Roma. Il Fattore Umano nella Cybersecurity: Una intervista a I. Corradini (Themis)

fino-a-prova-contraria.blogautore.espresso.repubblica.it/2022/09/17/roma-il-fattore-umano-nella-cybersecurity-una-intervista-a-i-corradini-themis

Isabella Corradini è presidente e direttore scientifico di Themis, centro ricerche socio-psicologiche e criminologico-forensi, e fondatrice del Link&Think Research Lab, focalizzato sugli aspetti sociali dell'innovazione digitale.
Psicologa sociale e criminologa, è esperta di cybersecurity e safety con approccio basato sul fattore umano, con riferimento sia agli ambiti aziendali che agli scenari digitali. Oltre a condurre attività di ricerca in ambito nazionale e internazionale, è docente in diversi master universitari e in corsi specialistici.
Fa parte del network Women&Technologies (Associazione Donne e Tecnologie) e vanta importanti esperienze a livello internazionale, tra le quali l'attività di mentor e speaker per il progetto "Women in Cyber Mentorship Programme" dell'ITU (International Telecommunication Union).
È membro di diversi comitati tecnico-scientifici e editoriali (Construction of Social Psychology, Psychology Applications and Development, InScience Press) e attiva in progetti di educazione sul digitale in ambito scolastico, come Programma il Futuro, un'iniziativa educativa nazionale attiva dal 2014 nella scuola italiana, per il quale è responsabile dell'area "cittadinanza digitale".
Autrice di numerose pubblicazioni, sull'argomento oggetto di questa intervista si segnala in particolare il volume sulla cybersecurity pubblicato dalla Springer "Building a Cybersecurity Culture. How to Bridge the Gap Between People and Digital Technology" (2020) ed il recente discussion paper per EU-OSHA (European Agency for Safety and Health at Work) "Incorporating occupational safety and health in the assessment of cybersecurity risks".
È inoltre responsabile scientifico della rivista digitale Reputation Today, focalizzata sull'importanza della reputazione nella società contemporanea.
Secondo uno studio di Trend Micro, Defending the Expanding Attack Surface, l'Italia si colloca al primo posto in Europa per numero di attacchi ransomware subiti nel primo semestre 2022. Il ransomware è quell' attacco che consiste nel crittare i file sul dispositivo dell'utente, che così si ritrova impossibilitato ad usarlo, a meno che non paghi un riscatto.
D: Se è evidente che i cybercriminali sfruttano ogni vulnerabilità, in particolare quelle degli utenti, è meno evidente la scarsa educazione e consapevolezza dei rischi che si corrono quando si aprono link, si scaricano app e si naviga in rete. Il fattore umano è pertanto un elemento imprescindibile della cybersecurity, ancora però molto sottovalutato. Cosa si intende per fattore umano nella cybersecurity?
R: Pensiamo a come i cybercriminali riescono ad attaccare con successo: in molti casi sono le persone ad aprire file infetti (ad esempio attraverso email o messaggi WhatsApp che sembrano provenire da mittenti legittimi, il cosiddetto phishing) o a scaricare app maligne, col risultato di infettare il proprio dispositivo. Insomma, come hanno sempre fatto nella storia dell'umanità, i truffatori sfruttano le debolezze umane per trarne un

vantaggio. L'ingegneria sociale, vale a dire la strategia psicologica su cui si basano le email di phishing o le telefonate ingannevoli, funziona proprio perché sfrutta le abitudini delle persone e le loro fragilità emotive. Senza poi tenere conto di come vengono scelte e conservate le password. Tanti possono essere gli esempi che vedono il fattore umano tra le cause del buon successo degli attacchi. Ecco perché si dice che il fattore umano è l'anello debole della catena della sicurezza. Ma può diventare quello forte, se adeguatamente preparato e aggiornato. Esperienze di ricerca e di progetti formativi che ho guidato, e da cui sono scaturite varie pubblicazioni sul tema, mi hanno confermato sul campo che senza considerare la "dimensione umana e sociale" della cybersecurity non si va da nessuna parte.

D: Immagino che non sia affatto facile da gestire, perché richiede interventi di ben altra natura rispetto alle soluzioni tecnologiche.

R: Chi propone di sostituire l'essere umano con le più innovative tecnologie cercando di automatizzare la sicurezza, ad esempio mediante applicazioni dell'Intelligenza Artificiale, non ha capito l'essenza del problema: non esistono ricette miracolose, sia le tecnologie che gli esseri umani debbono essere gestiti. Per intenderci meglio: non sto dicendo che le soluzioni tecnologiche non siano importanti, anzi. Sto dicendo che senza la consapevolezza delle persone sui rischi in rete, sull'uso responsabile delle tecnologie e sull'importanza della protezione dei dati, quelle stesse soluzioni perdono di efficacia.

D: Sono le persone ad essere destinatarie delle conseguenze derivanti dagli attacchi cyber. E' questo un altro aspetto determinante che in qualche modo si collega al fattore umano. Cosa ci dice in proposito?

R: Un attacco informatico andato a segno causa inevitabilmente disservizi alle strutture coinvolte. Ma pensiamo a quegli attacchi che vanno a colpire infrastrutture critiche del Paese, come ad esempio ospedali o centrali elettriche. Un attacco cyber può trasformarsi in un evento critico per la sicurezza e la salute delle persone. Ci si concentra quasi esclusivamente sui danni economici che ne derivano, sulla perdita dei dati, sulla compromissione della reputazione dell'organizzazione colpita, ma c'è anche altro: la manipolazione di una macchina può mettere fisicamente a rischio la vita delle persone, se ad esempio gli hacker prendono il controllo di dispositivi medicali. Può anche accadere che venga messa a rischio la sicurezza del lavoratore mentre sta svolgendo la sua attività da remoto, a causa di un malfunzionamento dei dispositivi informatici coinvolti (ad esempio, perdita del segnale wireless). Questo connubio tra cybersecurity e rischi per la salute delle persone non viene mai adeguatamente considerato. Invece, su richiesta dell'Agenzia europea per la sicurezza e la salute sul lavoro (EU OSHA), ho recentemente realizzato un articolo di inquadramento su questi importanti aspetti https://osha.europa.eu/en/publications/i... Speriamo che il messaggio di coniugare safety e cybersecurity, mettendo al centro le persone, cominci ad essere considerato nella giusta prospettiva.

D: Quale potrebbe essere allora la prospettiva per una cybersecurity efficace?

R: Fino ad oggi si è proceduto attendendo che gli attacchi arrivassero per poi intervenire. Ma così facendo si opera sempre in emergenza. Io credo che bisogna iniziare con un'attività di diagnosi per vedere cosa non ha funzionato e perché, e poi capire cosa è necessario fare e dove bisogna intervenire. Un problema di questa portata non si affronta in un giorno. Quando sento dire che il problema della cybersecurity è legato al fatto che

mancano all'appello migliaia di specialisti tecnici di quest'area non mi sembra che si stia facendo una diagnosi corretta, o quantomeno completa. Certo, anche questa carenza è parte del problema, ma mi chiedo perché ci siamo ridotti oggi a lamentarci di queste mancanze invece di affrontarle per tempo, visto che la cybersecurity non è un argomento nuovo. Sono infatti parecchi anni che gli attacchi sono in continua crescita e riguardano ormai tutto il mondo. Qualche critica (purchè sia costruttiva) ci vuole, altrimenti si continua a perseverare con uno degli errori maggiori, vale a dire incensarsi per ciò che si andrà a fare, evitando di guardare in faccia la realtà.
D: Creare cultura della sicurezza, la vera sfida è una formazione ed una educazione alla sicurezza?
R: Decisamente questa è la vera sfida. Anche perché creare una cultura della cybersecurity significa proprio investire sulla formazione delle persone e in modo continuativo. Significa lavorare sul loro atteggiamento mentale per creare quella consapevolezza necessaria a individuare le minacce e a gestirle. Ma attenzione: non basta andare in aula con una check-list per trasformare le persone, dal momento che non sono robot telecomandati, ma esseri umani con tutta la loro complessità. Come dico spesso, un corso di formazione può instillare l'idea dell'importanza della sicurezza, cambiare i comportamenti è ben altra cosa.
D: Per creare una cultura della cybersecurity è necessario prima di tutto sensibilizzare i decisori politici che, ormai da qualche anno, hanno certamente una maggiore consapevolezza del problema…
R: La strada da percorrere è ancora lunga. Questa consapevolezza ha portato alla nascita di un'agenzia dedicata, l'ACN (Agenzia per la Cybersicurezza nazionale), un passo davvero molto importante. Ma non basta dire che c'è l'Agenzia a dover risolvere i problemi, ci vuole un investimento a livello culturale in grado di coinvolgere tutto il paese. Sono necessarie inoltre competenze diversificate, un'integrazione tra le cosiddette hard e soft skills. Altrimenti si rischia di avere una visione parziale della cybersecurity, o meglio, una visione ancora troppo "tecnica" che, come vediamo dai dati impietosi degli ultimi anni, non funziona. In poche parole, non basta preparare guerrieri cyber, serve educare cittadini digitali consapevoli. E serve farlo bene e al più presto.
D: Lei ha parlato di soft skills, tra le quali indubbiamente rientra la comunicazione: in che modo questa può essere considerata rilevante per la cybersecurity?
R: Vedo almeno tre aspetti rilevanti. Il primo è che la comunicazione rientra tra quelle competenze trasversali che permettono di lavorare e di relazionarsi in modo efficace all'interno di un'organizzazione, e quindi è prioritaria anche nella cybersecurity. Una comunicazione inadeguata sui rischi cyber, ad esempio, non favorisce la consapevolezza di tali rischi. Un altro aspetto riguarda la carente o inefficace comunicazione di crisi in caso di attacco cyber, che può produrre conseguenze disastrose. Per alcuni attacchi informatici subiti da importanti organizzazioni, la (non) comunicazione o un suo uso scoordinato rischia di produrre più danni dell'attacco stesso, perché mina prima di tutto la fiducia degli utenti. È chiaro che non vanno rivelati dettagli dell'accaduto, ma il fatto che sia successo non può essere negato! Proprio il negare, far finta di niente o cambiare versione ogni volta che conviene non è una strategia consigliata, perché alimenta la confusione. Come dico spesso, l'incertezza è ormai parte del nostro tempo, ma va comunicata e gestita nel modo giusto. Infine, c'è un rischio relativo alla comunicazione che non va

sottovalutato: il fatto che gli attacchi cyber siano ormai all'ordine del giorno e che colpiscano vittime illustri, rischia di far scemare via via la motivazione dell'utente a mettere in campo le necessarie misure di difesa, percependo tali eventi come qualcosa a fronte dei quali non c'è protezione che tenga. Un effetto di "desensibilizzazione emotiva", potremmo dire, vale a dire anestetizzante, che induce le persone ad accettare passivamente quello che accade. Un po' come avviene quando coloro ai quali dici che è importante proteggere i propri dati ti rispondono: "inutile preoccuparsi della privacy, tanto sanno già tutto di noi!"

Isabella Corradini è Presidente e Direttore Scientifico di Themis, centro ricerche socio-psicologiche e criminologico-forensi, e fondatrice del Link&Think Research Lab, focalizzato sugli aspetti sociali dell'innovazione digitale. Psicologa sociale e criminologa, è esperta di cybersecurity e safety con approccio basato sul fattore umano. Fa parte del network Women&Technologies (Associazione Donne e Tecnologie). Autrice di numerose pubblicazioni, in particolare il volume sulla cybersecurity pubblicato dalla Springer "Building a Cybersecurity Culture. How to Bridge the Gap Between People and Digital Technology" (2020) ed il recente discussion paper per EU-OSHA (European Agency for Safety and Health at Work) "Incorporating occupational safety and health in the assessment of cybersecurity risks".

D: Secondo un recente studio di Trend Micro, Defending the Expanding Attack Surface, l'Italia si colloca al primo posto in Europa per numero di attacchi ransomware subiti nel primo semestre 2022. Il ransomware è quell' attacco che consiste nel crittare i file sul dispositivo dell'utente, che così si ritrova impossibilitato ad usarlo, a meno che non paghi un riscatto. Se è evidente che i cybercriminali sfruttano ogni vulnerabilità, in particolare quelle degli utenti, è meno evidente la scarsa educazione e consapevolezza dei rischi che si corrono quando si aprono link, si scaricano app e si naviga in rete. Il fattore umano è pertanto un elemento imprescindibile della cybersecurity, ancora però molto sottovalutato. Cosa si intende allora per fattore umano nella cybersecurity?

R: Pensiamo a come i cybercriminali riescono ad attaccare con successo: in molti casi sono le persone ad aprire file infetti (ad esempio attraverso email o messaggi WhatsApp che sembrano provenire da mittenti legittimi, il cosiddetto phishing) o a scaricare app maligne, col risultato di infettare il proprio dispositivo. Insomma, come hanno sempre fatto nella storia dell'umanità, i truffatori sfruttano le debolezze umane per trarne un vantaggio. L'ingegneria sociale, vale a dire la strategia psicologica su cui si basano le email di phishing o le telefonate ingannevoli, funziona proprio perché sfrutta le abitudini delle persone e le loro fragilità emotive. Senza poi tenere conto di come vengono scelte e conservate le password. Tanti possono essere gli esempi che vedono il fattore umano tra le cause del buon successo degli attacchi. Ecco perché si dice che il fattore umano è l'anello debole della catena della sicurezza. Ma può diventare quello forte, se adeguatamente preparato e aggiornato. Esperienze di ricerca e di progetti formativi che ho guidato, e da

cui sono scaturite varie pubblicazioni sul tema, mi hanno confermato sul campo che senza considerare la “dimensione umana e sociale” della cybersecurity non si va da nessuna parte.

D: Immagino che non sia affatto facile da gestire, perché richiede interventi di ben altra natura rispetto alle soluzioni tecnologiche.

R: Chi propone di sostituire l’essere umano con le più innovative tecnologie cercando di automatizzare la sicurezza, ad esempio mediante applicazioni dell’Intelligenza Artificiale, non ha capito l’essenza del problema: non esistono ricette miracolose, sia le tecnologie che gli esseri umani debbono essere gestiti. Per intenderci meglio: non sto dicendo che le soluzioni tecnologiche non siano importanti, anzi. Sto dicendo che senza la consapevolezza delle persone sui rischi in rete, sull’uso responsabile delle tecnologie e sull’importanza della protezione dei dati, quelle stesse soluzioni perdono di efficacia.

D: Sono le persone ad essere destinatarie delle conseguenze derivanti dagli attacchi cyber. E' questo un altro aspetto determinante che in qualche modo si collega al fattore umano. Cosa ci dice in proposito?

R: Un attacco informatico andato a segno causa inevitabilmente disservizi alle strutture coinvolte. Ma pensiamo a quegli attacchi che vanno a colpire infrastrutture critiche del Paese, come ad esempio ospedali o centrali elettriche. Un attacco cyber può trasformarsi in un evento critico per la sicurezza e la salute delle persone. Ci si concentra quasi esclusivamente sui danni economici che ne derivano, sulla perdita dei dati, sulla compromissione della reputazione dell’organizzazione colpita, ma c’è anche altro: la manipolazione di una macchina può mettere fisicamente a rischio la vita delle persone, se ad esempio gli hacker prendono il controllo di dispositivi medicali. Può anche accadere che venga messa a rischio la sicurezza del lavoratore mentre sta svolgendo la sua attività da remoto, a causa di un malfunzionamento dei dispositivi informatici coinvolti (ad esempio, perdita del segnale wireless). Questo connubio tra cybersecurity e rischi per la salute delle persone non viene mai adeguatamente considerato. Invece, su richiesta dell’Agenzia europea per la sicurezza e la salute sul lavoro (EU OSHA), ho recentemente realizzato un articolo di inquadramento su questi importanti aspetti https://osha.europa.eu/en/publications/i... Speriamo che il messaggio di coniugare safety e cybersecurity, mettendo al centro le persone, cominci ad essere considerato nella giusta prospettiva.

D: Quale potrebbe essere allora la prospettiva per una cybersecurity efficace?

R: Fino ad oggi si è proceduto attendendo che gli attacchi arrivassero per poi intervenire. Ma così facendo si opera sempre in emergenza. Io credo che bisogna iniziare con un’attività di diagnosi per vedere cosa non ha funzionato e perché, e poi capire cosa è necessario fare e dove bisogna intervenire. Un problema di questa portata non si affronta in un giorno. Quando sento dire che il problema della cybersecurity è legato al fatto che mancano all’appello migliaia di specialisti tecnici di quest’area non mi sembra che si stia facendo una diagnosi corretta, o quantomeno completa. Certo, anche questa carenza è

parte del problema, ma mi chiedo perché ci siamo ridotti oggi a lamentarci di queste mancanze invece di affrontarle per tempo, visto che la cybersecurity non è un argomento nuovo. Sono infatti parecchi anni che gli attacchi sono in continua crescita e riguardano ormai tutto il mondo. Qualche critica (purchè sia costruttiva) ci vuole, altrimenti si continua a perseverare con uno degli errori maggiori, vale a dire incensarsi per ciò che si andrà a fare, evitando di guardare in faccia la realtà.

D: Creare cultura della sicurezza, la vera sfida è una formazione ed una educazione alla sicurezza?

R: Decisamente questa è la vera sfida. Anche perché creare una cultura della cybersecurity significa proprio investire sulla formazione delle persone e in modo continuativo. Significa lavorare sul loro atteggiamento mentale per creare quella consapevolezza necessaria a individuare le minacce e a gestirle. Ma attenzione: non basta andare in aula con una check-list per trasformare le persone, dal momento che non sono robot telecomandati, ma esseri umani con tutta la loro complessità. Come dico spesso, un corso di formazione può instillare l'idea dell'importanza della sicurezza, cambiare i comportamenti è ben altra cosa.

D: Per creare una cultura della cybersecurity è necessario prima di tutto sensibilizzare i decisori politici che, ormai da qualche anno, hanno certamente una maggiore consapevolezza del problema…

R: La strada da percorrere è ancora lunga. Questa consapevolezza ha portato alla nascita di un'agenzia dedicata, l'ACN (Agenzia per la Cybersicurezza nazionale), un passo davvero molto importante. Ma non basta dire che c'è l'Agenzia a dover risolvere i problemi, ci vuole un investimento a livello culturale in grado di coinvolgere tutto il paese. Sono necessarie inoltre competenze diversificate, un'integrazione tra le cosiddette hard e soft skills. Altrimenti si rischia di avere una visione parziale della cybersecurity, o meglio, una visione ancora troppo "tecnica" che, come vediamo dai dati impietosi degli ultimi anni, non funziona. In poche parole, non basta preparare guerrieri cyber, serve educare cittadini digitali consapevoli. E serve farlo bene e al più presto.

D: Lei ha parlato di soft skills, tra le quali indubbiamente rientra la comunicazione: in che modo questa può essere considerata rilevante per la cybersecurity?

R: Vedo almeno tre aspetti rilevanti. Il primo è che la comunicazione rientra tra quelle competenze trasversali che permettono di lavorare e di relazionarsi in modo efficace all'interno di un'organizzazione, e quindi è prioritaria anche nella cybersecurity. Una comunicazione inadeguata sui rischi cyber, ad esempio, non favorisce la consapevolezza di tali rischi. Un altro aspetto riguarda la carente o inefficace comunicazione di crisi in caso di attacco cyber, che può produrre conseguenze disastrose. Per alcuni attacchi informatici subiti da importanti organizzazioni, la (non) comunicazione o un suo uso scoordinato rischia di produrre più danni dell'attacco stesso, perché mina prima di tutto la fiducia degli utenti. È chiaro che non vanno rivelati dettagli dell'accaduto, ma il fatto che sia

successo non può essere negato! Proprio il negare, far finta di niente o cambiare versione ogni volta che conviene non è una strategia consigliata, perché alimenta la confusione. Come dico spesso, l'incertezza è ormai parte del nostro tempo, ma va comunicata e gestita nel modo giusto. Infine, c'è un rischio relativo alla comunicazione che non va sottovalutato: il fatto che gli attacchi cyber siano ormai all'ordine del giorno e che colpiscano vittime illustri, rischia di far scemare via via la motivazione dell'utente a mettere in campo le necessarie misure di difesa, percependo tali eventi come qualcosa a fronte dei quali non c'è protezione che tenga. Un effetto di "desensibilizzazione emotiva", potremmo dire, vale a dire anestetizzante, che induce le persone ad accettare passivamente quello che accade. Un po' come avviene quando coloro ai quali dici che è importante proteggere i propri dati ti rispondono: "inutile preoccuparsi della privacy, tanto sanno già tutto di noi!"