prospettiveinORGANIZZAZIONE
Rivista trimestrale di Organizzazione Aziendale
ISSN: 2465-1753

MAN IN THE MIRROR OR MAN IN THE MIDDLE? ARTEFATTI DIGITALI E CYBER RESILIENZA

Posted on 4 Febbraio 2022 by Neri Martina e Niccolini Federico

Category: Tecnologia ed Innovazione Organizzativa

Artefatti e cybersecurity. Perché associarli? Gli artefatti possono diventare una pericolosissima vulnerabilità informatica ed allo stesso tempo, se inseriti in una cultura coerente, un veicolo privilegiato di cyber resilienza, per identificare, anticipare, resistere e adattarsi ai sempre più frequenti, mutevoli e pericolosi cyber attacchi.

INTRODUZIONE

Le regole di distanziamento sociale resesi necessarie a causa della pandemia da Covid-19 e successive varianti, hanno portato ad un'accelerazione delle attività digitali inimmaginabile fino al 2019, costringendo anche le organizzazioni più restie al cambiamento digitale a proiettarsi nell'ecosistema delle *social technologies* e delle comunicazioni digitali con diverse attività lavorative e processi.

L'ecosistema digitale, ancora di salvezza o fonte di profitto per molte aziende nello scenario pandemico, è quello in cui però prosperano e si sviluppano anche le attività dei cyber criminali.

Il cyber crime, che già prima della pandemia a livello globale "vantava un fatturato" superiore a quello della droga (secondo il Norton Cybersecurity Insight, già nel 2018 era di 388 miliardi di dollari), ha opportunità senza precedenti nelle condizioni di digitalizzazione, anche forzata, imposte dallo scenario pandemico. A livello mondiale, centinaia di milioni di aziende e lavoratori sono stati catapultati nel lavoro digitale. È così che gli hacker hanno rapidamente colto questa ghiotta occasione; in particolare, terreno fertile è stata la scarsa

competenza digitale di un numero elevatissimo di operatori che si è trovato ad operare all'interno dell'oceano digitale, senza però avere gli opportuni strumenti e conoscenze, potremmo dire "vele e remi" abbastanza adatti, per poterci navigare agilmente. Gli attacchi sono così aumentati sensibilmente in termini di frequenza, ma anche e soprattutto in termini di quantità e livello di sofisticazione.

Secondo il rapporto della maggiore autorità nazionale in termini di informazioni sulla cybersecurity (CLUSIT), nel 2020 l'incremento dei cyber attacchi a livello globale è stato pari al 12% rispetto all'anno precedente; il trend di crescita nei quattro anni precedenti si era mantenuto pressoché costante, ma è importante segnalare un aumento degli attacchi gravi del 66% rispetto al 2017. La pandemia ha, poi, caratterizzato l'andamento, soprattutto in termini di modalità e distribuzione degli attacchi. In particolare, i cyber criminali, nello sferrare i loro attacchi, hanno sfruttato due elementi: il disagio collettivo e la difficoltà vissuta da molti settori.

Ritornando al Norton Security Insight, questa volta del 2021, secondo tale fonte lo scorso anno solo in 10 paesi quasi 330 milioni di persone sono state vittime dei cyber criminali. Le vittime hanno impiegato in tutto 2.7 miliardi di ore nel cercare di risolvere i problemi causati dagli attacchi. Dal punto di vista economico, un dato emerge in modo sconcertante; per il 2021 è previsto che il cyber crime infliggerà danni per un totale di 6 trilioni di dollari ai soggetti ed organizzazioni vittime di attacchi.

Con riferimento al contesto italiano, sempre secondo il CLUSIT, nel 2021 la categoria *"Multiple Targets"* ha costituito un quinto degli attacchi registrati; in questa categoria sono compresi attacchi verso vittime appartenenti a settori differenti ma colpiti in parallelo dallo stesso attacco. La considerazione che emerge è che gli attacchi non sono più collegati ai vincoli territoriali o alla tipologia di bersaglio.

Tornando però indietro nel tempo di soli due anni, già nel 2019 il CLUSIT aveva opportunamente segnalato come la somma delle tecniche di attacco "più banali", come i così detti Distributed Denial of Service (DDoS), Vulnerabilità note, Account cracking, Phishing e Malware semplice, rappresentava più dei due terzi (il 63%) del totale degli attacchi. Questo fa si che i cyber criminali possano realizzare attacchi gravi e portati a termine con successo, con relativa semplicità e a costi molto bassi. Questo fenomeno è confermato anche nel 2021, con trend in lieve crescita per tutte le categorie sopra citate, in particolare per le vulnerabilità note e per DDoS.

I dati fino ad ora esposti evidenziano come il fenomeno del cyber crime sia in costante ascesa, accelerata dalla pandemia globale, e che molto probabilmente nei prossimi anni sarà lecito aspettarsi un trend in ulteriore aumento.

IL FABBISOGNO DI CYBER RESILENZA E LA RISPOSTA CULTURALE

La domanda che sorge spontanea in tale scenario è la seguente: quali sono leve che un'organizzazione può attivare per essere cyber-resiliente?

Essere cyber-resilienti, e quindi avere la capacità di identificare, anticipare, resistere e adattarsi di fronte ad un evento digitale avverso e potenzialmente distruttivo, è di fondamentale importanza alla luce della situazione descritta. Infatti, la densità e l'impatto sempre più consistente dei cyber attacchi, fa sì che non sia possibile pensare di fronteggiare questo fenomeno solo attraverso soluzioni sporadiche e di mero stampo tecnologico. Con i trend e le tipologie di attacchi sopramenzionati tutti i componenti dell'organizzazione sono potenziali

vittime e quindi è importante che siano attivamente coinvolti nella lotta alle nuove sfide del dominio cyber.

In tale scenario, lavorare sulla cultura organizzativa, in particolare sugli artefatti, è fondamentale per raggiungere la cyber resilienza. È noto che la cultura organizzativa presenta tre livelli differenti: gli assunti di base, le norme e valori e gli *artefatti*. Questi ultimi sono la parte più visibile e riconoscibile di questa importantissima variabile latente dell'organizzazione. Gli artefatti si osservano anzitutto nell'ambiente fisico, sociale e adesso anche digitale che l'organizzazione costruisce: architettura, tecnologia, layout degli uffici, modo di vestire, modelli comportamentali visibili o udibili, il linguaggio scritto e parlato, riti, cerimonie, simboli, ma anche elementi virtuali, come le comunicazioni ed i profili social, sono i più importanti. Anche se gli artefatti sono visibili, a volte non sono sempre facilissimi da interpretare; infatti, la difficoltà sta nel comprendere il loro significato recondito, il modo in cui si collegano tra di loro e le ragioni che li ispirano.

Gli artefatti ricoprono un ruolo fondamentale e polivalente anche in termini di sicurezza all'interno dell'ecosistema digitale in cui lavorano le organizzazioni. Da un lato, possono essere sfruttati dai cyber criminali al fine di sferrare pericolosi cyber attacchi; d'altra parte, proprio con gli artefatti, e quindi attraverso la cultura organizzativa, si può attivare il cambiamento necessario per operare in modo resiliente all'interno del dominio cyber.

MY FAVORITE WINTER COAT: ARTEFATTI COME VULNERABILITÀ

Muovendo da una definizione poco usata di cultura (quella di Davies et. al), questa è *"the way things are done around here"*. Difatti, attraverso la cultura, coloro che operano all'interno dell'organizzazione si comportano e reagiscono allo stesso modo al verificarsi di determinate situazioni.

In tale prospettiva, quando gli artefatti sono espressione di una cultura non abbastanza flessibile per adattarsi a cambiamenti così repentini, come quello causato dalla pandemia, gli artefatti possono diventare un veicolo di vulnerabilità. In particolare, tali manifestazioni osservabili della cultura possono essere vissute come ciò che potremmo definire un *"favorite winter coat"*. In sostanza, qualcosa che ci fa sentire al sicuro, come il nostro maglione invernale preferito, ma che può non essere adatto al contesto in cui ci troviamo e rischia di trarci in inganno o irrigidirci. Sono così proprio gli artefatti che, in molti casi, vengono sfruttati dai cyber criminali per perpetrare un attacco ai danni di un'organizzazione. Quando gli artefatti, e quindi la manifestazione della cultura, vengono intercettati dal cyber criminali, la manifestazione stessa può diventare un veicolo di contagio, in questo caso cyber, come descritto nel paragrafo successivo, in cui i cyber criminali dirigono i cyber attacchi per carpire informazioni critiche per l'organizzazione e farne un utilizzo fraudolento.

MAN IN THE MIRROR O MAN IN THE MIDDLE?

È stata usata l'espressione "informazioni critiche", poiché, in questo contesto e in accordo con quanto osservato in precedenza circa l'aumento di quantità, qualità e sofisticazione dei cyber attacchi, parlare solo di informazioni sensibili rischierebbe di essere riduttivo. Gli hacker possono infatti arrivare a qualsiasi tipo di informazione critica per il business che risieda all'interno dell'organizzazione. Tra queste possiamo ricordare, a titolo di esempio, brevetti, piani di sviluppo di prodotti, business plan, prototipi software/hardware, fino a

informazioni relative a processi e dinamiche interne (anche all'interno di messaggi e-mail o di testo) o codici di accesso a conti correnti bancari e numeri di carte di credito.

Ponendo l'attenzione sugli artefatti digitali, come ad esempio una rete intranet, dove i membri dell'organizzazione possono comunicare tra loro per la gestione delle attività di business, quello che può accadere è che la trasmissione possa essere alterata o ritrasmessa dagli hacker, di modo tale che le parti *credano* di comunicare tra loro. In questo caso il cyber criminale si interpone nella comunicazione nascondendosi come un "*man in the middle*".

In uno degli attacchi che rientra in questa categoria, lo eavesdropping, il cyber criminale realizza delle connessioni indipendenti tra chi comunica; in realtà i messaggi vengono ritrasmessi in modo tale che gli attaccati credano di comunicare con l'utente scelto, ad esempio un collega, attraverso una connessione privata, mentre invece la conversazione è nota, e talvolta indirizzata e completamente controllata dal cyber criminale. Di conseguenza i messaggi possono essere intercettati, o possono anche esserne scritti di nuovi.

Dal punto di vista tecnico, l'attacco può avere successo solo se nessuna delle due vittime ha la possibilità e gli strumenti per rendersi conto di star utilizzando una connessione che ormai è compromessa. L'eventuale verifica potrebbe avvenire tramite diversi metodi, come ad esempio password di riconoscimento o altri canali di comunicazione. È chiaro che anche lo stesso linguaggio può essere sfruttato dai cyber criminali.

Richiamando i dati esposti precedentemente, la categoria di cyber attacchi appartenenti alla tipologia *phishing*, e più in generale all'ingegneria sociale, rimangono stabili rispetto al 2019 e rappresenta il 15% del totale dei cyber attacchi.

L'ingegneria sociale sfrutta il comportamento umano e ottiene informazioni riservate, attraverso l'utilizzo di atteggiamenti persuasivi. Appartenente a questa categoria è il *phishing,* con l'intento di rappresentare non solo i pesci dell'oceano digitale che abboccheranno all'amo, ma anche la marea di informazioni che verranno pescate; in sostanza, i cyber criminali si fingono soggetti affidabili inviando comunicazioni compromesse attraverso canali digitali. Una quota crescente di cyber attacchi basati su *phishing* si riferisce a *BEC scams (Business E-mail Compromise)*, che infliggono danni economici sempre più ingenti alle loro vittime.

Quest'ultimo è detto anche *whaling*; tale termine deriva da *whale*, proprio a voler sottolineare l'enorme animale che abboccherà all'amo, e quindi all'attacco. L'obiettivo è ottenere informazioni critiche e rilevanti per l'organizzazione (soprattutto quelle con alto valore economico e commerciale). In genere, questo tipo di cyber attacco è indirizzato a coloro che hanno un ruolo specifico e rilevante all'interno dell'organizzazione; infatti, target primari possono essere figure come i CEO, i manager o, ancora, un collega fidato. Operativamente, una o più mail fraudolente e compromesse, vengono inviate agli indirizzi e-mail dell'individuo obiettivo; la richiesta che viene fatta è in genere quella di fornire dati critici e rilevanti, o di autorizzare pagamenti che inevitabilmente sono indirizzati ai conti dei cyber criminali.

Importante è l'impatto finanziario di questo fenomeno; infatti, nel 2020 sono state registrate perdite per quasi due miliardi[1]. I casi FACC e Leoni sono piuttosto esplicativi di quanto detto sopra.

Nel 2016, la FACC, produttrice austriaca di componenti aerospaziali ha subito un attacco tramite artefatto digitale. I cyber criminali avevano inviato, fingendosi il suo direttore, Walter Stephan, una mail fasulla ad un responsabile finanziario, chiedendo di trasferire del denaro su un conto per un progetto (ovviamente falso) di

acquisizione. Questo cyber attacco, conosciuto come *fake president incident*, è costato all'azienda 42 milioni di euro. Le ripercussioni del cyber attacco sono state ingenti. Stephan è stato licenziato. Si è inoltre verificata una perdita operativa di 23,4 milioni di euro nell'anno finanziario, contro una perdita di 4,5 milioni relativa all'anno precedente.

Sempre nel 2016, la Leoni AG, uno dei principali produttori mondiali di fili e cavi, è stata vittima di un cyber artefatto, il BEC; il cyber attacco è costato all'azienda 40 milioni di euro e un calo del valore delle azioni del 2%. Anche in questo caso, una email compromessa è stata inviata ad un membro del dipartimento finanziario della fabbrica di Bistrita, in Romania; l'email sembrava essere inviata da uno dei dirigenti tedeschi, che ordinava di trasferire 40 milioni di euro su un conto bancario estero. Ma perché proprio il dipartimento finanziario di Bistrita? Tra le quattro fabbriche in Romania, questa era l'unica autorizzata ad effettuare trasferimenti di denaro. Questa informazione è particolarmente rilevante e dimostra come alla base di ogni cyber attacco ci sia un attento studio dell'organizzazione nella sua totalità.

In entrambi i casi, i cyber criminali, inserendosi come "man in the middle", hanno portato così a segno i loro attacchi.

HOW TO MAKE THE CHANGE: ARTEFATTI COME OPPORTUNITÀ DI DIFESA

Se gli artefatti, in diverse manifestazioni, possano diventare una vulnerabilità, è però anche vero che questi possono assolvere il ruolo di opportunità di difesa.

È noto, infatti, che la cultura, ha una forte funzione di adattamento esterno. Secondo la nota definizione di Schein, "la cultura organizzativa è l'insieme coerente di assunti fondamentali che un dato gruppo ha inventato, scoperto o sviluppato imparando ad affrontare i suoi problemi di adattamento esterno e di integrazione interna, e che hanno funzionato abbastanza bene da poter essere considerati validi, e perciò tali da poter essere insegnati ai nuovi membri come modo corretto di percepire, pensare e sentire in relazione a quei problemi." Ciò, vale anche per migliorare la cyber resilienza.

Nel percorso verso la cyber resilienza, infatti, si parte spesso dal livello esteriore, per influenzare ed orientare stabilmente gli altri due livelli.

Con l'artefatto si cerca di influenzare il secondo livello, i *valori,* ovvero i principi fondamentali regolano il comportamento dei membri dell'organizzazione e in base ai quali è possibile distinguere i comportamenti giusti da quelli sbagliati, anche nel dominio cyber. Ma il vero obiettivo è il terzo livello, il più profondo, cioè gli *assunti di base*. occorre infatti arrivare a incidere sulle concezioni più implicite e soprattutto inconsce, per far sì che nasca una consapevolezza cyber nel modo in cui i membri dell'organizzazione percepiscono, pensano e sentono le attività digitali. Per divenire organizzazioni cyber-resilienti è necessario che la cybersecurity diventi un valore dato per scontato, che entra a far parte delle abitudini e delle idee a cui si fa riferimento in modo automatico, e quindi inconscio, di una percentuale sempre maggiore, tendente al 100% dei dipendenti.

Tutto ciò in accordo anche con il conosciuto modello delle dinamiche culturali di Hatch, che, declinato su queste tematiche, presuppone che la cultura della cyber sicurezza diventi insieme di processi attraverso cui artefatti appositamente orientati sono creati nel contesto dei valori e degli assunti dell'organizzazione; in

questo modo, i valori e gli assunti di cyber sicurezza sono mantenuti, o modificati, attraverso l'utilizzo e l'interpretazione di artefatti costruiti ad-hoc.

Attraverso artefatti digitali, e in particolare intranet e relativi social aziendali (come Yammer), può essere veicolato un nuovo paradigma valoriale orientato alla cyber-resilenza. Informazioni di varia natura circa le dinamiche cyber possono essere veicolate tramite gli artefatti. Attraverso gli strumenti di comunicazione digitale possono essere diffuse nuove e semplici procedure, policy, regole comportamentali, informazioni mirate riguardanti la condizione cyber globale, nazionale o del settore di appartenenza, oppure storie edificanti di aziende simili che hanno subito cyber attacchi. Talvolta alcuni semplici e reiterati messaggi, come lo "Stop. Think. Connect", mantra della filosofia "Stay Safe Online", può avere un'elevata efficacia. Tutto questo influenzerà lentamente i valori e gli assunti di base, fino allo sviluppo di un adeguato livello di consapevolezza, il quale permetterà la formazione di adeguate conoscenze e competenze per fronteggiare le minacce del dominio cyber. La cyber consapevolezza è quindi un'attenzione continua e regolare volta a proteggere l'organizzazione. È al riguardo importante richiamare il pensiero di Von Solms, in quale, già ad inizio millennio, aveva ben chiaro che è fondamentale lavorare anche sugli artefatti per attivare spirali cognitive che portino alla cyber consapevolezza, intendendo con quest'ultima la condizione in cui tutti gli attori organizzativi sono talmente ben informati e formati rispetto ai loro obiettivi in termini di cybersecurity, in modo tale che questa diventi un aspetto naturale delle attività di business quotidiane.

In linea con queste considerazioni, diverse aziende hanno attivato programmi di diffusione di conoscenze cyber, finalizzate a creare una cultura della cyber sicurezza diffusa capillarmente in modo rendere realmente cyber resiliente l'organizzazione. La gamma di artefatti utilizzabili è ampia, si spazia dai semplici messaggi sopracitati, ai programmi di formazione on line, fino agli artefatti digitali avanzati, come la *gamification;* in questo caso, per diffondere le conoscenze e i nuovi valori vengono utilizzati dei videogiochi, delle simulazioni e dei video interattivi. Anche se l'utilizzo di videogiochi potrebbe sembrare bizzarro, sono diverse le organizzazioni che se ne servono regolarmente e per cui questi elementi diventano parte edificante e quindi integrante della cultura cyber della cybersecurity. La rivista Forbes, a tal proposito, ne evidenzia alcune. La PWC attraverso il suo *"Game of Threats",* utilizza la simulazione per mostrare quali sono gli step da percorrere per proteggere la propria organizzazione durante un cyber attacco. Ancora, IBM con il suo *"Cybersecurity Ops: Terminal"* utilizza la simulazione per risolvere problematiche cyber, impersonando diversi ruoli all'interno dell'organizzazione, ad esempio un general manager.

In sintesi, individuata la nuova scala dei valori al fine di fronteggiare le sfide del dominio cyber, questi sono stati veicolati proprio tramite un artefatto digitale; è questa la strada *"to make the change"* e rendere realmente più cyber resiliente l'organizzazione.

CONCLUSIONE E DISCUSSIONE

Ad oggi, a prescindere da vincoli territoriali e settoriali, i cyber attacchi sono sempre più frequenti, sempre più efficaci e sempre più sofisticati. I trend sono in continua crescita e non c'è da aspettarsi una diminuzione per gli anni futuri, soprattutto a seguito dell'immersione, spesso necessariamente forzata, nell'oceano digitale e delle nuove dinamiche innescate dallo scenario pandemico.

È stato osservato che gli artefatti, in questo nuovo scenario, possono assumere un duplice ruolo di veicolare

vulnerabilità ed opportunità.

Pur essendo distanti dal nucleo più profondo della cultura organizzativa, gli artefatti possono essere intercettati dai cyber criminali soprattutto al fine di rubare il patrimonio di informazioni critiche dell'organizzazione stessa, oltre che ingenti quantità di denaro.

Tuttavia, una volta identificato il paradigma valoriale che chiude il *gap* tra la nuova e la vecchia scala dei valori, gli stessi artefatti possono essere adoperati per infondere gradualmente nell'organizzazione le conoscenze e competenze necessarie al perseguimento dei nuovi obiettivi in termini di cyber resilienza.

Quando la cultura organizzativa, in tutte le sue componenti, è allineata rispetto agli obiettivi interni di cybersecurity e alle dinamiche esterne del dominio cyber, l'organizzazione è in grado di evolversi da un atteggiamento di mera difesa ad uno proattivo. Questo significa navigare nell'oceano cyber con resilienza.

La cyber resilienza, in questa sede è concettualizzata in modo olistico come capacità *identificare*, *anticipare, resistere e adattarsi* ad un evento distruttivo ed avverso che si verifica nell'ambiente, cioè un cyber attacco.

Opportune conoscenze sviluppate e trasmesse tramite gli artefatti, serviranno ad alimentare le capacità anticipatorie dell'organizzazione; questo significa che l'organizzazione potrà migliorare la propria abilità di identificare i rischi potenziali e assumere delle decisioni idonee per mitigare gli effetti e operare in modo stabile anche durante il cyber attacco; in sostanza l'organizzazione sarà in grado di anticipare o rispondere in modo rapido ad un evento ad alto impatto potenziale che avrebbe potuto interrompere o compromettere le attività aziendali. Da tutto ciò deriverà una maggiore capacità di apprendimento e adattamento rispetto al verificarsi dell'evento avverso; in altre parole, l'organizzazione manterrà un adattamento positivo durante l'evento avverso, in modo da emergerne rafforzata.

Infine, le conoscenze e i nuovi valori interiorizzati e diventati una naturale componente della quotidianità e delle attività dell'organizzazione, concorreranno all'innesco di meccanismi di apprendimento double loop, grazie ai quali sarà possibile tenere viva la cultura della cyber sicurezza.

Bibliografia essenziale

Clusit, (2020). Rapporto sulla sicurezza ICT in Italia. Milano: CLUSIT.

Clusit, (2021). Rapporto sulla sicurezza ICT in Italia. Milano: CLUSIT.

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713

Davies, H. T. O., Mannion, R., Jacobs, R., Powell, A. E., & Marshall, M. N. (2007). Exploring the relationship between senior management team culture and hospital performance. Medical care research and review, 64(1), 46-65.

Hatch, M. J. (1993). The dynamics of organizational culture. Academy of management review, 18(4), 657-693.

Schein, E. H. (1983). The role of the founder in creating organizational culture. *Organizational dynamics*, *12*(1), 13-28.

Schein, E. H. (1985). Defining organizational culture. Classics of organization theory, 3(1), 490-502.

Schein, E. H. (1990). Organizational culture (Vol. 45, No. 2, p. 109). American Psychological Association.

Schein, E. H. (2010). *Organizational culture and leadership* (Vol. 2). John Wiley & Sons.

Solms, B. V. (2000). “Information security-The third wave?” Computers & security, 19, 615.

Sitografia

https://www.forbes.com/sites/dollar-general/2021/09/22/the-retail-standout-thats-giving-a-boost-to-reading-and-literacy/?

NOTE

[1] 2020 Internet Crime Report a cura di Federal Bureau of Investigation (FBI).