prevenzione del Covid-19 hanno contribuito a tenere alta l'attenzione sul tema. L'analisi di tale esperienza, soprattutto per gli aspetti comportamentali, può portare contributi utili in altri campi, come quello della cybersecurity. Partiamo dal presupposto che anche in questo ambito le persone possono fare la differenza: se da un lato il fattore umano è riconosciuto come l'elemento critico nella sicurezza, è altrettanto evidente che sono le persone preparate e consapevoli dei rischi a costituire l'elemento chiave della prevenzione. Come evidenziato da vari report nazionali ed internazionali[3], infatti, minacce non necessariamente sofisticate quali il *phishing* e lo *spear phishing* (verso target specifici), grazie all'impiego di tecniche a base psicologica come l'ingegneria sociale (*social engineering*), continuano ad avere ottime probabilità di successo[4]. Oltre ad essere causa o concausa di attacchi cyber, emerge anche la possibilità che in taluni casi conseguenze fatali coinvolgano gli esseri umani. Attacchi informatici ben congegnati possono avere un impatto non solo sul funzionamento di strutture vitali di una nazione, le cosiddette infrastrutture critiche, ma determinare effetti sulla salute delle persone, perfino metterne a rischio la vita. Secondo quanto riportato da diversi quotidiani, un attacco hacker ad un ospedale tedesco avrebbe provocato il collasso dei sistemi informatici della struttura, costringendo il personale sanitario a rimandare alcuni interventi e la somministrazione di cure, con conseguente morte di una paziente[5]. Vanno poi considerate le conseguenze psicologiche e sociali prodotte dagli attacchi cyber che includono, ad esempio, la perdita di fiducia nelle tecnologie, problemi di ansia e depressione[6]. La cybersecurity non può, quindi, essere ridotta ad una questione puramente tecnologica, date le diverse implicazioni connesse agli esseri umani, che vanno dalla protezione dei dati la cui compromissione può danneggiare la reputazione di individui – e organizzazioni – agli aspetti di salute e sicurezza. Altri esempi possono essere di supporto in tale analisi. Si pensi, ad esempio, alle auto a guida autonoma dove la

[3] Si vedano, ad esempio, i report annuali di Verizon (Data Breach Investigation Report). https://www.agi.it/economia/news/2020-05-19/rapporto-verizon-attacchi-informatici-8653061/

[4] Si veda la lista delle top 15 minacce cyber del report di ENISA 2020 e riferite al periodo Gennaio 2019-Aprile 2020.

[5] Si veda, ad esempio, https://www.wired.it/internet/web/2020/09/18/cyber-attacco-ospedale-morte/

[6] M. Bada, J. R.C. Nurse, The Social and Psychological Impact of Cyber-Attacks, Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press, London, p.73-92 (2020)

combinazione tra falle nella tecnologia ed errore umano può essere causa di incidenti mortali[7]. Analoga considerazione può essere fatta per i droni: pur ricorrendo a sistemi di Intelligenza Artificiale o a tecnologie *unmanned* a pilotaggio remoto, è evidente che un controllo umano sia sempre indispensabile, proprio per non lasciare il pieno controllo alla sola macchina[8]. La necessità di rimettere al centro l'essere umano è una questione vitale, sia per le ricadute sociali delle tecnologie digitali, sia per gli aspetti di opportunità, dal momento che senza il contributo di persone preparate e consapevoli dei rischi, il raggiungimento di una cybersecurity efficace è un obiettivo difficilmente raggiungibile.

Cultura della sicurezza: oltre gli stereotipi e per il bene comune

Il digitale è ormai parte integrante della vita di individui e organizzazioni e i rischi connessi alla sua diffusione sono sempre più trasversali, dalla sottrazione del patrimonio informativo di aziende strategiche di un paese alla compromissione del loro funzionamento. In tal senso, prendendo spunto dal dibattito scientifico e di quanto discusso nel precedente paragrafo, la proposta di considerare la cybersecurity come un bene pubblico (*public good*) appare quanto mai attuale. D'altro canto, l'analogia con la salute pubblica ispira anche misure applicabili per la sicurezza informatica, quali la prevenzione, il contenimento, la mitigazione ed il recupero[9]. Anche in questo caso, determinante ai fini di un positivo risultato è il coinvolgimento attivo e responsabile della comunità; la resilienza di istituzioni e organizzazioni passa necessariamente anche attraverso un'adeguata *igiene digitale*. Riguardo poi il ruolo rivestito dagli individui e dai loro comportamenti, occorre rinnovare gli approcci culturali lavorando almeno su due elementi chiave. Il primo è il superamento dello stereotipo che vede il fattore umano come punto debole della cybersecurity, anziché come parte integrante della soluzione[10]. Il secondo attiene ad una visione più ampia dei destinatari ai quali ci si rivolge: sono i cittadini (al tempo stesso lavoratori in organizzazioni pubbliche e private, giovani

[7] https://www.repubblica.it/tecnologia/2019/11/21/news/uber_auto_a_guida_autonoma_responsabilita_umana_e_del_software_per_l_incidente_mortale-241593528/

[8] Melzer, N., Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare. European Parliament (2013)

[9] Si veda, ad esempio, D.K. Mulligan, F.B. Schneider: *Doctrine for cybersecurity*. Daedalus 140(4), 70–92 (2011)

[10] V. Zimmermann, K. Renaud: Moving from a "Human-as-Problem" to a "Human-as-Solution" cybersecurity mindset. Int. J. Hum. Comput. Stud. 131, 169–187 (2019)

studiosi, ecc.) ad utilizzare quotidianamente i dispositivi digitali per le molteplici attività quotidiane, spesso inconsapevoli dei rischi di sicurezza ai quali si espongono. Un adeguato piano di sensibilizzazione richiede, quindi, di considerare la diversità dei destinatari e degli strumenti da impiegare, così come il ricorso all'integrazione di diverse competenze e discipline. Se, infatti, per problemi tecnici le soluzioni tecnologiche sono quelle più appropriate, le criticità legate al fattore umano richiedono competenze di natura psicologica e sociale. Infine, per un'efficace cultura della cybersecurity, così come per una produttiva trasformazione digitale del Paese, è indispensabile adoperarsi per il superamento del gap tra essere umani e tecnologie digitali[11]. In tal senso, doveroso è il coinvolgimento del mondo della scuola, dove la necessità di sviluppare attività finalizzate alla consapevolezza digitale per i più giovani è imperativo. Lavorare in questa direzione risponde non solo ad esigenze di sicurezza, ma anche alla necessità di far comprendere le tante opportunità offerte dalle tecnologie digitali, promuovendo al contempo un pensiero critico rispetto al loro uso. Si tratta di attività indispensabili se si vuole costruire una società di persone capaci di affrontare le sfide future della società digitale.

Bibliografia

Bada M., Nurse J. R.C.: *The Social and Psychological Impact of Cyber-Attacks*, In V. Benson and J. McAlaney (Eds.). Emerging cyber threats and cognitive vulnerabilities, 73-92. Academic Press, London.

Corradini I.: *Building a Cybersecurity Culture in Organizations - How to Bridge the Gap Between People and Digital Technology*, Springer (2020)

Corradini I., Nardelli E.: *Developing Digital Awareness at School: A Fundamental Step for Cybersecurity Education* (2020). In Corradini I., Nardelli E., Ahram T. (eds) Advances in Human Factors in Cybersecurity. AHFE 2020. Advances in Intelligent Systems and Computing, vol 1219. Springer (2020)

Corradini I., Nardelli E.: *People&Tech. Igiene digitale, norme base di prevenzione* https://www.key4biz.it/peopletech-igiene-digitale-norme-base-di-prevenzione/187606/

[11] I. Corradini, Building a Cybersecurity Culture in Organizations. How to Bridge the Gap Between People and Digital Technology, Springer, 2020.

ENISA: *List of top 15 threats*. From January 2019 to April 2020 https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-enisas-list-of-top-15-threats

Melzer, N.: Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare. European Parliament (2013)

Mulligan, D.K., Schneider, F.B.: *Doctrine for cybersecurity*, Daedalus 140(4), 70–92 (2011)

Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022, https://www.agid.gov.it/it/agenzia/strategia-quadro-normativo/piano-triennale

Taddeo, M.: *Is Cybersecurity a Public Good*? Minds & Machines 29, 349–354 (2019).

WEF: *Why cybersecurity matters more than during the coronavirus pandemic*, https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/

Verizon: *Data Breach Investigation Report 2020*, https://enterprise.verizon.com/resources/reports/dbir/

Zimmermann, V., Renaud, K.: *Moving from a "Human-as-Problem" to a "Human-as-solution" cybersecurity mindset*. Int. J. Hum. Comput. Stud. 131, 169–187 (2019)

ISABELLA CORRADINI — Psicologa sociale e del lavoro, criminologa, è esperta di sicurezza (*safety* e *security*) con approccio basato sul fattore umano. È direttore scientifico di Themis, centro ricerche socio-psicologiche e criminologico-forensi, e fondatrice del Link&Think Research Lab, focalizzato sugli aspetti etico-sociali dell'innovazione digitale. Ha più di quindici anni di insegnamento a livello accademico nell'ambito della psicologia sociale e della psicologia del comportamento criminale. È referente per l'Ordine degli Psicologi del Lazio dell'area "rischi psicosociali, salute e sicurezza". È responsabile dell'area "consapevolezza digitale" di un progetto educativo nazionale attivo da più di sei anni nella scuola italiana (Programma il Futuro). È membro di diversi comitati tecnico-scientifici (per es. Master Homeland Security dell'Università Campus Bio-Medico di Roma, Centro Studi di Intelligence Economica presso Università di Roma Tor Vergata) e editoriali (per es. Psychology Applications and Development, InScience Press). È autrice di numerose pubblicazioni nazionali ed internazionali, tra le quali si segnala il volume *Building a Cybersecurity Culture. How to Bridge the Gap Between People and Digital*

Technology (Springer, 2020). È inoltre curatrice per la Franco Angeli di una collana editoriale sul tema della reputazione e responsabile scientifico della rivista digitale Reputation Today.

Si precisa che le opinioni esposte nel presente elaborato, ricevuto e reso disponibile nell'ambito dell'iniziativa Call for Papers #CASD2020, sono attribuibili esclusivamente all'autrice e non rispecchiano necessariamente il punto di vista del Centro Alti Studi per la Difesa.