Cybersecurity Trends

Edizione italiana, N. 4 / 2020

INTERVISTE VIP:

ELEONORA MATTIA
MAURA FRUSONE
BARBARA MASUCCI
LISA DOLCINI

GLOBAL CYBER SECURITY CENTER

ISSN 2559 - 1797 / ISSN-L 2559 - 1797

NUMERO ESCLUSIVO DONNE IN CYBER

Cybersecurity Trends

Leggi la rivista **online** quando e dove vuoi!
Puoi scegliere tra news, articoli, approfondimenti, rubriche e contenuti multimediali.

Guarda le video interviste VIP, le video pillole ed ascolta la web radio per rimanere aggiornato sulle ultime news della cybersecurity.

Nella sezione Rubriche:
Cybersecurity Pills
The Hack of the Month
Novità dalle Aziende
Offerte di Lavoro
Novità dalle Università
Eventi

www.cybertrends.it

Indice

Il Cybercrime è l'unica azienda che non ha risentito del lockdown

Autore: Carola Frediani

Il 2020 è stato un anno duro, la cybersicurezza non ha fatto, sotto questo profilo, eccezioni. La pandemia ha mostrato in modo esemplare come la cybercriminalità sia soprattutto opportunistica, capace di modellarsi sulle crisi, sugli spunti dettati dall'attualità, perfino sull'apparato normativo. Come ha scritto l'Europol nel Report annuale dello scorso ottobre (IOCTA 2020), i criminali hanno modellato le loro attività per farle aderire meglio alla narrativa pandemica, sfruttando al meglio l'incertezza della situazione e il bisogno diffuso di informazioni dell'opinione pubblica. Le ansie generate dal COVID-19 e i provvedimenti delle autorità hanno fatto da esca, sia che si trattasse di una mappa sui contagi, di un documento governativo, di una app per tracciare i contatti. I cyber criminali hanno saputo cogliere le possibilità offerte da uno smart working di massa, forzato, affrettato, praticato di continuo, non sempre ben organizzato tecnicamente, per tentare di aggirare i perimetri delle difese aziendali ed entrarci attraverso le case dei lavoratori, che operando da remoto, erano fatalmente più isolati, "atomizzati" si potrebbe dire oltre che digitalmente "stressati", quindi meno lucidi. Hanno innovato molto sui ransomware, aggiungendo alla cifratura dei dati la minaccia del leak, della fuga di informazioni, creando dei siti dove pubblicare quanto "esfiltrato", prima di attivare la cifratura. Si sono persino spinti a richiedere riscatti più elevati, a grandi player aziendali, con il preciso intento di alzare la posta il più possibile. Così se qualche anno fa parlavamo di "ransomware as a service" ora siamo già al "leak as a service", con circa una quindicina di gruppi cybercriminali a dividersi la scena.

A queste fenomenologie si aggiunge la crescita di un social engineering sempre più mirato, con in cima ai pericoli la truffa del Business Email Compromise (con varianti della truffa del CEO) in cui gli attaccanti simulano una finta identità, (fornitore, Ceo, cliente) al fine di farsi accreditare risorse economiche con svariati espedienti. Un tipo di truffa in crescita – come conferma lo stesso Report Europol- che si basa, nei casi più raffinati, su una notevole conoscenza delle organizzazioni aziendali. Alle mail tradizionali si aggiungono gli Sms e persino i messaggi Whatsapp, quando non le telefonate, tutti canali potenziali attraverso cui praticare atti illeciti. Perfino i deepfake, audio/video con voce del tutto ricreata, hanno fatto capolino fra gli strumenti utilizzati degli attaccanti.

In questo delicato contesto il settore sanitario diventa sempre più un target di attacchi a diversi livelli: dal *ransomware* cybercriminale agli *hacker* di Stato che cercano informazioni da sottrarre nei laboratori di ricerca sui vaccini.

Una cosa è certa: nessuno era pronto alla pandemia (sebbene questa tipologia di rischio fosse ben presente nell'agenda di molti Stati), né tanto meno alle conseguenze socio economiche di una emergenza di tali proporzioni. I più reattivi sono stati, purtroppo, i cybercriminali, che hanno mostrato organizzazione e idee chiare. Portiamoci nel nuovo anno questa consapevolezza, se vogliamo voltare pagina e uscire dal tunnel della crisi dentro cui ci siamo cacciati. ■

BIO

Carola Frediani è cybersecurity awareness manager per un importante rivenditore online. Ha scritto di nuove tecnologie, cultura digitale, privacy e hacking per Wired, L'Espresso, Corriere della Sera, La Stampa, Sky.it. Fra i suoi libri, #Cybercrime. Attacchi globali, conseguenze locali (Hoepli, 2019), Guerre di rete (Laterza, 2017) e Deep web. La rete oltre Google (Quintadicopertina, 2014). Nel tempo libero scrive una newsletter gratuita su temi cyber, intitolata Guerre di Rete (https://guerredirete.substack.com/)

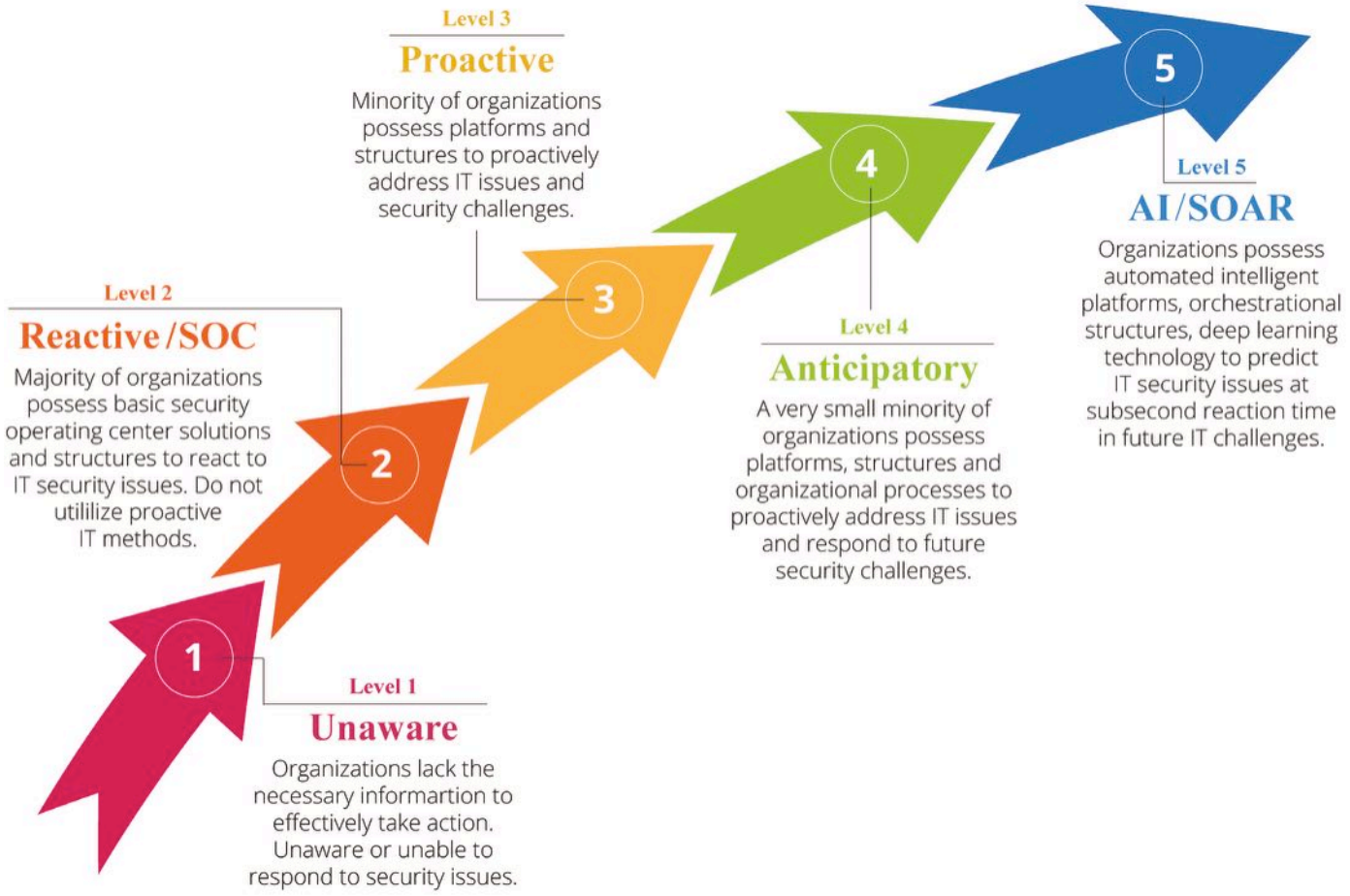
Una buona strategia di cyber security ha bisogno di tre componenti. Competenza, reattività, consapevolezza del rischio.

Intervista VIP con Marta Frusone, Head of Channel Kaspersky

Maura Frusone è un profilo brillante di donna manager, alle prese con temi di frontiera per la vita delle imprese. A lei fanno capo diverse responsabilità nel settore Marketing, sviluppo del business e nella gestione del Canale dei Partner e dei Distributori per Kaspersky, player globale leader nel campo della sicurezza informatica. Maura ha sempre sentito il fascino delle tecnologie occupandosi fin dagli "albori" di e-commerce, per poi "immergersi" nell'universo dei software gestionali. "Nel breve giro di pochi anni – spiega nell'intervista – è sorprendente come sia cambiato profondamente il ruolo della cybersecurity non solo all'interno delle aziende, ma anche per la vita dei comuni cittadini. La dinamica di un'evoluzione prepotente impone una grande reattività della tecnologia e una grande preparazione del fattore umano. Sono queste componenti che rendono il mio lavoro in Kaspersky gratificante, le sfide sono continue, così come le occasioni di misurarsi con l'innovazione, che in sé rappresentano il volto più affascinante di ogni avventura professionale".

Dott.ssa Frusone, l'evoluzione tecnologica impone un aggiornamento continuo delle strategie di intervento e di contrasto. Quali profili di rischio e quali tipologie di minacce devono essere fronteggiati con la massima priorità?

Attualmente la principale minaccia con cui devono vedersela le imprese è rappresentata dagli attacchi *ransomware*, si tratta di *malware* utilizzati per criptare i dati al fine di richiedere un riscatto. Bisogna considerare che i gruppi criminali che si nascondono dietro a questi attacchi hanno negli ultimi tempi spostato la loro attenzione dagli utenti privati alle aziende, come dimostrano molti casi che la cronaca recente ha puntualmente riferito, e che hanno interessato l'ambito sanitario. Fatti molto gravi perché entra evidentemente in gioco non solo il patrimonio di informazioni riservate e di denaro, ma anche la vita delle persone. Negli ultimi due anni i comuni attacchi ransomware sono stati sostituiti da quelli che noi abbiamo definito



ransomware 2.0. Siamo di fronte ad attacchi sempre più mirati che utilizzano un processo di estorsione che non si basa più solo sulla crittografia, ma implica anche la pubblicazione online di dati riservati. Non è solo la reputazione aziendale che viene messa a repentaglio. Se i dati pubblicati violano norme come l'HIPAA o il GDPR, è possibile che vengano intraprese anche azioni legali, con delle conseguenze che vanno oltre le perdite finanziarie.

Gli attacchi che ci sta descrivendo presentano tipologie molto sofisticate, difficili da individuare e neutralizzare. Per i security manager vita dura non crede?

Di certo lo scenario è complesso. In questa fase è molto importante che le aziende implementino tutte le buone pratiche in materia di sicurezza informatica poiché il ransomware è spesso solo la fase finale di una violazione della rete. Nel momento in cui il ransomware viene implementato, l'attaccante ha già eseguito una ricognizione della rete, identificato i dati confidenziali e provveduto all'esfiltrazione. Identificare l'attacco in una fase iniziale, prima che gli attaccanti raggiungano il loro obiettivo finale, permette, infatti, un notevole risparmio economico.

Quali azioni bisogna metter in campo per migliorare il livello di protezione degli asset?

Come prima cosa, è necessario migliorare il livello di sicurezza dei singoli endpoint, quindi assicurarsi del fatto che siano dotati di soluzioni tecnologiche in grado di individuare malware non noti, con una componente di rilevamento euristica molto evoluta ed in grado di fornire una protezione *"behavior-based"*. Queste soluzioni tecnologiche devono essere accompagnate da tecnologie EDR che permettono ai team di IT security di effettuare delle azioni immediate, almeno per differenziare gli incidenti più gravi da quelli generici. Talvolta anche l'adozione di soluzioni e tecnologie Anti-Ransomware, che sono state sviluppate negli ultimi anni contro i ransomware generici, si è rivelata molto efficace, proprio per la capacità che hanno di bloccare la possibile cifratura delle macchine. Un altro strumento di difesa fondamentale è la preparazione. È importante verificare

di non avere sistemi vulnerabili esposti, o sistemi con credenziali deboli. Altro aspetto che non va trascurato: bisogna effettuare attività di *vulnerability assessment* e di *penetration testing* periodici, per cercare di capire quelle che sono le criticità delle aziende e porvi rimedio. Risulta, inoltre, molto utile, una pianificazione attenta per quanto riguarda le azioni di *incident response*. Nel caso, infatti, di incidenti informatici di una certa gravità, avere un preciso piano di risposta può fare la differenza, rivelandosi come un fattore decisivo per la riduzione dei danni.

BIO

In Kaspersky dal 2014 ha ricoperto diversi ruoli prima come Business Development per le vendite online, successivamente come Head of Marketing con riconoscimenti nel 2018 come Miglior Marketing Manager nel mondo dell'ICT e per la migliore strategia di Marketing. Dal 2019 ricopre il ruolo di Head of Channel e ha la responsabilità di guidare l'ecosistema dei Partner e Distributori sul territorio italiano e Malta, oltre che sviluppare i modelli a subscription con le Telco. In passato si è occupata di sviluppo prodotto, trade marketing per il segmento dei Large Account e SMB, gestione di canali di vendita diretta e indiretta nell'ambito del mercato IT, Digital media e Office products per il Gruppo Buffetti, Seat Pagine Gialle e Tele+ Digitale. Ha conseguito l'Executive MBA e ha un master di specializzazione sull'E-commerce.

Qual è, a suo giudizio, il livello di preparazione delle aziende in un ambito come la sicurezza divenuto ormai decisivo per lo sviluppo del business?

La cultura della cybersecurity è cresciuta negli ultimi due anni, insieme alla consapevolezza dei rischi e delle perdite che un'azienda può subire a fronte di un attacco cyber. Il livello di competenza in questo ambito si mantiene, però, eterogeneo, spesso correlato alle dimensioni dell'azienda e alla crucialità del dato che gestiscono. Le aziende di fascia Enterprise hanno dei team interni di esperti di sicurezza che nella maggior parte dei casi usano degli strumenti di threat intelligence molto evoluti che hanno lo scopo d'individuare le minacce al primo stadio e analizzarle. Diverso il caso delle PMI, che non dispongono di questa competenza al loro interno, si affidano a strumenti automatizzati che hanno una detection evoluta e permettono di gestire eventuali incidenti. ■

Giovani donne nella cyber security, sfida che non possiamo perdere

Autore: Elena Mena Agresti

Il 2020 sarà ricordato come l'anno della pandemia e del maggiore utilizzo delle tecnologie da parte dell'intera popolazione soprattutto in Italia rimasta negli ultimi anni fanalino di coda dell'Europa nell'utilizzo del digitale. L'Italia infatti risulta nella 25° posizione su 28 Stati nell'Indice di Digitalizzazione dell'Economia e della Società (DESI 2020) della Commissione europea.

Se è vero che la pandemia ci ha colti di sorpresa e ha avuto, e continua ad avere purtroppo risvolti drammatici, al tempo stesso ci ha costretti ad accelerare alcuni processi che seppur avviati da tempo tardavano a prendere piede come la transizione al digitale. Basti pensare all'utilizzo massiccio dello smart working, l'erogazione di servizi pubblici e privati online, la didattica a distanza. Volenti o nolenti, siamo stati tutti costretti senza distinzione di età, genere, impiego, grado di istruzione dai più piccoli come i bambini ai più grandi, a un utilizzo maggiore del digitale. Sicuramente con tutte le limitazioni del caso, con l'utilizzo di strumenti e processi in molti casi forniti e definiti in emergenza e da rivedere e raffinare, siamo arrivati in pochissimi mesi dove non siamo riusciti in anni.

Mater artium necessitas, è un antico detto latino, specchio della saggezza popolare. Tradotto significa che la necessità è la madre delle abilità. Così è stato, nella emergenza riusciamo, infatti, a fare cose inaspettate. Ogni famiglia, ogni insegnante, ogni studente, ogni dipendete pubblico o privato,

BIO

Laureata in Ingegneria Aerospaziale presso l'Università La Sapienza di Roma, opera per la Fondazione GCSEC e il CERT di Poste Italiane. Esperta di compliance, standard internazionali, governance dell'information security, gestione dei rischi, security audit, formazione eawareness, ha partecipato a tavoli tecnici internazionali dell'ISO e OCSE per la revisione e lo sviluppo di standard e linee guida di information security.
È stata responsabile scientifico di tre corsi di master in cyber security istituiti nel 2015-2016 con l'Università della Calabria e Poste Italiane eattualmente collabora con numerose università italiane in corsi di cyber security. Ha lavorato presso diverse società di consulenza, tra cui in Booz & Company nella practice Risk, Resilience and Assurance. Membro di Europrivacy e della Oracle Community for Security, è Lead Auditor ISO/IEC 27001:2013 e ISO 22301 e ha conseguito le certificazioni STAR Auditor e ISIPM Project Management.

durante il lockdown ha dovuto continuare a svolgere le proprie attività di studio o lavorative da casa con un computer, un tablet o uno smartphone sviluppando e raffinando competenze informatiche e digitali.

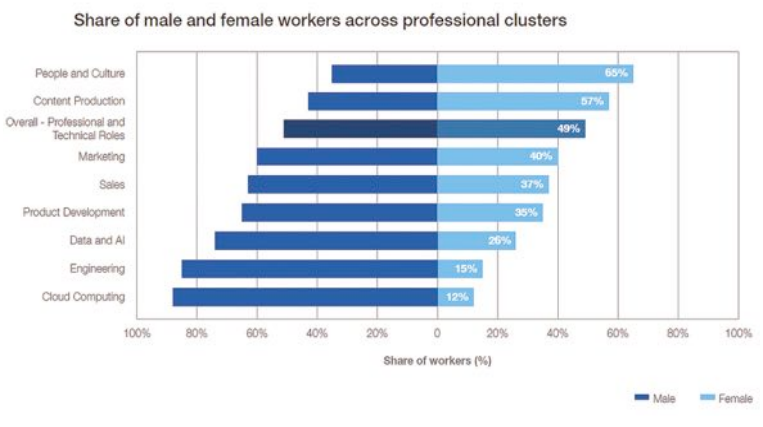
Nonostante l'uso molto più pervasivo del digitale, ancora oggi i giovani sembrano essere poco interessati agli aspetti della cyber security e inconsapevoli delle insidie e dei rischi associati. Con troppa superficialità, ingenuità o mancanza di consapevolezza **agiscono online senza considerare le insidie in esso presenti**. Molte ricerche fanno emergere lo scarso utilizzo di strumenti per tutelare l'identità digitale, i dati personali e, si potrebbe dire più in generale, la vita stessa che si svolge in un orizzonte "virtuale".

Consapevolezza e formazione: asset cruciali della società digitale

Le giovani donne ancor più degli uomini sembrano essere distanti da queste tematiche sia in termini di utilizzo consapevole delle tecnologie sia di interesse a una possibile carriera professionale in questo ambito. Ma come mai? Alla radice esiste un problema culturale. **La cyber security viene ancora percepita come un argomento per "tecnici" per "hacker" per "nerd"** e non alla portata di tutti, pertanto perché preoccuparsi di qualcosa per la quale non è possibile fare nulla? Al tempo stesso, i giovani non ritengono di essere un potenziale bersaglio e che proteggere i propri dati e le proprie informazioni non sia così importante, non c'è nulla da nascondere. **Pigri e disinteressati, si accontentato di essere soprattutto utilizzatori, magari abili, degli strumenti tecnologici senza di fatto conoscerli veramente**. Così incuranti dei rischi si "gettano nella rete", senza sapere che minacce sempre più sofisticate sono finalizzate a sfruttare le tante vulnerabilità dei sistemi digitali, che i comportamenti incauti amplificano in misura preoccupante.

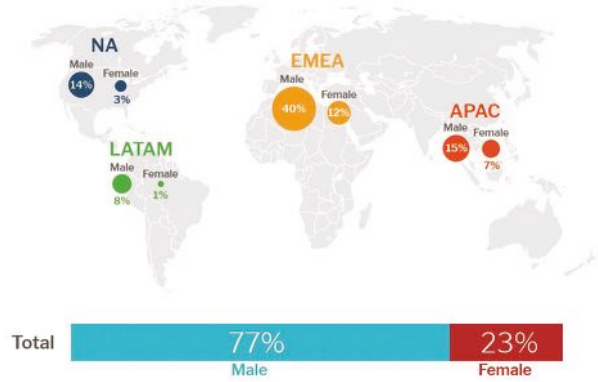
Il gender gap: un'emergenza globale

Percepita come materia per tecnici diventa molto distante per le donne ancora restie ad intraprendere una carriera nel settore della cybersecurity. Secondo il Global Gender Gap Report 2020 del World Economic Forum, il cosiddetto gender gap è un problema mondiale che si nota particolarmente nel settore dell'informatica e delle aree STEM (Scienza, Tecnologia, Ingegneria e Matematica). Le donne rappresentano solo **il 19% degli specialisti di sicurezza informatica**, il 12% degli Ingegneri dell'automazione, 13% degli sviluppatori Android, 18% degli ingegneri di robotica. I settori del Marketing, vendite e sviluppo del prodotto sono invece più vicini alla parità di genere, con le donne che rappresentano rispettivamente il 40%, 37% e 35% della forza lavoro.



Global Gender Gap Report 2020 – World Economic Forum

Il gap di genere deriva da diversi fattori. Di sicuro stereotipi e preconcetti culturali sul ruolo della donna nelle società e nel mondo del lavoro oltre che condizioni di lavoro poco attraenti per le donne e percorsi di carriera poco chiari nella sicurezza informatica spesso poco sfidanti. Risulta, infatti, da un'indagine internazionale di Kaspersky del 2019 (Cybersecurity Through the CISO's Eyes) che solo il 23% dei manager della cyber security (CISO) di grandi aziende è donna mentre il 77% sono uomini.



Cybersecurity Through the CISO's Eyes, Kaspersky 2019

Cosa possiamo fare per avvicinare le giovani donne al mondo della cybersecurity?

Diffondere l'interesse e la passione per l'informatica e la cyber security tra le giovanissime al fine di modificare le loro abitudini nell'utilizzo del digitale, le scelte scolastiche e universitarie. Renderle partecipi in prima persona con concorsi, competizioni (es. CyberChallenge), giochi a squadre. Per essere efficaci è necessario parlare il loro linguaggio spesso diretto, per immagini, che riassume concetti in un tweet, un video di 60 secondi.

Stimolare un cambiamento culturale della società partendo dalla scuola, dalle famiglie ma con un **importante coinvolgimento delle istituzioni e delle aziende che potrebbero attuare politiche e programmi** specifici di sensibilizzazione per eliminare alcuni stereotipi e preconcetti culturali e trasferire quelli che sono i comportamenti corretti da attuare nel digitale possibilmente in modo divertente. Il più grande problema risiede nell'incapacità di suscitare interesse ed entusiasmo. La cyber security è percepita ancora da molti come un argomento serio, pesante e spesso noioso quando invece potrebbe risultare intuitivo e persino divertente.

I linguaggi innovativi "motori" del cambiamento

In questo senso, sono molte le attività che possono essere organizzate. Bisogna considerare che l'utente medio preferisce scorrere velocemente titoli e contenuti più che leggere, non ama ascoltare a lungo e con attenzione. Diventa perciò di importanza cruciale l'utilizzazione di linguaggi **multimediali come video pillole, tutorial, web serie con scopi divulgativi ed educativi e quiz online, tornei a premi o gaming per creare interesse e coinvolgimento anche negli utenti più giovani, con risultati importanti anche sul fronte dell'apprendimento**. Per incoraggiare i giovani, e in particolare le donne, ad avvicinarsi ad una carriera nel mondo della cyber security sarebbe, inoltre, opportuno **creare dei modelli positivi da seguire** attraverso momenti di confronto sin dalle scuole medie e superiori. In questa ottica si rileverebbero molto utili gli incontri presso le scuole con professioniste del settore che possono contagiare con il loro entusiasmo. Le storie di successo sono un fattore di stimolo per gli studenti, allo stesso modo raccontare le difficoltà superate serve a temprare lo spirito e a forgiare la volontà, contribuendo a quel cambiamento culturale che è poi la chiave per rinnovare l'immagine e il ruolo delle donne nel settore strategico della cyber security.

La responsabilità di istituzioni e aziende

Le aziende potrebbero incoraggiare più donne a intraprendere percorsi di carriera nel settore della Cyber Security, attraverso **iniziative di orientamento professionale** presso le scuole medie e superiori, di ***tutoring*** **e** ***mentoring*** **a supporto delle giovani donne**, e anche attraverso la promozione di **Cyber Security competition, offrendo pari opportunità per consentire anche alle donne di raggiungere ruoli di leadership**. In diverse realtà sono stati definiti dei programmi a livello nazionale per attrarre studenti nella sicurezza informatica fin dalla tenera età e progettate campagne specifiche dedicate al mondo femminile.

La **CyberFirst Girls Competition**, (per citare un esempio interessante) è un'iniziativa dell'agenzia governativa inglese NCSC (National Cyber Security Centre) rivolta alle ragazze tra i 13 e i 15 anni che offre un ambiente divertente e stimolante per ispirare la prossima generazione di giovani donne a prendere in considerazione una carriera nella sicurezza informatica.

CyberFirst Girls Competition è una competizione a squadre, ognuna composta da 4 studentesse, che si sfidano per risolvere una serie di enigmi legati alla sicurezza informatica. Dal 2017, 36.000 ragazze hanno preso parte al programma e il 98% delle partecipanti dello scorso anno ha dichiarato di voler saperne di più sulla sicurezza informatica. La finale della CyberFirst Girls Competition del 2020 ha visto le migliori otto squadre impegnate nel proteggere i Giochi Olimpici dagli attacchi informatici. La King Edward's School Bath, risultata vincitrice, ha ricevuto laptop per la scuola e un assegno di 1.000 sterline da spendere in apparecchiature IT. Tutte le ragazze che hanno raggiunto la finale sono state invitate a un tour di 10 Downing Street, la residenza del Primo Ministro nonché sede del Governo Regno Unito. Risulta decisivo, per attuare programmi di questo genere, il coinvolgimento delle istituzioni, oltre che la definizione di un budget dedicato allo sviluppo di skill e competenze in Cyber Security.

La "rete" delle iniziative

Numerose, inoltre, le iniziative nate a livello nazionale ed internazionale dedicate alle donne nel mondo della cyber security. I principali obiettivi si focalizzano: nella promozione del ruolo e della visibilità delle donne, nella definizione degli strumenti, nell'affinamento delle conoscenze che possono facilitare l'inserimento nel mondo del valoro, nella messa in campo di programmi di formazione, tutoraggio e mentoring che andranno sviluppati per tutto l'arco della carriera professionale.

Le attività previste spaziano da corsi di formazione specifici, a programmi educativi per le bambine già dai 7 anni, **conferenze, seminari, meeting virtuali, giornate dedicate al recruiting, momenti ludici e virtuali, competizioni Capture The Flag, cyber competition.**

Nella tabella che segue sono raccolte solo alcune delle numerose iniziative nate nel panorama internazionale.

INIZIATIVA	DESCRIZIONE
WICS Spain (SPAGNA)	Iniziativa nata per promuovere e rendere visibile il ruolo delle donne nella cybersecurity in Spagna, così come la diversità di genere nel settore. Mira a costruire insieme un mondo digitale più sicuro e più inclusivo.
Australian Women in Security Network (ASWN) (AUSTRALIA)	Una rete aperta di persone che mira a far crescere il numero di donne nella comunità della sicurezza. Mettono in contatto le donne del settore e coloro che cercano di entrare nel campo con **gli strumenti, le conoscenze, la rete e le piattaforme necessarie per creare fiducia e interesse.**
Code Like A Girl (GLABALE)	Organizzazione internazionale nata per avvicinare le donne al mondo della **tecnologia e dello sviluppo del codice.**
SANS Women's Immersion Academy (USA)	Per ridurre il gap di genere, SANS Institute ha creato la SANS CyberTalent Immersion Academy, un programma intensivo e accelerato di formazione di livello mondiale SANS e certificazioni GIAC per un inserimento rapido ed efficace nella sicurezza informatica. La partecipazione all'Academy non comporta alcun costo coperto per il 100% da borse di studio.

INIZIATIVA	DESCRIZIONE
CSWI, Cyber Security Women's Italy (ITALIA)	Gruppo di Lavoro dell'AIPSI, che intende raggruppare tutte le donne attive professionalmente, in qualsiasi ruolo e a qualsiasi livello, nella sicurezza digitale. Una prima iniziativa in programma è **stata indagine online sul lavoro femminile nella cybersecurity in Italia**.
WIIS Italy (Women in International Security) (ITALIA)	Un network globale dedicato a **promuovere la leadership e lo sviluppo professionale delle donne** nel campo della pace e della sicurezza internazionali.
Women for security (ITALIA)	Community tutta al femminile impegnata nell'accrescere il valore del ruolo femminile e, di conseguenza, provare a **chiudere il gender gap nell'ambito della cybersecurity italiana**.
WoSEC Women of Cybersecurity (GLOABALE)	Una community per le donne interessate alla cybersecurity. I vari capitoli di WoSEC si incontrano sia virtualmente che di persona nelle città di tutto il mondo. Le attività spaziano da **conferenze a seminari, brunch e altri incontri sociali**.
Women's Society of Cyberjutsu (WSC) (USA)	Community nazionale non profit volta a far progredire le donne nelle carriere nel settore della sicurezza informatica fornendo programmi e partenariati che promuovono la **formazione pratica, networking, istruzione, tutoraggio, condivisione delle risorse e molte altre opportunità professionali**.
WiCyS (Women in CyberSecurity) (GLOBALE)	Organizzazione senza scopo di lucro, con partner internazionali di rilievo, che riunisce le donne nella sicurezza informatica del mondo accademico, della ricerca e dell'industria per condividere conoscenze, esperienze, networking e tutoraggio. WiCyS aiuta a costruire una forte forza lavoro per la sicurezza informatica con l'uguaglianza di genere facilitando il reclutamento, la conservazione e l'avanzamento delle donne sul campo. WiCyS offre **tutoraggio, apprendimento, networking e sviluppo professionale alle donne** in tutte le fasi della loro carriera nel settore della sicurezza informatica. Promuove **Virtual Cybersecurity Competition/Game** per rafforzare le competenze.
ECSO's Women4Cyber (EUROPA)	Fondazione privata europea senza scopo di lucro con l'obiettivo di promuovere, incoraggiare e sostenere la partecipazione delle donne nel campo della sicurezza informatica. Intende incoraggiare e promuovere la formazione, il miglioramento delle competenze e la riqualificazione di ragazze e donne verso l'istruzione e le professioni in materia di sicurezza informatica.
LATAM Women in Cybersecurity (WomCy) (AMERICA LATINA)	Un'organizzazione senza scopo di lucro - composta da donne - con un focus sullo sviluppo della Cybersecurity che offre consulenza sulla sicurezza informatica per i segmenti Education, Corporate e Foundations. Per guidare le ragazze o giovani donne verso il mondo della cybersecurity ha istituito **programmi formativi per le scuole (dedicati alle ragazze dai 7 ai 17 anni) e le università**.
She Secures (AFRICA)	Organizzazione nata nel Lagos e Nigeria **per sensibilizzare sui temi della cybersecurity e guidare le donne interessate a far parte del settore così come creare Cyber Savvy Kids in Africa**. L'organizzazione intende creare una rete educativa, costruire skills, garantire mentorship e intership, opportunità di lavoro e cyber security Hackathons.

Le iniziative riassunte sono nate con l'obiettivo di colmare il divario di genere dei professionisti della sicurezza informatica. La differenza di genere favorisce il confronto e un approccio vario alla risoluzione dei problemi. Ricordiamoci che la promozione del confronto e della diversità sono alla base della crescita sociale, della competitività, dell'innovazione, ragionamento ancora più valido in settori per definizione multidisciplinari come la cybersecurity.

Occorre colmare la disparità di genere e ripensare a 360° il ruolo della donna nella cyber security non più rilegato ai soli aspetti tecnici od operativi. Come definito dalla organizzazione *Code like a Girl* "la tecnologia che costruiamo oggi determina il mondo in cui vivremo domani. Ma se quel mondo viene costruito sotto la guida di solo una piccola parte della nostra comunità, che tipo di mondo avremo?" Favorire la parità di genere significa anche adottare valori come il rispetto, l'inclusione, la diversità, l'umanità, le pari opportunità. Stiamo vivendo la quarta rivoluzione industriale. Non possiamo permetterci di perdere la sfida della parità di genere, che va affrontata nella famiglia, nella scuola, nelle istituzioni, nelle aziende, nel mondo della ricerca.

Non ci può essere ambito della vita sociale escluso, se vogliamo fare del mondo in cui viviamo un posto migliore, aperto ai valori del rispetto e dell'inclusione. ■

Cybersecurity awareness nelle organizzazioni: perché è necessaria

Autore: Alessandra Rose

Risulta sempre più evidente che la minaccia informatica maggiormente insidiosa per le organizzazioni, consista negli attacchi che sfruttano l'ingenuità e l'inadeguata preparazione in tale ambito, dei dipendenti. Molto più degli attacchi diretti alla rete. Il fattore umano, attraverso gli aspetti emotivi e i fattori cognitivi, infatti, può influenzare pratiche e comportamenti dell'individuo nel cyberspazio rendendolo vulnerabile e, seppur in maniera non intenzionale, una minaccia per l'organizzazione.

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.

Per comprendere meglio l'esigenza di fare sensibilizzazione sulla cybersecurity, 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[1]. 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, gestualità, postura) e quello testuale (i contenuti in forma scritta).

Questi "segnali" agevolano l'interpretazione del contenuto della comunicazione, consentendo alle persone di determinare le motivazioni e

BIO

Da sempre interessata alle dinamiche socio politiche ed appassionata di studi sul comportamento umano, si è prima laureata in Scienze Politiche e Relazioni Internazionali con una tesi sulle politiche di formazione in Poste Italiane, poi iscritta al corso di laurea in Psicologia e Salute a La Sapienza Università di Roma, dove tuttora studia e collabora a ricerche e studi promossi dal Dipartimento di Psicologia Dinamica e Clinica. Specialista in Sicurezza delle Informazioni ed esperta in Media e Comunicazione, lavora in Poste Italiane dal 2002. Il suo percorso nel campo dell'Information Security inizia nel 2014 con un'esperienza nel Centro Servizi Privacy, e prosegue negli anni successivi tra formazione e collaborazioni a progetti di ricerca. Attualmente, oltre alla ricerca, si occupa della creazione di contenuti web e social, nonché dell'organizzazione e della gestione di workshop ed eventi presso il Distretto Cyber Security di Poste Italiane.

le intenzioni dei partner relazionali, così come la loro affidabilità e il loro stato emotivo. Di conseguenza, lo scambio di segnali durante l'interazione sociale influenza la percezione della presenza sociale[2] sia in ambiente offline che online. Appare ovvio che l'interazione face to face garantisca una presenza sociale più elevata rispetto a quella mediata dalla tecnologia, proprio grazie alla maggiore disponibilità di segnali verbali e visivi e quindi alla più agevole trasmissione di vicinanza ed immediatezza. Al contrario, la presenza sociale risulta di intensità inferiore nell'interazione online, in virtù del fatto che il canale testuale è meno efficace nel consolidare immediatezza e connessione.

Vulnerabilità dell'utente: elementi psicologici

Non possiamo sottovalutare la disinibizione e il potere che scaturiscono dall'anonimato e quanto questi condizionino la comunicazione e di conseguenza la sicurezza.

L'anonimato è percepito grazie all'assenza dei "segnali" di comunicazione e si struttura su diversi livelli, in base all'utilizzo di accorgimenti come pseudonimi, tool per nascondere l'identità e controllo delle impostazioni sulla privacy. In questo modo, a livello individuale, l'anonimato può portare a ridurre l'inibizione e favorire la messa in atto di comportamenti che offline sarebbero ritenuti negativi o addirittura sconvenienti. Questo perché gli individui hanno la sensazione di non essere identificati né ritenuti responsabili delle loro azioni.

La disinibizione online, soprattutto se combinata con l'intensità di forti emozioni e bisogni di base, può influenzare il comportamento di una persona e favorire una forte polarizzazione di gruppo[3] rispetto all'interazione F2F, fino a far aumentare i comportamenti aggressivi e offensivi (commenti e messaggi lesivi, molestie, bullismo, incitamento all'odio raziale o religioso). Essa si combina con gli elementi variabili della personalità, manifestandosi in molti casi come una lieve deviazione dal comportamento consueto, o nei casi più gravi, come veri e propri cambiamenti comportamentali.

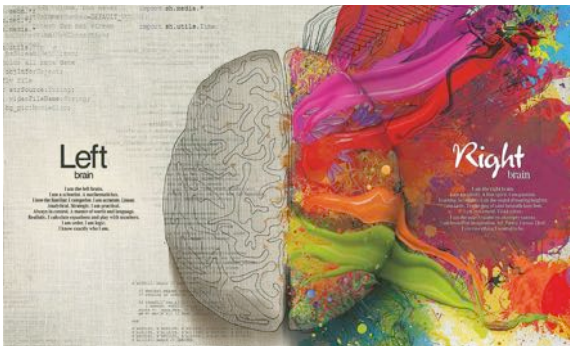
Come possiamo intuire, quindi, l'anonimato online, in particolare se associato alla disinibizione, può anche spingere gli utenti ad accedere a contenuti illegali (come nel caso di materiale pedopornografico), a scaricare file multimediali che violano il copyright, a visitare siti malevoli, o addirittura a diventare membri di organizzazioni criminali o sette online. Ecco come la stessa "ombra" che protegge l'attaccante, rende debole la vittima: quando gli utenti sentono di potersi nascondere nella rete senza esporsi con la propria identità, avvertono una sensazione di comfort e protezione che induce un abbassamento delle difese e contemporaneamente aumenta le possibilità di essere manipolati, ingannati e truffati.

Vediamo nello specifico quali sono i fattori, esogeni ed endogeni, su cui fanno leva le tecniche di manipolazione in ambiente cyber.

Tra i fattori esogeni, troviamo la distanza fisica e la dimensione temporale:

La **spersonalizzazione.** Essa deriva dalla possibilità di comportarsi in maniera differente rispetto alla vita reale, grazie alla condizione di *distanza fisica* dagli altri utenti. La cyber-psicologia vede il cyberspazio come un'estensione del mondo psichico dell'individuo. La condizione di mancanza di indicatori fisici che si verifica quando ci si trova dietro ad uno schermo, dà all'utente la sensazione di essere invisibile ed anonimo, la percezione del pieno controllo della comunicazione, abbatte l'imbarazzo e mitiga la trasmissione delle reazioni emotive. Questo livello di disinibizione lo induce ad abbassare gli automatismi difensivi, e spesso lo induce anche a sottovalutare situazioni di pericolo o potenziali truffe;

La **velocità.** È una caratteristica dei processi decisionali in rete. Nel mentre nella vita reale per la maggior parte delle truffe tradizionali sono necessarie tempistiche dilatate, su internet si tratta spesso dell'istante di un click, che per la sua durata concede molto meno tempo per attivare le aree del cervello che permettono un'analisi precisa sulle azioni che si stanno compiendo.



Tra i fattori endogeni, cioè quelli legati intrinsecamente alla psicologia del soggetto[4], abbiamo le caratteristiche temperamentali e le organizzazioni di personalità, e gli stili relazionali.

L'**impulsività**, caratteristica temperamentale, fornisce una risposta rapida e irrazionale del nostro comportamento che influenza enormemente le capacità di valutazione di una situazione ed il corretto svolgimento del processo decisionale, inibendo talvolta il riconoscimento immediato di una minaccia ed aumentando dunque la probabilità che l'utente cada in una trappola cyber.

Gli **schemi motivazionali interpersonali**[5], cioè un sistema cerebrale e mentale complesso che regola il comportamento e le emozioni in vista di una meta ben definita[6]. Fondandosi su disposizioni innate, selezionate nel corso dei processi evoluzionistici, tali propensioni ad agire verso obiettivi specifici, regolano le forme di interazione fra un soggetto e l'ambiente. Nel caso della cybersecurity, gli schemi motivazionali che potrebbero consentire più facilmente un attacco sono:

a. La paura

Si tratta dell'emozione direttamente collegata alla sopravvivenza. Essa attiva immediatamente il bisogno di aiuto in quanto genera preoccupazione, malessere e disagio, insieme alla sensazione di urgenza, che spinge l'utente a trovare una soluzione in fretta;

b. L'altruismo

Il senso atavico di appartenenza ad una tribù conferisce all'uomo la definizione di "essere sociale".

Ciò implica la collaborazione e l'assistenza reciproca, il "mutuo soccorso", che traslato in epoca moderna può essere definito con il concetto più generico di bontà, che altro non è che una forma di accudimento innata che ci spinge ad aiutare gli altri quando capiamo che hanno estremamente bisogno di noi;

c. La competizione

In natura, la legge del più forte stabilisce attraverso la lotta fisica il rango, che garantisce qualità e quantità di cibo superiori, e il rispetto da parte del gruppo. Fornire un obiettivo accattivante o addirittura agonistico, che alluda alla predominanza rispetto agli altri, crea un'occasione di riuscita per l'attaccante;

d. Il sesso

Il bisogno sentimentale o meramente fisiologico di soddisfare i bisogni legati a quest'area, è probabilmente allo stato attuale la vulnerabilità più sfruttabile da parte dei criminali informatici. Ciò avviene perché l'esperienza emotiva del desiderio e del piacere erotico (spinta dalla necessità del proseguimento della specie) è atavica. E maggiori sono gli ostacoli nel raggiungimento dell'oggetto del desiderio, maggiori sono le emozioni che scaturiscono dal sistema motivazionale sessuale come per esempio gelosia, paura del rifiuto, paura dell'abbandono, pudore. Ai giorni nostri, il pudore che ci consente di convivere in un sistema di società "civile", contemporaneamente regola e reprime il sistema sessuale dell'individuo. Pudore che diminuisce consistentemente quando le circostanze ambientali lo consentono, per esempio le condizioni di intimità di un luogo appartato o, la spersonalizzazione[7] in seguito ad una riduzione delle percezioni sensoriali come quando l'utente si trova ad interagire con un device che fisicamente lascia tutto il mondo al di fuori, ma gli consente al tempo stesso di esplorarlo ed attraversarlo.

Naturalmente, questi parametri si alterano in presenza di spinte emotive come ad esempio l'aggressività, l'ossessione, la dipendenza, che scaturiscono da disagi e disturbi psichici.

Una dimostrazione di come vengano sfruttate queste vulnerabilità psicologiche dell'individuo possono essere le tecniche di phishing. Le e-mail di phishing trasmettono spesso un senso di urgenza su cui l'attaccante fa leva per spingere l'utente a fare clic su un collegamento dannoso e a fornire informazioni personali o private. Quando le persone sono troppo impegnate e troppo distratte per agire in sicurezza, un modo per sferrare l'attacco potrebbe essere quello di sfruttare i loro «processi automatici» come le loro abitudini o le azioni che compiono senza pensare davvero. L'ambito aziendale, ad esempio, è preso di mira dalla Business Email Compromise (BEC), una truffa sofisticata le cui vittime sono quasi sempre dipendenti nel settore economico-finanziario che effettuano pagamenti tramite bonifico bancario. Spesso questa truffa viene portata a termine grazie alla compromissione di un account di posta elettronica aziendale, che può avvenire o attraverso un'intrusione prettamente informatica, o per mezzo di tecniche di *social engineering*.

Quest'ultimo, infatti, si articola in diverse fasi di attacco, una delle quali consiste proprio nello sfruttamento delle caratteristiche emotive dell'individuo. Gli attaccanti, utilizzando persuasione ed empatia, instaurano un rapporto con la vittima allo scopo di conquistare la sua fiducia per carpire le informazioni desiderate (password, numero di conto corrente, nomi, dati riservati, etc). Quella che si mette in atto è una vera e propria manipolazione, che si avvale oltre che di notevoli competenze informatiche, anche di abilità e conoscenze pluridisciplinari che spaziano dalla psicologia cognitiva all'antropologia, dalla psicologia sociale alla sociologia dei gruppi.

Nelle Organizzazioni, la carenza di sensibilità e di consapevolezza dei vertici aziendali *(awareness)* e la mancanza di adeguate sessioni o training di formazione per i dipendenti, possono aumentare notevolmente il grado di esposizione alle minacce cyber, in particolare agli attacchi che si avvalgono delle tecniche di ingegneria sociale e *human hacking*. Gli impatti negativi generati possono essere innumerevoli e di grossa portata: perdite economiche, danni relativi alla Riservatezza, Integrità, Disponibilità dei dati, danni reputazionali, perdita di continuità operativa (Business Continuity), e tanti altri. Sono infatti centinaia le aziende colpite ogni giorno da frodi finanziarie e milioni le mail contraffatte che inducono a compiere azioni dannose. Ed è realmente molto complesso difendersi da attacchi che sfruttano le caratteristiche psicologiche e gli elementi emotivi delle persone, come la fiducia negli altri, la reciprocità, la dissonanza cognitiva[8], la scarsità di conoscenza o anche il disagio nel disattendere un compito.

Non esistono misure di sicurezza valide in assoluto ma è possibile fare leva sul comportamento per mitigare il rischio. Come? Per quanto riguarda la dimensione organizzativa, la contromisura più efficace resta sempre la formazione del personale, fornire gli strumenti adeguati a riconoscere gli schemi di attacco per poterli contrastare. ■

1 K. M. Christopherson, The positive and negative implications of anonymity in Internet social interactions: "On the Internet, nobody knows you're a dog". Computers in Human Behavior 23 (2007), pp. 3038–3056.
2 Def.: il senso divicinanza eimmediatezza che si sviluppa mentre gli individui interagisconoe comunicano. È il "collante sociale"che consente lo sviluppo di intimità e fiducia, due aspetti chiave della formazione e del mantenimento delle relazioni sociali (come quelle affettive, familiari, sentimentali e professionali)
3 Def.: In Psicologia delle Organizzazioni, si parla di polarizzazione nell'ambito delle discussioni di gruppo, quando si verifica l'allontanamento dalle posizioni mediane a favore di uno dei due poli estremi, che di regola è il polo cui si tende per i valori diffusi nel gruppo.
4 Ci si riferisce ad un soggetto stabile ed equilibrato, in condizione di salute mentale.
5 Liotti G., Monticelli F., I sistemi motivazionali nel dialogo clinico,Raffaello Cortina Editore, Milano, 2008
6 Ivaldi A., Il trattamento dei disturbi dissociativi e di personalità. Teoria e clinica del modello relazionale fondato sui sistemi motivazionali, Franco Angeli Edizioni, Milano, 2016
7 Cfr. pag 2
8 Psic.: la condizione di tensione o disagio avvertita a causa del manifestarsi di due idee opposte e incompatibili

Sfatiamo certi miti: le donne? Più brave anche nell'Information Technology

Intervista VIP con Barbara Masucci Professore Associato di Informatica, Dipartimento di Informatica dell'Università di Salerno.

UNIVERSITÀ DEGLI STUDI DI SALERNO

Professoressa, "Programmazione Sicura" ***oltre ad essere la denominazione del corso che la vede impegnata presso l'Università di Salerno è un tema cruciale per lo sviluppo dell'Information Society. Può tratteggiare in sintesi i contenuti formativi di questa iniziativa?***

Il corso di *"Programmazione Sicura"* è stato introdotto tra gli insegnamenti offerti dal Corso di Laurea Magistrale in Informatica presso l'Università di Salerno nell'a. a. 2017-2018 ed è giunto alla sua quarta edizione. Dapprima proposto tra gli insegnamenti a scelta offerti dall'indirizzo "Sicurezza Informatica" della Laurea Magistrale, negli anni successivi è stato inserito anche negli indirizzi *"Sistemi Informatici e Tecnologie del Software"* e *"Data Science e Machine Learning"*, coinvolgendo un numero sempre maggiore di studenti.

L'insegnamento introduce i concetti fondamentali della Programmazione Sicura ed approfondisce le metodologie e le tecniche necessarie per la valutazione della sicurezza di un programma. L'obiettivo dell'insegnamento è quello di fornire agli studenti un insieme di linee guida per scrivere programmi sicuri; tali linee guida sono sviluppate come un insieme di lezioni apprese da casi di studio e riguardano vari linguaggi di programmazione e di scripting e diversi sistemi operativi, con particolare enfasi sui sistemi Unix-like. In particolare, il corso offre agli studenti la possibilità di studiare in profondità alcune tipologie di vulnerabilità, allo scopo di comprendere sotto quali ipotesi esse si verificano, che conseguenze determinano e quali sono le soluzioni più idonee a prevenirle.

Quali sono le ragioni del successo crescente, registrato in questi anni?

La forte connotazione pratica della metodologia di insegnamento, mirata a stimolare la curiosità degli studenti mediante la proposta di *"sfide"* che essi

devono tentare di risolvere, è probabilmente una delle ragioni principali per cui un numero sempre maggiore di studenti, anche iscritti ad indirizzi non necessariamente legati alla Sicurezza Informatica, ha deciso di inserire l'insegnamento di *"Programmazione Sicura"* nel proprio Piano di Studi.

Il corso di* "Programmazione Sicura" *si fonda su un metodo innovativo.* CTF *è l'acronimo che racchiude la sfida dal profilo forse più innovativo. Possiamo spiegare di che cosa si tratta?

CTF è l'acronimo di *"Capture The Flag"* (cattura la bandierina) e viene utilizzato, a livello internazionale, per indicare una categoria di competizioni di Sicurezza Informatica in cui lo studente è messo alla prova, allo scopo di raggiungere uno specifico obiettivo (la bandierina) che indica che la *sfida* è stata vinta. Durante il corso di *"Programmazione Sicura"*, vengono proposte *sfide CTF* relative a diverse tematiche, quali l'iniezione locale e remota di codice arbitrario e l'alterazione della memoria, mettendo a disposizione degli studenti diverse macchine virtuali su cui fare prove in piena autonomia e libertà.

La prima categoria di sfide *(iniezione locale)* presuppone che gli studenti abbiano a disposizione una shell sulla macchina vittima per l'immissione diretta di comandi: la sfida si conclude con la cattura della bandierina nel momento in cui gli studenti riescono ad eseguire un certo programma, per il quale non dispongono dell'autorizzazione necessaria, iniettandone direttamente il codice all'interno dell'eseguibile del programma vulnerabile residente sulla macchina vittima. La seconda categoria di sfide *(iniezione remota)* presuppone che gli studenti non abbiano un accesso locale alla macchina vittima, ma debbano utilizzare un vettore di attacco remoto per la cattura della bandierina. Infine, nella terza categoria di sfide *(alterazione della memoria)* gli studenti catturano la bandierina se riescono ad alterare il contenuto della memoria in uso da un programma, allo scopo di modificarne il flusso di esecuzione o di eseguire codice arbitrario.

L'Information Security è un ambito che siamo abituati a considerare come prettamente maschile. Sta cambiando qualche cosa in questo senso?

E' un argomento delicato, che non riguarda solo il mondo della Sicurezza Informatica, ma quello della Computer Science in generale. Attualmente, la percentuale di studentesse iscritte al Corso di Laurea Magistrale in Informatica presso l'Università di Salerno è di circa il 10% del numero totale, ed essa riflette quello che accade anche al Corso di Laurea (triennale) in Informatica. Per incrementare queste percentuali, il Dipartimento di Informatica dell'Università di Salerno è impegnato nella realizzazione di una serie di iniziative volte a incoraggiare il sesso femminile ad intraprendere gli studi in ambito informatico. Credo, più in generale, che sia necessario sfatare il mito che l'Informatica sia una disciplina più affine all'universo maschile che a quello femminile ed incoraggiare le donne, in particolare coloro che dimostrino una spiccata propensione verso le materie scientifiche, ad intraprendere gli studi e quindi la professione in questo ambito, contribuendo con la loro sensibilità, creatività, intuito e talento all'innovazione digitale per il futuro della nostra società.

Vi sono dei progetti orientati a far maturare un salto culturale orientato a riconoscer alle donne il ruolo e l'importanza che meritano?

Tra le iniziative a cui il Dipartimento di Informatica partecipa, va ricordato il progetto *Coding Girls,* proposto dalla Fondazione Mondo Digitale e dall'Ambasciata degli Stati Uniti in Italia. Lo scopo del progetto è quello di agevolare il raggiungimento della parità di genere nel settore scientifico e tecnologico, agendo su diversi fronti, tra i quali la lotta a pregiudizi e stereotipi di genere, la formazione paritaria e l'orientamento alle carriere del futuro, e proponendo diverse iniziative mirate a stimolare nelle ragazze delle Scuole Medie e Superiori la curiosità verso le scienze informatiche, evidenziandone aspetti particolarmente consoni all'intelletto femminile.

Il programma CyberChallenge.it

La sua Università partecipa all'edizione italiana della* Cyberchallenge, *che ha la finalità di attrarre nuovi talenti. Un compito arduo non crede?

CyberChallenge.IT è un programma di formazione, organizzato dal Laboratorio Nazionale di Cybersecurity del CINI, che coinvolge diverse sedi in tutta Italia, tra cui l'Università di Salerno. Il programma, indirizzato agli studenti di età compresa tra i 16 e i 23 anni

ed iscritti presso Scuole Superiori o Università italiane, mira ad incuriosire ed identificare giovani talenti, incentivando il loro interesse per le discipline informatiche, oltre che a mostrare loro le opportunità professionali offerte dall'iniziativa. L'auspicio è quello che i giovani talenti individuati possano costituire la prossima generazione di professionisti nell'ambito della Cybersecurity, indispensabile per garantire la sicurezza del nostro Paese. Si tratta, senza dubbio, di un compito arduo ma la particolare tipologia dell'offerta formativa, basata sull'alternanza di didattica tradizionale e proposta di accattivanti sfide CTF, unita alle possibilità per gli studenti di incrementare la propria visibilità presso aziende e istituzioni italiane ed internazionali, ha riscosso un successo crescente negli anni.

***Quali sono le tappe principali di* CyberChallenge.IT?**

Il percorso formativo si conclude con la formazione di *TeamItaly,* la Squadra Nazionale di Cyberdefender, della quale vengono chiamati a far parte i ragazzi che hanno avuto maggior successo, sia a livello individuale che come gioco di squadra, durante le varie fasi di *CyberChallenge.IT*. La squadra *TeamItaly* rappresenta l'Italia alla *European Cyber Security Challenge (ECSC)*, la competizione internazionale organizzata ogni anno dalla European Union Agency for Cybersecurity (ENISA) con lo scopo di favorire lo scambio di conoscenza e talenti in tutta Europa.

Le minacce si stanno sempre più evolvendo, anche gli hacker hanno cambiato pelle rispetto alle prime celebri "apparizioni". Di quali competenze hanno bisogno le aziende per affinare strategie di governance del rischio e di individuazione delle vulnerabilità che siano al passo con i tempi?

Le competenze richieste per essere al passo con i tempi sono quelle che si acquisiscono in corsi specializzati, quali ad esempio quelli offerti dal curriculum *"Sicurezza Informatica"* del Corso di Laurea Magistrale in Informatica presso l'Università di Salerno. Non dimentichiamoci che il termine *"hacker"* ha cambiato radicalmente significato nel tempo. Oggi, esso viene utilizzato con un'accezione prevalentemente negativa, per indicare coloro che fanno uso delle proprie competenze per violare sistemi informatici, rendere inutilizzabili risorse, rubare e divulgare dati sensibili, al fine di ottenere un vantaggio economico o politico. Ma il significato originario del termine aveva invece un'accezione totalmente positiva e iniziò a circolare all'inizio degli anni Sessanta tra i membri del *Tech Model Railroad Club* del Massachussets Institute of Technology (MIT) di Cambridge, per identificare coloro che, inizialmente accomunati dalla passione per il modellismo ferroviario, amavano esplorare i dettagli dei sistemi informatici e i modi con cui estenderne le capacità. Non è un caso che molti dei membri del club abbiano rivestito un ruolo di primaria importanza nella storia della Computer Science.

Senza formazione non ci può essere sicurezza

Vi sono minacce che dobbiamo temere in modo particolare?

Al giorno d'oggi, i pericoli che possono derivare agli utenti in seguito a un cyber-attacco sono numerosi e possono avere effetti disastrosi, cosicché appare evidente la crescente necessità delle aziende di affinare strategie di gestione dei rischi e di individuazione delle vulnerabilità, allo scopo di difendersi nel miglior modo possibile. Pertanto, è necessario avere una profonda conoscenza

BIO

Barbara Masucci è nata a Salerno il 27/11/1972. Nel 1996 ha conseguito la Laurea in Scienze dell'Informazione, con votazione di 110/110 e lode, presso l'Università di Salerno e nel 2001 il titolo di Dottore di Ricerca in Informatica, presso la stessa università. Durante il Dottorato di Ricerca ha svolto periodi di studi e ricerca all'estero: da Settembre 1999 ad Aprile 2000 presso il Centre for Applied Cryptographic Research, Department of Combinatorics and Optimization, University of Waterloo, Ontario, Canada, e nel Luglio 2001 presso il Departament de Matemàtica Aplicada IV, Universitat Politècnica de Catalunya, Barcelona, Spagna. Dal 2019 è Professore Associato di Informatica presso il Dipartimento di Informatica dell'Università di Salerno. Dal 2002 al 2019 è stata Ricercatore Universitario presso lo stesso dipartimento.I suoi interessi di ricerca riguardano la Crittografia e la Sicurezza Informatica, ed in particolare l'analisi e la progettazione di protocolli crittografici efficienti e sicuri.

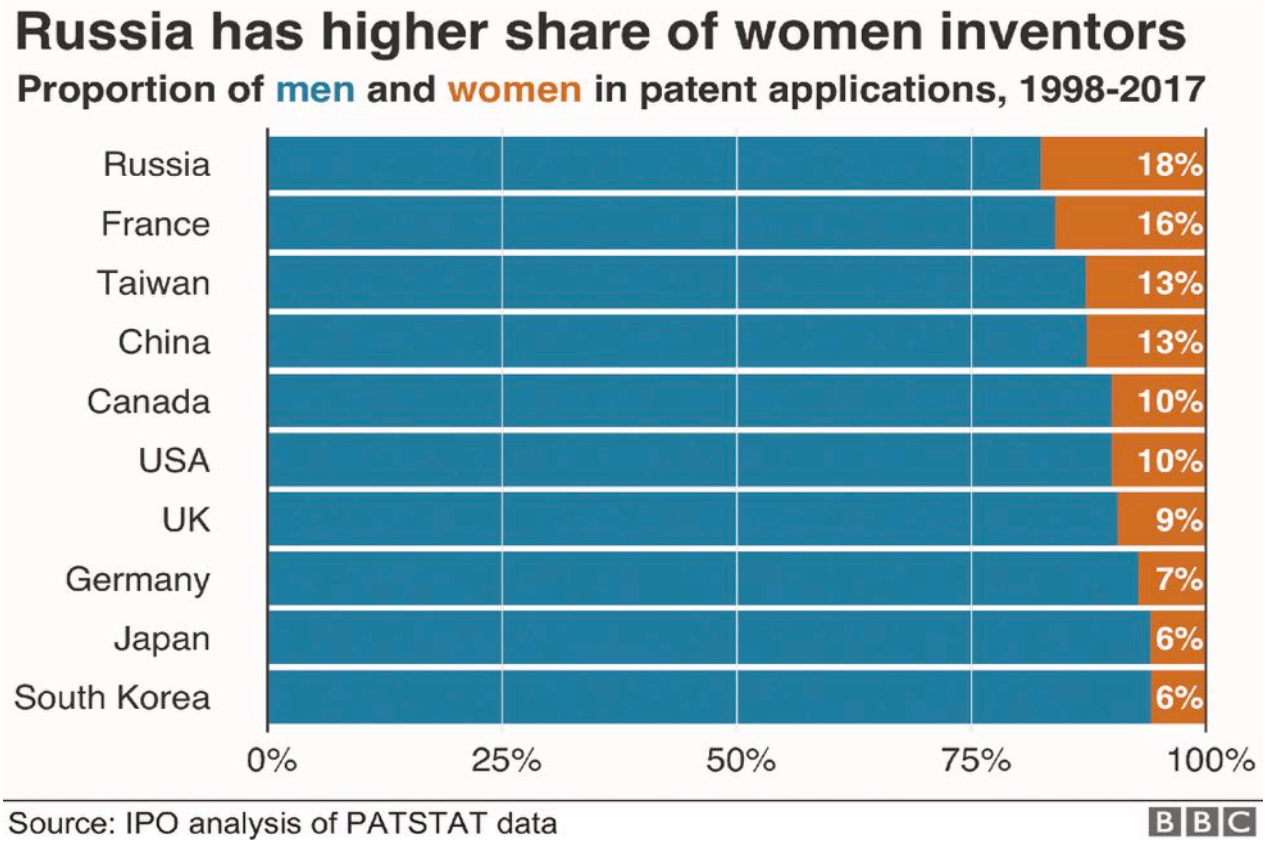
relativa al modo di agire degli attaccanti, focalizzandosi su come le stesse metodologie e tecniche da essi utilizzati per effettuare gli attacchi possano diventare strumenti per proteggere i sistemi informatici. Una volta acquisito il background tecnico e metodologico tipico di un attaccante, sarà possibile valutare lo stato e i fabbisogni, in termini di sicurezza, di sistemi complessi.

In Inghilterra esiste un programma di* Cyberchallenge *per le donne. In Italia è percorribile una strada simile?

Per quanto riguarda l'Italia, *CyberChallenge.IT* è giunto alla sua quinta edizione: per il 2020 sono stati 4452 i giovani iscritti, di cui solo il 13,6% di sesso femminile, e 560 i ragazzi selezionati. Un dato incoraggiante, se si pensa che nelle edizioni precedenti la percentuale di presenze femminili tra gli iscritti oscillava tra il 9% e l'11%. Dall'analisi dei dati relativi alle diverse edizioni del programma formativo, si evidenzia, purtroppo, il *gender gap* di cui abbiamo parlato prima. Secondo il rapporto *"Cracking the Code: Girl's and women's education in Science, Technology, Engineering and Mathematics (STEM)"*, pubblicato dall'UNESCO, la disparità di genere nello studio delle STEM deriva dal contesto culturale e sociale in cui le donne vivono.

In conclusione: quali sono a suo avviso i principali ostacoli da rimuovere?

La convinzione che l'Informatica sia una disciplina più affine all'universo maschile che a quello femminile è ancora troppo radicata nella collettività, e con essa l'idea che lo stereotipo del professionista informatico sia quello di un nerd che svolge un lavoro non adatto ad una donna. Credo che sia necessario impegnarsi al più presto a favorire le iniziative volte a colmare questa disparità di genere e ad educare, sin dall'infanzia, il sesso femminile a prediligere attività di tipo tecnologico e scientifico. ■



CERT STAR

CERT STAR è un programma di incontri a porte chiuse dedicato ai **CERT** e ai **SOC** italiani volto ad alimentare le **competenze**, promuovere la **cooperazione** e la **condivisione** di esperienze. Nel corso degli incontri sono analizzate a livello tecnico **operativo** le principali **tematiche** "core" dei team di security.

INCONTRI 2021

- **Gennaio e dicembre** Competizione cert star
- **Marzo** Machine Learning e Cyber Security
- **Maggio** Cyber Threat Intelligence
- **Luglio** Monitoring and Investigation
- **Settembre** Ransomware
- **Novembre** IA e Cyber Security

NOVITÀ

- Incontri online
- Attività di laboratorio
- Competizioni Read/Blue Team
- Momenti di condivisione
- Webinar
- Momenti conviviali

Più donne manager nella sicurezza? Una questione di cultura

Autore: Isabella Bragantini, Luxottica Group

L'evoluzione tecnologica e la digitalizzazione fanno ormai parte del nostro modo di vivere e del nuovo modo di fare business, migliorando i servizi e la rapidità di comunicazione. In particolare, per il periodo di pandemia che stiamo vivendo, si sono rivelate essenziali nel far fronte alla necessità di lavorare da remoto, nel rispetto del distanziamento e garantendo la continuità operativa.

BIO

Isabella Bragantini, laureatasi nel 2000 in Ingegneria Gestionale all'università degli Studi di Udine, ha iniziato la sua carriera nell'ambito dell'Information Technology, prima come Business Analyst e poi come Project Manager in Luxottica, seguendo diversi progetti anche internazionali relativi a diversi processi aziendali su diverse aree quali Produzione, Acquisti, Controlling e Finance. Da quasi 4 anni lavora nell'Information Security a livello Corporate di Luxottica Group, da quando si è costituita la funzione ha partecipato fin da subito a tutte le iniziative di governance, prevention, detection e responce, in particolare per l'ultima area ha seguito il progetto di individuazione e attivazione del SOC avvenuta nel 2018.

Allo stesso tempo la maggior esposizione, interconnessione, la smaterializzazione delle informazioni e dei luoghi fisici di archiviazione, la rapidità di introduzione di nuove tecnologie, l'automazione possono esporre le aziende e le persone a nuove minacce e la sfida da affrontare è di riconoscerle attraverso strumenti e procedure di protezione e prevenzione.

I fattori di rischio da considerare sono molteplici: dalle vulnerabilità dei nuovi strumenti adottati, come le piattaforme di collaboration, soprattutto se non aziendali, ai dispositivi ad uso personale, fino a quelli legati alle nuove modalità operative, come il lavoro in ambienti domestici o accessibili al pubblico, per questo è nata la necessità di ribadire e rafforzare regole e procedure aziendali, permettendo allo stesso tempo di renderle più vicine alla vita di tutti i giorni, coadiuvate purtroppo da esempi reali, come tentativi di phishing o social engineering.

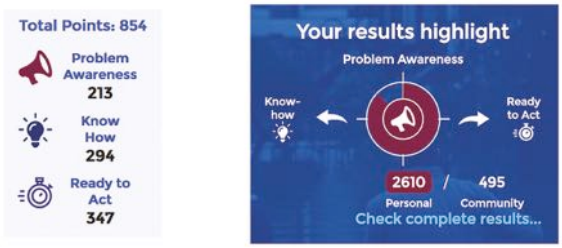
Aumentando i fattori di rischio, in proporzione devono aumentare le opportunità di miglioramento in termini di sicurezza delle informazioni e

questo riguarda sì l'ambito di IT Security e Information Security, ma include e permette ancora più sinergia tra la Security e le diverse funzioni aziendali, quali HR, Finance, ingegneria e prodotto, comunicazione. Questa maggiore sensibilizzazione ha permesso di divulgare nuove policy di sicurezza, collegate allo smartworking, comunicazioni di awareness sulla protezione del dato e sull'uso dei dispositivi, per un rafforzamento di procedure di controllo interno.

Principali minacce e l'importanza della awareness

Una delle principali minacce in aumento nel periodo di lockdown è stato il phishing, soprattutto con tema Covid19, o la business e-mail compromise, attraverso le quali viene adescata la preda portandola a cliccare su link fraudolenti, oppure su allegati malevoli. Una volta cliccato, il rischio è che venga richiesto di inserire le credenziali, sfruttando le stesse per continuare l'attacco su altri fronti, oppure lanciare un malware. Per evitare di essere vittima di tali minacce, il sistema è di accrescere tra i dipendenti la consapevolezza di ciò che va evitato, come fare a riconoscerlo, e fornire una chiara spiegazione delle conseguenze e impatto. La security awareness diventa per forza un termine chiave, non solo utile per la sicurezza dell'azienda, ma utile anche nella vita privata e familiare.

L'awareness sulla sicurezza informatica non è un argomento attraente per i non addetti ai lavori, anzi è visto spesso come un argomento distante dall'essere umano, come invece è qualsiasi tipo di crimine. L'awareness sulla sicurezza informatica non è un argomento attraente per i non addetti ai lavori, anzi è visto spesso come un argomento distante dall'essere umano, come invece è qualsiasi tipo di crimine. Oggi, le possibilità di diffondere questa consapevolezza sono molteplici, per esempio attraverso pillole descrittive o dei video esplicativi. Molte aziende usano la gamification creando una sorta di gara tra i diversi uffici o tra i colleghi di pari livello. Uno strumento per misurare poi l'efficacia dei corsi sono le simulazioni di phishing che in base al risultato permette di reindirizzare l'utente che non ha raggiunto il punteggio a un piano di nuovi corsi.



(a) (b)

La minaccia della frode non riguarda solo le aziende, ma è una minaccia a cui tutti, anche nella vita privata, siamo esposti. È per questo che la formazione dovrebbe partire fin da subito, già tra i ragazzi o i bambini, ovvero quando si incomincia ad utilizzare sistemi iper-connessi. L'ambiente scolastico è il contesto più favorevole dove iniziare ad introdurre tale argomento. Oggi tutti hanno un telefono o un pc a casa, tutti sono dotati di connessione internet e l'utilizzo di social web, sistemi di chat e messaggistica, sono di ordinaria amministrazione: queste risorse, però, aumentano anche il rischio di essere vittima di un attacco informatico o di frode.

Una delle conseguenze importanti collegata alla poca attenzione a questi temi anche privatamente è il furto di dati. Come persona di Information Security, i primi concetti che mi vengono in mente sono protezione, privacy, le pesanti sanzioni previse dal GDPR, crittografia, *masking* e sistemi di *data loss prevention*. Questo significa che le aziende sono tenute giustamente a proteggere i dati di privacy dei propri dipendenti e dei propri clienti. Il paradosso è che gli stessi dati che vengono protetti dalle aziende, nella vita privata la maggior parte delle persone è disposta a fornirli in cambio di accessi a determinati servizi o a determinate informazioni: con un click rilasciamo il consenso alla privacy, spesso senza esserne consapevoli di come verranno utilizzati i nostri dati. Pochissime persone leggono il consenso al trattamento dei dati, forse solo quando è composto da pochi bullet point. Questo è un altro tema che deve diventare familiare fin dai primi momenti in cui si entra in un mondo connesso.

TEN TIPS TO PROTECT YOUR PRIVACY

Your privacy is valuable and worth protecting. The *Privacy Act 1988* protects your personal information, however, there are steps you can take to protect your privacy. Personal information is information or an opinion that identifies you, or could identify you. Some examples are your name, address, telephone number, date of birth, medical records, bank account details and opinions.
These ten tips will help you protect your personal information, and your privacy.

Australian Government
Office of the Australian Information Commissioner

www.oaic.gov.au

Strategie di contrasto e comportamenti "virtuosi"

Possiamo ritenerci pronti ad affrontare questo mondo in evoluzione, ma allo stesso tempo così esposto, se continuiamo a sviluppare sistemi di Information Security sempre più robusti e capaci di migliorare la sicurezza in termini di: *Comportamenti*, attraverso la formazione di tutti gli interessati, *Tecnologie,* aggiornando e migliorando continuamente le tecnologie di protezione e di esercizio, *Processi ed Organizzazione,* nella definizione di ruoli e regole che limitino l'esistenza di singoli punti critici per le applicazioni, le tecnologie e le infrastrutture.

Aumentando i sistemi di Prevenzione, Rilevazione e Risposta ad incidenti di sicurezza o *data breach* (e.g. Segregazione delle reti; *Hardening* delle macchine; Firewall; VPN; antivirus; ATP; Strong Authentication; Cifratura dati; ecc.). Ogni azienda a seconda del contesto, della sua maturità in sicurezza informatica, dovrà poi sviluppare i fattori che ritiene più opportuni per tutelarsi al meglio dal cyber risk, tenendo conto di questi punti fondamentali:

- approcciare la security come un ecosistema di elementi, riferibile alle persone, ai processi ed alle tecnologie;
- valutare continuamente e dinamicamente l'esposizione al rischio considerando sia le minacce esterne che interne;
- "hope for the best, plan for the worst";
- investire in prevenzione, ma prepararsi e pianificare anche per gli eventi peggiori consolidando e migliorando le procedure di reazione;
- monitorare continuamente ed imparare dagli incidenti/quasi incidenti, sia propri che di terzi, raccogliendo tutti gli input.

Come sa bene chi opera in questo campo, la sicurezza assoluta non esiste, è un continuo *trade off* tra rischi, opportunità, costi e tempi ed è pertanto sempre in evoluzione. L'importante è conoscere il rischio, che va analizzato e monitorato, per capire se accettarlo o prevenirlo. Volendo in conclusione soffermarmi sulla realtà specifica del mio lavoro, e della condizione femminile nell'ambiente della sicurezza informatica va detto che il gentil sesso ha una rappresentanza dell'11%, risultato certo non gratificante dovuto probabilmente al fatto che questo ambito disciplinare è stato tradizionalmente visto come un terreno ostico, "da nerd", per usare un termine gergale.

Fortunatamente questa prospettiva sta cambiando oggi questo campo appartiene a ognuno di noi, almeno nella "postura" siamo tutti un po' "nerd", incurvati sui nostri pc, tablet o telefoni per ore e ore, spesso non abbiamo né il tempo né la possibilità di parlare con nessuno. Siamo di fronte a un grande tema del nostri tempo, che ha soprattutto una valenza culturale. La sensibilità e l'avversione al rischio, che caratterizza l'atteggiamento

delle donne, potrebbero essere considerati degli oggettivi punti deboli, non bisogna dimenticare che solo coltivando la *diversity* le organizzazioni possono crescere e andare incontro al cambiamento. Le donne anche, ma direi soprattutto nel nostro ambiente può contribuire in modo decisivo a far crescere la consapevolezza del rischio informatico, in tutte le complesse manifestazioni che la contemporaneità fa a tutti noi quotidianamente sperimentare. ■

© immagine tratta dal libro „Il fattore umano nella cyber security - Valori e strategie da costruire insieme", ed. Franco Angeli.

Non fatevi hackerare la vita! Come creare una blockchain per preservare la propria sanità mentale

Autore: Imma Orilio, fondatrice, CREMETE srls

Sono nata il giorno che IBM ha presentato al mondo il primo Mainframe, e sono cresciuta con quella generazione di genitori che cercava di tenerti buona e attaccata alle sottane. Ma ricordate la canzone di Cat Stevens *"Father and son"*? beh io ero una di quelle che non sentivano ragioni, dovevo andare, dovevo capire, dovevo cercare.

Allevata da Alberto Manzi, ho subito capito che la cultura sarebbe stata la mia via di fuga (consapevolezza subliminale al tempo, poiché avevo solo tre anni, ma illuminante poiché saper leggere mi avrebbe consentito di non dipendere da papà per le favole, visto che arrivava sempre tardi e il più delle volte stanco, e mamma aveva sempre troppo da fare con quel rompiscatole che frignava dalla culla).

Crescendo tra Topolino e Selezione del Reader's Digest ho alimentato la mia sete di sapere e di libertà sognando viaggi e aspettando il riscatto di Paperino contro l'avversa fortuna. In verità nel tempo cominciava a serpeggiare sempre di più in me il sospetto che il mio affetto immotivato per una categoria di emeriti co*** come Paperino e Paperoga e la mia spiccata avversità rispetto ai personaggi stereotipati di Paperina e Topolina, stesse già covando la bestiolina di Satana che sarebbe venuta alla luce alcuni anni dopo, ma nel dubbio continuavo a cercare, fuori e dentro di me, il capo per dipanare la matassa ingarbugliata del mio io adolescenziale.

La bimba di 4 anni seduta sul tavolo della cucina col papà, che attendeva il primo allunaggio, e che alle elementari divorava gli articoli di Barnard, pubblicati da Selezione, era cresciuta ormai e doveva prendere una decisione: medicina o tecnologia?

Qualcosa mi diceva che queste due strade erano simili ma non potevo intraprenderle insieme, e poiché negli anni 80 i medici erano una categoria

molto in difficoltà, optai per qualcosa di molto avveniristico: l'ingegneria aerospaziale. Da questo momento in poi nasce la consapevolezza che inserirmi lavorativamente sarebbe stato fortemente dipendente dalla mia capacità di applicare una tecnica zen allo sviluppo di un profilo professionale resiliente in grado di adattarsi senza necessariamente adeguarsi agli ambienti lavorativi che negli anni 80-90 non è che fossero poi così tanto aperti.

D'altra parte, se ancora solo qualche anno fa qualcuno mi indicava in un contesto lavorativo come "la signora bionda" probabilmente la cura è stata peggiore del malanno, poiché ancora molti sono certi di potersi consentire certi atteggiamenti perché "tanto non succede nulla…" (illusi!).

Il riscatto lo assapori quando poi, sul campo operativo la tua posizione è considerata per quel che vale (purtroppo non tanto spesso e comunque mai in regime di dipendenza), ma ha sapore amaro quando tale considerazione si tramuta in timore e, di conseguenza, in tentativo di esclusione. Che sia però chiaro che queste mie considerazioni non vogliono essere lamentazioni veterofemministe, visto che l'atteggiamento che riscontro è essenzialmente giustificato dal fatto che, in quanto elemento con una personalità definita e dichiarata, in contesti in cui la ragion di stato richiede un equilibrio non chiaramente espresso ma sottilmente leggibile, la mia figura è percepita come un elemento "da studiare" e potenzialmente critico (in entrambe le accezioni del termine).

È altrettanto vero però che laddove il fabbisogno di supporto è chiaro ed impellente invece ti accolgono come il *deus ex machina* e ti stendono tappeti rossi, ma sempre sperando che comunque, risolto il problema, tu li utilizzi per varcare gloriosamente l'uscita.

Ma come si arriva a questo punto guardandosi indietro con soddisfazione?

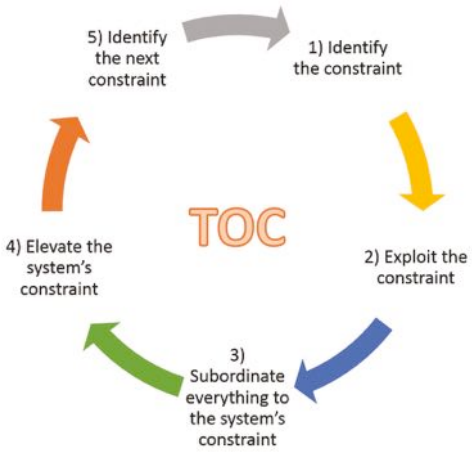
Costruendo la propria vita come una blockchain.

La vita, per poter chiarire l'analogia, è un registro su cui il tempo disegna, attraverso gli eventi, dei "blocchi" che rappresentano i nostri ricordi e costruiscono la nostra esperienza. Quanto più questi blocchi sono mantenuti integri e preservati a monte, dall'ingerenza esterna, tanto più la personalità che si costruisce risulta forte. E poiché questo processo continua per tutta la vita, se le modalità di approccio al futuro si rafforzano, sulla base dell'esperienza, ma senza sconvolgere essenzialmente i propri modelli mentali, si riesce a governare, per quel che è possibile, l'evento prossimo, sviluppando strumenti che ti diano sufficiente probabilità, se non di successo, quanto meno di danno limitato.

D'altra parte, chi non ha dubbi nella vita, ma se ad ogni bivio che si propone, fossimo sempre disponibili a invalidare l'intera struttura su cui abbiamo basato la nostra vita, modificando radicalmente degli atteggiamenti o cancellando la memoria dei nostri errori, creeremmo un "sistema vita" instabile e facilmente *"hackerabile"*.

E quando si giunge al punto che sai che quello che hai avanti è sicuramente meno di quello che ti sei lasciato alle spalle, cominci ad applicare gli strumenti che sono diventati ormai propri del tuo modello mentale, per essere, se si può, felice.

Il mio "modello organizzativo" è basato sulla Teoria dei Vincoli (*Theory of Constraints,* concetto di filosofia del management elaborata da Eliyahu Goldratt ed esplicitamente spiegata nel suo capodopera "The Goal", pubblicato nel 1984) , che si basa sull'assunzione che in ogni sistema, a prescindere dalla sua complessità, esistono pochi fattori significativi che impediscono o rendono difficile il raggiungimento di un determinato obiettivo.



Lo sforzo, dunque, non deve essere teso a individuare quelle cose, poche e fondamentali, che possono essere abilitanti alla serenità e perseguirle con tutte le proprie forze, ma fortemente conoscere quelle che sicuramente mineranno questo percorso e scansarle con grande destrezza.

Buona vita a tutte. ■

BIO

La storia professionale dell'ing. Imma Orilio è un'evoluzione naturale di un innato eclettismo. Nasce come ricercatore del Centro Italiano di Ricerche Aerospaziali dove approda con una laurea *cum laude* in ingegneria aeronautica e specializzazione in materiali compositi e Controlli Non Distruttivi. Dopo 11 anni di ricerca intraprende la carriera direttiva in DEMA, azienda del settore della produzione aeronautica, e poi, nel 2006 arriva un incarico pubblico in un'azienda Sanitaria dove ricoprirà per 10 anni il ruolo di esperto di innovazione tecnologica e CIO. È qui che comincia il suo cammino nel campo della cybersecurity intraprendendo un progetto di conversione del CED aziendale sviluppato nel 2009 secondo i canoni della della privacy by design e by default, della virtualizzazione e sviluppando un sistema informativo che nel 2013 viene definito *"cloud ready"*. Oggi ha fondato la società CREMETE srls, raccogliendo professionisti di elevata e riconosciuta esperienza che si occupa di consulenza strategica, organizzativa e tecnologica rivolta tanto alla sanità pubblica e privata quanto in generale agli ambienti produttivi industriali.

Una vita dai mille colori e molta cyber security, il tutto... in uniforme

IGPR
POLIȚIA ROMÂNĂ
IPJ SIBIU

Autore: Crina Șoaita (Peteleaza),
Agente-Capo, Polizia Nazionale Romena,
Ispettorato Provinciale di Sibiu

BIO

Crina si è laureata col massimo dei voti in "Legge nazionale" presso l'Università "Lucian Blaga di Sibiu". Dopo aver vinto il concorso e terminato *summa cum laude* il corso della Polizia Nazionale (Scuola Nazionale di Polizia di Campina), ha eseguito con successo i rigorosi addestramenti del Centro di formazione e sviluppo della Polizia Nazionale *"Nicolae Golescu"* di Slatina. Assegnata presso l'Ispettorato Provinciale di Sibiu della Polizia Nazionale Romena, è stata per dieci anni una delle rarissime donne a far parte dell'ufficio di sicurezza e ordine pubblico. Per merito, dal 2013 venne promossa ed entrò a far parte del Dipartimento di Prevenzione e Analisi del Crimine, dove a lungo si impegnò a fare *awareness* su tutti i fronti, dai bambini più piccoli agli adolescenti fino ai CEO di ditte di ogni taglia. Col suo prezioso *backround* - 10 anni ad arpeggiare le strade e sei a capire e spiegare la cybersecurity, da novembre del 2019 lavora, sempre a Sibiu, presso il reparto di detenzione e arresto preventivo della Polizia Giudiziaria (l'equivalente di una unità territoriale della Direzione Centrale Anticrimine della Polizia dello Stato in Italia).

Quando mi è stato proposto di scrivere questo articolo per la rivista italiana Cybersecurity Trends sono stata subito autorizzata dai miei superiori. È stato per me un piacere ed un onore accettare e mi sono chiesta: "ma perché un numero sulle donne in cyber security?".

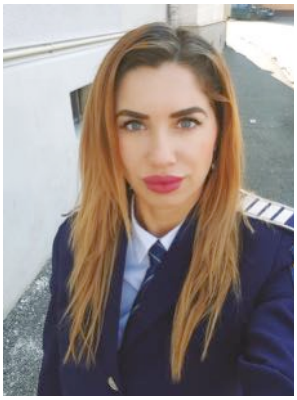
Per la Romania suona un po' strano, perché proprio in questo campo le donne sono molte, sia nei Servizi dello Stato che nel settore privato. Poi, mi sono ricordata che la mia carriera, come accennato nel titolo, è alquanto "variopinta", basti pensare che da adolescente lavoravo come commessa in

una gioielleria per pagarmi le lezioni per diventare fotomodella, un sogno che è diventato un hobby che mi permetto di fare, di tanto in tanto, con mio marito complice come fotografo ...

Ma quando ho finito la scuola - eravamo nella «fase neolitica» dell'era digitale - mi sono iscritta alla facoltà di giurisprudenza dell'università di Sibiu dove ho conseguito una laurea in diritto. Poi scelsi di entrare in Polizia, dove noi donne eravamo quasi in parità con i nostri colleghi maschi sia presso la Scuola Nazionale di Polizia di Campina che terminai nel 2003, sia presso il Centro di formazione e sviluppo della Polizia Nazionale *"Nicolae Golescu"* di Slatina che frequentai immediatamente dopo.

Come donna, l'unico momento difficile sono stati i miei primi dieci anni al servizio dei cittadini, perché il destino mi fece ritrovare assegnata all'ufficio di sicurezza e ordine pubblico del dipartimento di Sibiu. Lì si che eravamo poche, e per forza di cose, ho dovuto superare le mie paure e guadagnarmi il rispetto dei cittadini di Sibiu, soprattutto di quelli che avevano qualcosa da nascondere...

Per 10 anni sono rimasta tra le pochissime donne a lavorare sul campo, il più avvincente nelle forze dell'ordine. Il servizio si svolgeva in tre turni a rotazione e la vita correva al ritmo della caccia ai borsaioli, ai ladri di negozi, ai furfanti di ogni genere, giorno e notte. Apprezzata e spesso premiata dai mei superiori, con riconoscimenti e piccoli bonus, iniziai progressivamente a collaborare con i dipartimenti "superiori" (polizia giudiziaria, dipartimento di lotta contro la criminalità organizzata) e anche con la procura. Alla fine, fui assegnata all'ufficio di analisi dell'unità territoriale di Sibiu, passando così molte serate a gestire le attività della Polizia Stradale.



Grazie a questo background, entrai nel 2013 a far parte del Dipartimento di Prevenzione e Analisi del Crimine, dove la mia passione per la cybersecurity nacque quasi immediatamente. Infatti, il Dipartimento nella sezione Prevenzione, ricopre esattamente gli stessi compiti svolti, al servizio dei cittadini e delle aziende, dalla Polizia delle Comunicazione in Italia. Ma in Romania, come in molti paesi dell'Europa orientale, ci sono tantissime donne, in alcuni reparti siamo chiaramente in maggioranza.

Mi ricordo le serate passate a cercare online materiale adatto e a osservare il fenomeno e l'evoluzione dei crimini digitali, perché ogni mattina il mio compito era quello di preparare materiale di prevenzione su vari argomenti, per aiutare i cittadini e gli studenti ad evitare di finire vittime di criminali. Ogni giorno, con il materiale in mano, mi recavo presso scuole elementari, medie, licei, scuole superiori, facoltà universitarie, ma anche presso società commerciali in tutta la provincia di Sibiu, per svolgere corsi interattivi. Ogni giorno dovevo scegliere un altro argomento, e, come non detto, una delle domande più pressanti da parte, soprattutto, da studenti di ogni età era: *"Come proteggermi dal crimine online? ".*

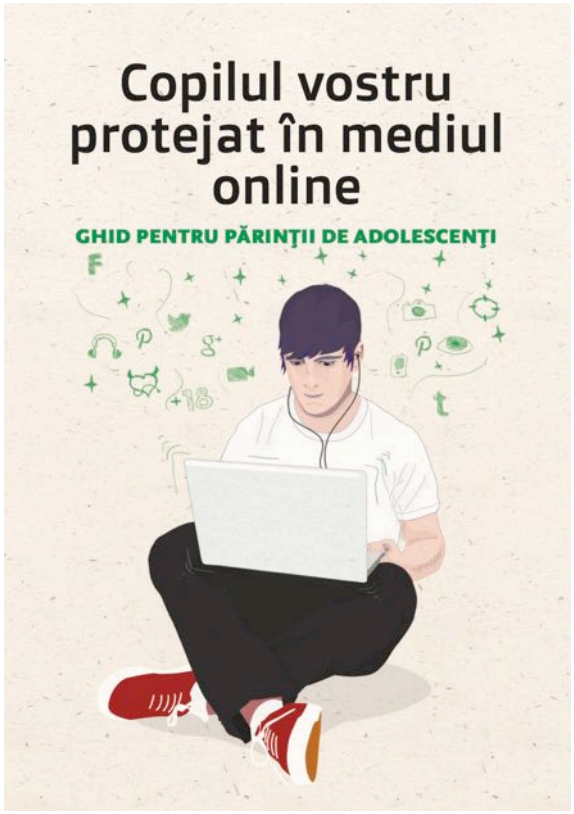
Proprio quell'anno, la Swiss Webacademy lanciò la prima edizione del convegno annuo *"Cybersecurity-Dialogues Romania"* e per organizzare campagne di sensibilizzazione destinate a bambini e adolescenti chiese la collaborazione della Polizia Nazionale. Non solo i nostri superiori accolsero con favore l'iniziativa, ma permisero a tutto il team di prevenzione di seguire l'intero convegno e di godere dei suoi momenti di socializzazione.

Anno dopo anno, le presentazioni e le discussioni con i responsabili delle varie strutture centrali nazionali attive nel campo della security, così come con i vip di tutti i settori di più di 30 paesi – ricordo con piacere, per quanto riguarda l'Italia, le discussioni con Nicola Sotira e Massimo Cappelli – sono state le vere lezioni che hanno permesso a tutto il team di migliorare la qualità dei nostri materiali, e di poter rispondere tempestivamente alle domande, sempre nuove e legate alle varie mode online, di bambini e adolescenti.

Abbiamo anche imparato a collaborare con gli specialisti del mondo privato, una pratica che era solo agli albori nella capitale ma quasi assente nelle provincie. Alcuni di loro ci hanno regalato molte "dritte" su nuove app, i loro pericoli, la loro intrusività, e come spiegare facilmente queste minacce ai loro utenti.

Con il passato accademico, mio e di molti colleghi, il nostro team è anche riuscito ad introdurre connotazioni giuridiche alla nostra attività, perché molti comportamenti dannosi (tra minorenni o contro i minorenni) non rappresentano necessariamente reati penali ma possono essere aggiunti a rischi penali. A seconda della giurisdizione questi comportamenti illeciti possono chiaramente implicare un'accusa penale ma ci sono azioni che fanno parte di una zona grigia tra condotta criminale e non penale.

Grazie al generoso sostegno dell'ITU (ONU) ed al lavoro della Swiss Webacademy, il convegno del 2015 ha lasciato un segno al nostro team: finalmente avevamo in mano, grazie ad un fondo per la stampa messo a disposizione dalla Giunta Provinciale, ben quattro volumi tradotti in rumeno da regalare a bambini, adolescenti, professori e genitori: le due linee guida dell'ITU (Child Online Protection Programme) e due delle migliori pubblicazioni della *"Empowering Children Foundation"* (all'epoca *"Nobody's Children Foundation"*), sostenuta dal governo polacco, molto più idonee alla realtà delle scuole e dei licei rumeni.



In effetti, se insegnare e discutere personalmente con i giovani e con i loro professori rimane sempre lo strumento principale della prevenzione, le linee giuda consultabili tranquillamente a casa in caso di problema sono altrettanto un *asset* che va a completare, o meglio, a consolidare, i risultati del nostro lavoro nel campo.

Da destra a sinistra: l'équipe di Prevenzione della Polizia Nazionale, Sibiu con il Comandante Nicolas Greth (vice-direttore della Scuola della Polizia Nazionale Francese, Belfort), Frédéric Gaudun (Direttore della pianificazione e tutela ITC, Repubblica e Cantone dello Jura, ed il Capitano Patrick Ghion (Capo della sezione forensica della Poilzia di Stato di Ginevra) durante «Cybersecurity-Dialogues Switzerland», 2018.

Per di più, i convegni di Sibiu ci hanno portato a fare visite annuali di perfezionamento (nel campo delle crisi e del cyber) presso l'Accademia della Polizia Nazionale francese, a Belfort, e a partecipare ai primi convegni di "Cybersecurity-Dialogues Switzerland", grazie anche agli ottimi rapporti intrattenuti con la Polizia di Ginevra, in particolare con il Capo della sezione forense, il Capitano Patrick Ghion.

Dal 2017, anno nel quale la giornata di awareness del convegno ha battuto il record europeo di prevenzione per i minorenni, in un solo giorno erano presenti 1059 alunni, le cose sono però cambiate. Un'unità speciale si occupa ormai delle aziende, mentre il nostro team continua a fare prevenzione solo fino alle scuole secondarie di primo grado, per i liceali si sono rivolti agli specialisti della DCCO (Dipartimento di lotta contro il Crimine Organizzato). Infatti, in Romania, gli adolescenti dimostrano un reale talento nativo di "geek", portandoli spesso, in modo inconsapevole, a compiere atti illegali. Il messaggio deve quindi essere duro e preciso, ma anche positivo: *"con i vostri talenti, entrate a far parte di organizzazioni come l'OWASP, diventate stagisti in*

6 ITtrends EVENIMENT Nr. 9 - Septembrie 2017

Record UE: 1.059 de copii conștientizați pe probleme de securitate la Sibiu

În cadrul celei de a 5-a ediții a conferinței „Cybersecurity Romania", miercuri, 13 septembrie 2017, a fost organizată o zi de conștientizare, în parteneriat cu Consiliul Județean Sibiu și Prefectura Sibiu. Ziua de conștientizare pentru copii și adolescenți a fost organizată la Hotel Ramada Grand Ballroom, în cadrul a două sesiuni, una pentru copii între 8-12 ani și a doua pentru copii între 13-18 ani.

În cadrul sesiunilor au susținut prezentări:

- viceprimarul Sibiului, Răzvan Pop, care a împărtășit din experiența proprie pe net, ca tânăr politician și în calitate de istoric;
- reprezentanți ai Poliției Sibiu, specializați pe prevenție, care au asigurat un contact între tinerii locali și autoritățile din zonă;
- ofițeri de rang înalt ai IGPR, departamentul de prevenție, care au avut prezentări bazate pe experiența lor și pe analize privind comportamentul specific grupelor respective de vârste;
- ofițeri de rang înalt ai IGPR, departamentul de luptă împotriva crimei organizate, care au împărtășit preocupările cu care se confruntă zilnic în privința agresiunii asupra unor victime din rândul tinerilor, dar și în privința recrutării de tineri talentați în cadrul unor acțiuni de crimă organizată pentru a-i determina să devină „cărăuși" sau black hats;
- specialiști ai sponsorului principal Telekom Romania, care au prezentat bune practici privind măsurile de precauție ce trebuie luate la navigarea pe internet de pe telefonul mobil;
- conducerea Swiss Webacademy care a organizat și un joc bazat pe întrebări și răspunsuri, adaptat grupelor de vârstă.

La sfârșitul evenimentului, copiii au primit mici cadouri oferite de sponsorii Telekom și Beromir și ghidul ITU COP.

La eveniment au participat 1059 de elevi și profesori, din 42 de clase, 22 din ciclul primar și 20 din licee, ceea ce a constituit un nou record de participare. Evenimentul a fost mediatizat de Agerpres.

În după amiaza aceleiași zile, Swiss Webacademy, Telekom Romania și BISS au organizat o sesiune de conștientizare pentru adulți, la care au participat reprezentanți ne-tehnici din companii și din administrația publică. ■

www.ittrends.ro

aziende di IT e poi, dopo la laurea, venite a lavorare nello Stato o nel privato. Ma soprattutto non lavorate mai per persone sconosciute, e non cedete alla tentazione di guadagnare denaro facile perché rischiate di entrare a far parte del crimine organizzato".

E qui è doveroso sottolineare che se riusciamo - per chi vuole ascoltarci - ad ottenere risultati di qualità con i giovani è proprio grazie alla DCCO, che dal 2015 è leader europeo in materia di lotta alla porno-pedofilia e in materia di frodi online, motivo per cui questi due settori sono posti sotto la presidenza dalla Polizia Romena nel seno della struttura cyber di Europol, l'EC3.

Questo accenno, anche se suona "patriottico" era doveroso perché proprio la mia passione per la cyber security mi ha spinta a cambiare nuovamente dipartimento. Da nove mesi, lavoro al reparto di detenzione e arresto preventivo della Polizia Giudiziaria, un campo strettamente legato all'attività online, come è stato dimostrato dagli arresti spettacolari eseguiti negli ultimi tre mesi nel territorio nazionale, portando dietro le sbarre molti organizzatori di gruppi specializzati nella creazione di "white cards" con *fullx* bancari esteri, la cui manodopera, che spesso si tratta di minorenni, utilizza i bancomat per ritirare la massima somma quotidiana consentita. Seppur le somme sequestrate, pari a decine di milioni di euro, appaiono enormi, sono solo una minima parte del settore delle frodi.

"Pocket money settimanale" appena sequestrata a casa di un "piccolo hacker", Sibiu, 20.11.2020 (200 Lei = 50 €, ndr)

Aspetto quindi con grandissimo interesse i prossimi convegni per continuare ad imparare sempre di più su realtà criminali diventate priorità assolute per i vertici delle più grandi strutture, sia statali che private.

E auguro a molte giovani donne italiane di entrare nel campo della sicurezza informatica e, perché no, di diventare poliziotte: c'è qualcosa in questa professione che il privato non potrà mai offrire: rispetto, solidarietà quotidiana e, non raramente, amicizie reali e profonde, almeno tra noi "modesti" agenti e sottoufficiali. E, nel campo della prevenzione, un contributo inestimabile se si fa bene il proprio lavoro: vedere dopo una lezione interattiva un bambino o un adolescente con il sorriso fino alle orecchie non spaventato ma grato dopo aver compreso meglio il mondo digitale in cui vive e che sarà il suo mondo per tutta la vita!

Per di più, con o senza l'uniforme non perderete la vostra femminilità: è oggi finalmente considerata e promossa come un'asset preziosissimo, in un mondo finora molto maschile, di beneficiare di doti e di talenti che portano un "opinione diversa", quella che possiamo avere noi, donne! ■

Politiche di inclusione nel Laboratorio Nazionale di Cybersecurity del CINI. Nasce CyberEquality.IT

Center for Cyber Security and International Relations Studies

UNIVERSITÀ DEGLI STUDI DELL'AQUILA

Autrici: Prof.ssa Dajana Cassioli, Dott.ssa Agnese Morici

Negli ultimi anni produrre un numero sufficiente di laureati nelle aree matematico-scientifiche, tecnologiche e ingegneristiche (STEM) è divenuta una priorità in tutto il mondo. Si prevede che le occupazioni in STEM cresceranno circa due volte più velocemente rispetto agli altri settori non-STEM. Nonostante questo, il numero di iscritti continua a decrescere. Inoltre, la presenza delle ragazze in corsi STEM è veramente bassa e questo rende disponibile soltanto la metà dei talenti a rispondere alla elevatissima richiesta di laureati.

Il Laboratorio Nazionale di CyberSecurity (LNCS) ha creato un gruppo di coordinamento al livello nazionale, il **CyberEquality.IT**, che opera all'insegna dell'inclusività per colmare il divario digitale in Italia, attraendo quei talenti che si "autoescludono" da percorsi nelle carriere STEM e, in particolare, nella cybersecurity.

La persistenza dello squilibrio di genere nelle scelte dei percorsi di studio e di carriera nelle aree matematico-scientifiche, tecnologiche e ingegneristiche (STEM) è uno dei temi più dibattuti e più studiati da anni nelle discipline delle scienze dell'educazione, ma anche in sociologia e psicologia. La diversità degli approcci è di per sé indicativa della complessità del fenomeno, e della necessità di approfondirne la comprensione a più livelli per pensare e realizzare interventi efficaci.

cini Cybersecurity National Lab

Molte sono le componenti cognitive, pedagogiche e sociali che concorrono alla formazione delle scelte in ambito scolastico e di carriera, al di là delle capacità e delle disposizioni individuali di base. I due antecedenti più prossimali sono l'***aspettativa di successo*** e la percezione del ***valore*** associato alla riuscita in un determinato compito o campo. A loro volta, numerosi fattori sia a livello macro-sociale che a livello di contesti di vita più prossimali (familiari e scolastici, ad esempio) concorrono a modulare ciascuno di questi due antecedenti.

L'esistenza di una stereotipizzazione di genere per una disciplina, che può manifestarsi attraverso i comportamenti di genitori e insegnanti (ma non solo) o attraverso l'assenza di modelli di ruolo dello stesso genere in un determinato campo, è una componente cruciale nella formazione di aspettative e di valore percepito del successo in quell'ambito. ***Componenti affettive*** (ad esempio le emozioni associate all'apprendimento e alla riuscita

in ciascun ambito) e ***identitarie*** (quali il senso di appartenenza e di rilevanza del campo di studi o lavoro per sé e per la propria identità) svolgono un ruolo di mediazione cruciale. È evidente che, benché diversi antecedenti svolgano un ruolo critico, alcune componenti sono più complesse da modulare in quanto radicate nel contesto socio-culturale più ampio, mentre altre sono più accessibili all'azione mirata del singolo docente e dei contesti educativi nel loro insieme.

In ogni caso, incrementare la consapevolezza sulle componenti macro del processo, e allo stesso tempo fornire strumenti operativi per ***incorporare la dimensione di genere nella progettazione didattica disciplinare*** del singolo docente, sono entrambi livelli di azione che possono contribuire ad affrontare operativamente gli squilibri di genere in ambito STEM. Il gruppo di lavoro CyberEquality.IT si propone, tra gli altri obiettivi, di definire degli interventi formativi che possano incuriosire le ragazze in età scolare ad approfondire temi di cybersecurity e sensibilizzare i docenti sui rischi di stereotipizzazione inconscia.

Quali Interventi Formativi

In letteratura è possibile ritrovare numerosi contributi che illustrano esperienze e strategie diverse di intervento sul tema, sia dal punto di vista strettamente didattico (modificare approcci e strategie di insegnamento, rimodulare i materiali di studio, etc.) che psicologico (riconoscimento e contrasto degli stereotipi, promozione della cultura e del valore della scienza a livello familiare e culturale, etc.). Le evidenze dimostrano che ciascuna di queste componenti può contribuire in modo efficace allo scopo, ma evidenziano anche come gli effetti possano essere limitati o addirittura in alcuni casi paradossalmente controproducenti. Un approccio complesso e multidisciplinare è quindi auspicabile per erogare interventi formativi efficaci, con obiettivi di base mirati a favorire la consapevolezza sul tema (contributo sociopsicologico), da un lato, e a coinvolgere i docenti nell'elaborazione di strategie didattiche disciplinari appropriate (contributo pedagogico-didattico), dall'altro.

CyberEquality.IT, in quanto azione a respiro nazionale, ha organizzato diversi appuntamenti di confronto tra i partecipanti, per condividere le esperienze maturate nelle varie sedi afferenti e stilare delle direzioni di intervento sul tema dell'incremento della partecipazione femminile ai contesti professionali in ambito cybersecurity. Si conviene che la formazione dovrebbe essere rivolta ai:

BIO

Dajana Cassioli è prof.ssa associata di Ingegneria delle Telecomunicazioni presso l'Università dell'Aquila. La sua ricerca riguarda comunicazioni wireless, reti 5G e B5G, e sicurezza. È presidentessa dell'IEEE AG WIE Sez. Italia e ex-presidentessa dell'Italy Chapter IEEE VT06/COM19. È coordinatrice del nodo dell'Università dell'Aquila del Laboratorio Nazionale di Cyber-Security del CINI. Ha ricevuto lo StG ERC VISION (Video-oriented UWB-based Intelligent Ubiquitous Sensing) nel 2010 e il PoC Grant ERC iCARE (Moblle health-Care system for monitoring toxicity and symptoms in cAncer patients Receiving diseasE-oriented therapy) nel 2016.

Agnese Morici è collaboratrice del Center For Cyber Security and International Relations Studies. E' associate di Women For Security, la prima community di cyber ladies italiane supportata dal CLUSIT. Da anni è attiva sul territorio italiano per promuovere l'importanza della Women Peace and Security Agenda delle Nazioni Unite, con alcune attività effettuate presso il MAECI in collaborazione con Women In International Security. Ha conseguito il Master in Protezione Strategica del Sistema Paese: cybersecurity, intelligence, infrastrutture critiche. Ha lavorato per la NATO, su progetti di sicurezza regionale con +30 militari del Nord Africa e Medio Oriente e per l'industria difesa telecomunicazioni satellitari. Ha coordinato diversi progetti a livello internazionale e nazionale nel settore della difesa e sicurezza.

1. docenti delle scuole di ogni ordine e grado, strutturato su due livelli, quello della formazione tecnica e della formazione per una rivisitazione degli approcci didattici al fine di contrastare gli stereotipi di genere;
2. nuovi talenti, strutturato su moduli e percorsi di complessità crescente.

Prospettive di genere nella didattica delle discipline

La formazione tecnica ai docenti delle scuole di ogni ordine e grado dovrà fornire loro gli strumenti didattici e la conoscenza tecnica per poter addestrare i nuovi talenti femminili come *cyberdefenders*. Questo tipo di formazione è abbastanza standard e si avvale di competenze e buone pratiche maturate in molti anni di attività del LNCS. In questo articolo, invece, ci preme chiarire quali

sono le tematiche e le metodologie da applicare nella formazione dedicata ad istituire dei percorsi didattici che includano e valorizzino le prospettive di genere e che minimizzino l'applicazione di stereotipi. Corsi di questo tipo ambiscono a formare figure in grado diriconoscere stereotipi e pregiudizi che sono alla base delle differenze di genere e dei ruoli che vengono attribuiti nella nostra società, e che sappiano sviluppare riflessioni critiche e strumenti per un ***approccio di genere nella scuola***, sulle diverse discipline e sui rapporti in classe, per realizzare una formazione e ***un'educazione al rispetto delle differenze e delle pari opportunità***.

Occorre formare i docenti delle scuole in modo che sappiano sviluppare progettualità educative e didattiche (disciplinari e interdisciplinari) attraverso uno sguardo inclusivo dei generi; utilizzare metodologie e strumenti nella didattica laboratoriale per educare alla parità tra uomini e donne, al riconoscimento delle differenze, alle relazioni tra i generi; conoscere e analizzare le problematiche di genere nei contesti formativi, sociali e culturali.

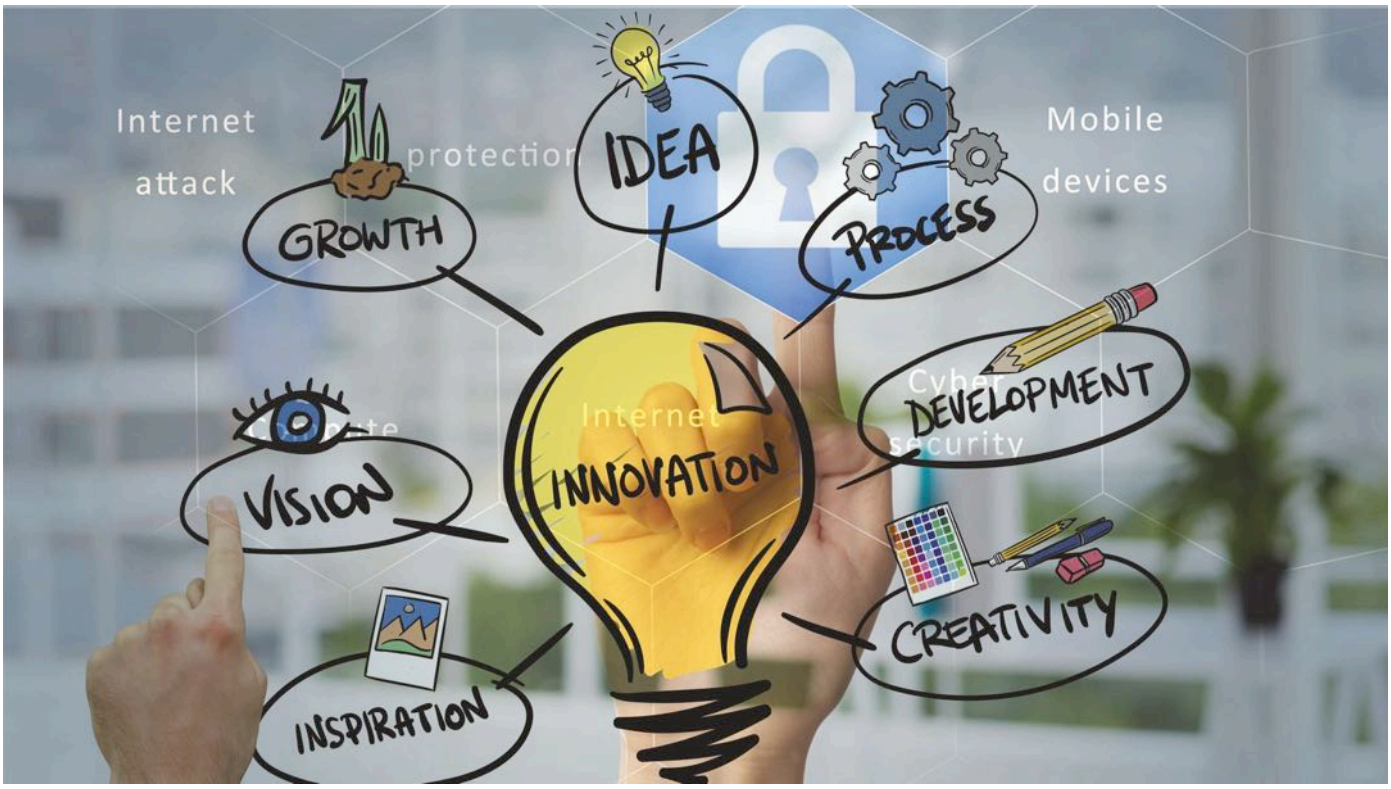
Formazione dei nuovi talenti femminili

Da quanto emerso nei brainstorming in seno al CyberEquality.IT, dovrebbero essere organizzate attività didattiche riservate alle ragazze, in modo da creare un ambiente meno competitivo e più collaborativo, favorevole alla creazione di una community di ragazze. Tale formazione è volta a migliorare le capacità personali *(soft skill)* prima di indirizzare le ragazze nei contesti competitivi, per dare loro consapevolezza e fiducia *(empowerment)*. Abbiamo voluto raggruppare queste attività in due diversi contesti formativi: il *Laboratorio di Innovazione Creativa*, a cui le ragazze possono partecipare durante il periodo scolastico, e un Summer Camp" di una settimana durante l'estate.

In entrambi i contesti è fondamentale che l'attività didattica si sviluppi attraverso il ***mentoring***, l'***addestramento***, il ***gioco*** e le ***competizioni***.

Nel laboratorio di innovazione creativa dovrebbero confluire esperienze di laboratori dedicati a cui parteciperebbero piccoli gruppi di 4-6 ragazze, ognuno gestito da una mentore, che rappresenti un modello di ruolo. Si dovrebbero prevedere diversi livelli di formazione a cui indirizzare le ragazze sulla base di un questionario di autovalutazione somministrato loro all'inizio del percorso, fornendo loro autoconsapevolezza delle proprie inclinazioni personali e del proprio talento *(empowerment)*. Per affascinare le ragazze si dovrebbe puntare su una educazione all'***uso creativo della tecnologia*** applicato a diversi contesti applicativi, perché le ragazze in genere apprezzano l'utilità concreta di quello che fanno e imparano ed è importante collocare nel giusto contesto applicativo gli strumenti di programmazione a blocchi, programmazione Python, sicurezza informatica e privacy, analisi forense digitale e fattori umani di sicurezza informatica (*ingegneria sociale* = modo in cui estranei con intenti dannosi tentano di ottenere informazioni personali e / o danneggiare risorse). È anche importante trasmettere loro il messaggio che il primo obiettivo della cybersecurity è quello di proteggere se stesse. Bisogna anche valorizzare la loro creatività, per esempio attraverso esperienze di *story telling o creazione di scenari virtuali.*

Molto importante è l'approccio alla ***gamification***, che prevede la competizione su sfide di tipo Capture-The-Flag (CTF). Esistono approcci già consolidati, come ad esempio *PicoCTF* [1] o *CyberLand* [2] . Attraverso giochi



online divertenti e interattivi, si introducono concetti chiave nella sicurezza informatica come l'uso di firewall, wifi pubblico ed e-mail di phishing. Gli studenti comprendono come restare al sicuro online, scoprono alcuni ruoli chiave nel settore della sicurezza informatica e la capacità di fare squadra per proteggere i sistemi dagli attacchi. Poiché le ragazze hanno processi cognitivi complementari a quelli dei ragazzi, è necessario selezionare CTF specifiche per le ragazze, che possano suscitare il loro interesse, appassionarle: CTF più soft, più orientate alla logica, per poi andare più sul coding, e successivamente sul reverse engineering. Per sviluppare i *soft skills* è utile prevedere a conclusione di tali percorsi formativi anche presentazioni *(pitch)* o brevi video che raccontino l'esperienza maturata.

Durante la pausa estiva le ragazze hanno più tempo per dedicarsi a corsi di formazione extracurriculari. Infatti, tipicamente le ragazze frequentano maggiormente i licei, in particolare il liceo classico, mentre la presenza di ragazze presso gli istituti più orientati all'informatica e alla tecnologia è comunque ridotta. Per questo, il CyberEquality.IT ritiene estremamente utile istituire un ***CyberCamp***, ossia una settimana di formazione per sole ragazze durante l'estate, progettata per fornire una visione completa dei fondamenti della sicurezza informatica e dell'infrastruttura IT, competenze aziendali di base e integrata da un focus sulla leadership e l'intelligenza emotiva. Esempi di Summer Camp di successo dedicati alle ragazze, ma orientati più all'informatica e alle STEM in generale, sono il Summer Camp *Ragazze Digitali* [4]e il *PinKamP* [5]. Noi proponiamo un campo di addestramento completo di cinque giorni che copra tutte le aree dei domini della sicurezza delle informazioni e le migliori pratiche del settore insieme a seminari interattivi su leadership, intelligenza emotiva e sviluppo personale, orientato all'apprendimento pratico, all'apprendimento dei percorsi di carriera nel settore della sicurezza informatica da parte di professionisti, e al networking con un team di altri studenti. Anche in questo caso è importante

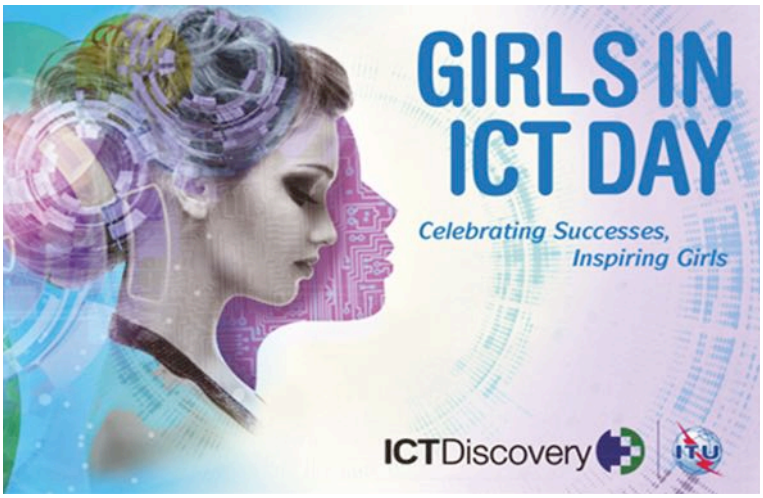
prevedere delle competizioni a squadre attraverso la *gamification*. Tematiche importanti nella formazione a questo livello spaziano dalla ***open source intelligence***, che utilizza le informazioni disponibili pubblicamente come motori di ricerca, archivi pubblici, social media e altro per acquisire una conoscenza approfondita su un argomento o target, alla ***scansione e ricognizione***, che insegna come identificare e utilizzare strumenti adeguati per acquisire informazioni su un obiettivo, inclusi i suoi servizi e le potenziali vulnerabilità, alla ***enumerazione e sfruttamentoper*** identificare exploit e vulnerabilità utilizzabili e utilizzarli per aggirare le misure di sicurezza nel codice.

Integrazione nei programmi scolastici

Per riuscire ad attrarre le ragazze, anche quelle che non sono consapevoli del proprio talento in ambito cybersecurity, e che non possiedono una conoscenza pregressa in informatica, è necessario che le attività formative appena descritte siano integrate nei programmi scolastici. Infatti, in genere si tende a scartare gli impegni extra curriculari che richiedono un impegno elevato, a meno che c'è già un forte interesse per la materia. In generale, le scuole superiori hanno un monte ore basso riservato all'informatica, specialmente i licei tradizionali. Ci si può muovere all'interno del perimetro delle ore di approfondimento, o anche rimodulando i contenuti della tipologia didattica sullo stesso monte ore. Oppure, si può configurare come una attività nell'ambito dei "percorsi per le competenze trasversali e per l'orientamento" (PCTO), ossia la ex-alternanza scuola-lavoro. Attraverso un gruppo di lavoro dedicato ai *Rapporti con Le Scuole*, il CyberEquality.IT si occuperà di analizzare i programmi dei vari tipi di scuola per poter presentare delle proposte mirate, concordando con i docenti le modalità. Ci si ispirerà a programmi che sono già di successo, per es. *codinggirls* [3], che il CyberEquality.IT analizzerà attraverso il gruppo di lavoro dell'*Osservatorio al Femminile*. Bisogna coinvolgere i docenti delle scuole instillando la consapevolezza che si tratta di una missione di sicurezza nazionale, che porta valore aggiunto a tutto il paese. Infine, accreditando sulla piattaforma SOFIA la formazione dei docenti delle scuole come descritta nel paragrafo 1, i docenti avrebbero il giusto riconoscimento nel loro ruolo importantissimo di educatori delle future generazioni.

Comunicazione

Il ruolo della comunicazione è fondamentale per presentare la cybersecurity come realmente è: un mondo stimolante in cui la creatività e la logica sono risorse imprescindibili. Le ragazze dovrebbero rendersi conto di quanto può essere emozionante e significativo il lavoro nella sicurezza informatica e nell'informatica con il nostro approccio al gioco e all'addestramento pratico, provando gli attacchi informatici nel mondo reale, scoprendo come gli esperti di sicurezza informatica svolgono un ruolo fondamentale nella protezione dei nostri ospedali, banche, esercito e servizi di polizia! Anche la comunicazione può nascondere delle stereotipizzazioni di genere, persino nel linguaggio. CyberEquality.IT curerà anche questo aspetto, all'insegna dell'inclusività, perché ciò che conta è il talento individuale e la capacità di fare squadra, tutto il resto non c'entra.



Conclusione

Il Laboratorio Nazionale di Cyber Security del CINI si è dotato del CyberEquality.IT, un gruppo di lavoro trasversale che opera un coordinamento al livello nazionale con l'obiettivo di colmare il divario di genere nella cyber security. Il CyberEquality.IT si è interrogato sulle cause della scarsissima presenza femminile in ambito cybersecurity ed ha avanzato delle proposte, che verranno realizzate nel prossimo futuro. Si tratta di definire dei percorsi di formazione per i docenti, che includano le prospettive di genere nella formazione didattica. E di offrire alle ragazze in età scolare, giovanissime, un contesto femminile nel quale accrescere l'autoconsapevolezza del proprio talento in contesti ad appannaggio maschile, dove le ragazze possano creare la propria community, avere dei riferimenti *(rolemodels)* e acquisire le giuste conoscenze per poter emergere. Abbiamo tracciato delle direzioni sulle quali è opportuno muoversi subito, per costruire un domani più cyber, più equo, ***CyberEquality.IT.***

Ringraziamenti

Le autrici desiderano ringraziare tutto il gruppo CyberEquality.IT per gli innumerevoli spunti di riflessione emersi durante i dibattiti, che hanno popolato questo articolo. Un ringraziamento speciale va a Claudia Canali, dell'Università di Modena e Reggio Emilia, per il suo contributo strutturato ai dibattiti nel CyberEquality.IT.

Bibliografia

[1] https://picoctf.org
[2] https://www.cybersecuritychallenge.org.uk/what-we-do/schools-programme/cyberland
[3] https://www.rainews.it/dl/rainews/articoli/settima-edizione-coding-girls-formazione-ragazze-stem-fondazione-mondo-digitale-21f6226f-1dbc-4b3e-b36c-393de57fdf11.html
[4] https://www.ragazzedigitali.it
[5] http://www.pinkamp.disim.univaq.it ■

Serve alle donne un lavoro di qualità

Intervista VIP a Eleonora Mattia

"Con la proposta di legge n. 182 dell'11 settembre 2019 siamo alle ultime battute in IX Commissione lavoro e pari opportunità del Consiglio regionale. Il testo è stato emendato e votato dai commissari e, una volta approvata la norma finanziaria, passerà all'esame dell'aula. Sono fiduciosa che a breve la Regione Lazio avrà una nuova legge quadro sull'occupazione femminile, quanto mai urgente per far fronte alle nuove sfide del mercato del lavoro. Nel 1977, grazie alla tenacia di Tina Anselmi, il Parlamento italiano approvava la legge n. 603 che ha attuato l'articolo 37 della Costituzione in materia di parità retributiva tra uomini e donne. Oggi in Italia, dopo 43 anni, ancora una donna su due non lavora e il divario salariale raggiunge picchi del 52% di retribuzione in meno per le lavoratrici autonome. La proposta di legge è un tassello del grande lavoro che come Regione Lazio stiamo portando avanti per costruire un mondo a misura di uomini e di donne".

Eleonora Mattia, Presidente della *IX Commissione Lavoro formazione, politiche giovanili, pari opportunità, istruzione, diritto allo studio* della **Regione Lazio**, in quest'intervista rilasciata in esclusiva a Cyber Security Trend entra nei contenuti del **Progetto di Legge 182** di cui è stata la prima firmataria, che intende mettere fine allo sfruttamento della donna, che opera da protagonista oggi più di ieri sulla duplice delicata frontiera del lavoro e della vita familiare, in un bilanciamento di competenze, affetti e responsabilità che ha degli effetti sulla salute complessiva di tutto il corpo collettivo.

Onorevole, quali scenari si potranno aprire per l'universo femminile quando entrerà in vigore il nuovo strumento normativo?

La legge prevede come dicevo all'inizio molte aree di intervento. Si presenta come una normativa quadro sul macro-tema del lavoro femminile e prevede una sezione dedicata all'imprenditoria femminile che potrà godere di fondi finalizzati al sostegno delle aziende virtuose, così da incentivare la cultura aziendale. C'è una grande attenzione al tema della formazione sia in ambito universitario che di formazione continua, con focus su materie STEM e in generale sui percorsi altamente specializzanti per combattere la segregazione di genere che si manifesta nella scelta degli studi e nelle progressioni di carriera. Sono, inoltre, presenti misure per contrastare l'abbandono lavorativo e incentivare l'occupazione femminile tramite appositi sportelli donna nei centri per l'impiego, il supporto al reinserimento lavorativo delle donne vittime di violenza prese in carico dalla rete regionale dei centri e case rifugio e delle donne disabili, oltre che forme di supporto economico – attuabili tramite lo strumento del microcredito – destinati per tutte le donne in condizioni di disagio sociale.

Più si sale nella scala gerarchica, nelle organizzazioni sia pubbliche che private più si avverte la disparità tra uomo e donna. La legge interverrà anche su questo aspetto?

La sua sollecitazione mi permette di ricordare che lo strumento normativo che abbiamo messo in campo definisce un focus per la rappresentanza paritaria nei luoghi decisionali: abbiamo previsto che in tutte le nomine regionali un genere non potrà essere rappresentato, su scala annuale, per più di 2/3 e abbiamo previsto forme di premialità per i Comuni che nella composizione delle Giunte si impegnano a rispettare la parità tra donne e

uomini. Aggiungo infine, per rispondere all'esigenza di conciliare tempi di vita e di lavoro nonché di bilanciare il carico di lavoro di cura, abbiamo predisposto dei voucher per l'acquisto di servizi di *baby sitting* in alternativa alla fruizione del congedo parentale (poco retribuito) per le donne e, sempre nella stessa ottica, dei bonus economici per i padri che restano a casa in alternativa alle mamme.

Esistevano in seno alla Regione Lazio esperienze passate di cui vi siete avvalsi o il lavoro della Commissione che Lei presiede è partito praticamente da zero?

È sempre molto importante guardare con attenzione e rispetto quello che è stato fatto. In quest'ottica abbiamo, perciò, cercato di recuperare le tante buone pratiche già messe in atto dalla Regione, per renderle strutturali, come per esempio, da ultimo, il criterio delle quattro gare da 190 milioni in cui il 16% del punteggio complessivo sarà riservato alle imprese partecipanti che dimostreranno all'interno del proprio organico la presenza di donne nei ruoli apicali, l'assenza di verbali di conciliazione ed una attenzione per la sostenibilità sociale.

Occupazione femminile in Italia: i dati dell'emergenza

Buone pratiche

Confermano i dati Censis che siamo tra i paesi con più basso tasso di occupazione femminile: il 57%. Nazioni come la Germania (70%) o la Svezia (addirittura 81%) ci surclassano. Nel Mezzogiorno il dato dell'occupazione femminile si è addirittura fermato a cinquanta anni fa. Quali sono i principali motivi di un gap sicuramente intollerabile?

Secondo il *Global gender gap index* 2020 - il report che monitora su vari fattori la parità di genere in 153 paesi nel mondo - l'Italia si attesta al 76esimo posto con un punteggio di 0.707 (da 0 a 1). In Europa siamo quasi il fanalino di coda, seguiti solo da Grecia (84), Malta e Cipro (90 e 91). Se ci soffermiamo solo sul dato occupazionale la situazione è complessa: una donna su due non lavora e i divari territoriali sono molto ampi: dal tasso di occupazione minimo del 29,4% in Campania al 65% in Trentino-Alto Adige, a fronte di un dato complessivo per gli uomini (che studiano meno e con risultati sensibilmente inferiori) che è del 73,4%. I fattori alla base di questa evidente disparità sono molteplici. In primis, una cultura che ancora vede nelle donne gli unici soggetti deputati al lavoro di cura e quindi spesso nella condizione di dover rinunciare (perché inconciliabile o non conveniente) al proprio percorso lavorativo al fine di poter assolvere a una "essenziale funzione familiare" come sancito dalla nostra stessa Costituzione all'articolo 37. Al di là, comunque, delle statistiche va tenuto presente che il tasso di occupazione da solo non è sufficiente né a spiegare il problema, né a definire un obiettivo. Quello che serve per le donne è lavoro di qualità, adeguatamente remunerato, con posizioni dirigenziali equamente distribuite, servizi pubblici che supportino le scelte individuali e mettano tutte in condizione di realizzare pienamente se stesse.

Nel suo ultimo saggio il sociologo Domenico De Masi insieme a un folto gruppo di studiosi definisce quella dello Smart Working come la "rivoluzione del lavoro intelligente". Sul piano teorico, questa la tesi di fono, si apre una porzione di tempo "liberato" dall'ufficio tradizionale cui bisognerà conferire valori, diritti e significato. Nella pratica succede però quello che spesso i testi non prevedono: la percentuale di donne che trovano ancora più faticoso svolgere mansioni e incarichi in tempo di pandemia, operando da casa è pari al doppio degli uomini. Dobbiamo concludere che il COVID ha generato un vero e proprio "impatto di genere"?

Assolutamente sì. C'è un impatto di genere legato ai tassi di mortalità che mostrano come il COVID-19 abbia colpito maggiormente gli uomini, ma che allo stesso tempo siano state le donne a pagare il prezzo più alto sotto svariati punti di vista. Se inizialmente il virus era stato definito come un grande "equalizzatore", a uno sguardo più attento sulle caratteristiche occupazionali dei settori a rischio (di contagio ed economico) appare un quadro tutt'altro che equo dell'impatto della crisi fra i generi. Di fatto sta accadendo che in un contesto già fragile come quello italiano, la natura asimmetrica di questa crisi rischia di indebolire ulteriormente l'insoddisfacente partecipazione femminile al mercato del lavoro.

Sono state sempre in primo piano le donne durante questa emergenza che purtroppo non è ancora finita. In primo piano ma anche fatalmente le più esposte con quali conseguenze?

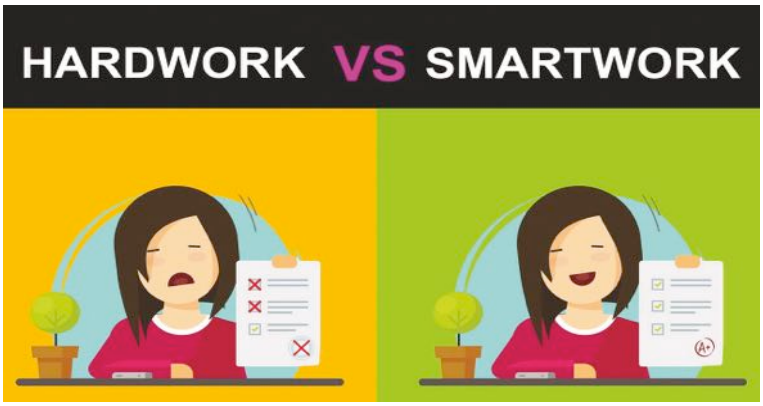
Sicuramente le donne sono state massivamente in prima linea nella lotta al virus, costituendo il 70% della forza lavoro impiegata nei settori sanitario

e sociale. Questa evidenza incontrovertibile le ha però sottoposte a una costante esposizione al contagio nelle strutture sanitarie e assistenziali. Data la segregazione verticale di genere del settore, infatti, le donne sono occupate principalmente nelle mansioni a diretto contatto con i pazienti (che sono per altro come sappiamo quelle meno retribuite) mentre gli uomini dominano nelle mansioni decisionali, che si svolgono a distanza da pazienti. Va poi aggiunto che tutte le donne occupate in settori compatibili con modalità di lavoro agile hanno "sofferto" questa nuova dimensione digitale. Se lo *smart working* presenta sulla carta molti vantaggi in termini di conciliazione dei tempi di vita, in realtà la combinazione con la didattica a distanza e il sovraccarico di lavoro di cura (per i figli, per i parenti anziani e/o malati, per congiunti disabili) ha rappresentato un mix esplosivo a sfavore delle donne.

Smart working e lavoro femminile: un binomio da declinare

Innovazione tecnologica: Smart Working e lavoro femminile come si declina questo rapporto?

Il tema è complesso e anche lo *smart working* presente molteplici vantaggi, ma anche altrettante insidie. Sicuramente non possiamo prescindere oggi, nel parlarne, dall'esperienza del *lockdown*. Come è emerso da svariati studi sul tema, si può parlare di un impatto di genere della quarantena e in particolare di un diverso impatto nella rimodulazione delle prestazioni



lavorative. Secondo l'inchiesta di "Valore D", durante la chiusura, una donna su tre ha lavorato più di prima, riuscendo a fatica, e neanche in tutti i casi, a mantenere un equilibrio tra il lavoro e la vita domestica. Basta pensare che tra gli uomini il rapporto è stato di uno su cinque per capire la differenza. Questa fenomenologia ha un nome: *"extreme working"* ed è rappresentata dalle difficoltà che connotano la modalità agile, che richiede grande disciplina (tanto che per molti è stata una vera e propria sperimentazione) per assolvere a un carico di lavoro di "cura extra", declinato in vari modi: supporto alla didattica a distanza, cura e intrattenimento dei bambini più piccoli, cura della casa, dei congiunti malati o non autosufficienti. Si tratta di un'esasperazione di storture preesistenti, aggravate dalla situazione emergenziale.

La tecnologia non doveva essere un'opportunità di miglioramento della qualità del lavoro e della vita?

Non si tratta di demonizzare la tecnologia, sarebbe un atteggiamento sbagliato oltre che miope, così come non dobbiamo pensare che la "gabbia" della pandemia possa essere rappresentata nel lungo termine, dallo *smart working*. Quello che va analizzato con attenzione è tutto ciò che tale modalità lavorativa svela. Se durante la quarantena è sembrato che il problema potesse riguardare la chiusura della scuola, più in generale la vera questione è la mancanza (o l'eccessivo costo) dei servizi educativi e del tempo pieno. Per essere chiari: il tema che va affrontato non riguarda tanto il maggiore carico di lavoro domestico dovuto alla chiusura in casa, ma che a parità di ore lavorate fuori, la cura degli equilibri e delle esigenze che tengono in piedi gli assetti della famiglia, intesa in senso lato, ricada automaticamente e quasi esclusivamente sulle spalle delle donne. Ritornando al tema centrale della nostra

BIO

Eleonora Mattia è Presidente della IX Commissione Lavoro, Formazione, politiche giovanili, pari opportunità, istruzione, diritto allo studio, Regione Lazio.
Avvocata, da sempre affianca attività politica e lavorativa ed è impegnata in ambito sociale, sui temi del lavoro e al fianco delle donne. Fin da giovanissima realizza inchieste per diverse testate, tra cui L'Unità, occupandosi in particolare dell'emergenza della Valle del Sacco e maturando grande interesse per le questioni ambientali, sensibilità che ha riportato nello svolgimento della sua attività come amministratrice locale. È stata, infatti, vice sindaca e assessora alla Cultura e Politiche sociali nel Comune di Valmontone, dove è cresciuta e vive. Dal 2018, invece, è Consigliera regionale del Lazio e Presidente della Commissione Lavoro, Formazione, Politiche giovanili, Pari opportunità, Istruzione, Diritto allo studio. Grazie alla sua iniziativa legislativa e alla sua tenacia, la Regione Lazio si è dotata di una delle più avanzate leggi sull'equo compenso per i liberi professionisti, di una norma sul plastic free e sulla parità di genere nelle nomine di competenza regionale. Nell'ambito del suo impegno per la difesa delle donne più fragili, ha ideato per le scuole statali e paritarie di secondo grado e gli istituti di formazione professionale del Lazio il Premio in Colasanti ed è stata la promotrice del Protocollo, sottoscritto dalla Regione Lazio e l'Ordine degli Avvocati di Roma, per la tutela legale, sia in ambito civile che penale, delle donne vittime di violenza e stalking. È stata, inoltre, prima firmataria della legge regionale, avanguardia in Italia, sul sistema integrato di educazione e istruzione per l'infanzia ed è prima firmataria della proposta di legge regionale sulla parità salariale e la valorizzazione delle competenze femminili, sulla tutela del lavoro agile e sui patti educativi di comunità.

intervista voglio precisare che il principale gap salariale non ha luogo in azienda dove non si ottengono le promozioni o, nel caso delle lavoratrici autonome, nella svalutazione della propria professionalità che comporta parcelle inferiori. Il problema principale è l'ingente e ingiustificabile quota di lavoro non retribuito che viene quotidianamente e per tutta la vita svolto da ciascuna di noi, spesso senza il minimo riconoscimento.

Quello che dice ricade sul terreno molto dibattuto della riforma del welfare. In particolare nell'ambito del cosiddetto* work life balance *molto deve essere ancora fatto, basti pensare che nell'ultimo anno 37mila donne hanno lasciato il lavoro quest'anno dopo la prima gravidanza. Un dato allarmante. Perché la carriera deve "costare" così tanto alle donne?

I dati su maternità e lavoro sono ancora drammatici e purtroppo nessuna legge da sola, per quanto importante, sarà sufficiente a modificare questo scenario. La parità tra uomini e donne nella società è un obiettivo tanto ambizioso quanto complesso e pertanto richiede un approccio trasversale e multidimensionale in tutte le politiche pubbliche - il cosiddetto *gender mainstremining* - e in particolare sulle politiche sociali e di welfare che hanno un fortissimo impatto sulla vita delle donne. Per questo sono molto orgogliosa del lavoro fatto, per esempio, con la legge regionale 7/2020, che considero un grande risultato, tra i più gratificanti da quando sono stata eletta.

Ci spiega il motivo di tanta soddisfazione?

Su mia proposta e dopo quarant'anni, abbiamo dato alla Regione una nuova legge sui servizi educativi per la fascia 0-6 anni, la prima legge regionale in Italia che attua il sistema integrato previsto dal decreto legislativo 65/2017 mettendo al centro i diritti delle bambine e dei bambini in maniera paritaria fin dalla tenera età e allo stesso tempo consentendo ai genitori – e alle mamme in particolare – di vivere la genitorialità serenamente, con un welfare di supporto che accompagni il ritorno al lavoro e sostenga la conciliazione dei tempi di vita. Detto in sintesi: la legge mira a contrastare i fenomeni della dispersione scolastica e della povertà educativa, garantendo pari condizioni di accesso e partecipazione ai servizi educativi per le bambine e bambini, senza distinzione alcuna di genere, sesso, etnia, età, disabilità

e orientamento religioso delle famiglie, garantendo pari opportunità di educazione, istruzione, cura, relazione e gioco.

Un cambio di marcia non da poco. Siamo maturi per fare un salto in avanti così forte?

Siamo obbligati a farlo, altrimenti non ci potrà essere un progresso reale della società nel suo complesso. Dietro al testo l'idea è quella di ridare valore sociale alla maternità e alla paternità attraverso un investimento serio in infrastrutture sociali. La sfida di una legge quadro sui servizi per l'infanzia persegue indirettamente l'obiettivo di incrementare l'occupazione femminile migliorando gli strumenti di conciliazione, ma consente anche di ripensare il modello di welfare familiare e redistribuire il carico di lavoro di cura ancora eccessivamente sbilanciato a sfavore delle donne. Certamente è necessario anche un cambiamento nella cultura del lavoro per cui, da una parte, la maternità non dovrà essere più percepita come un ostacolo nella vita lavorativa delle donne e, dall'altra, la paternità deve uscire dall'invisibilità attuale all'interno del percorso lavorativo maschile, acquistando al contempo valore.

Le nuove povertà

"Viviamo in un mondo nel quale le donne sono doppiamente povere, per la loro fatica a entrare nell'universo del lavoro e viverci". Sono parole tratte dall'ultima enciclica di papa Francesco. Ha ragione il Santo Padre ad insistere con grande energia e continuità su una questione ritenuta da molti osservatori come una delle grandi emergenze del nostro tempo?

Apprezzo molto il fatto che Papa Francesco faccia luce su un tema cruciale come quello della povertà femminile, di cui in Italia si parla molto poco e spesso male. Se, infatti, si discute molto di disoccupazione femminile o di divario salariale, raramente si arriva più a fondo nel riconoscere che ci sono milioni di donne che vivono in condizioni di indigenza o non dispongono di redditi propri. Nel report Istat "Povertà in Italia" emerge chiaramente che a pagare il prezzo più alto dei tassi di disuguaglianza nel Paese sono le donne di cui, nel 2017, 2 milioni e 277 mila vivevano in condizioni di indigenza. A questo bisogna aggiungere che non essendoci indicatori che permettono di misurare la distribuzione delle risorse economiche tra i componenti dei nuclei familiari è difficile dare conto della complessità della povertà femminile, spesso interconnessa ad altri aspetti economici e socio-culturali.

Cosa vuol dire essere "poveri" oggi?

La definizione è molto delicata e complessa. Guardiamo all'universo femminile che stiamo analizzando. Una donna che vive sotto la soglia di povertà non è esclusivamente sinonimo di non avere una dimora o sufficiente denaro a fine mese. Significa anche non lavorare e dover

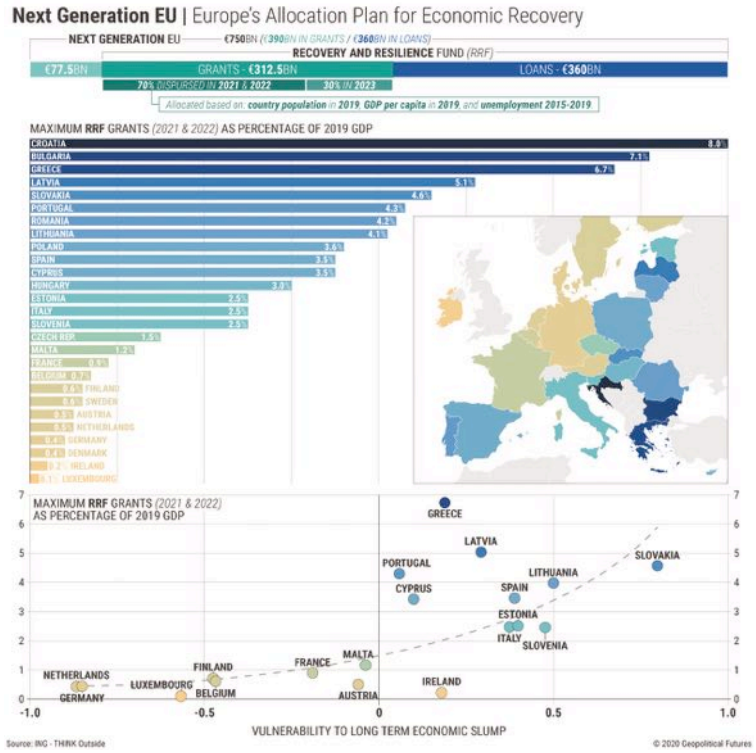
dipendere economicamente da un'altra persona, essere costrette in una relazione malsana o addirittura violenta per avere un tetto sulla testa per sé o per i propri figli, essere una o una donna anziana sola, una donna divorziata con figli a carico, una lavoratrice povera perché sottopagata o occupata in settori poco remunerativi. Questo è un problema sociale, serio e strutturale, che deve trovare spazio nel dibattitto pubblico.

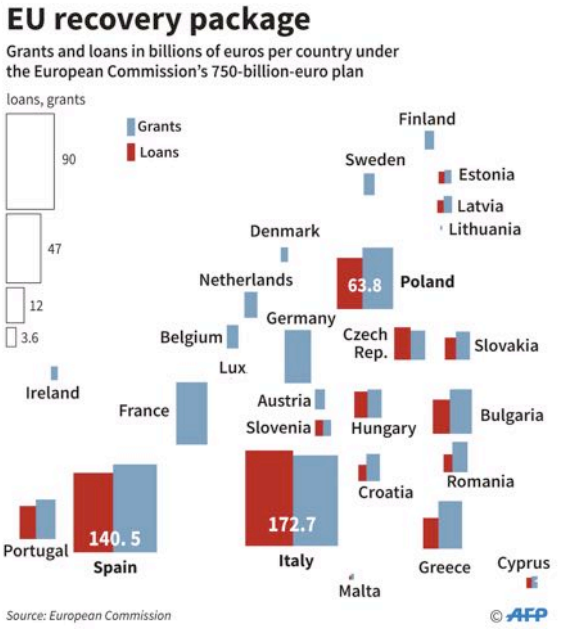
La legge di bilancio, ha dichiarato la ministra per le pari opportunità Elena Bonetti, deve farsi carico di alcuni aspetti importanti che vanno dal sostegno dell'imprenditoria femminile, agli asili nido, al rientro delle donne nel mondo del lavoro, al rafforzamento dello studio delle materie che rientrano nella cosiddetta area "STEM". Occorre varare – ha detto l'esponente dell'esecutivo, un vero e proprio* recovery plan *della parità di genere. Qual è il suo giudizio in merito all'operato di questo governo?

Il governo sta facendo un enorme lavoro di mediazione e di ascolto per raccogliere nel modo più partecipato possibile la grande opportunità che il *Recovery Fund e Next Generation Eu* rappresentano. Un tema a cui tengo molto, come è evidente, è quello dell'istruzione. Quella di ampliare, rafforzare e integrare la copertura dell'offerta dei servizi educativi e scolastici per i bambini tra 0 e 6 anni nonché degli interventi a sostegno della genitorialità è una delle priorità che si sono imposte sull'agenda nelle discussioni relative all'utilizzo dei fondi europei, riconoscendo il ruolo centrale della filiera educativa nel dotare i bambini, sin dai primissimi anni di vita, delle competenze necessarie per affrontare gli ostacoli nel loro percorso di vita. Come già ricordato credo che questa sia un aspetto cruciale sul lungo termine per incidere sulle disuguaglianze di genere, rafforzando al contempo le comunità territoriali e sostenendo le famiglie. Al Piano nidi nazionale, si aggiungono due misure che ritengono fondamentali per partire dalla famiglia nel garantire pari opportunità: riforma del congedo di paternità obbligatorio con l'elevazione da 7 giorni a 3 mesi e la gratuità delle spese sostenute nei primi mille giorni di vita dei figli.

In conclusione Le chiedo: sulla grande partita della formazione, fondamentale per la competitività del paese, a che punto siamo?

Molto aspetti li abbiamo già toccati in questa discussione. Credo sia importante soffermarsi sul capitolo della formazione universitaria, gli incentivi sulle materie STEM e in generale sull'educazione digitale e finanziaria, utile a colmare un altro gap importante che è quello relativo alla cultura tecno-scientifica. Risulterà decisivo guardare oltre il *Recovery Fund*, per adottare un meccanismo di valutazione preliminare dell'impatto di genere degli interventi che saranno finanziati. Non dimentichiamoci che le politiche pubbliche non sono neutre, hanno, infatti, un impatto differente su uomini e donne ed è quanto mai urgente che questo venga riconosciuto e tenuto in debito conto. ■





L'impatto delle tecniche di ingegneria sociale sulla cyber security

Autore: Natalia A., Centro CYBERINT del SRI (Servizio Romeno di Intelligence)

ATTACCHI DI INGEGNERIA SOCIALE: DEFINZIONI

PHISHING

Il termine Phishing si riferisce a un tipo di tecnica di ingegneria sociale utilizzata per individuare le persone che fanno o meno parte di un'organizzazione al fine di spingerli a condividere informazioni riservate. I primi hacker online hanno utilizzato gli indirizzi e-mail per "rubare" informazioni riservate, come password e dati finanziari.

VISHING

Il Vishing è una tecnica di ingegneria sociale basata su tecnologie di messaggistica vocale basate su IP (principalmente Voice Over Internet Protocol, o VoIP) attraverso la quale si induce la vittima a fornire informazioni personali, finanziarie o altre informazioni riservate allo scopo di ottenere una ricompensa finanziaria. Il termine vishing è composto da una combinazione di voce e phishing.

WATERING HOLE

Il termine "Watering Hole" che significa letteralmente "pozza d'acqua" o "abbeveratorio" si riferisce all'avvio di un attacco contro le imprese e le organizzazioni che l'aggressore sta prendendo di mira. In uno scenario di attacco gli hacker compromettono un sito web accuratamente selezionato inserendo un exploit derivante da un'infezione da malware.

In Romania la sicurezza informatica rappresenta un aspetto fondamentale della sicurezza, nel cui ambito è garantito il quadro normativo per la realizzazione della cooperazione e dell'integrazione bilaterale con i requisiti internazionali. La sicurezza informatica garantisce uno scambio rapido ed efficiente di informazioni tra le autorità competenti che sono responsabili della lotta all'uso delle tecnologie dell'informazione e della comunicazione a fini criminali o terroristici. Le tecnologie dell'informazione si sono diffuse in tutti i settori della vita reale, come quello sociale, culturale ed economico. La rapida transizione in seguito alla grande evoluzione di una società industriale verso una società dell'informazione ha generato importanti trasformazioni nella società. La comunicazione nell'era dell'informazione e l'accesso ai dati attraverso una rete offrono notevoli vantaggi a tutti gli individui, poiché l'evoluzione e la conoscenza della tecnologia contribuisce all'evoluzione della società, facilita la produttività e migliora la qualità della vita.

Nell'ultimo decennio si sono verificati numerosi attacchi informatici, sia in Europa che a livello nazionale. L'impatto negativo sulle imprese/istituzioni causato dalle minacce informatiche si riferisce ad esempio al furto di dati e informazioni personali, al furto della proprietà intellettuale. A questo proposito, la sicurezza delle informazioni rappresenta una risorsa importante quando si tratta di eliminare le vulnerabilità, i rischi e le minacce nel campo del cyber intelligence e di ridurre i rischi a livello organizzativo.

Le persone sono costantemente esposte a minacce informatiche online, sia che svolgano il loro lavoro quotidiano in ufficio sia che trascorrano del tempo a casa con la famiglia. Spesso la consapevolezza del pericolo a cui sono esposti i cittadini è minima e il comportamento adottato non è sufficiente per i danni

causati da attacchi così complessi. Anche se in Romania, sia sul web che sui vari mass-media, vengono pubblicati numerosi articoli e rapporti che fanno riferimento a incidenti di sicurezza e al loro impatto sulla società, i singoli o le organizzazioni non adottano le misure più rapide e appropriate per eliminare o prevenire il pericolo (chiara mancanza di cultura informatica).

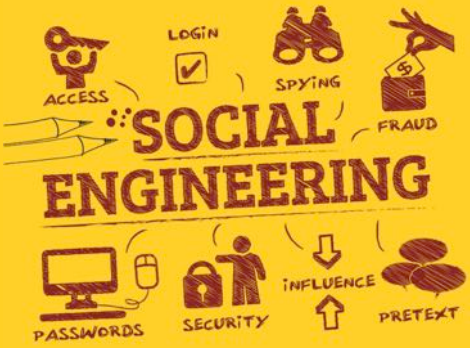
Il social engineering rappresenta l'arte di manipolare le azioni delle persone al fine di far rivelare o rubare varie tipi di informazioni. Il termine è comunemente applicato alla frode allo scopo di raccogliere informazioni, ai furti di identità o all'accesso ai sistemi informatici. Gli attacchi basati sul social engineering includono l'interazione interpersonale che comporta una comunicazione diretta (ad esempio di persona o per telefono) o un'interazione mediata da mezzi elettronici (vari mezzi elettronici, e-mail, social network e Internet).

Inoltre, il social engineering è l'atto di ottenere l'accesso non autorizzato a un sistema informatico o a informazioni sensibili, come le password, utilizzando la fiducia e rafforzando i rapporti con coloro che hanno accesso a tali informazioni.

Il social engineering può essere definito come un modo efficiente e prolifico per accedere a sistemi sicuri e informazioni sensibili, ma richiede anche un minimo di conoscenze tecniche. Gli attacchi di social engineering vanno dalle e-mail di phishing agli attacchi più complessi che utilizzano una gamma sofisticate di tecniche di social engineering. Il social engineering agisce manipolando i normali comportamenti umani e, in quanto tale, le soluzioni tecniche per garantire la protezione sono limitate. Di conseguenza, la migliore difesa è quella far conoscere agli utenti le tecniche utilizzate dagli ingegneri sociali e di aumentare la consapevolezza di come sia le persone

che i sistemi informatici possano essere manipolati per creare un falso livello di fiducia. Questo può essere integrato da un approccio organizzativo verso la sicurezza che, promuove la condivisione dei problemi, applica le regole

ATTACCHI DI INGEGNERIA SOCIALE: DEFINZIONI



SMSishing

Lo SMSishing è una tecnica di ingegneria sociale attraverso la quale i dati personali di un utente possono essere rubati utilizzando il servizio di messaggi brevi (SMS) di un cellulare. Lo SMSishing (SMS + phishing), così denominato da McAfee, una società di sicurezza informatica, consiste nell'inviare un link di un sito web tramite SMS a un utente di smartphone. Quando l'utente si collega al sito web, sullo smartphone viene installato un cavallo di Troia che consente il controllo dello stesso da parte di terzi.

BAITING

L'attacco baiting è come un cavallo di Troia che usa strumenti fisici e si concentra sulla curiosità o sull'avidità della vittima. In questo tipo di attacco gli hacker lasciano dischetti infettati da malware, CD-ROM o chiavette USB in spazi chiusi o aperti, accessibili alle persone, ai quali attaccano tag con messaggi creativi e interessanti e aspettano che le vittime li prendano.

SPEAR-PHISHING

Gli attacchi di spear-phishing si riferiscono a e-mail che appaiono legittime, inviate a un target di persone utilizzando informazioni contestuali rilevanti allo scopo di far rilevare informazioni sensibili agli aggressori o di fare installare malware sui loro computer. Gli aggressori analizzano il profilo psico-socio-comportamentale delle vittime, come la posizione all'interno dell'organizzazione, gli interessi, le abitudini, la situazione finanziaria e familiare. Di solito gli aggressori inviano un numero ridotto di e-mail di spear-phishing per attirare l'attenzione di un numero ridotto di persone o gruppi.

di sicurezza delle informazioni e supporta gli utenti nell'attenersi ad esse. Ciò nonostante, un aggressore determinato con sufficiente abilità, risorse e, infine, fortuna, sarà in grado di impossessarsi delle informazioni che sta cercando.

Gli attacchi social engineering si realizzano rafforzando il rapporto con la/e vittima/e utilizzando tecniche e strumenti psicologici, soprattutto per quanto riguarda il controllo delle emozioni. Questi attacchi sono i più pericolosi ed efficaci perché coinvolgono le interazioni umane. Esempi di tali attacchi sono il baiting e lo spear-phishing. Gli attacchi di tipo tecnologico vengono eseguiti tramite Internet e i social network, siti web, servizi online per raccogliere le informazioni desiderate, quali password, dati delle carte di credito e risposte a domande di sicurezza. Gli attacchi fisici si riferiscono ad azioni fisiche compiute dall'aggressore per raccogliere informazioni sulla vittima. Un esempio di tale attacco è la ricerca fisica di documenti.

Gli attacchi di ingegneria sociale possono combinare vari aspetti discussi in precedenza, come ad esempio quello umano, tecnico, sociale e fisico. Esempi di attacchi di ingegneria sociale sono: "phishing, impersonation, shoulder surfing, dumpster diving, furto di documenti importanti, diversion theft, software falso, baiting, quid pro quo, pretext, tailgating, finestre di Pop-Up, robocalls, ransomware, social engineering online, reverse social engineering e social engineering telefonico". Gli attacchi possono anche essere classificati in due categorie a seconda che l'entità coinvolta sia l'uomo o il software. Possono anche essere classificati in tre categorie in base a come avviene l'attacco: attacchi sociali, tecnici e fisici. Analizzando le diverse classificazioni esistenti degli attacchi di social engineering, possiamo anche classificare questi attacchi in due categorie principali: diretti e indiretti. Gli attacchi classificati nella prima categoria si basano su un contatto diretto tra l'aggressore e la vittima per effettuare l'attacco. E si riferiscono ad attacchi effettuati attraverso il contatto fisico, il contatto visivo o le interazioni vocali. Possono anche richiedere la presenza fisica dell'aggressore nell'area di lavoro della vittima per effettuare l'aggressione. Esempi di tali attacchi sono: "accesso fisico, shoulder surfing, dumpster diving, social engineering telefonico, pretexting, impersonation e furto". Gli attacchi classificati nella categoria indiretta non richiedono la presenza dell'aggressore per sferrare un attacco. L'attacco può essere lanciato a distanza tramite malware veicolato tramite allegati o messaggi SMS. Esempi di attacchi sono: phishing, software contraffatto, finestre PopUp, ransomware, SMSishing, social engineering online.

L'ultimo decennio ha dimostrato che il cyberspazio ha acquisito un'importante dimensione strategica, per quei Stati che gli attribuiscono un valore almeno pari a allo spazio aereo, marittimo e terrestre. La messa in sicurezza del cyberspazio è necessaria per proteggere gli interessi nazionali. A questo proposito, sia a livello europeo che nazionale, gli attacchi informatici sono un elemento comune in operazioni militari complesse e in conflitti internazionali. Nel XXI secolo, un secolo di tecnologia e di informazione, gli attacchi effettuati nello spazio virtuale sono diventati molto più diversificati, subendo un'amplificazione a livello di attori, metodi e tecniche utilizzate.

L'impatto delle tecniche di ingegneria sociale

Oggi la nostra società è considerata una società dell'informazione, l'utilizzo dell'informazione è una delle attività più importanti. L'informazione è considerata come una risorsa essenziale per ogni individuo. In questo senso, l'informazione ha un valore importante per la società ed è imperativo proteggersi per non cadere nelle mani dei nemici. In molti casi, l'informazione è la base da cui si costruiscono le strategie di successo.

La complessità dei metodi e degli attacchi utilizzati dagli hacker ha aumentato l'attenzione delle enti di sicurezza in termini di protezione dello spazio virtuale. La Romania e gli Stati dell'Unione Europea, così come altri paesi, sono diventati molto più dipendenti sia dai componenti della rete di infrastrutture critiche che dalla tecnologia dell'informazione. Questi temi sono importanti per difendere gli strumenti digitali strategici.

La protezione del cyberspazio è vitale in quanto garantisce il funzionamento delle istituzioni governative, delle infrastrutture critiche e del commercio. È noto che lo spazio virtuale oltrepassa i confini geografici e gran parte di esso è al di fuori del controllo e dell'influenza di uno Stato.

I cyber attacchi e la sicurezza informatica sono presenti in tutti i settori sopra presentati, poiché la tecnologia è avanzata e ogni attacco lanciato per danneggiare gli interessi di uno Stato è oggi chiamata guerra ibrida che in alcune situazioni può essere identificata come guerra informatica. Nel campo della cyber intelligence, gli aggressori informatici utilizzano l'ingegneria sociale e le tecniche associate ad essa per ottenere informazioni preziose sulle persone e sulle aziende in cui operano. Gli hacker adottano comportamenti specifici delle tecniche di ingegneria sociale che mirano alla manipolazione sia umana che informativa per raggiungere i loro obiettivi. All'interno del ciclo dell'ingegneria sociale, sia teoricamente che

praticamente, l'anello più debole della catena della sicurezza è il fattore umano.

In uno studio condotto dall'Ufficio federale per la sicurezza dell'informazione, è emerso che un impiegato su sei ha la tendenza a interagire con un'e-mail di phishing o di spear-phishing e a rivelare così informazioni sensibili sull'attività dell'azienda. Utilizzando tecniche di social engineering, con l'aiuto di strumenti di raccolta di informazioni, gli aggressori possono causare danni notevoli.

È stato dimostrato che il comportamento umano è sempre stato facile da plasmare e influenzare attraverso la tecnologia e lo spazio virtuale ha fatto sì che gli individui fossero più interessati all'avventura. Anche se per la psicologia, il pensiero degli individui è stato addestrato ad adattarsi e ad evolversi nel mondo reale, persiste ancora l'illusione che l'ambiente online sia più sicuro rispetto alla vita reale. La capacità di nascondere espressioni non verbali come il linguaggio del corpo e le espressioni facciali offre l'opportunità agli individui di sentirsi anonimi nell'ambiente virtuale. La presenza ininterrotta nell'ambiente online stimola negativamente la capacità di giudizio e aumenta il livello di impulsività. «La disinibizione è facilitata dalle condizioni ambientali del cyberspazio - mancanza di autorità percepita, anonimato, senso di distanza o movimento fisico.

A livello di cyberpsicologia, questo tipo di manifestazione comportamentale nell'ambiente online è chiamato «effetto di disinibizione online», concettualizzato da John Suler. L'evoluzione tecnologica, tuttavia,

cambia il comportamento umano, non sempre in senso positivo ed evolutivo. Le vulnerabilità e le tendenze nell'ambiente reale possono acquisire una valenza critica nell'ambiente virtuale, con un carattere pericoloso e aggressivo.

BIO

All'interno del Centro Nazionale Cyberint, la passione di Natalia è nata assistendo alla rapida evoluzione della tecnologia che copre tutti gli ambiti della vita reale - la parte sociale, culturale ed economica. Mentre l'ingegneria sociale è diventata una delle tecniche più importanti per sfruttare le vulnerabilità umane, la sua voglia di studiare e ricercare questo dominio si è rafforzata ispirata dal bisogno di identificare e rimediare agli effetti prodotti da questi attacchi sugli individui.

Per quanto riguarda l'impatto delle tecniche applicate, si può parlare di un impatto distruttivo nella misura in cui l'obiettivo perseguito è quello di ottenere informazioni sensibili. A seconda del tipo di temperamento e della personalità del bersaglio, l'aggressore utilizza i suoi strumenti di lavoro e applica una tecnica appropriata in relazione alle possibilità di successo. Poiché gli individui hanno fiducia nell'ambiente virtuale e lo trovano un posto molto più sicuro e dove si è liberi di esprimere le proprie opinioni e idee e di adottare comportamenti non autentici, il grado di impatto delle tecniche di ingegneria sociale aumenta notevolmente. La tecnologia e l'ambiente virtuale accessibile a tutte le categorie di individui sociali, ha un alto potenziale di aggravare un disturbo non realistico perché i disturbi mentali di un individuo si intrecciano armoniosamente con l'attendibilità e la complessità delle informazioni disponibili nell'ambiente virtuale.

Oggi, l'ingegneria sociale è diventata una delle tecniche più utilizzate per sfruttare la vulnerabilità delle persone. Conosciuta come l'arte dell'inganno, l'ingegneria sociale è direttamente legata al successo delle tecniche utilizzate per promuovere attacchi virtuali mirati. Questi attacchi mirano a sfruttare l'anello più debole di una struttura di sicurezza: l'uomo. Lo scopo principale è quello di mantenere i contatti con le persone, di compromettere la struttura di sicurezza dell'azienda, provocando perdite di vario tipo.

Le minacce informatiche applicate sotto forma di tecniche di ingegneria sociale sono diventate onnipresenti e le organizzazioni di tutto il mondo sono alla ricerca di modi per ridurre questo tipo di minaccia. Molti di questi rischi provocati dal social engineering possono essere identificati attraverso un'ampia gamma di tecniche di sicurezza informatica, progettate per proteggere i sistemi informativi delle organizzazioni. Le tecniche di ingegneria sociale - che implicano

manipolazione, influenza o inganno, utilizzate per accedere alle informazioni o ai sistemi - sono in aumento. Lo sfruttamento delle vulnerabilità degli individui è la base per il successo delle tecniche di ingegneria sociale e si ottiene attraverso una combinazione di interazioni umane ed emozioni.

I cambiamenti prodotti nella società, sia nella sfera del pensiero individuale sia in campo tecnologico, si sono manifestati così rapidamente che è diventato molto più difficile rendersi conto della differenza tra le tendenze passeggere e gli aspetti comportamentali in continua evoluzione. Le azioni svolte nell'ambiente online possono essere compiute nella vita reale, e questo aspetto mette in evidenza il fatto che l'ambiente virtuale influenza sostanzialmente il mondo reale e viceversa

La possibilità di identificare e accedere all'impronta digitale informatica, soprattutto per quanto riguarda l'utilizzo dei dati nelle aziende informatiche, richiede l'acquisizione di strumenti tecnici in grado di garantire la sicurezza. Inoltre, in questo contesto, è necessario adottare un'educazione preventiva, sia tra i diretti destinatari dell'influenza dei media e delle imprese compromesse, sia tra tutti i cittadini. L'aumento e la diversificazione degli attacchi informatici attraverso l'impiego di complesse tecniche di ingegneria sociale comporta l'adozione di una strategia che mira a sviluppare una sicurezza culturale, soprattutto nello spazio informatico. La capacità di utilizzare i social network e le piattaforme per diffondere messaggi personalizzati e su misura, anche per categorie di pubblico marginali che, purtroppo, potrebbero essere sedotte e incantate da contenuti devianti e diversificati con elementi violenti che cercano di incitare comportamenti e azioni antisociali o aggressive (compresa l'autoaggressione) riflettono un'esigenza ancora più forte di individuare regole e strumenti di responsabilità legale (auto-radicalizzazione attraverso l'ambiente online).

In questo contesto, è necessario realizzare e sviluppare un insieme di leggi nazionali e di accordi internazionali che possano essere una base per lo sviluppo corretto ed etico di questo campo.

La crescente migrazione verso l'ambiente virtuale ha fatto emergere vulnerabilità sia nel fattore umano che ne campo tecnologico. È importante che la società acquisisca un patrimonio di conoscenze sulla cultura della sicurezza informatica. Le risposte a tutti gli aspetti riguardanti l'interazione umana con il cyberspazio sono offerte da una nuova disciplina - la cyberpsicologia.

Bibliografia

1. Anshul Kumar, Mansi Chaudhary, Nagresh Kumar, European Journal of Advances in Engineering and Technology - Social Engineering Threats and Awareness: A Survey, 2015, http://www.ejaet.com/PDF/2-11/ EJAET-2-11-15-19.pdf.
2. Andreea-Maria Târziu, Anastasia Ciupercă, Protezione e sicurezza delle informazioni a livello delle autorità pubbliche nazionali della Romania, 2015, https://mpra.ub.uni-muenchen.de/ 77711/1/ MPRA_paper_77711. pdf.
3. ResearchGate, CANDY: A Social Engineering Attack to Leak Information da Infotainment System, iunie 2018, https://www.researchgate.net/ publication/ 326640482_CANDY_A_Social_Engineering_Attack_to_ Leak_Information_from_Infotain men t_System.
4. Romică Cernat, Răzoiul cibernetic și terorismul cibernetic - Trăsături și răspunsuri la aceste amenințări, Nr. 3, 2020, http://gmr.mapn.ro/app/ webroot/fileslib/upload/files/ arhiva%20GMR/ 2020%20gmr/3%20 202020%20gmr/CERNAT.pdf.
5. Medialine, Instrumente de constientizare a Securitatii impotriva Ingineriei Sociale! https:// www.medialine.ag/ro/instrumente-de-constientizare-a-securitatii-impotriva- ingineriei-sociale/.
6. Mary Aiken, L'effetto cibernetico: Psihologia comportamentului uman în mediul online, 2016, Editura Niculescu, https://books.google.ro/books?id=npPSDwAAQBAJ&pg=PA286&lpg=PA286&dq=amenintarile+cibernetice+inginerie+s ocia la&source=bl&ots=WzACqXCZId=WzACqXCZId&sig=ACfU3U0YWn_FiIFiE4Th6PcW0Z8UBiHDtg& hl=r o&sa=X&ved=2ahUKEwjS27y7w6zqAhVj- SoKHcyuAPc4ChDoATADegQIChAB#v=onepage&q&f=falso.
7. Koceilah Rekouche, Early Phishing, 2011, http://arxiv.org/ftp/arxiv/ papers/ 1106/1106.4692.pdf
8. Oscar Celestino Angelo Abendan II, Watering Hole 101, 13 febbraio 2013, https:// www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/137/watering-hole-101.
9. Imperva, Social Engineering, https://www.imperva.com/learn/ application-security/social- engineering-attack/.
10. Mishra Sandhya și Depriya Soni, SMS Phishing and Mitigation Approaches, 2019, https:// sci- hub.tw/10.1109/IC3.2019.8844920.
11. Gunter Ollman, The vishing guide, mai 2007, http://www.infosecwriters.com/ text_resources/ pdf/IBM_ISS_vishing_guide_GOllmann.pdf. ■

Il security manager del futuro non può avere "genere"

Intervista VIP con Lisa Dolcini

Lisa Dolcini, marketing manager di Trend Micro Italia, sottolinea l'importanza dell'apporto femminile nel campo strategico della cybersecurity. "C'è molto da fare per un'effettiva parità, non solo sul terreno delle politiche pubbliche e nel ridisegno di un nuovo welfare – spiega – perché è la mentalità delle aziende che deve cambiare. La discriminazione è il retaggio di un'incultura, non più tollerabile, perché oltre a mortificare la sfera dei diritti dell'uomo toglie competitività al tutto il sistema – paese".

BIO

Lisa ha alle spalle una carriera significativa nel settore IT, iniziata oltre 15 anni fa in Hewlett Packard e che la vede protagonista in Trend Micro a partire dal 2005, quando entra a far parte del team Marketing & Communication. Nel corso degli anni, Lisa ricopre ruoli sempre più prestigiosi e di maggiore responsabilità, diventando prima Field Marketing Manager e occupando successivamente la posizione di Channel Marketing Manager, consolidando le sue abilità e competenze nelle campagne di marketing e di comunicazione, sia corporate che di prodotto, nella gestione dei partner e delle alleanze strategiche, nella cura dei piani e dei programmi per il canale e nella gestione e organizzazione eventi. Come Head of Marketing Trend Micro Italia, Lisa si cocentra su tutte le attività che riguardano, oltre che il canale, anche gli utenti finali, le PMI, le enterprise, i System Integrator e gli altri vendor partner strategici.

Dott.ssa Dolcini, cominciamo da una vostra eccellenza che sta proprio ai piani alti. Eva Chen, CEO di Trend Micro è stata inserita tra i 100 leader IT più importanti al mondo. Una donna ai vertici, al di là dei tradizionali schematismi fondati sulla cultura del pregiudizio e della discriminazione. Cosa vuol dire questo riconoscimento per l'universo femminile?

Eva Chen oltre ad essere CEO è anche una delle fondatrici di Trend Micro, per cui credo a maggior ragione che questo riconoscimento possa rappresentare una soddisfazione per tutta l'azienda, per il valore riconosciuto al suo valore e all'impegno e attenzione posti all'uguaglianza di genere all'interno della società.

Close the gap ***è un progetto di Trend Micro finalizzato a colmare la differenza di genere (ne stanno nascendo molti anche in seno alle Università, di cui riferiremo in questo numero della rivista). "Viviamo in un mondo nel quale le donne sono doppiamente povere, per la loro fatica a entrare nell'universo del lavoro e viverci". La voce autorevole del Papa si è sollevata in una denuncia che tutti dovremmo fare nostra. Quali sono le finalità del progetto e come intende smuovere quella mentalità retriva che di fatto frena l'innovazione nelle imprese e nelle istituzioni?***

Close the gap è un programma che ricade nell'orizzonte delle iniziative formative che stiamo portando avanti. Lo scopo precipuo è quello di supportare le donne nella ricerca lavorativa. Opera in tutto il mondo con associazioni che hanno questo stesso obiettivo. Bisogna tenere presente che oggi esiste un enorme divario di competenze nella tecnologia, specialmente nel settore della sicurezza informatica. La nostra azienda ritiene, in particolare,

che le donne e una forza lavoro diversificata possano e debbano essere il futuro della sicurezza informatica poiché la diversità è la chiave dell'innovazione e dei progressi. In quest'ottica Trend Micro si impegna ad aiutare le donne e altri talenti ad apprendere le competenze di cui hanno bisogno per far avanzare le loro carriere, creare collegamenti e assicurare posti di lavoro all'interno dell'azienda, dei partner o altre organizzazioni. Importante a questo proposito ricordare la collaborazione con Girls in Tech, un'organizzazione no-profit, per promuovere la consapevolezza e le opportunità di formazione per le donne, nelle carriere tecnologiche in tutto il mondo. Altro aspetto che merita attenzione il "Cultural Shift", definizione che serve a sottolineare come la cyber security sia un settore che richiede collaborazione per la progettazione. Non ci sono problemi di sicurezza risolti o soluzioni progettate da una sola persona o genere.

La* Cyber security *è un ambito che siamo abituati a considerare come prettamente maschile. Sta realmente cambiando qualcosa in questo ambito ritenuto ormai strategico?

Sempre più spesso, anche grazie ai programmi STEM e organizzazioni come Girls in Tech o Women for Security, la presenza femminile si sta accreditando anche in quegli ambiti storicamente ritenuti roccaforti maschili, tra cui la Cyber Security. Vedere sempre più spesso presenze femminili ai vertici di aziende IT o in posti di responsabilità di settori come la security dimostra che il cambiamento, soprattutto di mentalità, è iniziato anche se c'è ancora molto da fare.

L'emergenza sanitaria e il massiccio ricorso allo smart working secondo i dati diffusi dal Censis hanno reso ancora più difficile la vita alle donne. Le tecnologie non sono dunque una opportunità di liberare il tempo, perché possono creare nuove imprevedibili forme di "schiavitù". Qual è il suo giudizio in merito, anche alla luce della sua esperienza di manager?

Il bilanciamento della vita privata e quella professionale è sempre stato una delle difficoltà maggiori incontrate dalle donne che lavorano, questo momento che possiamo definire "eccezionale" ha solo estremizzato ed enfatizzato un problema storico. Lo smart working ha dilatato il tempo dedicato al lavoro; al contempo, il lockdown ha richiesto un'attenzione e un *effort* maggiore per la gestione dei figli e delle attività domestiche. Il tutto nello stesso arco temporale, perciò si è rilevato tutto più difficile.

Sul terreno molto dibattuto della riforma del welfare e del* work life balance *molto deve essere ancora fatto, basti pensare che nell'ultimo anno 37 mila donne hanno lasciato il lavoro quest'anno dopo la prima gravidanza. Un dato certamente allarmante. Ritrovarsi così indietro sulle politiche di conciliazione risulta mortificante non crede?

Ritengo ci siano diversi ambiti su cui si dovrebbe lavorare; non solo politiche di supporto alla famiglia e di conciliazione ma anche il cambio di mentalità all'interno delle aziende. Basti pensare quanto sia difficile ottenere un part time, mentre quando lo si ottiene, caso "fortunato", spesso la contropartita è il demansionamento.

La donna dell'anno "D" scelta dai lettori di La Repubblica è Anna Grassellino, 39 anni ingegnere elettronico, scienziata italiana che negli USA sta progettando il più potente computer quantistico mai creato al mondo. "Una di quelle donne - ha commentato la direttrice del settimanale Valeria Palermi - che ci rendono intollerabile la mediocrità". Questo dimostra, se ancora ce ne fosse bisogno, la grande capacità di leadership che le donne possiedono. Malgrado questo la disparità di salario e di trattamento rimane drammatica, così come rimane minimale la percentuale di donne al comando di aziende e istituzioni. Quali correttivi possono e devono essere messi in atto per voltare pagina?

Il problema della disparità salariale si somma alle tante questioni che ho cercato di evidenziare prima, tutte segnate da un approccio culturale che vede la gestione della famiglia completamente (o quasi) sulle spalle delle donne, salari più bassi e più difficoltà di carriera. È necessario cambiare mentalità, altrimenti la parità di genere diventa pura e semplice utopia.

In conclusione Le chiedo: è azzardato affermare che il profilo del security manager del futuro ideale sarà donna?

Mi piace definire il profilo del security manager del futuro senza "genere", ma con competenze, conoscenze e capacità di sviluppare un piano di cybersecurity e di risk management cucito sulle esigenze specifiche dell'azienda. ■

Bibliografia

Vera Zamagni
Occidente
Ed. Il Mulino

Il destino di una civiltà nell'era della tecnica

Autore: Vera Zamagni *

In cerca di una definizione

Ci vuole coraggio per accingersi a trattare un tema come "Occidente", sul quale sono stati scritti moltissimi volumi e saggi, che sostengono tutto e il contrario di tutto. Mi sono persuasa a dedicarmi a questa avventura perché ritengo che siamo in una congiuntura storica piena di rimescolamenti intellettuali, taluni positivi che servono a "disincrostare" sedimenti storici che minacciano di anchilosare idee e principi basilari per la vita umana, altri invece rischiosi, perché minano i pilastri stessi della nostra civiltà. Uno di questi pilastri è che la realtà storica non può essere negata, anche se può essere reinterpretata. Quanti libri sono stati scritti sulla Seconda guerra mondiale? Ciascuno di questi libri ha avanzato una descrizione/interpretazione diversa delle sue vicende, ma nessuno mai si è però posto l'obiettivo di provare che la guerra non c'è mai stata, un'operazione indegna di attenzione da parte di chiunque, men che meno da parte di intellettuali. Sta invece accadendo con "Occidente" proprio quello che non ci si sarebbe aspettati, ossia si sta iniziando a dubitare che l'Occidente, in quanto civiltà occidentale, sia mai esistito. Ciò avviene paradossalmente perché la civiltà occidentale (di cui "Occidente" è un'abbreviazione) ha talmente intriso di sé il mondo, che ha finito con l'assumere una multiforme caratterizzazione, difficile da definire. Certamente, non è perché siamo in difficoltà con la definizione di qualcosa che questo qualcosa – sia un'idea sia un oggetto – non esiste. In realtà la civiltà occidentale è esistita, oserei dire, "anche troppo": i suoi confini sono incerti e permeabili; i suoi contenuti sono sfuggenti; le sue origini sono miste; la sua evoluzione presenta molteplici contraddizioni. Tuttavia, la sua presenza ha fatto la differenza per il mondo intero, a tal punto che tutte le civiltà non occidentali hanno dovuto fare i conti con l'Occidente, mentre il contrario non è vero. Ancora oggi centinaia di milioni di persone cercano di imitare l'Occidente o addirittura di sbarcarvi. L'Occidente è nato come Europa (la cui radice etimologica significa "dove il sole va a dormire", ossia Occidente), ma è poi andato fuori dall'Europa. Quando nacque, inglobò elementi di civiltà non europee, combinandoli però in una sintesi costruita in Europa, che si allontanava dai concetti di "fato" e di "ciclicità" per sposare quelli di "provvidenza" e "ascensionalità". Va però sgombrato il campo da un'illusione funesta: che esista una civiltà solo buona e che questa sia la civiltà occidentale. La civiltà occidentale ha avuto i suoi risvolti altamente negativi e distruttivi, di cui mi occuperò specificamente nel capitolo secondo.

Le eredità dell'Occidente

Anzi, proprio per le capacità tecnologiche acquisite dall'Occidente e per la sua pervasiva presenza nel mondo, gli aspetti negativi della civiltà occidentale hanno portato a danni immensamente superiori a quelli di altre civiltà. E questa è una riflessione che dovrebbe incentivare una responsabilità molto maggiore da parte di quegli "occidentali" che hanno ancora oggi in mano le leve di quel che succede nel mondo, ma che non può esimere dal riconoscere le eredità positive della civiltà occidentale. Ciò che la distingue, infatti, dalle altre civiltà (anch'esse un insieme di aspetti buoni e cattivi) è il fatto che ha saputo costruire categorie di pensiero e realizzazioni pratiche tali da permettere alle persone di vivere una vita con maggiore chance per lo spirito umano di esprimersi creativamente, sia limitando progressivamente i lavori di mera routine degradante sia permettendo una lunghezza di vita tale da dare agio a ciascuno di far fiorire i propri talenti. Che poi questi frutti della civiltà occidentale non si siano diffusi a tutta l'umanità è in parte dovuto agli effetti perversi di certe azioni perpetrate dagli occidentali stessi (come diremo), ma in parte è anche dovuto alla difficoltà da parte di civiltà diverse da quella occidentale di abbandonare certe loro istituzioni ostative, un tema che approfondiremo. Anche coloro – e sono una schiera crescente – che parlano di declino dell'Occidente sono inevitabilmente portati a riconoscere che l'Occidente c'è stato. Fra questi, alcuni si rallegrano del declino, confidando che una civiltà successiva a quella occidentale possa essere meno distruttiva e più felicitante, ma non sono pronti a indicare su quali basi possa essere fondata questa loro fiducia. Forse sull'illusione che sia stato il capitalismo occidentale a rendere gli uomini cattivi e una volta sradicato il capitalismo gli uomini si comporteranno da fratelli? Ma quando il capitalismo non c'era, c'erano forse meno guerre e meno conflitti? Forse che guerre e conflitti si sono verificati solo in Occidente? Le storie di Caino e Abele e di Romolo e Remo dovrebbero avere insegnato che l'uomo è un Giano bifronte, in qualunque contesto storico e sociale si venga a trovare. Altri si rammaricano, invece, di una possibile perdita dell'Occidente, paventando una regressione a condizioni generali di vita peggiori di quelle attuali, a causa della perdita di quell'"universalismo" dei principi che ha finora garantito l'accumulazione di conoscenze e la condivisione di istituzioni inclusive, in quanto pensate per un'applicazione, appunto, universale. L'approfondimento di questi temi seguirà la seguente scansione: innanzitutto, cercherò di definire l'identità dell'Occidente, e sarà la parte più corposa del testo; seguiranno poi un focus sui "demoni" dell'Occidente e, infine, una riflessione sugli scenari di crisi ed eventuale "superamento" dell'Occidente. Di crisi in Occidente se ne vede tanta, ma di segni

che qualche altra civiltà sia attrezzata oggi per soppiantarne il nucleo culturale se ne vedono davvero pochi, tanto che un illustre studioso come Franco Cardini finisce col preconizzare che "altri [...] ne raccoglieranno [...] e ne porteranno avanti il legato. Ma quali "altri"? L'interrogativo rimane aperto…

*Il testo che pubblichiamo per gentile concessione dell'editore é un estratto dell'introduzione del saggio "Occidente" ■

Federica Spampinato
La nuova scienza del rischio
Ed. Guerini e Associati

L'importanza di rimettere al centro l'uomo

Autore: Federica Spampinato*

Vivere, di per sé, è un'esperienza pericolosa. Ogni giorno prendiamo delle decisioni e per farlo, inconsapevolmente o meno, raccogliamo segni, dati, informazioni sulla base delle quali fondare le nostre scelte. Anche scegliere, in un certo senso, è un'esperienza pericolosa.

Proteggere e proteggersi dovrebbe essere la priorità dell'essere umano, il cui bisogno primario per potersi dire in vita è respirare e il secondo, si potrebbe dire, continuare a respirare.

Quando ho scoperto perché è nata la nuova Scienza del Rischio e di cosa si occupa ho capito che in sé portava, prima ancora dei protocolli operativi, l'introduzione di un modo inedito di occuparsi dell'uomo, rimettendolo al centro con i suoi bisogni primari. Nell'ambiente sociale contemporaneo in cui la logica dominante sembra essere la performance, quello della nuova Scienza del Rischio che rimette l'uomo al centro – e il cui motto è, appunto, Life first! – è un atteggiamento piuttosto sovversivo.

Ho deciso così di raccontare l'evoluzione della Cindynics, la Scienza del Rischio, e di rendermi testimone del lavoro, delle teorie e delle tecniche della nuova Scienza del Rischio, che nasce con un gruppo di ricercatori e professionisti europei e il cui corpus era ancora inedito nel suo complesso, fino a questo momento […]

Mi sono immersa nella Scienza del Rischio in un momento decisivo e, a mio avviso, interessante: quello tra il pre e il post Covid-19. Ho visto i promotori e gli specialisti della disciplina diffondere la nuova visione e i nuovi metodi per neutralizzare il rischio in diversi Paesi. Li ho visti farlo prima che si espandesse la pandemia globale: attraevano un certo pubblico di lungimiranti specialisti, imprenditori, opinion leaders o board members che sposavano la visione innovativa del rimettere al centro la protezione dell'uomo, prima di tutto e a qualunque costo. Poi li ho visti diffondere la stessa visione e gli stessi metodi a pandemia iniziata: l'adesione diventò globale e immediata da parte di ogni tipo di pubblico, incontrando il beneplacito anche degli interlocutori più tradizionalisti e radicati ai metodi classici. Era come se tutti, improvvisamente, si fossero convertiti alla visione della nuova Scienza del Rischio, capendo all'unanimità che quello che si stava facendo per la protezione dell'uomo, a più livelli, non era sufficiente, e la prova era sotto gli occhi di tutti […]

La rivoluzione, per così dire, "copernicana" è avvenuta grazie a quella che più avanti chiamerò "scuola di pensiero di KELONY®", che è la prima agenzia di Risk-Rating al mondo e che ha teorizzato e implementato nuovi protocolli per la neutralizzazione del rischio sovvertendo l'intero panorama dei metodi classici di risk management con innovazioni avveniristiche. Il pensiero di KELONY® concepisce ogni azione all'interno di una visione che auspica che l'uomo ritorni a essere davvero la finalità dell'uomo, e che gli strumenti possano, di conseguenza, rimanere strumenti ed essere catalogati e usati in base alla precedente finalità, assistendo a una ri-prioritizzazione della vita umana. Questo ha un impatto sulle scelte politiche, economiche e sociali e mette con successo l'uomo – e il Pianeta – al riparo dal rischio.

Un approccio onnicomprensivo

Non serve attendere un futuro utopistico per avere teorie e applicazioni differenti ed efficienti rispetto a quelle di cui l'uomo si è servito fino a oggi (e di cui si serve ancora): la nuova Scienza del Rischio, che le ha brevettate e messe in produzione, esiste già. Questa disciplina non è sovrapponibile alla "sicurezza" per come la si intende oggi – ovvero come traduzione ambivalente dei termini anglosassoni safety e security, dove safety si riferisce alla prevenzione dei rischi endogeni (tipici dell'attività che si sta svolgendo) e security alla protezione delle persone dai rischi esogeni (atipici rispetto all'attività che si sta svolgendo) – ma, in un certo senso, ingloba tutti gli strumenti che si occupano di sicurezza in diversi ambiti (industriale, infrastrutturale, informatico, sportivo, sanitario, alimentare, bancario ecc.) con un approccio onnicomprensivo.

Non è nemmeno un sinonimo di risk management così come lo si conosce, perché il risk management, che letteralmente significa "gestione del rischio", si applica al rischio gestibile, come suggerisce anche l'etimologia […]

Nella visione della nuova Scienza del Rischio, che si può definire come l'unica dedicata specificamente al suo studio, il rischio preesiste all'uomo (analogamente al Big Bang) ed è per questo che la scuola di pensiero di KELONY® lo associa alla gravitazione universale newtoniana. Ha a che fare con la fisica delle particelle, con la meccanica quantistica, con il fuoricampo, con l'invisibile e con l'inesorabile. È una disciplina coraggiosa che non ha paura di

dire le cose come stanno, di parlare di fine, di morte, di disastri, per guardare con le lenti migliori nella direzione corretta. La Scienza del Rischio fa quello che alcune discipline, talvolta, si dimenticano di fare: rinobilita esplicitamente l'intuizione e l'immaginazione prima ancora di sottoporre modelli che diventino dogmi da cui poi estrarre il senso della loro stessa creazione. Per questo è anche una questione di grammatica: di morfologia, di sintassi, di semantica; di segni da decodificare, di protezione da codificare e mettere in atto.

Da questa si ricava una teoria della protezione universale, che di certo non elimina la morte dalla vita dell'uomo, ma ne rende lieta e maggiormente sicura la permanenza sul Pianeta, per lui e per le generazioni del futuro[…]

Proprio per questo intraprendo il cammino a partire dal rapporto tra l'uomo e il futuro ignoto, chiedendomi, innanzitutto: cos'è il futuro? Cos'è il non-futuro? E come vengono approcciati nel regime discorsivo contemporaneo?

* Il testo che pubblichiamo per gentile concessione dell'editore é un estratto dell'introduzione del saggio: "La nuova scienza del rischio" ■

Meredith Broussard
La non intelligenza artificiale
Ed. Franco Angeli

Gli esseri umani non possono essere un inconveniente

Autore: Meredith Broussard *

L'invecchiamento del computer

Nei miei piani per Bailiwick non c'è l'eternità. Prima o poi, lo metterò offline, lo archivierò e passerò a un altro progetto di software. Come un'automobile, o una pianta, o una relazione, un software ha bisogno di cure e attenzioni costanti. E, analogamente, ha un ciclo di vita. I siti web, le app e i programmi si rompono sempre perché i computer su cui sono caricati diventano obsoleti o hanno bisogno di essere aggiornati. Il mondo cambia. I software necessitano di aggiornamento. Quando si affida anche il più semplice dei siti web a una società, quella società inevitabilmente cambierà management, oppure sarà venduta, oppure aggiornerà i suoi server, e, altrettanto inevitabilmente, qualcosa andrà in malora. Ogni anno di vita di un software, si accumula un debito tecnico – il costo di mantenimento del software stesso, nonché delle aggiunte di patch o di riparazioni. In un editoriale sul New York Times, Andrew Russell e Lee Vinsel, docenti rispettivamente al Virginia Tech e alla State University of New York, hanno scritto che il 60% dei costi di sviluppo di un software serve per la manutenzione di routine, come la riparazione dei bug o gli aggiornamenti. Contrariamente a quanto si crede, l'enorme numero di ingegneri e sviluppatori di software di cui si prevede ci sarà domanda in futuro non sarà necessario per progetti nuovi e innovativi: il 70% degli ingegneri lavora già oggi alla manutenzione di prodotti esistenti, non alla realizzazione di nuovi. Il problema della manutenzione è utile per ricordarci che quello digitale non è più un mondo nuovo. Come i pionieri del primo boom del ".com", siamo nella mezza età. Se fissiamo l'inizio dell'era digitale agli anni di Minsky o Turing, essa è ormai in età avanzata. È tempo di essere onesti e realisti su ciò che va nella tecnologia e su ciò che è necessario per far sì che continui a funzionare. Io sono ottimista sulla possibilità di trovare una via per utilizzare la tecnologia per sostenere tanto la democrazia quanto la dignità dell'essere umano […].

All'interno della comunità del machine learning, ci sono stati dei passi verso una maggiore comprensione del problema delle disuguaglianze alimentate dagli algoritmi. Fondamentali in questo ambito sono la conferenza e la comunità Fairness and Transparency in Machine Learning. Nel frattempo, il Data Privacy Lab di Latanya Sweeney, docente di Harvard, all'Harvard Institute for Quantitative Social Science sta compiendo un lavoro all'avanguardia nel comprendere le potenziali violazioni della privacy in grandi set di dati, specialmente medici. Obiettivo del laboratorio è creare una tecnologia "che garantisca la protezione della privacy consentendo però alla società di raccogliere o condividere informazioni riservate (o sensibili) per molteplici scopi importanti" […].

Nel momento in cui questo volume sta andando in stampa, DocumentCloud contiene 3,6 milioni di documenti ed è stato usato da oltre 8.400 giornalisti in 1.619 testate nel mondo. DocumentCloud ha custodito i documenti per storie di grande impatto come i Panama Papers o quelli legati al caso Snowden. Il numero di data journalist nel mondo sta lentamente aumentando. L'annuale conferenza NICAR, l'evento annuale per i data journalist, nel 2016 ha superato per la prima volta il migliaio di partecipanti. Ogni anno, premi come il Data Journalism Award celebrano i progetti di giornalismo investigativo basato sui dati che hanno avuto un vero impatto. C'è ragione di essere ottimisti per il futuro. Questo volume ha trattato buona parte della storia e dei fondamentali della odierna tecnologia informatica. Per capire come le persone considerano i computer, ho deciso di visitare il luogo dov'è iniziata l'informatica: la Moore School of Engineering, nel campus della University of Pennsylvania. Qui i turisti possono osservare ciò che resta dell'ENIAC, considerato il primo computer digitale. In un certo senso, la casa dell'ENIAC è il luogo dove anch'io ho cominciato […].

Bibliografia - Cybersecurity Trends

Connettere il mondo richiede collaborazione

Connettere il mondo è un'attività di collaborazione. Dubito, tuttavia, che la tecnologia da sola sia la risposta. La tecnologia ha provocato lo sfaldamento del tessuto sociale in un modo che suggerisce che la connessione sociale in carne ed ossa sia oggi, per i gruppi e le istituzioni, più importante che mai. La comprensione e l'identità di un gruppo possono essere raggiunte al meglio attraverso l'interazione dal vivo e online, non soltanto attraverso uno schermo. Accanto al computer, una pila di libri abbandonati. Ho letto in silenzio i titoli: Life: The Science of Biology; Advanced Engineering Mathematics, III edizione; Students Solutions Manual to Accompany Advanced Engineering Mathematics, III edizione. C'era qualcosa di bello nel vedere la biologia accanto alla matematica, anche se i libri erano stati abbandonati da uno studente distratto. Lasciava ben sperare che lo studente pensasse sia all'evoluzione naturale che alla tecnologia. Fuori dal salone c'erano tre laboratori di informatica, ognuno pieno di decine e decine di computer. Tutti gli studenti nel salone ignoravano l'ENIAC. Alcuni stavano lavorando a una serie di problemi Python. Altri stavano discutendo se avrebbero già studiato o meno per il MCAT (Medical College Admission Test, il test di am- 256 missione alla Facoltà di Medicina). Altri ancora entravano con buste di plastica e contenitori in polistirolo: il pranzo proveniente dai furgoncini-ristorante parcheggiati fuori. Gli studenti nel laboratorio avevano un'aria seria, concentrata e adorabile al pari di tutti gli studenti universitari. Quegli studenti erano ciò che i ragazzi del Model UN volevano diventare di lì a pochi anni. I ragazzi sono fantastici. Adoro lavorare all'università. Un'università è un luogo così pieno di speranze e di solidarietà […]

Quando i computer sbagliano, tuttavia, sbagliano perché sono creati da esseri umani in specifici contesti sociali e storici. I tecnologi hanno delle particolari priorità che informano le loro decisioni sullo sviluppo degli algoritmi. Spesso, queste priorità li portano a oscurare il ruolo degli esseri umani nella creazione di sistemi tecnologici o di dati per l'addestramento delle macchine; peggio ancora, li portano a ignorare le conseguenze dell'automatizzazione sui luoghi di lavoro. Guardando l'ENIAC, sembra assurdo immaginare che questo ammasso di ferro potesse risolvere tutti i problemi del mondo. Eppure, man mano che l'ENIAC è diventato più piccolo e più potente, tanto che oggi ce lo possiamo portare in tasca, è sembrato più facile proiettare sui computer le nostre fantasie. Questo deve cessare. Trasformare la vita reale in matematica è un fantastico trucco di magia, ma troppo spesso la parte sconvenientemente umana dell'equazione viene spinta ai margini. Gli esseri umani non sono oggi, né sono mai stati, un inconveniente. Gli esseri umani sono coloro al servizio dei quali tutta questa tecnologia si suppone che debba essere. E non solo una piccola frazione degli esseri umani: tutti noi dovremmo essere inclusi e tutti noi dovremmo beneficiare dello sviluppo e delle applicazioni della tecnologia […].

*Il testo che pubblichiamo per gentile concessione dell'editore é un estratto del cap.12 del saggio "La non intelligenza artificiale" ■

Una pubblicazione

web for business
swiss webacademy

A cura del

Global Cyber Security Center

Redazione:
Laurent Chrzanovski e Romulus Maier (†)
(tutte le edizioni)
Per l'edizione del GCSEC:
Nicola Sotira, Elena Agresti

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Indirizzi:
Viale Europa 175 - 00144 Roma, Italia
Tel: 06 59582272
info@gcsec.org
Şcoala de Înot nr.18, 550005,
Sibiu, Romania

www.gcsec.org
www.cybersecuritytrends.ro
www.swissacademy.eu
www.cybertrends.it

BUCHAREST 5+

CHOICE FOR CYBER

Government of Romania

www.bucharest4cyber.ro