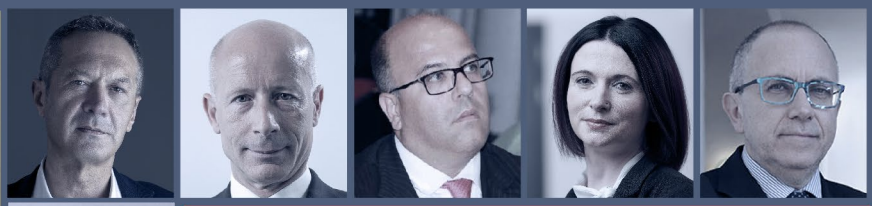
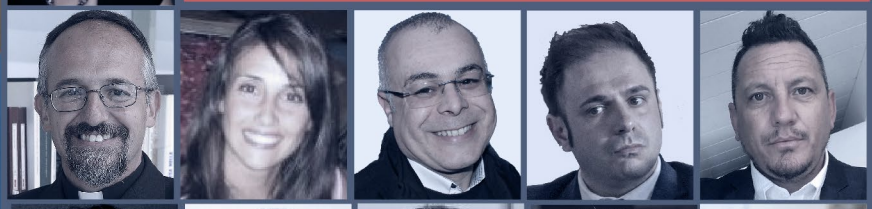
CYBER MAGAZINE

CYBER Think Tank ASSINTEL

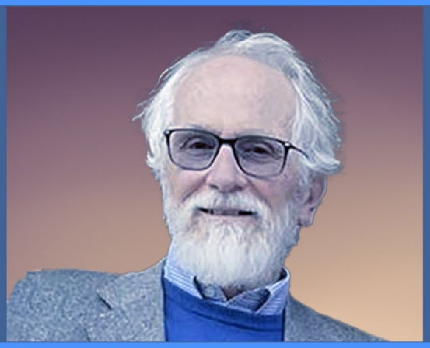
Gennaio 2024



Cyber Think Tank Assintel



Intervista Speciale ◆ Intervista Speciale ◆ Intervista Speciale ◆ Intervista Speciale



Intervista Speciale ◆ Intervista Speciale ◆ Intervista Speciale ◆ Intervista Speciale

Menti unite, confini digitali sicuri.

Partecipa al nostro think tank!

CYBER
Think Tank
ASSINTEL

Prossimo Incontro

24 gennaio

Ore 14:00

Chi siamo?

Il Cyber Think Tank Assintel è un hub di collaborazione in cui aziende e professionisti lavorano insieme per affrontare le sfide più pressanti in materia di sicurezza informatica a supporto degli Associati Assintel e del mercato in generale.

I nostri obiettivi

Il Cyber Think Tank affianca le aziende utilizzando standard, best practice e le migliori tecnologie disponibili in commercio.

COORDINATORE DEL CYBER MAGAZINE:

Pierguido Iezzi

COMITATO SCIENTIFICO DEL CYBER MAGAZINE:

Antonio Assandri, Gianpiero Cozzolino, Vittorio Orefice

REDAZIONE DEL CYBER MAGAZINE:

Federico Giberti, Melissa Keysomi, Daniela Grossi, Elisa Buonocore

CYBER THINK TANK ASSINTEL

INDICE

WEBINAR

Il Cyber Risk in produzione

La security OT partendo dalla base: mettere in sicurezza macchine e impianti

CYBER Think Tank ASSINTEL

Relatori

Carlo Wolter

Sergio Cazzaniga

Mario Testino

31 gennaio

12:00 - 13:00

Per info scrivi a:

segreteria@assintel.it

L'editoriale del Coordinatore di Cyber Think Tank Assintel Pierguido Iezzi

Gennaio 2024

Carissimi lettori,

È con grande entusiasmo che vi presentiamo il primo numero del 2024 del Cyber Magazine, curato con attenzione dal Cyber Think Tank di Assintel. Questa edizione, arricchita da una serie di articoli redatti da esperti di spicco del settore, si propone di esplorare temi di cruciale importanza nel campo della cybersecurity e della tecnologia digitale.

Tra i punti salienti di questo numero, desideriamo sottolineare l'inclusione di un'esclusiva intervista con il Ministro della Difesa, Guido Crosetto. L'approfondimento del ruolo cruciale della cybersecurity nei contesti geopolitici ed economici sarà al centro della discussione, evidenziando l'attenzione significativa che il Ministero della Difesa dedica a questo ambito strategico.

La conferma della qualità dei contenuti è un altro aspetto che ci rende fieri di presentare questa pubblicazione. In questo numero verranno trattati una vasta gamma di argomenti, dal trasferimento dei dati in conformità con la Direttiva 2016/680/UE sulla Polizia e Giustizia Penale al ruolo cruciale dell'intelligenza biologica nella sicurezza e molti altri che sicuramente contribuiranno a arricchire la vostra comprensione delle sfide e delle opportunità nel mondo della cybersecurity e dell'innovazione tecnologica.

Ringraziamo tutti voi per essere parte di questo viaggio e vi auguriamo una stimolante lettura!

Pierguido Iezzi

CYBER Think Tank ASSINTEL

CYBER
Think Tank
ASSINTEL

Threat Infosharing

Cyber Think Tank Assintel

Per info scrivi a:

segreteria@assintel.it

Intervista al Ministro della Difesa, On. Guido Crosetto.

Il Ministro della Difesa Guido Crosetto

Q1: Dalla guerra tradizionale a quella cibernetica, com'è cambiato l'approccio alla difesa. In cosa l'Italia deve ancora investire?

Negli ultimi anni la minaccia del settore cyber è cambiata drasticamente al punto che il cyberspazio è divenuto un nuovo dominio di operazioni al pari dei domini "tradizionali" (terrestre, marittimo, aereo) e, più recentemente, lo spazio. Nell'attuale contesto, in relazione all'incertezza del quadro internazionale, alla maggiore assertività di attori statali e non, passando per il *cybercrime*, tutti i paesi hanno indistintamente accelerato i programmi di rafforzamento delle proprie strutture organizzative e operative dedicate alla *cybersecurity*. Infatti, le forme moderne di conflittualità evidenziano come la componente tecnologica assuma un ruolo fondamentale sia quale fattore abilitante, sia quale elemento di competizione e confronto strategico.

Ciò di fatto implica l'esigenza di elevare il livello del confronto da quello classico del conflitto sul terreno, a quello della superiorità tecnologica e informativa tra gli attori coinvolti e di sviluppare capacità strategiche nazionali nei settori prioritari d'interesse.

Per questo motivo, la Difesa sta accelerando i propri processi di digitalizzazione e rivedendo il suo modo di operare attraverso una serie di iniziative volte ad assicurare anche nel c.d. dominio cibernetico i propri compiti istituzionali per garantire la protezione e la sicurezza degli interessi primari dello Stato. La sfida, quanto mai complessa, è quella di esprimere capacità operative all'avanguardia: dall'Intelligenza Artificiale, a servizi *cloud* evoluti, da info-strutture in ambito spaziale, tra cui le reti satellitari ad orbita bassa, a nuovi standard di cifratura e sicurezza delle informazioni e relativi effetti derivanti dallo sviluppo del *Quantum Computing.*

Questi sono solo alcuni dei settori d'interesse strategico non solo per la Difesa ma, come si può immaginare, per il Paese, con un ruolo centrale dell'industria, delle *start-up* e delle eccellenze che assumono una valenza strategica anche per lo sviluppo delle necessarie capacità nazionali in generale e di quelle più specificatamente a connotazione militare. Certamente, la Difesa non potrà sviluppare internamente tutte le proprie esigenze, ma potrà invece costituire uno dei principali *driver* dell'innovazione, in sinergia con le altre Pubbliche Amministrazioni, con il mondo accademico e il tessuto produttivo naziona-

le. Da questo punto di vista, soltanto nelle collaborazioni tra pubblico-privato si potranno individuare le necessarie soluzioni per conseguire la necessaria competitività dell'ecosistema produttivo nazionale.

Q2: Molti giovani, anche a seguito della guerra Russo – Ucraina, si stanno sempre più avvicinando alla cybersecurity, di che tipo di formazione e di competenze si parla?

Investire nella formazione di professionalità con specifiche competenze nel settore *cyber* è, al giorno d'oggi, non solo strategico ma anche essenziale. La carenza di professionisti con competenze adeguate in sicurezza cibernetica è una problematica globale per la quale anche la Difesa deve riuscire a trovare soluzioni idonee e forme innovative per attrarre i giovani talenti che escono dal mondo della scuola e dell'università.

Tra le iniziative già avviate, il reclutamento di laureati in ingegneria e informatica in grado di lavorare in un settore fortemente dinamico e stimolante come quello della cybersicurezza e delle operazioni cibernetiche. Il percorso formativo dei nostri operatori *cyber* coniuga sapere e saper fare, a similitudine di quanto avviene per il comparto di Forze Speciali. Dopo la prima fase di selezione, il personale frequenta uno specifico *iter* formativo che rappresenta un *unicum* per quanto concerne le competenze e le capacità professionali acquisite in ambito nazionale. Nel corso di studi si conseguono anche certificazioni *cyber* di livello internazionale. Al termine del periodo formativo di circa sei mesi, i neo specialisti sono impiegati in alcune delle realtà di eccellenza della Difesa, al fine di consolidare la formazione e operare nell'ambito delle varie attività nazionali ed internazionali, utilizzando alcune delle più avanzate soluzioni tecnologiche a disposizione, contribuendo al contempo allo sviluppo di nuove. Nel complesso, è stato realizzato un percorso formativo "non convenzionale", multidisciplinare e in continuo aggiornamento, anche attraverso l'osmosi e la sinergia con l'università, l'industria, le piccole e medie imprese e le *start-up leader* di settore. Il personale che andrà ad alimentare la forza *cyber* della Difesa, dopo un periodo in uniforme, potrà decidere se rimanere, usufruendo di forme di *retaining*, oppure "uscire" dalla Difesa e mettere le conoscenze acquisite a disposizione di altre Pubbliche Amministrazioni e del settore privato, anche per il conseguimento di una maggiore competitività sistemica.

Stiamo pensando a ulteriori iniziative per attrarre e rafforzare le competenze in ambito tecnologico a supporto dell'ecosistema Difesa, tra queste la realizzazione di una riserva *cyber* che possa coinvolgere anche le professionalità del mondo privato da attivare in caso di evento o crisi cibernetica, a completamento delle capacità esprimibili dalla Difesa.

Q3: Ogni volta che un governo ha espresso supporto all'Ucraina con tangibili segni di solidarietà, immediatamente ha subito un attacco hacker. Qual è lo stato di sicurezza attuale del nostro Paese e come la UE e l'Italia stanno rispondendo?

L'attuale scenario globale, dove ogni aspetto è legato all'ambiente digitale, è ormai caratterizzato dalla persistente presenza di attività cibernetiche malevole nei confronti delle funzioni e dei servizi essenziali (ovvero delle infrastrutture critiche) degli Stati che, sfociando in forti impatti nel mondo fisico, mirano a destabilizzarne la sicurezza e l'ordine pubblico.

Investire nella formazione di professionalità con specifiche competenze nel settore cyber è, al giorno d'oggi, non solo strategico ma anche essenziale.

A conferma di ciò, i dati rilevati ci dicono che tutte le tipologie di attacchi informatici continuano ad aumentare, anche a causa degli eventi connessi al conflitto russo-ucraino nell'ambito di operazioni cyber e campagne di disinformazione da parte di c.d. hacktivisti. Dal *cyberspace*, spesso coordinando, in modo ibrido, altre iniziative in campo economico, finanziario, diplomatico, o cognitivo, mediante campagne di comunicazione, si può raggiungere il centro di gravità della nazione, piuttosto che i centri nevralgici della società, dell'opinione pubblica, delle attività produttive e delle infrastrutture critiche nazionali, creando instabilità e tensioni sociali. Anche in questo istante, entità statali e non, nascoste nell'anonimato dello spazio cibernetico, attraverso organizzazioni c.d. *proxy,* conducono azioni malevole "sotto soglia" sfruttando le nostre vulnerabilità per raggiungere i propri obiettivi.

Immagine da: https://www.difesa.it/

Proprio per questo ogni Paese sta cercando di migliorare la propria capacità di comprendere e rispondere a questi fenomeni. Ne deriva quindi la necessità di disporre di un ecosistema nazionale resiliente e reattivo in grado di contrastare quotidianamente le attività ostili che vengono implementate nel dominio cibernetico.

Una sfida che coinvolge a livello nazionale in modo trasversale le Istituzioni, le Forze Armate e di Polizia, la Pubblica Amministrazione, le infrastrutture critiche e il settore privato. In tale ottica, coinvolgendo tutti i settori del Sistema Paese, è fondamentale sviluppare, attraverso interventi normativi ed investimenti dedicati, idonei meccanismi e capacità atti alla prevenzione e al contrasto di tali minacce concentrando le proprie forze a costante presidio e difesa del dominio cibernetico.

Da questo punto di vista, l'Italia negli ultimi anni ha fatto molto per migliorare la cybersicurezza e, in generale, la propria resilienza. La riforma dell'architettura nazionale cibernetica - attuata attraverso l'adozione del D.L. 82 del 14 giugno 2021 - ha istituito l'Agenzia per la Cybersicurezza Nazionale (ACN), con l'obiettivo di razionalizzare il sistema *cyber* del Paese. Al contempo, la costituzione, in via permanente, del Nucleo per la CyberSicurezza (NCS) quale cabina di regia nazionale per le procedure di allertamento, prevenzione e gestione di eventuali situazioni di crisi, costituisce un passo essenziale per comprendere la minaccia e rispondere in modo adeguato. In prospettiva, l'esigenza è quella di migliorare il coordinamento tra i vari attori nazionali attraverso procedure di gestione degli incidenti che, coinvolgendo in maniera permanente i c.d. Pilastri Cyber dell'architettura nazionale cibernetica, ottimizzino l'impiego e lo sviluppo delle capacità cibernetiche del Paese.

Nello stesso tempo, l'Unione Europea ha contribuito in modo rilevante a ridisegnare la materia della cybersecurity e della resilienza nazionale, dando vita a provvedimenti normativi sui quali si sono spesso ancorate e animate le iniziative dei singoli Stati. Da questo punto di vista, i programmi sia in ambito civile che in ambito militare porteranno ulteriori benefici alla sicurezza del Paese e a quella collettiva europea, in un contesto in cui la minaccia risulta transnazionale e priva di confini geografici.

Q4: Quali sono oggi le sfide principali che le tecnologie emergenti come la IA presentano per la protezione dei diritti digitali dello stato e dei suoi cittadini e quali gli strumenti che possono o devono essere utilizzati per tutelare privacy, sicurezza e libertà d'espressione?

L'Intelligenza Artificiale è tra le priorità strategiche dell'agenda del governo italiano. Come annunciato dal Premier durante il recente *summit* di Londra proprio sull'IA, la consideriamo la più grande sfida intellettuale, pratica e antropologica di quest'epoca e sarà uno dei temi al centro della Presidenza italiana del G7 del prossimo anno. La volontà è quella di organizzare a Roma una Conferenza internazionale su Intelligenza Artificiale e lavoro, a cui vorremmo partecipassero studiosi, *manager* e esperti di tutto il mondo per discutere metodi, iniziative e linee guida sull'IA. Stiamo anche lavorando per completare il Piano strategico nazionale per l'IA, costituendo un fondo specifico per sostenere le *start-up* italiane e comitati per studiarne l'impatto nei vari settori d'interesse.

L'Intelligenza Artificiale è tra le priorità strategiche dell'agenda del governo italiano.

La preoccupazione è che meccanismi decisionali opachi, discriminazioni e usi impropri di questi strumenti possano costituire un'intrusione nella nostra vita privata ed essere utilizzati per atti criminali, per produrre armi, per causare danni biologici a bassa tecnologia, attacchi informatici o altro; in altre parole, costituire una minaccia per la sicurezza e la difesa dello Stato.





Da questo punto di vista, la sfida è quella di maturare un approccio equilibrato tra innovazione e tutela dei diritti tramite meccanismi di *governance* multilaterali, ricercando la definizione di regole comuni e garantire barriere etiche all'intelligenza artificiale, nell'ambito di un quadro normativo adeguato necessario a sfruttare le opportunità che l'IA può offrirci. In tal senso, sosteniamo e collaboriamo con l'Unione Europea verso l'approvazione dell'*Artificial Intelligence Act*, con il quale l'Unione si è assunta responsabilmente il compito di garantire un uso attento del bene pubblico ed evitare usi distorti a fini commerciali o, peggio, di sicurezza. Come ha chiaramente indicato la Premier, l'obiettivo è quello di sviluppare dei "*guardrail* etici" ossia <<*un insieme di principi etici da porre alla base del governo dell'IA generativa e le tecnologie correlate, da seguire nello sviluppo nella diffusione e nell'uso di queste tecnologie, sia nel settore pubblico che in quello privato*>>. Ciò al fine di tutelare, da una parte, le opportunità derivanti dall'uso di queste tecnologie e dall'altra i diritti fondamentali. La priorità numero uno per i prossimi anni è fare in modo che l'Intelligenza Artificiale sia incentrata sull'uomo e controllata dall'uomo.

Q5: Qual è il livello di adozione della direttiva NIS da parte del nostro Paese?

La Direttiva sulla sicurezza delle reti e dei sistemi informativi dell'Unione ha stimolato tutti i Paesi ad adottare misure concrete. In Italia, il quadro normativo è stato ulteriormente rafforzato da provvedimenti, quali, ad esempio, l'istituzione del Perimetro di Sicurezza Nazionale Cibernetica. Un primo passo essenziale anche se il problema della *cyber* va inquadrato nell'ambito di un processo e in quanto tale deve essere continuamente aggiornato. In tal senso, si dovranno individuare le modalità e le risorse per elevare ulteriormente la sicurezza, coinvolgendo in modo sistemico le Istituzioni, la Pubblica Amministrazione e il settore privato.

Q6: Relativamente alla guerra in Israele, come pensa che cambierà l'approccio alla cybersecurity anche alla luce di quello che sta avvenendo?

Gli attuali conflitti stanno influenzando in modo significativo il campo della *cybersecurity*. Di fronte a minacce crescenti e sempre più sofisticate, è chiaro come essa costituisca un elemento fondamentale dell'attuale quadro nazionale e internazionale. La capacità di operare nello spazio cibernetico è diventata dunque una priorità per la sicurezza nazionale ed è uno dei fattori più significativi alla base dell'esigenza di evolvere verso un nuovo "paradigma della sicurezza", sempre più connesso con lo "sviluppo tecnologico". Governi e aziende stanno riconoscendo che gli attacchi informatici possono infliggere danni significativi, destinando maggiori risorse in questo settore. In prospettiva, le nuove tecnologie costituiscono un'opportunità, ma al contempo un ulteriore rischio. Ad esempio le tecnologie quantistiche costituiscono uno dei progressi tecnologici più eccezionali del nostro tempo,

con il *Quantum Computing* che sta aprendo orizzonti fino ad oggi inimmaginabili, superando le limitazioni dei tradizionali metodi di elaborazione dei dati. Ma, in questa straordinaria potenza computazionale emergono sfide significative come quelle per la sicurezza delle comunicazioni e la protezione dei dati. Infatti, il costante progresso nella capacità di calcolo dei *quantum computer* rappresenta una minaccia per la crittografia comunemente utilizzata ed è fondamentale riconoscere come ricerca e sviluppo nello stesso ambito tecnologico quantistico presentino le risorse per affrontare tali sfide. Ma, anche in questo caso, la sinergia pubblico-privato all'interno della visione del Sistema Paese è la risposta più lungimirante per combinare le competenze e gli investimenti necessari per affrontare anche questa sfida che - come altre - traguarda importanti opportunità. Da questo punto di vista, le sfide che ci aspettano sono enormi e complesse, ma sono sicuro che attraverso la sinergia e la cooperazione tra Istituzioni, mondo dell'impresa, dell'Università e della ricerca, troveremo le necessarie capacità, risorse e competenze. Sarà da ricercare, inoltre, nell'ambito delle organizzazioni internazionali di riferimento, NATO e UE, iniziative volte a rafforzare le capacità collettive a fronte di una minaccia per natura priva di confini geografici e transnazionale.

La Direttiva sulla sicurezza delle reti e dei sistemi informativi dell'Unione ha stimolato tutti i Paesi ad adottare misure concrete.

Scrivere e pensare nell'era digitale

"Per governare il prepotente sviluppo della tecnica dosi massicce di cultura critica".

A colloquio con Franco Lo Piparo, a cura di Massimiliano Cannata

"Il mondo è cambiato radicalmente, siamo appena agli inizi di una rivoluzione che non ha precedenti. Lo *Smartphone* che teniamo in tasca ha modificato la nostra vita quotidiana, il nostro modo di relazionarci, il nostro essere nel mondo. In questo contesto scrivere sarà un problema, semplicemente perché l'IA scrive meglio di noi. Distinguere tra la scrittura umana e quella artificiale non sarà facile. Cosa accadrà è difficile dirlo. Esercitare la critica, educare i giovani ad argomentare e contro argomentare, avrà un'importanza decisiva. La mia generazione, che è quella del '68, era abituata al confronto dialettico, oggi servirebbe un po' di contestazione, ben argomentata si intende, ma servirebbe". Franco Lo Piparo, filosofo del linguaggio, allievo di Tullio De Mauro, professore emerito dell'Università di Palermo, ha ricevuto a Mistretta il massimo riconoscimento alla carriera in occasione della XVIII edizione del Premio Maria Messina. Lo abbiamo intervistato traendo spunto dalla lezione che ha tenuto presso il Circolo Unione della città su una grande questione del nostro tempo: scrivere e pensare nell'era digitale. Intuitivamente crediamo tutti di conoscere il legame che sussiste tra scrittura e pensiero, spiegarlo è reso ancora più difficile dai cambiamenti in atto che stanno generando una nuova tecnica e una grammatica espressiva ancora poco conosciuta.

Prof Lo Piparo, abbiamo perso la bussola. Le categorie della conoscenza si stanno modificando, sollecitate dalla rivoluzione digitale?

Viviamo in un mondo digitalizzato. Lo sappiamo non da oggi. Siamo abituati ad avere in tasca un oggetto che ha una potenza di calcolo e una capacità di memoria superiore a quella dei PC che gli americani hanno utilizzato per lo sbarco sulla luna nell'ormai lontano 1969. I saperi enciclopedici, le informazioni più disparate, il nostro essere nel mondo "poggia" sullo *smart phone*. Consultiamo le app, che sono già una manifestazione dell'intelligenza artificiale, per andare al cinema, per cercare un medico, per sapere se c'è traffico, per scegliere un ristorante. Abbiamo fatto tutto questo pensando di essere e valere "più della macchina".

Fino a prova contraria è così, non crede?

Fino a prova contraria, appunto. Ma chi stabilisce il grado di intelligenza e la differenza tra l'uomo e la macchina? Il matematico inglese Alan Turing (1912-1954), aveva inventato il celebre test che consentiva, in ambiente isolato, di misurare la differenza di comportamento tra un individuo e un pc. L'elaboratore perdeva sempre, in quanto non sa parlare, né pensare con le parole, né tanto meno argomentare.

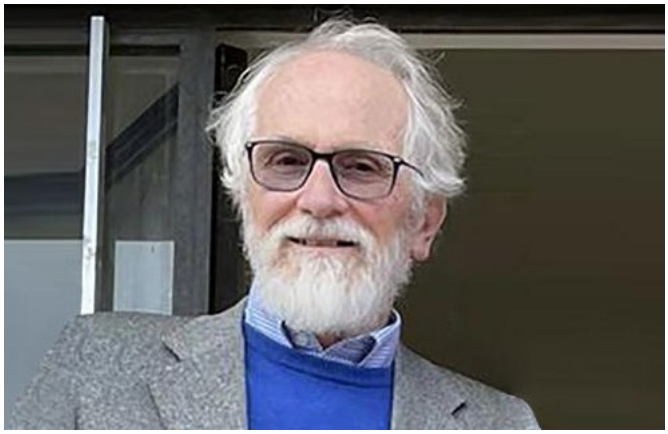
Quest'anno è successo però qualcosa di imprevisto.

A che cosa si riferisce?

Alcuni giornali americani prima e italiani poi, a cominciare da *Il Foglio*, hanno inserito un articolo prodotto con l'IA chiedendo ai lettori di riconoscerlo. Io stesso ho partecipato a questa sfida, ne sono uscito sconfitto. *ChatGPT* sigla che ormai conosciamo, e che si riferisce a questo eccezionale dispositivo digitale capace di intelligenza generativa, come la si definisce oggi, scrive meglio di uno studente mediamente colto, ma anche meglio di molti docenti. Ho scaricato la versione più avanzata e mi stupisco ogni volta che sollecito delle risposte.

Come spiega in un suo saggio: "Aristotele e il linguaggio" (ed. Laterza) la scrittura è una tecnica raffinata, la stessa tecnica che però oggi ci preoccupa per i suoi eccezionali sviluppi. Tanti timori infondati?

Difficile dare una risposta definitiva non sappiamo cosa accadrà. Non sono un apocalittico, e nemmeno un integrato, per usare le celebri categorie introdotte da Eco negli anni settanta. Cerco di essere realista. Ho fatto delle domande a *Chatgpt*, faccio leggere i miei articoli, le risposte sono puntuali e sensate. La cosa stupefacente è il tempo di elaborazione. Per scrivere un commento anche breve, o rileggere due cartelle noi abbiamo bisogno di parecchi minuti, la macchina risponde in 3-4 secondi. Trovo che sia un esito straordinario. Scienziati, filosofi, ingegneri, linguisti dovranno occuparsene per molti anni.



Le paure di Platone

Le paure del "Fedro" di Platone, testo che Lei utilizza molto nelle sue lezioni universitarie, di fronte alla nascita della scrittura alfabetica tornano di attualità con l'avvento dell'IA?

Platone guardava con sospetto alla scrittura alfabetica, pensava che creava dei falsi sapienti, persone ignoranti che si ritenevano colte venivano alla ribalta, facevano opinione, diremmo con il linguaggio attuale. Comprensibili i timori del grande filosofo. È sempre accaduto nella storia dell'umanità. Il telaio meccanico spaventava perché avrebbe tolto lavoro, anche l'invenzione della stampa sconvolse equilibri di potere. Basti dire che la riforma protestante non sarebbe stata possibile senza l'invenzione dei caratteri mobili. Per la prima volta un testo sacro non aveva più bisogno di un interprete, il pubblico vi poteva accedere liberamente, si trattò una rivoluzione, un salto grandissimo. La stampa mise sotto scacco non solo il potere della chiesa, ma anche quello delle monarchie dell'epoca. Bisognava riorganizzare tutto, ripensare la leadership, ma anche il lavoro. Anche la città nasce con la scrittura alfabetica che fissa le regole cui tutti devono attenersi. Senza Gutenberg la società, come la vediamo oggi, non sarebbe concepibile. Prima dell'avvento della scrittura l'oralità fondava la convivenza, utilizzando simboli, linguaggi e pratiche, che con l'avvento dell'era moderna si sono modificati. Pensiamo alla nascita dei giornali, al ruolo decisivo sulla formazione dell'opinione pubblica che hanno esercitato. Ma ora siamo ancora un passo ancora oltre.

Cosa vuol dire?

Che siamo tutti diventati soggetti attivi di scrittura pubblica. È questa la grande novità politica del web. Una novità tutta da studiare, che indignava l'ultimo Umberto Eco infastidito dalla possibilità che anche l'ultimo 'imbecille' potesse fare opinione intervenendo sulle varie piattaforme social. Eco si sbagliava, perché non si tratta di un fenomeno superficiale, le implicazioni sono molteplici e richiedono uno studio attento.

Byung-Chul Han, l'autore di "Infocrazia", a questo proposito denuncia la crisi dell'agire comunicativo. I Like non farebbero riflettere, negano l'ascolto, l'alterità, creano confusione tra identità e opinioni. L'idea di Habermas, della democrazia che si fonda sul confronto tra opinioni che nascono dalla discussione sembra esaurita. Con quali conseguenze?

Bisogna uscire da alcuni errori interpretativi. Si pensa che il like sia per definizione emotivo, verticale, che l'argomentazione sia invece orizzontale e razionale. Ma non sempre nell'epoca pre digitale noi umani eravamo razionali e argomentativi, mentre oggi saremmo tutti impulsivi, irrazionali, in una parola superficiali. Bisognerebbe interrogarsi su cosa sta dietro un like, che spesso presuppone delle argomentazioni.

Siamo tutti soggetti di scrittura pubblica

Costruire un "esito liberaldemocratico del digitale" ha scritto su *Il Foglio*. Proposta interessante, ma fino a che punto fattibile?

Mi rendo conto che è difficile da attuare, ma non abbiamo altra scelta. Lo stesso fatto che ci stiamo interrogando su questi problemi, dimostra che la democrazia non sarà certo il sistema ideale, ma non ne conosciamo di migliori. In Cina, Russia, Iran certe questioni non possono neanche essere poste. Esiste un capitalismo della sorveglianza, che supera ampiamente "1984" di Orwell. Quando usiamo questi strumenti siamo tracciabili. Eppure non ci chiediamo chi sono i proprietari degli algoritmi.

La fine dei confini, il tramonto del Leviatano e degli stati nazionali era stato già denunciato nel *La fine dei territori* celebre scritto di Betrand Badie. Identità camuffate, false notizie (l'Italia è il paese con il record di fake news) condizionano le scelte geopolitiche. Per rimanere al tema dell'intervista: siamo capaci di pensare a un ordine mondiale fondato su basi nuove?

In un mondo interconnesso non ci possono essere ricette semplici. L'unico approccio possibile è quello che definirei *liberal*, che significa conoscenza delle varie modalità con cui le versioni (ne abbiamo e ne avremo molte da ora in avanti n.d.r.) di *chatGPT* funzionano, esercitando CULTURA CRITICA. Le restrizioni legali servono poco, sarebbero rapidamente aggirate. La conoscenza è l'unica arma che abbiamo per sconfiggere il pregiudizio. La scuola e gli apparati culturali avranno il ruolo più importante in questo mondo complicato che abitiamo. Cerchiamo di non dimenticarlo mai.

Siamo tutti diventati soggetti attivi di scrittura pubblica.

Multidomain: il ruolo della cyber nei prossimi conflitti

A cura di Pierguido Iezzi

La storia umana, intrisa di conflitti e crisi, è un tessuto complesso che non può essere compreso senza esplorare le sue molteplici sfaccettature. Come disse Sun Tzu ne "*L'arte della guerra*", "Tutte le guerre si basano sull'inganno". Questo concetto è rispecchiato nella nostra società, dove gli ambiti sociali sono stati plasmati e influenzati dalla guerra, un tema profondamente esplorato in opere come "Guerra e Pace" di Tolstoj. La storia è un caleidoscopio di eventi, e come scrisse George Orwell in "1984", "Chi controlla il passato controlla il futuro. Chi controlla il presente controlla il passato".

L'uso dell'inganno in situazioni di conflitto è un'arte antica, come dimostra la famosa strategia del Cavallo di Troia. Questo principio si riflette nelle moderne operazioni multi-dominio (MDO), che integrano vari campi d'azione - terra, aria, mare, spazio, informazioni e cyber - per fronteggiare le nuove sfide poste dalle tecnologie emergenti. Questo approccio richiama la visione strategica di Sun Tzu: "L'apice dell'abilità militare consiste nell'attaccare la strategia del nemico". In "*La guerra dei mondi*" di H.G. Wells, assistiamo a una rappresentazione fantastica di come la tecnologia possa influenzare la guerra, un tema sempre più pertinente nel nostro mondo. La necessità di adattarsi alle nuove realtà è cruciale che deve costantemente aggiornare le sue dottrine per restare al passo con le evoluzioni che cambiano il volto della guerra. Questo processo di adattamento riflette la massima di Charles Darwin: "Non è la specie più forte quella che sopravvive, né la più intelligente, ma quella più reattiva ai cambiamenti".

La storia dell'umanità è un intreccio di conflitti e adattamenti, una narrazione continua che si evolve attraverso i secoli. La comprensione di questa storia richiede una visione olistica, che tenga conto delle innumerevoli variabili e sfaccettature di ogni epoca e società. Non più solo terra, mare e cielo. Il ventunesimo secolo ha rivoluzionato l'arena della guerra, espandendosi ben oltre i confini tradizionali della dottrina militare. L'evoluzione bellica si è spinta in spazi prima inimmaginabili: il cyberspazio e lo spazio si aggiungono ora alla triade clausewitziana, trasformando radicalmente il panorama della guerra moderna.

Questi nuovi teatri di guerra richiamano il pensiero di Carl von Clausewitz, il cui trattato "*Della guerra*" ha plasmato la comprensione militare per secoli. Oggi, però, le sue parole assumono una nuova risonanza: la guerra si estende oltre la forza fisica, abbracciando il regno digitale e astrale. In questo contesto, il concetto di "*Multi-Domain Warfare*" emerge come un paradigma fondamentale, enfatizzando la necessità di condurre operazioni militari integrate attraverso i 5 domini - terra, mare, cielo, spazio e cyberspazio - simultaneamente e in maniera sinergica.

L'ispirazione per questa visione olistica deriva dalla "legge olografica" del fisico David Bohm, che suggerisce come ogni parte del cosmo rifletta il tutto. Il campo di battaglia moderno è un mosaico di azioni interconnesse, dove ogni movimento in un dominio può avere ripercussioni significative negli altri. Intendo con questo che ogni singola mossa o decisione presa in uno specifico dominio, può avere ripercussioni di vasta portata anche negli altri domini in modi complessi e imprevedibili.

Prendiamo ad esempio la guerra ibrida (*Hybrid War*) che la Russia ha condotto e conduce tuttora contro l'Ucraina. Combinando operazioni militari vere e proprie con attacchi hacker, campagne mirate di disinformazione online e pressioni economiche globali attraverso il suo controllo dell'energia, la Russia sfrutta pienamente l'interconnessione tra domini diversi per massimizzare l'impatto destabilizzante della sua aggressione. Interconnessioni visibili e tangibili anche nei conflitti in zone marittime strategiche, come avviene nel canale di Suez. Il rischio di attacchi dei ribelli Houthi dello Yemen legati allo scontro Hamas-Israele, hanno impatti enormi sul commercio globale, un incremento dei costi dei prodotti e di conseguenza una capacità di influenzamento della posizione dei singoli cittadini. È enorme il vantaggio bellico che l'Ucraina ha avuto dal presidiare lo spazio con il supporto dei satelliti Starlink di Elon Musk. Il presidio o conflitto in un dominio può causare un effetto a catena, influenzando l'economia globale e la sicurezza nazionale di diversi paesi.

Questa complessa interrelazione tra azioni in domini diversi prende il nome di "*Multi-Domain Warfare*" e richiede un nuovo approccio olistico alla strategia e alle operazioni militari moderne. Un nuovo tipo di pensiero strategico, che deve abbracciare la complessità, deve adattarsi dinamicamente a un ambiente in continuo mutamento ma soprattutto deve presidiare necessariamente il cyberspazio. Nel cyberspazio, le guerre dell'informazione e i conflitti digitali rappresentano un nuovo fronte critico. Come nei racconti di fantascienza di Isaac Asimov, dove le tecnologie avanzate e l'intelligenza artificiale giocano un ruolo chiave, il cyberspazio diventa un campo di battaglia dove il controllo dell'informazione è tanto potente quanto le armi tradizionali. Allo stesso tempo, lo spazio extraterrestre, un tempo considerato un confine inesplorato e pacifico, ora si profila come una nuova arena di confronto strategico. Questa trasformazione richiama alla mente l'epica cinematografica di "*Guerra Stellare*", dove le battaglie si svolgono in dimensioni astrali e digitali, portando la guerra in un regno fino ad ora relegato alla fantasia.

Non più solo terra, mare e cielo. Il ventunesimo secolo ha rivoluzionato l'arena della guerra, espandendosi ben oltre i confini tradizionali della dottrina militare.

Sicurezza e fiducia (digitale) per abilitare il business

A cura di Danilo Cattaneo

Ogni business si basa sulla fiducia: i clienti si fidano del fornitore, i dipendenti si fidano del proprio datore di lavoro, l'imprenditore si fida che ci sarà una competition equa, o che comunque il sistema sarà in grado di individuare e correggere i comportamenti non corretti.

In una economia sempre più digitale, basata sulla gestione di dati e informazioni, in qualsiasi settore tradizionale o innovativo che sia, la fiducia può essere messa a dura prova da attacchi, incidenti, data breach, furti di identità, arrivando seriamente a compromettere l'immagine delle organizzazioni, la loro operatività, il vantaggio competitivo e l'efficacia di business.

Ecco perché per le organizzazioni pubbliche e private una strategia efficace di cybersecurity e di utilizzo dei servizi digitali avanzati contribuisce a costruire e mantenere la fiducia alla base del business, al contempo garantendo una governance efficace dei rischi e della compliance.

In questa strategia, un ruolo molto importante è ricoperto dagli strumenti di ***digital trust***: le firme elettroniche, l'identità digitale, le comunicazioni certificate, l'archiviazione elettronica dei documenti offrono alle organizzazioni strumenti per costruire e governare il proprio trustworthy digital life-cycle dell'informazione digitale, nel quale in ogni fase sono garantite sicurezza, integrità, accountability e, se necessario, la corretta allocazione delle responsabilità tra tutte le parti coinvolte interne ed esterne.

Per fare qualche esempio, l'entrata in relazione con la nuova clientela, il cosiddetto *onboarding*, è reso più sicuro grazie a strumenti e tecnologie di identità digitale, che abilita la riduzione dei tassi di frode di identità. La diffusione sempre crescente di identità affidabili come SPID e CIE in Italia, che in futuro convergeranno nel Wallet Europeo di identità digitale (EUDI), crea un asset fondamentale che le organizzazioni possono sfruttare per rendere veloce, facile ed economico riconoscere da remoto un prospect o un dipendente. L'ingresso in questi ecosistemi di identità è favorito dalla presenza sul mercato di soggetti aggregatori, come quelli previsti da AgID nella federazione SPID, che svolgono il ruolo di proxy per omogeneizzare e semplificare l'integrazione e l'utilizzo della identità digitale, mantenendo un forte presidio sulle dimensioni di compliance e di sicurezza.

Le soluzioni di *identity verification* entrano invece in gioco in tutti quei i casi in cui il soggetto non è già in possesso di una identità digitale, ma deve essere identificato. In questo momento le soluzioni *best of breed* sono di tipo *hybrid unattended:* si tratta di processi non presenziati, in quanto non richiedono la compresenza della persona e di un operatore durante il processo di verifica dell'identità, e si basano su un estensivo utilizzo di tecnologie AI. Questi processi, regolamentati dal technical standard ETSI 119 461, richiedono un processo di raccolta delle foto del documento di identità da dispositivo mobile al fine di ottenere evidenze con una buona risoluzione. Una volta raccolta foto del documento, la soluzione ne valida le caratteristiche di sicurezza grazie a tecnologie di *document anti-tampering*, estraendo e validando le informazioni rilevanti per l'identificazione come il numero del documento, la data di validità, il tempo di validità standard per quel tipo di documento, altre caratteristiche specifiche.

È in seguito necessario eseguire il *binding*, ovvero la sua associazione con la persona che l'ha presentato: entrano pertanto in gioco tecnologie di liveness detection e di biometria facciale, per garantire che la persona che sta presentando il documento sia reale (e non, ad esempio, una immagine artificiale) e che le caratteristiche del volto della persona siano compatibili con quelle della foto estratta dal documento validato.

Dove necessario, il tutto viene ulteriormente verificato da un operatore in back-office, appositamente formato, che mette in campo ulteriori controlli per validare, oppure rigettare, l'identità della persona.

Ora, è evidente come sia l'uso della identità digitale preesistente sia i processi di verifica dell'identità implicano un gran numero di controlli e verifiche e di come questi processi lascino "tracce" digitali che sono vere e proprie evidenze probatorie, che li rendono processi molto più sicuri degli equivalenti analogici e del riconoscimento in presenza, dove spesso si ha solo la fotocopia di un documento magari falso e quanto ricorda un operatore di sportello.

Ogni business si basa sulla fiducia!

Una volta identificato il cliente in maniera certa, viene naturale ricorrere agli strumenti di firma elettronica, quando vi è l'esigenza di sottoscrivere dei documenti, che con la firma anche se elettronici diventano immutabili. Tra questi la firma elettronica qualificata è certamente la soluzione più sicura e che garantisce la maggiore sicurezza grazie all'impiego di soluzioni PKI e tecnologie crittografiche, peraltro che stanno evolvendo verso algoritmi quantum-proof, e grazie alla presenza dei Prestatori di Servizi Fiduciari Qualificati (QTSP), soggetti a un complesso sistema di controlli, garanzie, auditing e governance tra i più robusti al mondo.

Le stesse tecnologie sono alla base di un particolare tipo di firma elettronica, la validazione temporale, che consente di dare certezza al momento in cui è avvenuta una transazione, fondamentale in contesti ad alto valore.

Nell'interazione con l'esterno dell'azienda, le soluzioni di eDelivery ricoprono un ruolo fondamentale per mantenere trust e sicurezza nello scambio di documenti, dati e informazioni. In Italia la soluzione più utilizzata è certamente la PEC, che infatti si fonda sulle stesse tecnologie crittografiche su cui si basa la firma qualificata. La Posta Elettronica Certificata sta per evolvere nella direzione di una ancora maggiore certezza, grazie alla trasformazione in REM – Registered eMail Qualificata: con l'evoluzione della normativa ogni casella sarà associata univocamente a una identità certa, e sarà necessaria la strong customer authentication per accedervi in scrittura e lettura. Il tutto in un framework europeo di interoperabilità che consentirà anche di poter interagire con altri sistemi di delivery basati sugli stessi standard.

Inoltre, alcuni servizi di PEC presenti oggi sul mercato integrano anche una serie di feature di sicurezza aggiuntive rispetto a quelle richieste dalla normativa: prodotti come phishing protection, password protection, security premium forniscono garanzie di protezione da frodi, furti di dati, attacchi informatici.

Per lo scambio documentale sicuro è anche possibile utilizzare sistemi di eDelivery di tipo *"store and notify":* questo tipo di sistema prevede che il mittente depositi presso il TSP documenti o dati indicandone il destinatario. Questi è poi notificato dal TSP così che, accedendo allo spazio riservato, possa entrare in contatto con il contenuto digitale. Tutte le azioni sono tracciate ed è anche possibile procedere alla identificazione del mittente a vari livelli di sicurezza, a garanzia della effettiva consegna di quanto inviato al corretto soggetto.

Nel *digital transaction lifecycle* per quanto descritto possiamo garantire sicurezza dalla creazione del documento, la sua gestione, la sua spedizione individuando i livelli di garanzia e trust più adeguati al contesto.

L'ultima fase del ciclo di vita è infine la sua archiviazione digitale: non è sufficiente lo storage dei dati e dei documenti in un disco o nel cloud, ma è necessario applicare processi e usare soluzioni che garantiscano il mantenimento non solo dell'integrità, dell'immutabilità e della disponibilità dei dati, ma anche della loro leggibilità. Sono soluzioni in cui il l'Italia ha una grande esperienza, e che stanno diventando anche uno standard a livello europeo grazie all'evoluzione del Regolamento eIDAS 2, che vede l'archiviazione diventare un servizio fiduciario, anche qualificato. Le soluzioni di *ePreservation* garantiscono non solo il mantenimento nel tempo del contenuto digitale, ma anche la sua distruzione sicura alla scadenza del suo *retention period*, consentendo pertanto il rispetto delle normative sul trattamento dei dati.

Le soluzioni di digital trust pertanto sono oramai strumenti fondamentali in una corretta governance aziendale delle informazioni. Sono soluzioni in cui l'Europa, e soprattutto l'Italia, ha una leadership consolidata e che sempre di più stanno diventando *building blocks* fondamentali su cui fondare modelli di business e vantaggi competitivi.

CYBER
Think Tank
ASSINTEL

La sicurezza digitale è un impegno. Unisciti al nostro Think Tank!

Prossimo Incontro:

24 gennaio
Ore 14:00

Valori:

1. Interazione
2. Integrazione
3. Coerenza
4. Concretezza

Cyber Think Tank Assintel

Per info scrivi a:
segreteria@assintel.it

Cyber Security Readiness: nasce un progetto di sistema per le PMI

A cura di Rocco Mammoliti

Il progetto PMI e Cyber Security Readiness, che ci vede impegnati insieme alla Direzione dei Servizi Innovativi e Tecnologici di Unindustria, il Competence Center 4.0 esprime un principio essenziale: dobbiamo impegnarci ad essere facilitatori del cambiamento per favorire la costituzione di un ecosistema produttivo integrato, costruito sulla centralità della sicurezza, concepita come valore condiviso. La solidarietà è, infatti, il collante di un impianto di protezione degli asset che deve svilupparsi nel superamento di vetuste convinzioni. Tutti gli stakeholders devono sentirsi coinvolti nella definizione di standard di protezione delle infrastrutture critiche e delle reti di connessione, non c'è un "grande" e un "piccolo", spazi e distanze sono abbattute nel tempo fluido dell'essere digitale. Per essere all'altezza delle sfide può risultare determinante affinare delle partnership tra attori pubblici e privati, che deve avere come protagonista quel fitto tessuto di PMI, che esprime da sempre l'ossatura economica del paese. L'innovazione tecnologica prima di essere praticata va compresa e governata attraverso il concorso di una molteplicità di saperi; ingegneri, giuristi, scienziati, umanisti devono operare fianco a fianco per rispondere al bisogno di protezione di istituzioni, cittadini e imprese.

La parola inglese *Readiness* letteralmente vuol dire "pronti", ma come e a che cosa verrebbe da chiedersi? Non risulta produttivo alcun posizionamento statico in attesa di eventi critici, calamità, possibili incidenti informatici, essere pronti oggi vuol dire saper mettere in campo capacità di sviluppare una corretta governance del rischio e di prevenzione delle vulnerabilità. "Siamo sulla stessa barca" la metafora pronunciata in "Fratelli tutti", l'Enciclica profetica di Papa Francesco che teorizza l'"ecologia integrale" come valore fondante della convivenza umana, diventa un mantra anche per il nostro "umile" lavoro quotidiano, orientato a garantire la sicurezza individuale e collettiva che passa attraverso il corretto funzionamento delle reti e della connettività a tutti i livelli. Siamo una "comunità di destino" nel mondo globalizzato, la linea di progresso che siamo chiamati a tracciare come classe dirigente manageriale e politica, non può ignorare la corresponsabilità come termine essenziale cui bisogna rifarsi per raggiungere risultati visibili. D'altra parte chi vorrebbe abitare una "casa" insicura, fatta di strumenti malfunzionanti esposta a manomissioni di diversa natura? Certamente nessuno, la "casa" dell'uomo del nostro tempo è l'intero pianeta che vogliamo attraversare con la serenità, che accompagna il desiderio della scoperta, della ricerca, dell'analisi che ha permesso all'individuo di imboccare la via del progresso e alla storia di camminare verso il futuro.

La sicurezza da vincolo a opportunità

Troppo spesso si è portati a considerare la sicurezza un costo, un adempimento, un peso da sostenere malvolentieri per imprenditori già vessati da una densità normativa e regolativa non facile da interpretare. Richiamerei a questo proposito uno scritto illuminante del filosofo della complessità Mauro Ceruti "Il vincolo e la possibilità". La cyber security è una possibilità che diviene opportunità, perché consente alle organizzazioni di migliorare i livelli di performance e di efficienza. La sicurezza aiuta il business, consentendo alle aziende di reggere i ritmi della competitività, non scordiamolo mai. Il percorso formativo "a tappe" che stiamo definendo nei dettagli, conferma che la sicurezza è un tendere verso, non si potrà mai raggiungerla in assoluto. La "postura" di cyber security di cui tanto si parla, è un fattore identitario in divenire, che non ha nulla di scontato. Nostro obiettivo è quello di dare un navigatore alle imprese, non ci sono certezze in un campo delicato per definizione, c'è bisogno di un orientamento forte, di individuare un percorso di senso che possa indirizzare con oculatezza risorse e investimenti.

Il primo appuntamento di formazione sarà dedicato non a caso al rapporto tra sicurezza e terze parti, proprio in ragione dell'avvertita necessità di allargare il perimetro di osservazione, che non ha più "recinti" limitati, nella dimensione virtuale. Sono, infatti, tante le sfide che dovremo affrontare a partire dalla certificazione che va sburocratizzata. È possibile fare *knowledge sharing*, risparmiando tempo e denaro prezioso, soprattutto evitando sovrapposizioni dannose. Sotto questo aspetto può risultare utile ripensare l'organizzazione, per disegnare un ecosistema delle imprese, (torno sul concetto espresso all'inizio) capace di interpretare un modello capitalistico basato sulla pratica di una "vigilanza intelligente".

Linee guide delle strategie di Cyber Security

Quattro sono le direttrici fondamentali che Poste Italiane ha fissato per definire le strategie di sicurezza informatica: prevenzione dei rischi, educazione all'uso degli strumenti tecnologici, centralità della ricerca, attitudine all'innovazione. Un player di queste dimensioni custodisce asset strategici per il Paese che giustificano l'adozione di misure di difesa eccezionali, sostenute da investimenti proporzionali alla propria esposizione nel mondo dei servizi digitali. Organizzazione, persone, regole, tecnologie, controlli e miglioramento continuo contribuiscono ognuno per la propria parte a mitigare continuamente il rischio di attacchi cyber, inclusi quelli attuati sfruttando i ransomware, che ormai occupano sistematicamente le pagine dei giornali. Come se non bastasse si fa strada il metaverso, una rivoluzione paragonabile all'avvento di Internet. Siamo chiamati a disciplinare gli aspetti della sicurezza informatica anche su questo delicato terreno: pensiamo alle sfide dell'AI, di cui ancora oggi non conosciamo l'esatta geografia come nemmeno le direttrici dello sviluppo.

La sicurezza aiuta il business, consentendo alle aziende di reggere i ritmi della competitività.

Phishing, smishing, insieme a sofisticate tecniche di social engineering vengono sempre più messi in atto per rubare le credenziali di milioni di utenti. Nell'orizzonte mutante di questa che Luciano Floridi ha definito "infosfera", una condizione in cui reale e virtuale si mescolano in maniera inscindibile diventa importante progettare e realizzare attività di *education & awareness* svolgendo nel contempo un monitoraggio sistematico anti-frode e anti-abuso, da implementare sfruttando lo strumento dei *Big-Data Analytics* e l'IA. La *cyber-hygiene* deve configurarsi come l'ambiente entro cui l'ecosistema della sicurezza dovrà evolvere.

Cyber resilienza come termine critico

Cyber-resilienza è il termine critico mutuato dalla fisica, su cui vorrei in conclusione insistere. In particolare la resilienza applicata alle organizzazioni produttive indica la capacità di attuare strategie e interventi volti ad anticipare, proteggere, resistere e recuperare una situazione di equilibrio il più rapidamente possibile dopo un attacco di qualsiasi entità. Poste Italiane adotta un sistema per la prevenzione, gestione e contenimento dei rischi ICT e conseguentemente degli incidenti informatici molto capillare e avanzato, che consente di presidiare i canali digitali, i sistemi e le infrastrutture ramificati sul territorio, gli operativi in mobilità, i data center e i sistemi di comunicazione, con una particolare attenzione agli elementi di *business-continuity*.

Ecco che la centralità del fattore umano torna ad imporsi. In ragione di questa consapevolezza abbiamo avviato diversi cantieri sulla *Cyber Security Readiness* in coerenza con i dettami del regolamento DORA, che riguardano molteplici aspetti di governo e gestione del rischio ICT, quali: l'aggiornamento delle librerie e delle contromisure di sicurezza, la rivisitazione delle metodologie di Analisi del Rischio e di valutazione della minaccia cyber, la ridefinizione dei ruoli e delle responsabilità di ciascun presidio interno, attraverso l'introduzione dei principi di *Security by Design*, rilevata a tutti i livelli, fino a garantire un elevato grado di formazione degli specialisti di sicurezza, dei dipendenti e dei vertici aziendali. È questa la strada maestra che dobbiamo imboccare, nell'orizzonte mutante dell'*information society*, che obbliga tutti a non abbassare mai il livello di attenzione sulle molteplici trasformazioni che segnano la contemporaneità.

Non puoi essere ciò che non puoi vedere

La Diversità in STEM: oltre il Gender Gap

A cura di Petra Chiste

Il mondo delle discipline STEM (Science, Technology, Engineering, and Mathematics - Scienza, Tecnologia, Ingegneria e Matematica) rappresenta un ambito fondamentale per il progresso e l'innovazione della società moderna. Questi campi, che vanno dalla ricerca scientifica allo sviluppo tecnologico, dall'ingegneria avanzata all'analisi matematica, sono i pilastri portanti dell'evoluzione tecnologica e scientifica. Tuttavia, nonostante la loro importanza cruciale, queste discipline sono spesso teatro di un marcato gender gap, un divario di genere che vede una rappresentazione sproporzionatamente bassa delle donne.

Ma siamo sicure che il Gender Gap sia l'unico aspetto da prendere in esame nelle e discipline Stem? Se da un lato abbiamo assistito a diverse iniziative verso l'inclusione delle donne, dall'altro rimangono numerose aree in cui la diversità è ancora poco rappresentata o mal compresa.

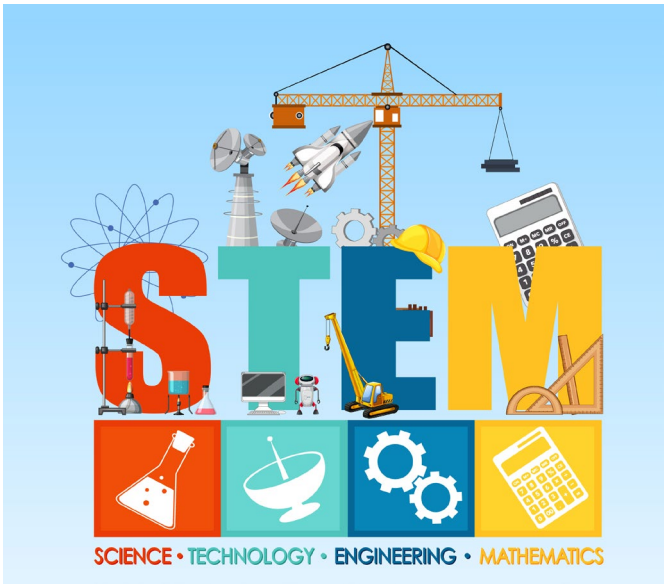
Attraverso un'analisi delle statistiche recenti e delle tendenze emergenti, cercheremo di capire non solo come e perché questo divario persista, ma anche quali siano le strategie e le iniziative intraprese per promuovere una maggiore inclusione e diversità in questi campi cruciali. Il nostro obiettivo è fornire ai professionisti del settore una visione chiara su come la diversità possa essere non solo promossa, ma anche sfruttata come leva per il successo in un'era di trasformazioni tecnologiche rapide e profonde.

Dove siamo?

Nonostante la crescente **rappresentazione femminile**, le donne sono ancora significativamente sottorappresentate in molte aree STEM, specialmente in ingegneria e informatica. Il report "*Diversity and STEM*" di NCSES[1] ha rilevato che le donne costituiscono solo il 35% della forza lavoro STEM negli Stati Uniti, con una percentuale ancora inferiore nelle posizioni di leadership e nei ruoli decisionali. Questa disparità è accentuata tra le donne di minoranze etniche, che affrontano sfide sia di genere che di razza. In Italia, la situazione riflette tendenze simili: secondo il report dell'Osservatorio Talents Venture e del progetto STEAMiamoci di Assolombarda[2] , la percentuale di ragazze iscritte ai corsi STEM sul totale delle donne iscritte all'università si è fermata al 18,3% dopo il record del 2017-18.

Un quadro peggiore si ha quando si analizzano dati rispetto all'**etnicità**. Gruppi come gli asiatici americani sono sovrarappresentati in certi settori STEM, mentre altre minoranze, quali afroamericani, ispanici e nativi americani, sono notevolmente sottorappresentati. Gli afroamericani, per esempio, costituiscono circa il 13% della popolazione degli Stati Uniti ma rappresentano solo il 9% della forza lavoro STEM.

Secondo i dati dell'ISTAT, nel 2023 la popolazione italiana è composta da circa 60 milioni di persone, di cui il 91,5% è di origine italiana. La restante parte della popolazione è composta da persone di origine straniera, che rappresentano l'8,5% del totale.



Il settore STEM è uno dei settori in cui la presenza di persone di origine straniera è più elevata. Secondo i dati del Ministero del Lavoro e delle Politiche Sociali, nel 2023 le persone di origine straniera occupate nel settore STEM rappresentano il 15,5% del totale dei lavoratori STEM.

Questa percentuale è in aumento negli ultimi anni, passando dal 12,5% nel 2018 al 15,5% nel 2023. Molto interessante è il quadro che si delinea sulla differenza di genere. La presenza di persone di origine straniera nel settore STEM è più elevata tra le donne che tra gli uomini. Nel 2023, le donne di origine straniera occupate nel settore STEM rappresentano il 18,5% del totale delle donne occupate nel settore STEM, mentre gli uomini di origine straniera occupati nel settore STEM rappresentano il 12,5% del totale degli uomini occupati nel settore STEM.

La rappresentanza delle persone con **disabilità** in STEM è un'ulteriore area critica. Le barriere includono ambienti di lavoro fisicamente inaccessibili e pregiudizi impliciti nel processo di assunzione. La mancanza di risorse educative accessibili in STEM limita ulteriormente le opportunità per le persone con disabilità in questi campi. Nel 2021 secondo il report di NCSES la percentuale di lavoratori con almeno una disabilità era del 11,2%, forse ancora più interessante è il dato legato al tasso di disoccupazione, mentre in generale in questo ambito abbiamo meno dell'8% di tasso di disoccupazione, per le persone con disabilità arriviamo oltre al 13%.

Infine, il background **socioeconomico** gioca un ruolo cruciale nell'accesso alle opportunità educative e professionali in STEM. Gli studenti provenienti da famiglie a basso reddito hanno minori probabilità di accedere a un'istruzione STEM di qualità, limitando le loro opportunità di carriera in questi settori. n Italia, questa dimensione può essere particolarmente rilevante, data la variabilità delle risorse educative tra le diverse regioni del paese. L'Italia affronta una sfida significativa legata al divario territoriale nelle competenze STEM[3]. I dati dei test Invalsi evidenziano un netto scarto tra gli studenti del centro-nord e quelli del mezzogiorno, già dalla scuola primaria, con un divario che si accentua nei percorsi di istruzione superiore orientati verso le STEM. Tale discrepanza è particolarmente marcata nei licei scientifici e istituti tecnici, dove si osservano divari di 35-38 punti. Inoltre, i capoluoghi del Nord Italia superano quelli del Sud in termini di competenze numeriche, rivelando un legame tra risultati scolastici e condizioni socioeconomiche. Questi dati sottolineano l'importanza di strategie mirate per l'equità nell'istruzione STEM a livello nazionale, cruciale per lo sviluppo di un settore tecnologico italiano competitivo e diversificato.

Ostacoli alla diversità

Il detto inglese "*you can't be what you can't see*", non puoi essere ciò che non puoi vedere nelle discipline STEM è quanto mai attuale. Ragazzi e bambini provenienti da contesti diversi, di genere femminile non si immaginano in discipline tecnologiche perché semplicemente non vedono modelli a cui ispirarsi.

Indipendentemente dalla minoranza che si analizza, l'ambiente STEM presenta delle sfide particolarmente complesse da superare. Uno degli ostacoli principali è l'**accessibilità degli spazi fisici** e delle risorse tecnologiche. Molti laboratori, aule, e luoghi di lavoro in STEM non sono adeguatamente attrezzati per essere accessibili a persone con varie disabilità o persone con una etnia differente. Questo include la mancanza di attrezzature adattate, software di assistenza, e altri supporti tecnologici che sono fondamentali per permettere la piena partecipazione.

Le istituzioni scolastiche di diverso grado spesso non forniscono **supporti e risorse adeguate** alle persone con disabilità, di minoranze etniche; mancanza di servizi di interpretariato, materiali didattici accessibili, e supporto pedagogico personalizzato, che sono cruciali per l'apprendimento e il lavoro in campo STEM.

Le barriere alla comunicazione possono essere particolarmente sfidanti; la mancanza di materiali in formati accessibili, come testi in braille o software di lettura dello schermo, libri in lingua originale, possono limitare la collaborazione e il coinvolgimento effettivo.

Le politiche organizzative possono non tenere conto delle esigenze specifiche delle persone con disabilità, di gruppi etnici specifici o di flessibilità necessaria per la conciliazione casa/lavoro. Questo si manifesta in una mancanza di flessibilità nelle procedure di lavoro, nei requisiti di assunzione, e nelle modalità di valutazione delle prestazioni, che non considerano adeguatamente le diverse abilità ed esigenze.

Si può infine sperimentare un senso di isolamento dovuto alla mancanza di colleghi con esperienze simili influenzando negativamente il benessere psicologico e le opportunità di networking professionale.

Vantaggi della Diversità in STEM

Un team diversificato è più innovativo, creativo e produttivo. Le persone provenienti da diverse background e prospettive portano con sé esperienze e conoscenze uniche che possono essere utilizzate per risolvere problemi complessi e sviluppare nuove idee.

La diversità di pensiero è un elemento essenziale per l'innovazione. L'avere persone con background culturali e punti di vista diversi in un campo in rapida evoluzione come il settore STEM favorisce la capacità di innovare e adattarsi. Le squadre composte da membri con esperienze e prospettive differenti hanno dimostrato una maggiore creatività e capacità di innovazione.

Numerosi studi hanno dimostrato un collegamento diretto tra la diversità di genere e culturale all'interno di un'organizzazione e il suo successo finanziario. Le aziende che adottano pratiche di inclusione e diversità tendono ad essere più profittevoli e innovative rispetto a quelle che non lo fanno. Infatti, un ambiente di lavoro che accoglie attivamente la diversità promuove l'apertura, la tolleranza e il rispetto reciproco, creando un clima lavorativo più produttivo e armonioso.

La rapida evoluzione tecnologica e al tempo stesso la carenza di competenze specializzate, spingono le aziende a ricercare in modo compulsivo sempre nuovi talenti, fornire un ambiente inclusivo permette di accedere a un'ampia gamma di talenti. In questo modo si riesce a posizionarsi meglio sia nei campi dell'innovazione tecnologica sia soprattutto nel mercato, offrendo prodotti maggiormente competitivi.

L'inclusione delle donne e dei gruppi sottorappresentati nel settore STEM è un tema di crescente importanza per le aziende che si impegnano a promuovere la sostenibilità sociale e ambientale. Dal punto di vista ESG, l'inclusione di questi gruppi non solo è una mossa etica e sociale, ma si configura come un passo necessario per affrontare le disuguaglianze persistenti, stimolando al contempo una crescita economica più equilibrata.

Iniziative e Soluzioni

Per promuovere la diversità e l'inclusione nel settore STEM, esistono una serie di iniziative, sia a livello europeo che internazionale. Queste iniziative offrono opportunità alle persone provenienti da diversi background, tra cui le persone con disabilità, di intraprendere una carriera in STEM.

Alcune delle principali iniziative internazionali sono:

Black in AI è un'organizzazione che si concentra sull'aumento della partecipazione delle persone di colore nel campo dell'intelligenza artificiale. L'organizzazione offre una serie di programmi e risorse per le persone di colore che desiderano intraprendere una carriera in AI, tra cui mentoraggio, networking e sviluppo professionale.

Girls Who Code è un'organizzazione internazionale che si concentra sull'insegnamento dell'informatica alle ragazze. L'organizzazione offre una serie di programmi e risorse per le ragazze che desiderano imparare a codificare, tra cui campi estivi, lezioni dopo la scuola e programmi di orientamento.

Code for America è un'organizzazione internazionale che si concentra sull'utilizzo della tecnologia per risolvere i problemi sociali. L'organizzazione offre una serie di programmi e risorse per i programmatori che desiderano utilizzare le proprie competenze per fare la differenza nel mondo, tra cui borse di studio, programmi di apprendimento e opportunità di volontariato.

Women in AI Europe è un'organizzazione europea che si concentra sull'aumento della partecipazione delle donne al campo dell'intelligenza artificiale. L'organizzazione offre una serie di programmi e risorse per le donne che desiderano intraprendere una carriera in AI, tra cui mentoraggio, networking e sviluppo professionale.

Equals-EU è un'iniziativa volta a promuovere la parità di genere nell'innovazione in Europa e in altri paesi partner. L'obiettivo principale è quello di promuovere l'equilibrio di genere nel settore tecnologico attraverso l'uguaglianza di accesso, lo sviluppo di competenze e opportunità di carriera.

Piano Nazionale Scuola Digitale (PNSD): Questo piano, varato dal Governo italiano, mira a innovare il sistema educativo attraverso la digitalizzazione e la promozione delle carriere in ambito STEAM (*Science, Technology, Engineering, Arts & Maths*). Include progetti come STEAM Lab, che offre percorsi competitivi in ambito STEAM per studenti di ogni ordine e grado, e iniziative come "Percorriamo il sentiero dei meccanismi meravigliosi" e "*Leonardo STEAM Lab*"

Progetto STEAMonEdu: Questo progetto europeo, di cui gli Stati Generali dell'Innovazione sono partner italiani, mira a implementare l'approccio STEAM nelle scuole a livello nazionale e europeo. Offre corsi di formazione gratuiti, un MOOC (*Massive Online Open Course*), e la sperimentazione di scenari educativi per promuovere STEAM.

Prospettive Future? Lascia fare al tempo, ma…

La diversità in STEM è un tema complesso e sfaccettato che va oltre il gender gap. Le donne, le persone di minoranze etniche, le persone con disabilità e le persone provenienti da sfondi socioeconomici svantaggiati sono ancora sottorappresentate in questi campi, nonostante la loro importanza cruciale per il progresso e l'innovazione della società.

Abbiamo visto che gli ostacoli alla diversità in STEM sono molteplici e radicati, e vanno affrontati a diversi livelli, dall'istruzione alla cultura aziendale. Le iniziative e le soluzioni che sono state messe in atto finora hanno avuto un impatto positivo, ma è necessario fare ancora molto per creare un ambiente STEM più inclusivo e diversificato.

Un mio stimato collega mi suggerisce sempre che alcuni problemi grandi trovano una soluzione con il cambio generazionale. Il collega appartiene ad una generazione decisamente più giovane della mia nelle sue parole vedo sicuramente quello slancio tipico dei giovani, ma vi sono anche delle basi molto solide di questa affermazione.

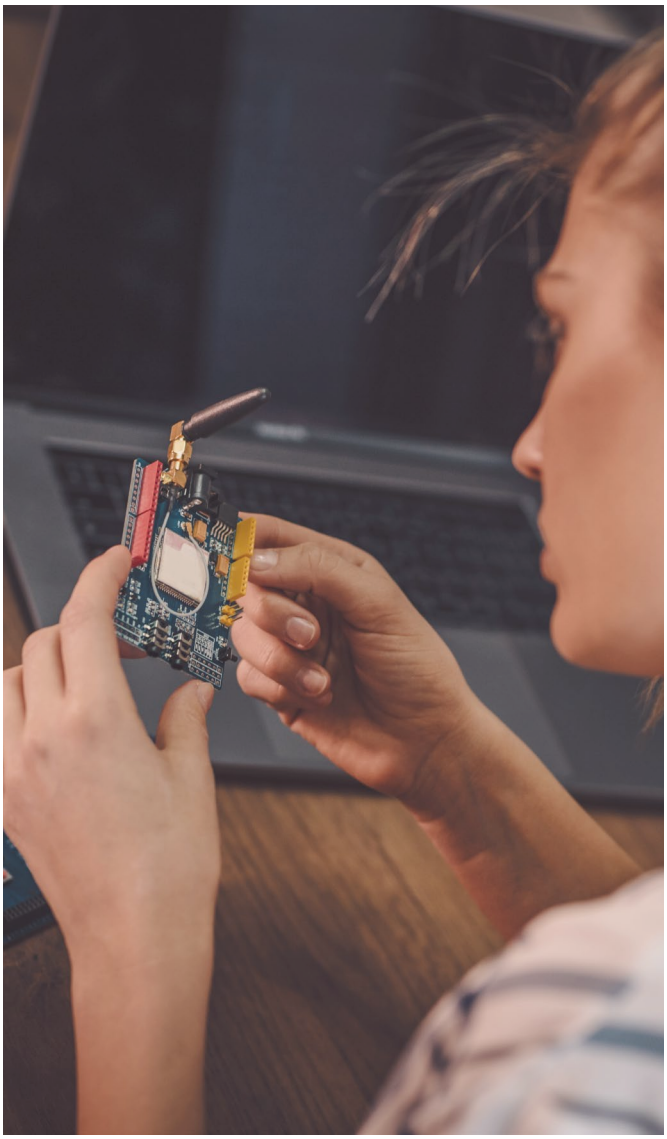
La generazione Z, la più digitale e sensibile ai temi globali, è anche quella più propensa a essere consapevole e aperta riguardo alla diversità. Con la giusta educazione e supporto, questa generazione ha il potenziale per contribuire a creare un settore STEM più equo e inclusivo.

Le prospettive future sono incoraggianti.

Ecco quindi alcune piccole raccomandazioni che ognuno di noi, all'interno del proprio ecosistema può mettere in atto: coinvolgiamo le scuole e le università in iniziative di sensibilizzazione alla diversità e all'inclusione in STEM attraverso attività di mentoring, networking e sviluppo professionale per studenti nelle nostre aziende, creiamo un ambiente di lavoro inclusivo e accogliente per tutti i dipendenti, indipendentemente dal loro genere, etnia, disabilità o background socioeconomico attraverso politiche e pratiche che promuovano la parità di accesso alle risorse; raccogliamo dati e monitoriamo i progressi compiuti nella promozione della diversità in STEM, questo ci aiuterà a identificare le aree in cui è necessario intervenire e a valutare l'efficacia delle iniziative messe in atto.

Sosteniamo la diversità, coltiviamo l'innovazione: insieme, possiamo costruire un futuro STEM più inclusivo e rappresentativo.

Un team diversificato è più innovativo, creativo e produttivo.



WEBINAR

Guerra al cyber spionaggio: Decifrare Ransomware, Infostealer e Botnet

Relatori:

Andrea Zapparoli Manzoni

Pierguido Iezzi

Antonio Assandri

CYBER Think Tank ASSINTEL

27 Febbraio

12:00 - 13:00

Per info scrivi a: segreteria@assintel.it

Trasferimenti di dati: conformità con la Direttiva 2016/680/UE sulla Polizia e Giustizia Penale (LED)[4]

A cura di Ranieri Razzante

Nella lotta odierna contro la criminalità, la cooperazione internazionale in materia penale è della massima importanza per garantire la tutela dello spazio di libertà, sicurezza e giustizia dell'UE. Questa cooperazione implica la condivisione delle informazioni necessarie, come i dati personali, non solo tra gli Stati membri, ma anche con i Paesi terzi.

Per consentire la libera circolazione dei dati personali a fini di contrasto all'interno dell'Unione, nonché per il trasferimento verso Paesi terzi e organizzazioni internazionali, è stata pubblicata la Direttiva 2016/680/UE sulla Polizia e la Giustizia Penale (c.d. *Direttiva* LED).

La LED garantisce un elevato livello di protezione dei dati personali, servendo al tempo stesso l'interesse pubblico, in particolare nel prevenire, indagare, accertare o perseguire reati, comminare sanzioni penali e salvaguardare la sicurezza pubblica da potenziali minacce.

L'art. 8 della LED stabilisce che il trattamento dei dati in relazione alla Direttiva sulla Polizia e la Giustizia Penale deve avvenire solo se ritenuto necessario per l'esecuzione di un compito svolto da un'autorità competente. Questo compito deve essere uno degli scopi specificati nel diritto dell'Unione o degli Stati membri.

Quando le Autorità competenti applicano la LED e la pertinente legislazione nazionale di recepimento, è fondamentale garantire che qualsiasi interferenza con i diritti degli interessati che potrebbe derivare dal trattamento previsto sia necessaria e proporzionale all'obiettivo di interesse pubblico che esse stanno perseguendo. Ciò include, giova ricordarlo, la prevenzione, l'indagine, l'accertamento o il perseguimento di reati o l'applicazione di sanzioni, nonché la salvaguardia e la prevenzione delle minacce. La pubblica sicurezza si riferisce alle misure e agli sforzi adottati dai governi e dalle comunità per salvaguardare il benessere e la sicurezza del pubblico in generale.

Nel corso della sessione plenaria finale del 27 settembre 2023, il Comitato europeo per la protezione dei dati (EDPB) ha adottato le Linee guida relative all'art. 37 della Direttiva LED. Tali Linee Guida sono state predisposte per offrire indicazioni pratiche sull'applicazione dell'art. 37 della LED, relativo al trasferimento di dati personali da parte delle autorità competenti dei paesi dell'Unione europea ad autorità di Paesi terzi o ad organizzazioni internazionali dotate di autorità di contrasto. Più specificamente, dette Linee Guida mirano a chiarire lo *standard* giuridico relativo alle garanzie adeguate che le autorità competenti devono applicare ai sensi dell'art. 37, comma 1, lettere a) e b), della LED, nonché gli elementi rilevanti per valutare la presenza di tali garanzie.

Le Linee Guida intendono fungere da punto di riferimento per i paesi dell'Unione europea nelle situazioni in cui cercano di stipulare o modificare accordi di trasferimento

basati sull'art. 37(a) della LED. In tal modo, queste linee guida forniscono anche indicazioni alle autorità nazionali per la protezione dei dati (DPA) quando sono chiamate a consultare o partecipare alla negoziazione di tali accordi, o quando successivamente ne valutano l'attuazione. Inoltre, le presenti linee guida affrontano le responsabilità delle autorità di protezione dei dati in relazione agli obblighi del titolare del trattamento come delineato nell'art. 37(2) e (3) del LED. Le Linee Guida sottolineano che qualsiasi trasferimento di dati personali deve garantire un grado di protezione sostanzialmente uguale nel paese terzo o nell'organizzazione internazionale che riceve i dati e che tali trasferimenti non dovrebbero, in nessun caso, ridurre il livello di protezione applicabile nell'Unione europea.

Le Linee guida vanno oltre le semplici raccomandazioni e forniscono invece una guida completa sull'uso di documenti giuridicamente vincolanti (come indicato nell'art. 37 (a) della LED) rispetto alle valutazioni da parte dei proprietari dei dati (come delineato nell'art. 37 (b) della LED). Si sottolinea che quest'ultima opzione deve essere utilizzata solo se esiste un'analisi approfondita del quadro giuridico e delle pratiche pertinenti che dimostrino che il trasferimento in questione è soggetto a garanzie adeguate. Inoltre, le Linee guida offrono consigli pratici, compreso un elenco di elementi essenziali che dovrebbero essere inclusi in un documento giuridicamente vincolante, nonché esempi per classificare e valutare le circostanze di un trasferimento.

Il vantaggio principale di questo strumento è la sua capacità di fornire un quadro strutturato ed esplicito per la condivisione dei dati personali nel contesto della giustizia penale e delle collaborazioni tra forze dell'ordine. Di conseguenza, le autorità nazionali coinvolte godranno di una maggiore certezza giuridica, che inevitabilmente aumenterà la conformità dei controllori e allevierà i loro profili di responsabilità. Inoltre, essi saranno esentati dal valutare l'adeguatezza della tutela della *privacy* nei paesi terzi o nelle organizzazioni internazionali. Tuttavia, ai sensi dell'art. 37, paragrafo 1, lettera b), LED, maggiore è la discrezionalità delle autorità nazionali competenti nel determinare le garanzie adeguate, maggiore sarà la responsabilità che avranno nel garantire la conformità ai requisiti LED.

La LED garantisce un elevato livello di protezione dei dati personali.

La strategia per la sicurezza economica dell'Unione europea

*A cura di Vittorio Calaprice**

*Le informazioni e le considerazioni espresse nell'articolo sono di Vittorio Calaprice e non riflettono necessariamente quelle ufficiali della Commissione europea.

Gli scambi commerciali aperti e basati su regole hanno certamente plasmato e avvantaggiato l'Unione europea sin dalla sua istituzione.

Tuttavia, le crescenti tensioni geopolitiche e una maggiore concorrenza geostrategica e geoeconomica, nonché shock come la pandemia di COVID e la guerra di aggressione della Russia nei confronti dell'Ucraina, hanno evidenziato i rischi che determinate dipendenze economiche comportano. Tali rischi, se non adeguatamente gestiti, possono infatti minare il funzionamento economie UE, i suoi interessi strategici e la capacità di agire.

Una strategia globale - che comprenda un'azione congiunta in tutte le politiche interne ed esterne e un insieme coerente di misure a livello dell'UE e degli Stati membri - è emersa dunque come necessaria per consentire all'Unione europea di valutare e gestire i rischi, mantenendo nel contempo la sua apertura e il suo impegno internazionale.

Questo obiettivo è stato proposto dalla comunicazione congiunta della Commissione europea e l'Alto rappresentante relativa alla strategia europea di sicurezza economica JOIN(2023)20.

La comunicazione mira a alla minimizzazione dei rischi derivanti da alcuni flussi economici nel contesto delle accresciute tensioni geopolitiche e dei rapidi cambiamenti tecnologici e definisce un quadro comune per assicurare la sicurezza economica attraverso la promozione della competitività dell'UE, la protezione dai rischi e partenariati con il maggior numero possibile di paesi per affrontare gli interessi comuni.

I rischi presentati da determinate relazioni economiche evolvono infatti rapidamente nell'attuale contesto geopolitico e tecnologico e si rende necessario un approccio globale per individuare, valutare e gestire in comune i rischi per la sicurezza economica dell'UE.

La strategia identifica quattro settori su cui effettuare una valutazione approfondita dei rischi per la sicurezza economica.

Rischi per la resilienza delle catene di approvvigionamento, compresa la sicurezza energetica

Si fa riferimento ai rischi di impennate dei prezzi, indisponibilità o scarsità di prodotti critici o fattori produttivi nell'UE, compresi, ma non solo, quelli legati alla transizione verde, quelli necessari per un approvvigionamento energetico stabile e diversificato e per i medicinali.

Rischi per la sicurezza fisica e la cibernetica delle infrastrutture critiche

Si tratta dei numerosi ed articolati rischi di perturbazioni o sabotaggio di infrastrutture critiche, quali condotte, cavi sottomarini, generatori di energia, trasporti, reti di

comunicazione elettronica, che possono compromettere la fornitura sicura e affidabile di beni e servizi o la sicurezza dei dati nell'UE.

Rischi connessi alla sicurezza tecnologica e a fughe tecnologiche

Sono quelli legati ai progressi tecnologici dell'UE, la competitività tecnologica e l'accesso a tecnologie all'avanguardia, realizzati attraverso pratiche dolose nella sfera digitale quali lo spionaggio o la fuga illecita di conoscenze. In alcuni casi, la fuga delle tecnologie rischia di rafforzare le capacità militari/di intelligence di coloro che potrebbero utilizzarle per minare la pace e la sicurezza, in particolare per le tecnologie a duplice uso come quelle quantistiche, i semiconduttori avanzati o l'intelligenza artificiale, e richiede pertanto misure specifiche di attenuazione dei rischi.

Rischi di strumentalizzazione delle dipendenze economiche a fini bellici o di coercizione economica

Sono quelle minacce di paesi terzi che puntino all'UE, ai suoi Stati membri e alle sue imprese attraverso misure che incidono sugli scambi o sugli investimenti al fine di provocare una modifica delle politiche interne

La strategia delinea le modalità per ridurre i rischi individuati mediante un approccio in tre fasi.

La prima è centrata sulla promozione della competitività dell'UE mediante il rafforzamento del mercato unico, il sostegno per un'economia forte e resiliente, gli investimenti in competenze e la promozione della base industriale, tecnologica e di ricerca dell'UE.

La seconda identifica la protezione della sicurezza economica dell'UE attraverso una serie di politiche e strumenti esistenti, la considerazione di nuovi strumenti e politiche per colmare eventuali lacune. Nella terza si affida ai partenariati ed a partner il compito di rafforzare la sicurezza economica, anche attraverso la promozione e la conclusione di accordi commerciali, il rinnovamento di nuovi partenariati e il rafforzamento dell'ordine economico internazionale basato su regole e le istituzioni multilaterali, come l'Organizzazione mondiale del commercio, nonché l'investimento nello sviluppo sostenibile mediante la strategia "*Global Gateway*".

La comunicazione definisce una articolata serie di azioni da implementare con atti successivi.

La prima è stata quella di condividere con gli Stati membri un quadro per la valutazione dei rischi sulla sicurezza economica dell'UE e la definizione di un elenco di tecnologie essenziali per la sicurezza economica e la valutazione dei rischi connessi al fine di elaborare misure di attenuazione adeguate. Tale valutazione è stata effettuata sulla base della raccomandazione C(2023)6689 del 3 ottobre 2023 che ha individuato nei semiconduttori avanzati, intelligenza artificiale, *quantum computing* e biotecnologie settori ad elevata sensibilità ed a rischio di fuga di tecnologia.

Inoltre si dà conto di avviare un dialogo strutturato con il settore privato per giungere a una comprensione collettiva della sicurezza economica e incoraggiare il settore a esercitare la dovuta diligenza e a effettuare la gestione dei rischi alla luce delle preoccupazioni per la sicurezza economica.

Altro obiettivo è il sostegno della sovranità tecnologica dell'UE e la resilienza delle catene del valore dell'UE mediante lo sviluppo di tecnologie critiche nel quadro di una nuova piattaforma per le tecnologie strategiche per l'Europa (denominata STEP).

Di rilievo la proposta di una serie di misure dirette a migliorare la sicurezza della ricerca, garantendo un'applicazione sistematica e rigorosa degli strumenti esistenti, nonché individuando e colmando eventuali lacune rimanenti.

Si punta anche a rafforzare la sicurezza economica dell'UE, compresi i pacchetti degli strumenti della

diplomazia ibrida e della diplomazia informatica, nonché il pacchetto di strumenti contro la manipolazione delle informazioni e l'ingerenza di soggetti stranieri. Infine sarà attribuita alla capacità di analisi dell'intelligence dell'UE il compito di concentrarsi specificamente sull'individuazione delle possibili minacce per la sicurezza economica dell'UE.

Con questo pacchetto di strumenti, si è dunque disegnata la cornice normativa ed operativa per garantire la protezione e la promozione della sicurezza economica dell'UE come elementi pienamente integrati nell'azione dell'Unione europea.

Sicurezza, l'intelligenza biologica è più importante di quella digitale

A cura di Alessandro Manfredini

"L'AI è uno strumento fondamentale, ma serve un security manager preparato per utilizzarla al meglio per difendersi dalle infiltrazioni criminali"

C'è solo un modo per sfruttare al massimo le potenzialità dell'intelligenza artificiale: investire sull'intelligenza biologica.

Una premessa doverosa. È del tutto evidente che l'avvento in maniera massiccia e diffusa dell'intelligenza artificiale rappresenti un'opportunità senza precedenti per l'implementazione dei livelli di sicurezza di moltissimi ambiti. Dalle infrastrutture fisiche critiche, agli esercizi commerciali. Dai sistemi di videosorveglianza delle nostre città, agli istituti di credito. Non esiste ambito o settore nel quale l'intelligenza artificiale non potrebbe rappresentare un'arma in più per la protezione dei cittadini, della loro incolumità, della loro salute, dei loro possedimenti e, perché no, dei loro dati personali.

Questo perché l'AI ci consente di raccogliere, organizzare, rielaborare e restituire una serie infinita di informazioni utili a sviluppare previsioni, programmare interventi infrastrutturali, definire piani operativi di intervento e prevenzione. Tutto grazie alla capacità elaborativa dei dati e alla capacità dell'intelligenza artificiale di lavorarli in tempi rapidissimi.

Ma dove risiede la soluzione, spesso si nasconde anche il problema. In questo caso l'anello debole dell'intero sistema sono proprio i dati. O meglio, i dataset di cui l'intelligenza artificiale si nutre per elaborare "pensieri" e risposte utili agli utenti e, in alcuni specifici casi, ai *Security manager.*

I principali modelli di apprendimento dell'Intelligenza artificiale sono essenzialmente due: il *machine learning* e il *deep learning.*

Il secondo è direttamente ispirato al cervello umano ed è in grado di indagare gli schemi complessi contenuti nelle grandi quantità di dati - nei testi, nelle musiche o nelle immagini - individuando i modelli ricorrenti ed estrapolandone informazioni accurate. Il tutto in perfetta autonomia e con il vantaggio di riconoscere gli errori comuni.

Più semplice, ma paradossalmente più vulnerabile è il primo modello, il *machine learning*.

In questo caso l'apprendimento avviene attraverso algoritmi che leggono e interpretano *dataset* più piccoli, ma in maniera progressiva, sviluppando previsioni tanto più accurate quanti più dati hanno a loro disposizione.

Ed è esattamente qui, nella somministrazione delle informazioni e dei dataset che si nasconde la principale minaccia per l'efficacia delle Intelligenze artificiali e di conseguenza per la sicurezza dei servizi ad essa affidata.

I cyber criminali, infatti, stanno iniziando a sfruttare l'impiego dell'intelligenza artificiale a proprio vantaggio e per farlo lavorano proprio sui dati appannaggio del machine learning.

L'inserimento fraudolento di informazioni non corrette all'interno di questi dataset può determinare un malfunzionamento progressivo dell'AI stessa, con conseguenze anche gravi per l'utenza.

Un esempio. La sostituzione dell'indicazione "livello d'allerta" con "livello di guardia" all'interno di una centralina pluviometrica potrebbe impedire il corretto funzionamento dei sistemi di avviso diretto della popolazione in caso di innalzamento eccessivo di un corso d'acqua. Invece di un'allerta di massimo livello, l'AI potrebbe trovarsi a segnalare un'allerta inferiore, pregiudicando l'entrata in funzione dei piani di protezione civile e pronto intervento.

Un'altra ipotesi, non meno pericolosa, è quella di un'infiltrazione a monte, in grado di compromettere e modificare anche solo parzialmente l'intero *dataset* da dare in pasto all'AI in una determinata azienda o in un determinato servizio. Il risultato è la compromissione delle intere previsioni e del funzionamento stesso dei sistemi informatici.

Per mettersi al riparo da fattispecie simili di cyber attacchi, c'è solo un rimedio: mettere il professionista al centro del sistema di sicurezza. Privilegiare cioè l'intelligenza biologica a quella artificiale, rendendo quest'ultima uno strumento nelle mani della prima.

E qui però si aprono altri due problemi dei quali il legislatore non può non tenere conto.

Il primo è quello della ridotta libertà di manovra che hanno i *security manager* nell'utilizzo dei sistemi di intelligenza artificiale.

Mentre negli Stati Uniti la regolamentazione generale è estremamente blanda, non altrettanto si può dire dell'UE; con il voto del 14 giugno scorso, infatti, il Parlamento europeo ha dato il via ad un processo che porterà Bruxelles a legiferare in maniera stringente sull'intelligenza artificiale entro le elezioni comunitarie del giugno prossimo. Al netto di due anni di compliance volontaria da parte delle aziende, quel che si rischia con questa norma è che le forze dell'ordine e i *security manager* abbiano armi spuntate nell'uso di questi sistemi, in particolare al confronto con i cybercriminali per i quali non esistono paletti.

Il secondo problema rischia di essere ancor più impattante. Nel settore della *security*, in particolare la *cyber*, mancano professionisti e aspiranti tali.

I dati diffusi dalla stessa Commissione europea raccontano che il 77% delle aziende soffre la mancanza di personale adeguatamente formato. Inoltre il Global *Cybersecurity Outlook* 2023 del *World Economic Forum*, sostiene che solo il 46% dei responsabili cyber aziendali sia convinto di avere all'interno della propria organizzazione le persone e le risorse necessarie a fronteggiare un attacco cibernetico.

Un gap di competenze cresciuto esponenzialmente negli ultimi 10 anni, in ragione dell'esplosione della domanda di figure professionalizzate.

L'effetto combinato di una regolamentazione eccessivamente stringente e di un percorso formativo non adeguato alle esigenze del mercato della security rende tutto questo un'emergenza nazionale e comunitaria. Purtroppo però le misure per invertire il trend, restituendo centralità all'intelligenza biologica, sono ancora tutte in fase sperimentale. E da verificare la loro efficacia.

Introduzione alla sicurezza della Supply Chain

A cura di Cristina Spagnoli

Definizione e importanza nell'economia globale attuale

L'economia attuale, fortemente globalizzata, è basata in modo importante su catene di fornitori appartenenti alle aree più diverse del mondo. Sperimentiamo questo fatto ogni giorno, salendo sulla nostra auto, azionata da componenti elettronici e meccanici provenienti da ogni parte del globo; andando al supermercato, dove oggi è sostanzialmente possibile trovare qualunque cosa; scaricando ed installando un software, prodotto da una *software house* che potrebbe essere nel quartiere affianco al nostro o dall'altra parte della terra, senza che per noi faccia alcuna differenza. È come se ci trovassimo all'interno di una rete di mutue dipendenze, ognuno facendo affidamento su qualcosa prodotto da qualcun altro. Questo è un concetto che nell'informatica torna spesso: quando si parla di *layer* di un protocollo, per esempio, ci si riferisce proprio al fatto che, nell'erogazione di un servizio ad un determinato livello, si faccia affidamento sui servizi offerti dal livello sottostante, per, insomma, non dover ogni volta reiventare la ruota.

I servizi offerti oggi racchiudono complessità via via sempre maggiori, ed è pressoché impensabile che una sola azienda racchiuda in sé tutte le competenze necessarie che le consentano di implementare tutto, dalla A alla Z, portandoli fuori dal proprio ambito o dal proprio *core business*.

In tutto questo come non pensare ai servizi basati sul cloud, che rappresentano oggi una parte importante nella filiera dei fornitori di ogni azienda.

È dunque chiaro che servizi e prodotti offerti dai fornitori rientrano necessariamente all'interno del perimetro di sicurezza aziendale, perimetro i cui contorni sono diventati sempre meno visibili.

Tendenze recenti e rischi in aumento

La tendenza è dunque quella di affidarsi sempre a fornitori esterni per tutto quello che non sia core business. Ma quali rischi per la sicurezza occorre essere pronti a mitigare? È chiaro che i fornitori rappresentano un asset di cui essere perfettamente a conoscenza e per i quali occorre indirizzare le problematiche di sicurezza, come per qualunque altro asset, ma con qualche difficoltà in più: si tratta di un asset sul quale non abbiamo controllo e, a volte, difficilmente individuabile. Ora occorre correlare questa affermazione con la criticità di cui spesso alcuni fornitori sono investiti nella gestione dei nostri servizi, dei nostri prodotti e della nostra vita aziendale, *e-mail*, gestione dell'identità, sviluppo degli applicativi, gestione dei sistemi e così via - per capire quanto, un problema di sicurezza su uno di questi, possa trasformarsi facilmente in un incubo. In Italia, inoltre, abbiamo migliaia di piccole e piccolissime aziende, che fanno parte di *supply chain* di aziende molto più grandi, e che sono ancora non sufficientemente mature dal punto di vista della sicurezza, diventando una facile porta di accesso verso le infrastrutture dei loro clienti. Una categoria di fornitori, poi, è particolarmente ambita dagli attaccanti: i *Managed Security Service Provider* (MSSP). Il motivo della loro appetibilità è facilmente intuibile: hanno le chiavi del regno di molteplici clienti, sono in possesso di dati riservati e approfonditi e un eventuale traffico di rete proveniente dalle loro infrastrutture, proprio in virtù del servizio erogato, sarebbe difficilmente giudicato anomalo.

Il 2023 ha visto l'uscita di diversi report relativi a questo argomento (SonaType, KROLL, KPMG, per citarne alcuni) tutti concordi nel dire che la tendenza degli attacchi alle *supply chain* è decisamente in crescita, perché si tratta di un business estremamente redditizio, con una amplificazione di impatto enorme (un attacco con successo verso uno di questi, ha impatto su molti) e perché spesso si attacca l'anello debole di una catena di difesa.

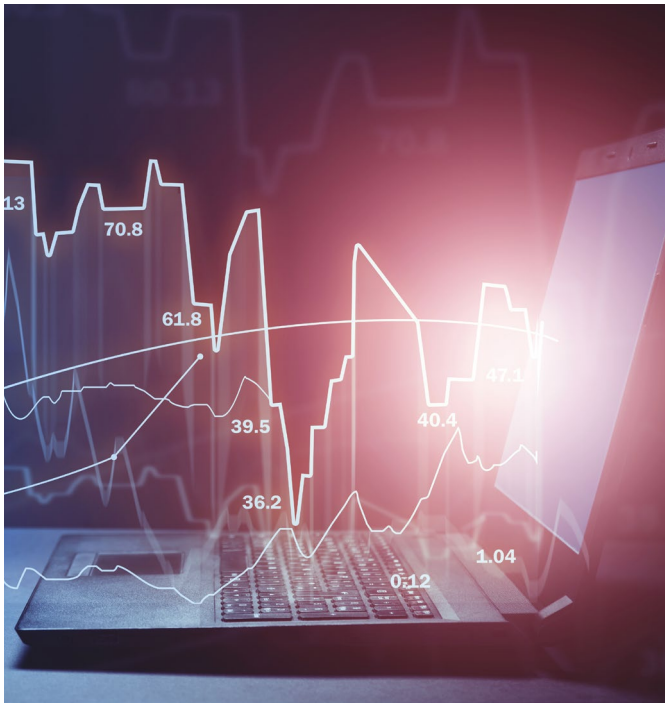
Attacchi alla Supply Chain di Rilievo

Le tipologie di attacchi che vedono sfruttare la *supply chain* come vettore di ingresso per raggiungere le vittime finali sono molteplici. Vediamo di analizzarne alcune sulla base di attacchi rilevanti avvenuti negli ultimi anni.

Compromissione di *Software* e *Firmware*: è il caso dell'attacco a *SolarWinds* del 2020. Gli attaccanti, probabilmente state sponsored, sono stati in grado di alterare il codice di un prodotto SolarWinds, Orion, introducendo una *backdoor* nel software, che si è poi trasformata in una backdoor nei server dei clienti attraverso i successivi aggiornamenti. Si è trattato di un attacco devastante, sia per la grande diffusione del software e quindi per la mole dei clienti successivamente coinvolti (circa 300.000), che per le tipologie di clienti impattati, che comprendevano decine di grossi nomi (NASA, NSA, ING Direct, US Pentagon, Symantec, TIM giusto per citarne alcune), che per le conseguenze che sui singoli clienti l'attacco ha avuto. È da notare, come nota a margine (ma poi neanche troppo), che ad ottobre 2023, la *U.S. Exchange Commission* (SEC) ha accusato il CISO di SolarWinds di "frode e carenze di controllo interno in relazione a presunti rischi e vulnerabilità di cybersicurezza noti", aprendo, di fatto, una stagione del tutto nuova nella gestione delle responsabilità delle figure apicali della sicurezza.

Abuso di Relazioni di Fiducia: il 2 luglio 2021, REvil, una *gang ransomware* ben conosciuta, attaccò circa un migliaio di *Managed Service Provider*, sfruttando delle vulnerabilità già scoperte ad aprile di quell'anno, ma la cui remediation non era stata completata, in un software di controllo remoto, *Virtual System Administrator (*VSA), prodotto dalla statunitense Kaseya. La particolare funzione del software lo poneva in una posizione critica all'interno delle aziende attaccate, sfruttando, di fatto, un trust tra Kaseya, gli MSP ed i loro clienti.

Attacchi ai Componenti Open Source: quello che è successo il 25 ed il 30 dicembre 2022 è significativo per capire come anche la *supply chain open-source* possa essere utilizzata dagli attaccanti per colpire. Tra queste due date, infatti, sfruttando il meccanismo della gestione delle priorità nelle dipendenze dei pacchetti python (il *Python Package Index*), alcuni cyber criminali hanno sostituito un pacchetto legittimo del framework di *Machine Learning PyTorch*, con uno con lo stesso nome, ma malevolo. Malevolo sì, ma quanto? Beh, diremmo molto. Conteneva, infatti, un *malware*, Triton, specializzato nel manomettere i dispositivi di sicurezza dei sistemi industriali: un report del *MIT Technology Review*, lo definisce il primo *malware* progettato per mettere in pericolo vite umane. Quindi, ricapitolando, parliamo di un *Framework* per il *Machine Learning* usato come vettore per un malware specializzato in sistemi di sicurezza industriale: i possibili target, dunque, non sono banali.



Furto di Credenziali e Token: il *phishing* continua a essere un vettore di attacco efficace contro la supply chain. Aziende e fornitori sono frequentemente presi di mira tramite e-mail ingannevoli per rubare credenziali o distribuire malware. Chiaramente se posso ottenere delle credenziali valide per sfruttare una VPN destinata ai fornitori, perché non farlo? Minimo rischio e massimo guadagno, multi-factor authentication permettendo, ovviamente.

L'attacco ad Okta nel 2023 è stato un grave incidente di sicurezza che ha esposto i dati dei clienti e sollevato preoccupazioni significative riguardo alla sicurezza della supply chain IT. Okta è un provider neutrale per la gestione dell'identità, per cui riveste un ruolo centrale per le infrastrutture dei suoi clienti.

Tra il 28 settembre e il 17 ottobre 2023, un threat actor ha ottenuto accesso non autorizzato ai file del sistema di supporto clienti di Okta, utilizzando delle credenziali rubate ad un amministratore. Alcuni di questi file contenevano token di sessione, i quali potevano essere utilizzati per attacchi di session hijacking. Gli attaccanti hanno abusato di queste credenziali per attaccare, con più o meno successo, alcuni dei clienti di Okta. Alcune analisi evidenziano come gli attaccanti abbiano trascorso almeno due settimane di tempo all'interno dell'infrastruttura di Okta. Quella di BeyondTrust in particolare, cliente Okta, sottolinea che il 2 ottobre, il loro team di sicurezza ravvisava dei movimenti sospetti all'interno della propria infrastruttura, da parte di un utente di supporto che utilizzava le credenziali locali di un amministratore Okta. Il 2 ottobre stesso BeyondTrust avvisava quindi Okta, senza che la cosa producesse, almeno apparentemente, alcun effetto, se non la pianificazione di qualche call di allineamento. Questo almeno fino al 19 di ottobre quando, effettivamente, Okta avvisava BeyondTrust di avere subito un *breach*.

Questo attacco sottolinea l'importanza critica delle misure di sicurezza, in particolare per i fornitori di servizi di identità e autenticazione che, come Okta, svolgono un ruolo fondamentale nella protezione dell'accesso a sistemi e dati aziendali. E sottolinea quanto sia importante non sottovalutare alcun aspetto, alert e segnalazione.

Backdoor in Prodotti Ampiamente Diffusi: un altro attacco emblematico delle possibili implicazioni della compromissione supply chain è quello che ha coinvolto 3CX nel marzo del 2023. 3CX produce un software per audio e video comunicazione, chiamato *3CX Desktop App*. Alcune versioni di questo software sono state utilizzate come *trojan horse* per arrivare a bordo dei computer degli utenti finali e, sostanzialmente, rubare loro dei dati. Come è potuto arrivare l'attaccante all'interno della rete di 3CX ? Compromettendo un'altra supply chain, quella relativa ad un prodotto software, X_Trader, evidentemente utilizzato da qualcuno all'interno dell'infrastruttura di 3CX. Una volta all'interno, l'attaccante è stato in grado di raccogliere credenziali e muoversi lateralmente, fino ad arrivare ai sorgenti del software di 3CX Desktop App e modificarli.

L'ultimo attacco di una certa rilevanza è quello che ha coinvolto la *Taiwanese Cyberlink*, produttrice di software multimediale e di riconoscimento facciale. In questo caso il threat actor, probabilmente il gruppo Nordcoreano *Diamond Sleet* (ZINC), è stato in grado di modificare il legittimo installer dell'applicazione *CyberLink*, includendo codice dannoso che scarica, decifra e carica un payload. Il file, che è stato firmato utilizzando un certificato valido rilasciato a CyberLink Corp., è ospitato su un'infrastruttura di update legittima di proprietà di CyberLink e include controlli per limitare la finestra temporale di esecuzione ed eludere il rilevamento da parte dei prodotti di sicurezza. Fino a questo momento, l'attività malevola ha impattato oltre 100 dispositivi in molti paesi, inclusi Giappone, Taiwan, Canada e Stati Uniti (Fonte Microsoft).

Strategie di Mitigazione

Come si capisce facilmente, dietro la sicurezza della supply chain si nasconde una complessità esponenziale. Come detto, le parti in gioco sono molteplici e non direttamente controllabili. Indubbiamente, ma ci rendiamo conto che attualmente questa sia utopia, sarebbe bene che ogni parte coinvolta nella supply chain fosse consapevole della necessità di avere una postura di sicurezza elevata, in modo da poter garantire sicurezza in maniera atomica e indipendente: a onor del vero, la legislazione europea, ha preso molto seriamente il problema, e sta cercando di indirizzarlo con diversi provvedimenti, anche se con qualche distorsione.

Al di là ed in attesa di questo, tuttavia, occorre predisporre un approccio strategico che farà parte di un percorso di maturità della sicurezza complementare alla messa a punto delle misure di sicurezza interne.

Vediamo quali possono essere alcuni punti su cui basare questo approccio:

Valutazione e Gestione del Rischio: identificare e valutare i rischi per la sicurezza associati con tutti gli elementi della supply chain. Questo include la valutazione dei fornitori, dei prodotti e dei servizi che sono parte della catena di fornitura.

Sicurezza dei Fornitori e dei Partner: sviluppare politiche e procedure per la gestione della sicurezza delle informazioni che coinvolgono fornitori e partner. Questo include contratti che definiscono chiaramente le aspettative in termini di sicurezza delle informazioni e i requisiti per la gestione degli incidenti.

Gestione dei Cambiamenti nella Supply Chain: stabilire processi per gestire i cambiamenti nella supply chain, inclusi i cambiamenti dei fornitori o dei loro prodotti, che potrebbero influenzare la sicurezza delle informazioni.

Continuità Operativa e Resilienza: assicurarsi che ci siano piani di continuità operativa e di ripristino in caso di incidenti che colpiscono la supply chain.

Sicurezza nell'Acquisizione di Prodotti e Servizi: integrare i requisiti di sicurezza nelle specifiche di acquisto dei prodotti e dei servizi.

Monitoraggio e Audit Regolari: monitorare continuamente i fornitori e le loro prestazioni in termini di sicurezza delle informazioni, e condurre audit regolari per garantire il rispetto dei requisiti di sicurezza. Può inoltre essere utile ricorrere ad audit esterni per verificare l'efficacia delle misure di sicurezza implementate nella supply chain.

Gestione delle Vulnerabilità e degli Incidenti: sviluppare e implementare processi per identificare, valutare e mitigare le vulnerabilità, e per gestire e rispondere agli incidenti di sicurezza che coinvolgono la supply chain. Questo processo deve comprendere la verifica dei sorgenti e delle librerie open source che utilizziamo: l'*open source* ha, infatti, da un lato lo svantaggio di lasciare agli attaccanti la possibilità di modificare sorgenti e dipendenze in modo probabilmente meno controllato, cosa peraltro, come si è visto, accaduta anche col *software closed source*, ma d'altro canto ha l'enorme vantaggio di permetterci ispezionare i qualsiasi momento ciò che utilizziamo attraverso tool automatici di *Static Code Analysis o Software Composition Analysis.*

Formazione e Consapevolezza: fornire formazione e aumentare la consapevolezza sulla sicurezza della supply chain tra i dipendenti e i partner per garantire che comprendano le politiche e le procedure.

Risposta agli Incidenti: Preparare e testare piani di risposta agli incidenti per affrontare eventuali violazioni o altri problemi di sicurezza che colpiscono la supply chain.

Best Practices e Standard del Settore

- ISO 28000 - Specifiche per sistemi di gestione della sicurezza nella supply chain
- ISO 27001
- Framework di Cybersecurity del NIST
- NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Conclusione

In questi anni, in particolare con l'avvento del *cloud*, abbiamo assistito allo sgretolarsi dei contorni del perimetro da difendere, facendo diventare quest'ultimo un concetto sempre più labile e di difficile identificazione. La *supply chain* contribuisce in maniera importante a questo sgretolamento, percorrendo un ponte che arriva direttamente al cuore dei nostri sistemi. La sua sicurezza è vitale per ogni azienda che voglia avere una postura di sicurezza avanzata ed una reale gestione del rischio.

CYBER
Think Tank
ASSINTEL

Assintel Cyber Hub

CYBER Think Tank ASSINTEL

Connettiti alla rete della sicurezza!

Obiettivo:

Mappare ed elencare le Aziende associate ad Assintel con competenze in ambito Cyber.

Progetto:

L'Assintel Cyber Hub è un Catalogo Annuale (verrà valutato nel corso dell'anno una differente cadenza di aggiornamento).

Per info scrivi a: segreteria@assintel.it

La cultura d’impresa nella metamorfosi digitale

A cura di Don Luca Peyron

La sociologia ha ben delineato come buona parte della metamorfosi culturale e sociale che l’occidente vive ha come causa prima la trasformazione digitale. La cultura d’impresa, la missione ma soprattutto la vision delle grandi imprese del settore digitale hanno plasmato, insieme ai loro prodotti, una consistente parte del modo di pensare e porsi nella realtà delle persone.

Di tutti, non solo dei giovani come comunemente avviene. La lingua, da sempre cartina di tornasole di una cultura, è uno degli specchi di questo cambiamento con l’introduzione non solo di molti neologismi, ma anche, se non soprattutto, l’addensarsi attorno a concetti proprio dell’ambito tecnico e tecnologico di significati e senso propri di altri domini.

Questa marcia veloce e queste connessioni profonde sono ben presenti ai lettori di queste note, che in modi differenti sono stati e saranno protagonisti di questo processo. Quanto questo significhi in termini di opportunità di mercato, sviluppo delle imprese, circolazione e mutazione aziendale ci è parimenti ben presente. Quanto vorrei qui condividere è un aspetto ulteriore che ha sempre fatto parte dell’impresa, ma mai come oggi è elemento decisivo.

Mi riferisco alla responsabilità ed alla opportunità straordinaria che oggi l’impresa tecnologica ha di incidere positivamente sulla società nel suo complesso, non semplicemente in termini di benessere economico, occupazione e sviluppo, ma in termini di sostrato culturale e, dunque, di quel benessere non meno importante, che è quello del senso, del significato, di ciò che non è numericamente apprezzabile, ma esistenzialmente decisivo. Forse decisivo nel senso più pieno del termine.

Lo sguardo credo che possa essere portato al di là della propria azienda, del proprio recinto e farsi più ampio, considerare come l’azione riverberi molto più in là del nostro parcheggio.

L’essere umano contemporaneo è frantumato, non più semplicemente liquido. Ha bisogno prima di tutto di essere ricomposto, di avere nuovi orizzonti di senso e significato che non possono essere un semplice aggiustamento di quanto ci ha preceduto.

La grande complessità del tempo presente non accetta soluzioni semplicistiche e richiede un guizzo in avanti dell’umano del suo proprio umano, compresa la sua dimensione trascendente. L’impresa può scegliere oggi di essere motore di una cultura che accompagni l’umano a non essere semplicemente funzione di un mercato, performante in ciò che fa, efficiente nel suo porsi al lavoro.

Ma umano, autenticamente umano ove il fare è in ultima analisi in funzione dell’essere e non dell’apparire. Un umano che non aspira a raccontarsi su LinkedIn, ma ad essere ricordato dalla sua famiglia, dai suoi collaboratori e colleghi. Un umano che è stimato perché, appunto, umano. Abbiamo imprenditori così tanto visionari da comprendere che ciò che vale non sempre si può mettere a bilancio?

Strategia di difesa cyber nell'industria 4.0

A cura di Piergiuseppe Delfino

La crescente interconnessione digitale delle aziende e la dipendenza sempre maggiore dalla tecnologia pongono una sfida critica alla sicurezza informatica interna. In un'epoca in cui le minacce cibernetiche sono sempre più sofisticate, è imperativo che le organizzazioni sviluppino e implementino strategie robuste per proteggere i propri dati e sistemi. Oggi il blocco di parziale o totale delle funzionalità informatiche di qualsivoglia azienda comporta rischi di divulgazione di dati riservati, perdita del business, oltreché ripercussioni sulle catene clienti/fornitori che potrebbero essere coinvolti negli incidenti informatici.

Un elemento fondamentale di una solida strategia di cybersecurity è la consapevolezza del personale. I dipendenti devono essere formati regolarmente sulle minacce cibernetiche, sui metodi di attacco più comuni e sulle pratiche di sicurezza delle informazioni. Questo contribuisce a ridurre la probabilità di cadere vittima di attacchi di phishing o di altre tattiche di ingegneria sociale ed in generale di attacchi che sfruttano gli utenti. Si veda la NIS2 direttiva europea che punta a rafforzare la sicurezza informatica nell'UE. Entrata in vigore il 17 gennaio 2023, la direttiva dovrà essere recepita dai singoli Stati membri entro il 17 ottobre 2024.

Definire e comunicare chiaramente le politiche di sicurezza è cruciale così come fare comprendere esattamente quali sono i rischi del mancato rispetto. Queste politiche dovrebbero coprire l'uso appropriato delle risorse informatiche, le password robuste, l'accesso ai dati sensibili e le procedure in caso di violazione della sicurezza. Un'implementazione rigorosa di queste politiche contribuirà a creare una cultura di sicurezza forte all'interno dell'organizzazione ma tutto passa per una accettazione di una postura più rigida che deve essere necessariamente comunicata dalle figure apicali dell'azienda.

Mantenere tutti i sistemi e software aggiornati è essenziale per rimediare alle vulnerabilità di sicurezza note. I criminali informatici spesso sfruttano falle di sicurezza in software obsoleti o non aggiornati, pertanto, garantire aggiornamenti regolari riduce significativamente il rischio di attacchi. Implementare rigorosi controlli degli accessi per garantire che solo le persone autorizzate possano accedere a determinati dati o sistemi. L'adozione di approcci come il principio del privilegio minimo può limitare l'estensione delle potenziali violazioni. Non di meno un sistema di monitoraggio continuo (o eventualmente un SOC ove possibile e/o necessario) è essenziale per identificare tempestivamente comportamenti anomali o attività sospette. L'uso di strumenti avanzati di analisi dei log e di intelligenza artificiale può aiutare a individuare potenziali minacce prima che causino danni significativi

La perdita di dati può avere conseguenze devastanti, sia a livello personale che aziendale. Incidenti come guasti hardware, attacchi informatici, errori umani o catastrofi naturali possono comportare la distruzione irreparabile di informazioni critiche. Un backup regolare assicura che i dati siano duplicati e archiviati in modo sicuro, offrendo un meccanismo per recuperare rapidamente le informazioni perse. Gli imprevisti sono inevitabili, ma la capacità di ripristinare rapidamente i dati può fare la differenza tra un breve contrattempo e una crisi prolungata. I backup consentono di recuperare le informazioni essenziali in tempi brevi, riducendo al minimo i tempi di inattività e contribuendo a mantenere la continuità operativa. Ad oggi le piattaforme di backup offrono forme ibride e delocalizzate per ridurre qualsivoglia rischio derivante anche da conflitti geopolitici anche introducendo protocolli "immutabili" che garantiscono quindi i backup esenti da qualunque evento ransomware.

Gli attacchi ransomware sono sempre più diffusi e pericolosi. I criminali informatici cifrano i dati dell'utente o dell'organizzazione e richiedono un riscatto per rilasciarli. Con backup regolari, è possibile ripristinare i dati senza cedere alle richieste degli attaccanti, garantendo la sicurezza dei dati senza finanziare attività criminali. Un sistema di backup affidabile contribuisce a garantire l'integrità dei dati nel tempo. Il deterioramento dei dati a causa di errori fisici o logici può essere mitigato con una strategia di backup ben gestita, garantendo che le informazioni conservino la loro qualità originale nel corso del tempo.

In molte industrie, esistono normative e leggi rigide che richiedono la conservazione sicura dei dati per un determinato periodo. L'implementazione di backup regolari aiuta a soddisfare tali requisiti normativi, riducendo il rischio di sanzioni legali e proteggendo l'organizzazione da possibili conseguenze negative. Nonostante tutti gli sforzi, nessuna organizzazione è immune da violazioni della sicurezza. Pertanto, è vitale avere un piano di gestione delle crisi ben definito. Questo piano dovrebbe delineare chiaramente i passaggi da seguire in caso di violazione, compresi i processi di notifica, le azioni correttive e la comunicazione con le parti interessate siano clienti che fornitori che Enti.

La cybersecurity interna richiede un approccio olistico che coinvolga il personale, le politiche, la tecnologia e la pianificazione per la gestione delle crisi. Solo attraverso una combinazione di consapevolezza, preparazione e azioni preventive, le organizzazioni possono sperare di difendersi efficacemente dalle sempre crescenti minacce cibernetiche. Investire nella sicurezza informatica interna non è solo un imperativo tecnologico, ma un elemento chiave per garantire la continuità e la fiducia nell'era digitale.

Infine una sorta di team "militare" che si sappia relazionare con Enti quali il CSIRT Italia istituito presso l'Agenzia per la cybersicurezza nazionale (ACN) rende imperativo il dialogo tra Aziende che dovessero essere colpite da eventi maligni al fine di identificare i responsabili e attivare opportune misure di contenimento per evitare l'espandersi delle contaminazioni.

In conclusione l'attivazione precoce delle misure di cybersecurity anche attraverso automi oggi costituiti dalla I.A. contribuisce a ridurre i costi associati alle violazioni della sicurezza. Investire in cybersecurity fin dalle fasi iniziali di un progetto o di un sistema permette di risparmiare risorse finanziarie e reputazionali a lungo termine. Una costante e corretta valutazione del rischio esportando in modo leggibile e trasversale a tutta l'azienda rende partecipi e sensibili tutti gli attori sul tema.

I tre punti, principali, per i prossimi anni per rendere più sicuri i nostri sistemi e prevenire il diffondersi di eventi malevoli saranno quindi:

- Responsabilità delle Aziende e dei singoli
- Rischio, valutazioni, impatti sul business
- Collaborazione, con Enti, Aziende ed in generale con i normali partner

Il fattore umano nell'era della digital transformation

A cura di Marco Santarelli

La digital transformation, con lo sviluppo ormai incessante delle tecnologie più avanzate per potenziare ogni ambito della nostra vita, dalla comunicazione alla difesa, porta con sé, come risvolto negativo, la tendenza a sfruttare queste tecnologie come strumenti di violenza e terrorismo, che minano la nostra sicurezza personale e quella nazionale e internazionale. Basti pensare ai social network e al web in generale e al dilagare della disinformazione e delle minacce cyber, quello che abbiamo chiamato terrorismo dal basso, o ai droni, strumenti di terrorismo dall'alto.

L'attacco del 7 ottobre sulla Striscia di Gaza da parte da Hamas, che sta per Ḥarakat al-Muqāwama al-Islāmiyya, Movimento Islamico di Resistenza, contro Israele ha mostrato una sorta di controtendenza, che ha favorito la riuscita dell'azione terroristica pianificata già da tempo, senza il minimo sospetto da parte dell'intelligence israeliana. In questo caso, infatti, la tecnologia è stata lasciata da parte a vantaggio del fattore umano.

Il fattore umano a favore del terrorismo: l'esempio di Hamas

Se l'intelligence israeliana, come è noto, fa leva totalmente sulla sua tecnologizzazione e ha costruito la sua forza negli anni su questo suo aspetto, Hamas si è affidata totalmente all'uomo, all'incontro de visu, allo scambio di documenti cartacei e di informazioni senza il minimo uso della rete internet, ma sfruttando la rete umana.

Come sostiene il giornalista Giovanni Minoli in un'intervista tv per il programma di La7 L'Aria che Tira, "Tutta l'intelligence, prevalentemente quella israeliana, si è basata sulla sorveglianza elettronica, mentre i capi di Hamas, reduci delle varie Intifada, hanno capito quello che Totò Riina sapeva, cioè che è meglio comunicare con i pizzini che con internet o il telefono. E nessuno sapeva come comunicavano. È la riscoperta dell'essere umano nell'intelligence. Lo spionaggio e il controspionaggio si possono fare solo se si riscopre che bisogna stare nei posti fisicamente, infiltrarsi, conoscere e avere rapporti con le persone. Israele progressivamente si è troppo tecnologizzata e i servizi segreti sono diventati prevalentemente sorveglianza elettronica. È un problema di partenza fondamentale che riguarda tutti i servizi segreti. Servono cose concrete fatte da uomini. In qualche modo esce sconfitta la tecnologia pura, l'affidarsi in modo eccessivo e quasi divino escludendo progressivamente l'uomo e la sua capacità di analisi" (https://www.iltempo.it/personaggi/2023/10/11/news/giovanni-minoli-servizi-segreti-israele-hamas-tecnologia-crollo-mito-laria-che-tira-37167284/amp/%60).

Secondo Minoli, il metodo di Provenzano e Riina, quello dei pizzini difficilmente intercettabili e dei deltaplani (nel caso di Hamas), è lo specchio di una "guerra povera ma con cervello". Così facendo, grazie alla loro reti di informatori e alle piantine delle abitazioni, i militanti di Hamas hanno saputo dove poter colpire indisturbati. Il mondo analogico di Hamas ha avuto la meglio su quello digitale di Israele e se in passato il primo è sempre stato alla portata di tutti, mentre il secondo restava privilegio di pochi, oggi il basso costo della tecnologia ha fatto sì che anche il semplice cittadino vi possa accedere, convertendosi in potenziale pericolo per la sicurezza altrui e rompendo il confine tra civile e militare. (https://www.iltempo.it/esteri/2023/10/15/news/israele-hamas-tecnologia-intelligenza-artificiale-deltaplani-pizzini-computer-37205868/).

Hamas ha fatto arrivare a Tel Aviv notizie incomplete, utilizzando finte fonti, addestrando contemporaneamente giovani sequestratori che si sono recati con i deltaplani in Egitto, dove ci sono scuole di volo. Dalle ispezioni dei cadaveri dei terroristi uccisi sono stati scoperti dei foglietti stampati a colori contenenti immagini di carri armati israeliani, con elenchi dei loro punti deboli e indicazioni su come usare al meglio i lanciarazzi. L'intelligence israeliana ha fallito perché si è affidata totalmente alla tecnologia, non considerando il fattore umano, sulla scia di quello che il criminologo francese Alian Bauer ha definito "feticismo tecnologico" qualche anno fa, in riferimento all'ondata di attentati che ha sconvolto l'Europa e che l'innovazione tecnologica non è riuscita ad evitare (https://www.huffingtonpost.it/archivio/2016/03/30/news/per_sconfiggere_il_terrorismo_serve_soprattutto_il_fattore_umano_-5560026/).

Il fattore umano a favore della sicurezza: la Humint

La Humint, acronimo di Human Intelligence, è quella branca del metodo Intelligence che consiste nella raccolta di informazioni per mezzo di contatti interpersonali, quindi attraverso fonti umane, fonti aperte e informatori. Le attività Humint più diffuse sono, ad esempio, il pattugliamento ordinario, la ricognizione speciale, le informazioni frutto del lavoro dei consiglieri militari d'ambasciata, la redazione di rapporti diplomatici, le confessioni dei prigionieri di guerra, le interviste di rifugiati e viaggiatori e le notizie fornite da organizzazioni non governative, fino alle operazioni di spionaggio vero e proprio. Il miglior investimento che uno Stato possa fare è sempre stato quello sulle risorse umane e sul fare rete per la condivisione tra Stati delle informazioni e delle competenze.

Nel caso specifico mediorientale attuale, quel "lunghissimo filo informativo" tessuto tra uomini nell'organizzare l'attacco di Gaza e la "fisicità umana del passaparola", come sottolinea Luisa Franchina, Presidente Associazione Italiana esperti in Infrastrutture Critiche, senza sfruttare nessun tipo di tecnologia, potevano essere intercettati se l'intelligence israeliana avesse messo in campo risorse umane e non solo apparati tecnologici (https://www.cybersecurity360.it/cybersecurity-nazionale/intelligence-israeliana-il-flop-hi-tech-contro-hamas-cosa-non-ha-funzionato/). Infatti, la strategia attuata da Hamas e tenuta nascosta per un anno, è stata di counter-intelligence, che può essere realizzata in maniera efficace solo attraverso il fattore umano, tant'è che tutta la struttura tecnologica israeliana di controllo, fatta di telecamere, sensori e sistemi d'attacco attivabili da remoto non è stata pronta a prevenire, o comunque a gestire, l'attacco del 7 ottobre. I droni, poi, sono stati utilizzati da Hamas per oscurare i sistemi delle torri di comunicazione così da impedire loro di rispondere tempestivamente (https://www.ilgiornale.it/news/guerra/manuali-campo-e-codici-riferimento-hamas-si-preparata-2224518.html).

Uomo vs tecnologia

In uno studio di Fabio Vanorio e Francesco D'Arrigo per l'Istituto Italiano di Studi Strategici "Niccolò Machiavelli" intitolato "Intelligence hyper-loop, su come la considerazione del concetto "human-in-the-loop" sia vitale per la rivoluzione digitale dello spionaggio" pubblicato a dicembre 2020 (https://www.strategicstudies.it/wp-content/uploads/2020/12/Edizioni-Machiavelli-Intelligence-Hyper-Loop.pdf), allo scopo "di indagare scientificamente sul ruolo che gli esseri umani possono svolgere nel promuovere o ostacolare il progresso tecnologico della Comunità Intelligence", il concetto di "Human-In-The-Loop" fa riferimento al rapporto Uomo-Macchina, i due aspetti principali alla base della crescita tecnologica di un sistema. L'Uomo è fondamentale nel favorire questa crescita in ogni ambito, così come nella costruzione delle sei fasi dell'Intelligence Loop, o Ciclo Intelligence, costituito da indirizzi di ricerca, pianificazione e direzione, raccolta, trattamento ed elaborazione, analisi e produzione, e disseminazione.

Il coinvolgimento dell'Uomo è importante proprio perché sa catalogare e studiare l'evoluzione specifica dell'AI e del Machine Learning applicate alle indagini. Anche se lo studio Vanorio-D'Arrigo segnala uno scricchiolio nel ruolo dell'essere umano nell'Intelligence Loop, in quanto se un processo organizzativo non funziona, la tecnologia più innovativa non può fare a meno di risentirne, l'elemento umano sa gestire i processi dell'Intelligence Loop. Sa anche prevedere i principi alla base dell'AI (5G, Machine Learning, Big Data). Il problema principale, ad esempio nelle indagini asimmetriche, è che molte volte non c'è il sufficiente contributo tra uomo e macchina. Si dovrebbe invece dare sempre più importanza alla branca dell'intelligence costituita da fonti umane e dall'interazione interpersonale.

In tal senso, con il progresso della tecnologia, la fonte umana non verrà depotenziata, ma si adeguerà. In tale direzione fondamentale è la Virtual Humint: l'insieme del lato umano della Humint e di quello virtuale del Socmint, ossia la Social Media Intelligence. La Virtual Humint, disciplina che si occupa maggiormente della creazione di identità virtuali in rete, soprattutto nelle piattaforme social, al contrario di quanto si possa pensare, riporta l'Uomo alla sua centralità nell'analisi e nella raccolta delle informazioni, andando a colmare così i vuoti che per forza di cose vengono lasciati dalla tecnologia. Uomo-Macchina possono funzionare senza che necessariamente la macchina, nel corso della sua evoluzione, sostituisca l'uomo.

Da questo "potenziamento" tecnologico sono derivate due scuole di pensiero. La prima è quella dei Big Data, che analizza i dati in maniera quantitativa attraverso l'uso di software di analisi di alta tecnologia, ma mancanti del "fattore umano" che fornisce quel dettaglio in più spesso fondamentale per la svolta di un'indagine. Questi software comportano un impegno di spesa, tempo di formazione del personale e gestione non indifferenti.

La seconda scuola di pensiero, che invece fa un'analisi qualitativa delle informazioni, è la cosiddetta Analyst Human Centric. Lo dice il nome stesso: l'analista umano è al centro dell'attività di indagine e i software sono marginali.

Per capire meglio la differenza di approccio tra i due metodi basta pensare alla lotta al terrorismo: con i big data si ottiene una visione complessiva e statistica degli eventi, mentre attraverso la Virtual Humint, l'analisi è svolta in maniera verticale e andando a fondo agli eventi partendo dagli specifici aspetti delle informazioni presenti nel cyberspazio e cercando anche nuovi spunti. Un esempio ce lo fornisce la grande attività svolta da Bellingcat, il sito di giornalismo inglese che con strumenti di open source gratuiti e i suoi giornalisti analisti, è riuscito a scovare gruppi terroristici dell'ISIS provenienti dal confine turco, un reparto speciale dell'ISIS, il Katibat al-Battar, a scoprire chi fossero i due agenti russi accusati di avere avvelenato Sergei Skripal e geolocalizzato i sicari dei narcos nello stato messicano di Chihuahua. Ricordiamo poi la campagna di propaganda dell'ISIS, CyberJihad, che recluta sempre più i suoi adepti attraverso i social network, quindi utilizzando il cyberspazio, lo stesso cyberspazio, in cui la Virtual Humint sa benissimo come muoversi, con lo stesso approccio metodologico che la Humint mette in pratica nel mondo reale. [(https://www.agendadigitale.eu/sicurezza/servizi-segreti-e-politica-la-lezione-della-cia-e-limportanza-del-fattore-umano-nellera-digitale/).](https://www.agendadigitale.eu/sicurezza/servizi-segreti-e-politica-la-lezione-della-cia-e-limportanza-del-fattore-umano-nellera-digitale/)

CYBER
Think Tank
ASSINTEL

I bambini passano troppo tempo con i device! Tra studi, percentuali, punto di vista medico e riduzione del quoziente intellettivo

A cura di Massimiliano Brolli

I bambini di oggi interagiscono attivamente con le tecnologie digitali fin dall'età prescolare. Secondo un recente studio del servizio Yandex Plus, un bambino su due di età compresa tra 5 e 7 anni ha il proprio smartphone o tablet.

Lo studio di Yandex ha utilizzando un sondaggio online dove hanno partecipato 1.450 utenti Internet attivi, residenti in città con una popolazione di oltre 100mila persone con bambini dai 3 ai 12 anni.

L'indagine ha mostrato che l'84% dei bambini in età prescolare utilizza i device non più di due ore al giorno. Tuttavia, con l'avanzare dell'età, il tempo trascorso davanti allo schermo aumenta.

Alle elementari il tempo trascorso davanti allo schermo dei bambini inizia ad aumentare gradualmente: il 33% dei genitori osserva che i bambini tra i 7 e i 10 anni trascorrono dalle 3 alle 5 ore al giorno sullo smartphone. Un cambiamento notevole si osserva all'età di 11-12 anni, quando più della metà degli scolari inizia a utilizzare uno smartphone o un tablet fino ad arrivare al numero impressionante di 8 ore al giorno.

Tra i bambini dai 3 ai 12 anni, l'83% utilizza Internet tramite i propri device, principalmente smartphone e tablet. Per i bambini in età prescolare questa cifra ammonta a due terzi e sale a oltre il 90% quando inizia la scuola.

Secondo lo studio, l'81% dei genitori dei bambini di età compresa tra 11 e 12 anni permette loro di scegliere autonomamente cosa guardare o leggere su Internet. Tra i genitori di bambini in età prescolare dai 3 ai 6 anni, questa percentuale è del 56%.

Tuttavia, nonostante la libertà di scelta piuttosto ampia, l'88% dei genitori limita in qualche modo l'interazione dei propri figli con i device. Alcuni monitorano attivamente le attività online dei bambini, altri stabiliscono limiti di tempo per l'utilizzo dei dispositivi o chiedono ai bambini di interrompere la visualizzazione di contenuti inappropriati.

Una nota positiva è il crescente interesse per i contenuti educativi. Se tra i bambini in età prescolare solo il 25% è interessato ai video educativi, tra gli scolari nelle scuole primarie questa quota è già del 40% e tra i bambini di età compresa tra 11 e 12 anni – 47%.

Il punto di vista medico

Ne siamo tutti consapevoli e ci conviene lasciare i bambini di fonte ai device in quanto la "baby sitter" elettronica è un miracolo per avere più spazi e libertà. Ora andremo invece ad analizzare quello che dicono i medici relativamente al numero di ore che i bambini possano passare davanti al video di un tablet o di uno smartphone.

Recenti studi riportano una situazione completamente non conforme rispetto a quello che costantemente viviamo, dove nel dettaglio viene riportato:

- **Da 0 a 2 anni:** si raccomanda di evitare il più possibile gli schermi dei dispositivi elettronici;
- **Da 2 a 4 anni:** in età prescolare, le indicazioni dei medici vanno da 5-10 minuti al giorno fino ad arrivare ad un massimo di un'ora di fronte allo schermo. Un'ora di fronte allo schermo dovrebbe essere considerato come un "premio" in specifiche circostanze;
- **Da 4 a 8 anni:** nella scuola d'infanzia ed elementare, la situazione cambia ma non drasticamente. Si parla di 30 minuti al giorno per arrivare ad un limite massimo di 60 minuti al giorno;
- **Da 9 a 10 anni:** anche in questa fascia di età i medici consigliano 60 minuti come limite per arrivare a 100 minuti al giorno;
- **Dai 10 anni in poi:** da questa fascia di età in poi i medici consigliano che spetta al genitore concordare il tempo che i bambini/ragazzi possano stare di fronte allo schermo di un device. Considerando il trend da 0 a 10 anni proposto dai medici, quanto riportato da Yandex nel suo studio relativamente a 11-12 anni, il numero di 8 ore è fuori da qualsiasi controllo.

L'utilizzo dei device in modo ossessivo da parte dei più giovani porta a degli effetti negativi. Alcuni segni facilmente apprezzabili da parte di un genitore sono quando il bambino:

- trascura interessi, hobby e amicizie;
- ha forti sbalzi d'umore o reagisce in modo irritato;
- soffre di mancanza di sonno e stanchezza;
- soffre di problemi di concentrazione.

La riduzione del quoziente intellettivo nei bambini

Gli smartphone stanno abbassando il quoziente intellettivo (QI) dei bambini e riducono le loro capacità linguistiche. Questo secondo dei nuovi studi pubblicati recentemente. Uno studio multimilionario ha scoperto che passare solo due ore davanti a uno schermo ha un impatto negativo sui bambini.

Nuove ricerche indicano che risulta in atto una inversione di tendenza relativamente all'effetto Flynn. Evan Horowitz, direttore della ricerca e comunicazione presso FCLT Global, ha dichiarato: "Le persone stanno diventando più stupide. Non è un giudizio; è un fatto globale".

Recenti studi condotti in Danimarca, Norvegia e Regno Unito stanno riscontrando un notevole rallentamento – e persino un'inversione – del QI. In effetti il QI si è abbassato in questa incredibile era tecnologica. Un articolo di Science Alert del 2018 di Peter Dockrill rileva che "Un'analisi di circa 730.000 risultati di test del QI da parte di ricercatori del Centro Ragnar Frisch per la ricerca economica in Norvegia rivela che l'effetto Flynn ha raggiunto il suo picco per le persone nate durante la metà degli anni '70 ed è diminuito in modo significativo fino ad ora."

Una delle principali preoccupazioni è la mancanza di concentrazione, che non solo riduce l'intelligenza complessiva, ma influisce anche sulla nostra capacità di affrontare compiti complessi e sulla capacità di prendere decisioni affidabili. Tutto questo sta mettendo a dura prova la nostra "intelligenza emotiva", poiché diventiamo vittime della stanchezza decisionale dovuta a troppi stimoli tecnologici.

La tecnologia sta cambiando il nostro concetto di tempo e siamo noi a subire il peso maggiore di questi abusi. C'è l'aspettativa – creata da un ecosistema digitale tecnologico nato per fare soldi - di risolvere i problemi alla stessa velocità con cui si clicca sui siti web. Inoltre, la quantità di informazioni online può dare a chi lavora a un progetto un falso senso di competenza.

In modo preoccupante, un altro importante studio ha rilevato che i bambini che trascorrono più di sette ore al giorno con i device elettronici mostrano un assottigliamento prematuro della corteccia cerebrale, che in genere avviene più tardi nello sviluppo di un individuo.

Un assottigliamento della corteccia è stato collegato a livelli di QI più bassi. I risultati scioccanti sono i primi di un innovativo studio statunitense da 300.000.000 di dollari che seguirà lo sviluppo del cervello di 11.000 bambini nell'arco di un decennio.

Ovviamente, l'impatto completo dell'uso dei device a lungo termine non sarà noto finché questi bambini non raggiungeranno l'età adulta, ma le prime indicazioni non sono buone. Si tratta di un avvertimento per tutti i genitori che hanno perso la battaglia per prendere il controllo sull'uso del telefono dei propri figli.

E il concetto di supremazia tecnologica?

Mentre la Cina contempla l'istituzione di un "coprifuoco" sull'uso di Internet per i minori di 18 anni, limitando l'accesso dalle 22:00 alle 06:00 del mattino, il panorama dei social network e l'intero ecosistema pubblicitario filo-americano sembrano catalizzare l'attenzione, rischiando di influenzare pesantemente e di indebolire il nostro futuro.

Piattaforme come TikTok, Facebook e Instagram, che ormai hanno un impatto politico ed economico paragonabile al PIL di alcune nazioni, sollevano interrogativi rilevanti per il mondo di domani. Parliamo del futuro poiché, fino ad oggi, gli eventuali cambiamenti sembravano distanti e poco tangibili, considerando il beneficio dell'incessante flusso di entrate dei giganti tecnologici di oltre oceano.

Nel mondo digitale, sembra che ci troviamo in una sorta di "Uroboro" gigante, simbolo egizio di un serpente che morde la sua coda, creando un ciclo senza inizio né fine. L'innovazione e la creatività laterale scaturiscono dalla nostra intelligenza: come potremo alimentare questa innovazione se l'effetto Flynn sta invertendo la tendenza?

CYBER THINK TANK ASSINTEL

Prossimo Incontro:

24 gennaio

Ore 14:00

Sicurezza collaborativa per un mondo digitale più sicuro!

CYBER Think Tank ASSINTEL

Per info scrivi a:

segreteria@assintel.it

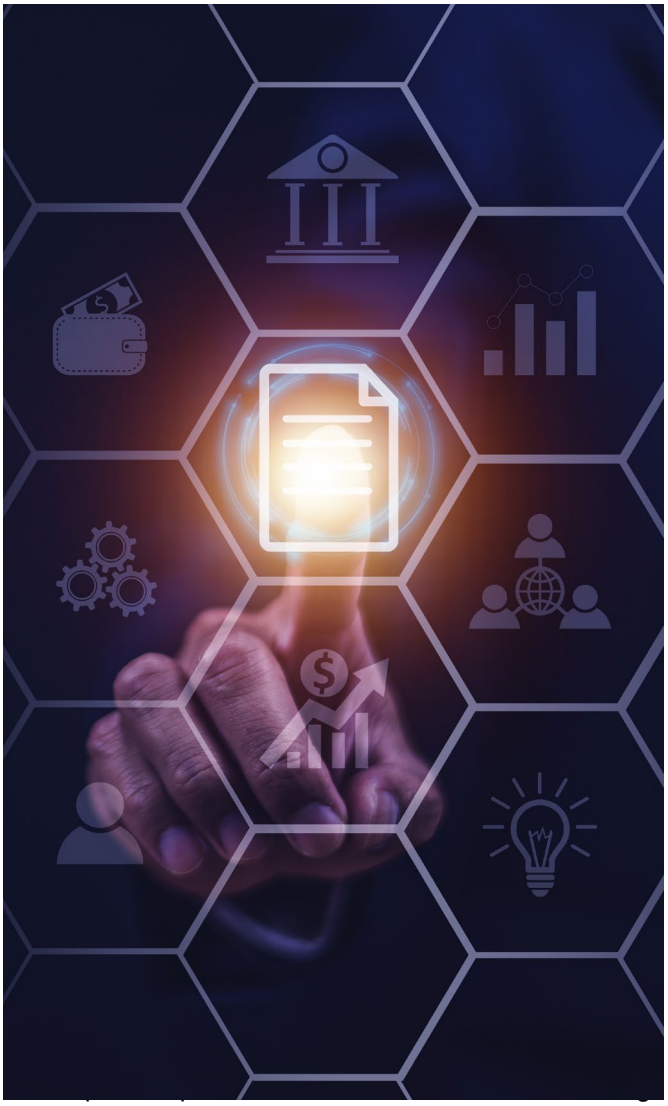
La Direttiva NIS2: cosa comporta la nuova direttiva europea sulla cybersicurezza nel 2024

A cura di Annita Larissa Sciacovelli

Il conflitto russo-ucraino ha portato sotto le luci dei riflettori i nuovi rischi per la cybersicurezza al cui contenimento si sono ampiamente dedicati euro-tecnocrati e giuristi a Bruxelles.

Nel dicembre 2022 l'Unione Europea (UE) ha adottato una serie di atti normativi, per obiettivi e per strumenti, necessari per far fronte a uno scenario di minacce (anche ibride) in continuo mutamento e che richiedono una vigilanza e un adattamento costanti.

Infatti, l'evoluzione dell'ecosistema digitale e la necessità di realizzare un alto e comune livello di sicurezza delle reti e dei sistemi informatici nei 27 Paesi europei, specie nei settori produttivi critici, ha spinto l'UE ad imporre un cambiamento di mindset per garantire il corretto funzionamento del Mercato Unico digitale.



attacchi, o meglio gli incidenti informatici, si traducano in costi economici e reputazionali molto rilevanti per le aziende. Questi costi potrebbero essere tali da essere riversati a carico del consumatore finale, oppure da incidere così gravemente sui conti delle aziende da costringerle a un ridimensionamento del personale o financo, in caso di perdite ingenti, a dichiarare il fallimento.

Da qui l'esigenza dell'Unione di ampliare il novero delle aziende tenute a rispettare le regole sulla cybersicurezza e, quindi, l'introduzione nella Direttiva NIS2 (UE 2022/2555) di nuove categorie di operatori dei servizi essenziali (OSE) e fornitori di servizi digitali (DSP), accanto agli operatori di servizi importanti. Tale direttiva, già entrata in vigore, dovrà essere resa esecutiva in Italia entro il 18 ottobre 2024, grazie ai decreti legislativi che il Parlamento adotterà a breve.

Le aziende che rientrano nel perimetro della NIS2 sono individuate sulla base del size-cap (di dimensioni medie, ex art. 2, par. 1, dell'allegato alla raccomandazione 2003/361/CE) e del settore produttivo (essenziale o importante). Ciò non esclude le imprese di piccole dimensioni se i loro servizi presentano particolari rischi per la sicurezza.

Si tratta di una incombenza impegnativa per le aziende che saranno inserite nel perimetro della Direttiva NIS2 ma che, come insegna l'esperienza oltreoceano, rappresenta l'unica soluzione per effettuare un controllo effettivo ed efficace delle loro criticità, maturità e postura nella cybersecurity.

Infatti, un recente rapporto del Parlamento europeo del 2023 evidenzia come l'esperienza liberista degli Stati Uniti, circa l'adesione volontaria delle aziende a schemi di postura e maturità della cybersecurity, non abbia portato a risultati soddisfacenti né in termini di investimenti né di sicurezza, specie riguardo alla gestione degli incidenti. Infatti, anche l'odierna strategia della cybersecurity della Casa Bianca è favorevole a introdurre regole e parametri obbligatori.

L'evoluzione delle minacce cibernetiche ha portato quindi l'UE a sostituire il primo strumento legislativo a livello dell'UE sulla cybersicurezza, la direttiva NIS (UE 2016/1148), redigendo una nuova versione basata su tre pilastri incardinati su: una policy di prevenzione degli incidenti informatici, un sistema di notifica degli incidenti e l'irrogazione di sanzioni.

Riguardo al primo punto, relativo alla policy di prevenzione degli incidenti informatici, è stato ampliato il novero dei settori che ricadono nell'ambito di applicazione della NIS 2 fra cui il settore dell'energia (che include nuove categorie di operatori come i partecipanti al mercato designati e gli operatori di punti di ricarica), i trasporti, le infrastrutture digitali (inclusi i cloud, i data center, gli ICT Service management e i digital providers), le banche, i mercati finanziari, la sanità (che include le attività di ricerca e produzione dei farmaci, di dispositivi medici e di dispositivi medico-diagnostici in vitro), la gestione dell'acqua potabile e delle acque reflue, la gestione dei rifiuti, le poste e di corriere, la pubblica amministrazione, lo spazio, il settore manifatturiero, quello chimico e quello dell'approvvigionamento alimentare, inclusa la produzione e la distribuzione, e le organizzazioni di ricerca.

Sugli stessi Operatori ricadranno obblighi importanti tra i quali, ex art. 20 della NIS2, quelli relativi agli organi di gestione stessi ai quali spetta l'approvazione di misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi della sicurezza delle reti e dei sistemi informativi per prevenire o ridurre al minimo l'impatto degli incidenti anche sui destinatari dei loro servizi.

Agli organi di governo dell'azienda spetta anche la supervisione dell'attuazione di tali misure ed essi potranno essere chiamati a rispondere delle violazioni delle norme testé indicate. L'obiettivo principale è quello di far sì che gli Operatori si dotino di sistemi di risk assessment e risk management - anche con riferimento alle aziende che fanno parte della catena di approvvigionamento (supply chain) - onde mitigare gli incidenti e garantire la business continuity. L'idea è quella di imporre una policy di gestione della cybersicurezza estesa anche agli anelli più deboli della catena produttiva e commerciale, tramite l'assunzione di responsabilità debitamente indicate in sede contrattuale, affinché l'outsourcing della produzione non si traduca nell'outsourcing del rischio.

Nel valutare la proporzionalità di tali misure, che rappresentano un elenco minimo di elementi di sicurezza di base e che devono essere debitamente documentate ai fini della accountability, si tiene conto del grado di esposizione dell'Operatore ai rischi, delle sue dimensioni e della probabilità che si verifichino incidenti e della loro gravità, compreso il loro impatto sociale ed economico (art. 21).

Il secondo pilatro della NIS2 è il sistema di notifica degli incidenti sui servizi forniti di cui devono essere informati il Computer Security Incident Response Team (CSIRT) e le Autorità competenti NIS, ossia i vari Ministeri competenti (art. 23).

Una volta verificatosi l'incidente, sull'Operatore ricade l'obbligo di notifica senza indebito ritardo sempreché si tratti di un incidente significativo, sarebbe a dire che abbia causato o sia in grado di causare una "grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato, o se "si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli" e se abbia effetti transnazionali.

Di regola, la notifica consta di una segnalazione rapida entro 24 ore dall'incidente, ed entro le 72 ore si deve procedere ad un aggiornamento con la valutazione della gravità e dell'impatto, nonché, ove disponibili, fornire gli indicatori di compromissione. Su richiesta di un CSIRT deve essere fornita una relazione intermedia sui pertinenti aggiornamenti della situazione. Entro un mese poi deve essere consegnata una relazione finale che indichi: una descrizione dettagliata dell'incidente, comprensiva della sua gravità e del suo impatto; il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente (che, però, viene raramente cercata e individuata); quali sono le misure di attenuazione adottate e in corso.

L'obiettivo principale è quello di far sì che gli Operatori si dotino di sistemi di risk assessment e risk management.

Le sanzioni pecuniarie amministrative, previste dall'art. 34, sono irrogate nel caso di mancato adempimento degli obblighi previsti. Per gli Operatori essenziali esse sono pari a un massimo di almeno dieci milioni di euro o a un massimo di almeno il 2 % del totale del fatturato mondiale annuo; mentre per gli Operatori importanti tali sanzioni sono pari a un massimo di sette milioni di euro o a un massimo di almeno l'1,4 % del totale del fatturato mondiale annuo.

Vale la pena di segnalare che la NIS2 ha introdotto anche altri obblighi a carico degli Operatori relativi, ad es., all'implementazione di misure di sicurezza obbligatorie o all'attuazione delle raccomandazioni di un audit.

Riguardo al terzo pilastro, quello relativo al controllo effettuato dagli Stati, esso si incentra su due regimi di vigilanza: uno ex ante ed ex post per gli Operatori essenziali, e uno solo ex post per gli Operatori importanti. Si tratta di due regimi di vigilanza che impongono al board dell'azienda interessata di dimostrare l'effettiva adozione delle misure di sicurezza e di segnalazione degli incidenti, pena la accountability del top management dell'azienda. Tale vigilanza può essere attivata anche dalle autorità statali, o da altri Operatori o dai cittadini stessi o su segnalazione dei media. L'art. 32 della NIS2 specifica poi in cosa consiste l'attività di vigilanza ad opera delle autorità statali relativa alle ispezioni in loco e alla vigilanza anche a distanza, all'audit sulla sicurezza periodici e mirati, effettuati da organismi indipendenti o dall'autorità competente, a scansioni di sicurezza, e a informazioni documentate sulle politiche di cyber security.

Va da sé l'importanza della zero trust architecture all'interno della azienda anche per controllare gli accessi interni, atteso che le minacce possono essere costituite anche da impiegati infedeli. A tal fine, è consigliabile segmentare le reti interne per evitare che i non addetti a lavori accedano a informazioni riservate, quali quelle relative alle banche dati dei clienti o al settore IP dell'azienda.

In conclusione, l'attuale forte dipendenza della società dalle infrastrutture digitali comporta che la sicurezza cibernetica delle aziende rappresenti per l'UE e per il Sistema Paese una sfida essenziale e imprescindibile. Tale sfida riguarda sì le vulnerabilità dei sistemi ma ancor più l'errore umano che resta una delle principali criticità aziendali. Peraltro, chi lavora con le aziende sa bene che la gestione dei rischi rappresenta un puzzle quotidiano che interessa i CDA e la governance delle stesse. In tale puzzle spesso manca il giusto riconoscimento del ruolo del CISO.

Non a caso, a partire dal 18 ottobre 2024 sarà fondamentale adottare le misure organizzative imposte dalla direttiva NIS 2 relative specificamente alla nomina di un responsabile della sicurezza informatica; alla definizione dei ruoli e delle responsabilità del personale coinvolto nella gestione degli incidenti e alla definizione delle procedure da seguire.

Tali scelte consentiranno il monitoraggio costantemente dei livelli di sicurezza informatica e l'aggiornamento delle risposte alle vulnerabilità, sia interne che esterne. Ovviamente, occorre evitare la sovrapposizione di ruoli e delle attività di analisi del rischio da parte delle molteplici figure professionali interessate (Auditor, DPO, Responsabili IT) favorendo un approccio integrato.

Occorrerà comunque attendere quanto sarà indicato dall'Agenzia dell'Unione europea per la cybersecurity nella seconda metà del 2024 circa l'individuazione di modelli e orientamenti di best practice sul tema.

Blockchain e Cybersecurity. Il binomio per assicurare la protezione dei dati

A cura di William Nonnis

Dopo l'emergenza pandemica del 2020 e le forti sollecitazioni provocate dall' Agenda Digitale europea del 2030 - che si prefigge di ottimizzare il potenziale tecnologico di tutti gli Stati membri, così da supportare e incentivare, grazie al mercato unico digitale, innovazione, progresso e crescita economica - molte delle nostre aziende hanno già reingegnerizzato, e molte altre si stanno preparando a farlo, i loro processi lavorativi, in chiave digitale.

La forte accelerazione, avvenuta negli ultimi anni, dell'utilizzo degli strumenti tecnologici su amplissima scala, se da un lato ha aperto trasversalmente la strada a larghe opportunità, impensabili prima, dall'altro ha indotto l'ingresso, nella società contemporanea, di nuovi e pericolosi rischi, dovuti ad un uso malevolo del digitale.

Poiché la corsa alla tecnologia da parte della popolazione media, a seguito della crisi sanitaria, è stata più veloce della consapevolezza di un suo corretto utilizzo, molti e di differenti tipologie, sono i danni subiti finora dalle numerosissime vittime del cybercrime, di chi cioè, per poca competenza o cattiva valutazione del rischio, ha subito truffe personali o è stato tramite inconsapevole di aggressioni hacker in aziende private e perfino pubbliche.

Ciò che si rende necessario, nel poco tempo che manca alla scadenza europea del 2030, nel nostro Paese, è l'acquisizione di una mentalità digitale, in tutto il tessuto sociale, cosicché sul doppio binario, sia professionale che personale, ciascun membro della comunità sia parte attiva e cosciente del profondo cambiamento in atto.

Essendo, infatti, la strumentazione digitale, sostegno ormai imprescindibile nelle attività quotidiane di ciascuno, tanto da essere considerata un'estensione stessa dell'uomo contemporaneo, il processo evolutivo che si sta svolgendo risulta essere irreversibile.

Per questo, una formazione tecnica, parallelamente ad una etica, per un uso sostenibile - oltreché responsabile - deve rappresentare un obiettivo prioritario, nell'ottica di accompagnare nel modo migliore tale cambiamento.

Infatti, nell'habitat digitale in cui ora siamo, la trasformazione che sta avvenendo, affinché sia fondamento di un benessere comune - condizione esclusiva da cui nasce il vero progresso - necessita di un nevralgico cambio di paradigma sociale, culturale ed economico, all'insegna della trasparenza e della fiducia sociale.

Un grande sostegno, in tal senso, ci viene offerto dalla stessa tecnologia, e nello specifico, dalla Blockchain, protocollo nato nel 2009 per permettere la veicolazione della prima criptovaluta, il Bitcoin. Riservata al solo settore economico per diverso tempo, tale tecnologia si è dimostrata essere fondamentale supporto nella notarizzazione dei dati (vale a dire un Timestamping, un processo grazie al quale è possibile apporre una marcatura temporale di data e ora dello scambio di beni o servizi, tra due o più soggetti) del tutto tracciabili, immutabili e quindi non manipolabili, tra due parti, senza più necessità di un'autorità terza superpartes, addetta alla verifica e al controllo della transazione.

Molti sono i settori professionali (da quello finanziario, a quello sanitario, alla supplychain) che possono giovarsi del libro mastro digitale rappresentato dalla Blockchain, poiché la veridicità dei dati in essa registrati, alza, e di molto, il livello qualitativo delle aziende che ne fanno uso, poiché il concetto di fiducia viene sostituito con successo da quello di verifica e di trasparenza, valore di fondamentale importanza nei circuiti in cui sia necessario monitorare tutta la filiera produttiva.

Infatti con la protezione data dalla crittografia e altri meccanismi presenti, con la capacità di resilienza dell'intera rete di fronte a un ipotetico attacco, nonché in virtù della scalabilità, la Blockchain può essere considerata la tecnologia a supporto della sicurezza infrastrutturale.

Grazie alla sua solidissima struttura, la Blockchain è in grado anche di resistere e contrastare l'esponenziale aggressione hacker degli ultimi tempi, contro aziende di qualunque tipologia, a scopo di estorsione o per strategie economiche. In virtù della decentralizzazione/distribuzione che, nella rete Blockchain, non utilizza grandi database per l'archiviazione dei dati, ma tutti i suoi nodi, sparsi in ogni angolo del mondo, è pressoché impossibile per gli hacker l'accesso alle informazioni. Accesso ulteriormente difficile da raggiungere per i malintenzionati digitali perché, fedele al suo principio di riservatezza, la Blockchain rende decifrabili i suoi dati solo alle persone autorizzate.

La Security by Design, in ambito di sicurezza, è l'approccio difensivo più idoneo alla resistenza ad attacchi hacker, perchè prevede in via di progettazione, e mai dopo come rimedio, uno specifico piano di difesa e resilienza, che nasce e si sviluppa parallelamente al sistema che si sta realizzando.

Nell'utilizzo della tecnologia Blockchain per Aziende pubbliche o private, la Security by Design è la conditio sine qua non per costruire un'architettura digitale robusta e affidabile, capace di trasmettere i dati da un nodo all'altro, garantendo l'affidabilità del contenuto e la blindatura dello stesso. Per assolvere l'assunto di protezione dei dati all'interno della tecnologia Blockchain, quando si progetta un sistema informatico per aziende, è necessaria una preventiva e buona analisi dei requisiti di sicurezza, specifici per ogni settore, costruita in base alle norme in vigore in materia di cybersicurezza.

Fondamentale è anche la realizzazione di smart contract impermeabili ad infiltrazioni malevole (se sviluppati in maniera corretta), così da poter garantire sempre il valore principe della Blockchain: la disintermediazione. E, una volta ultimato, il sistema di sicurezza informatico non deve dirsi concluso, perché un costante monitoraggio e aggiornamenti continui dei software possano essere efficaci scudi a nuove modalità di minacce. Ma, più ancora degli aspetti tecnici, è la gestione e la tutela delle chiavi pubbliche, e soprattutto private, da parte dei possessori, ad assicurare le informazioni dei valori transati, così come la responsabilità, la consapevolezza e una specifica formazione e sensibilizzazione al tema della sicurezza, sono e restano le variabili per la perfetta copertura dei dati da tutelare.

Gli attacchi informatici, abbiamo compreso, rappresentano nella società contemporanea un'enorme vulnerabilità per singoli cittadini, aziende e istituzioni pubbliche, con capacità tali da mettere sotto scacco un intero Stato, se colpito alle Infrastrutture Critiche, vale a dire a tutti quei servizi, risorse e processi di cui l'indisponibilità o il malfunzionamento determinano pesanti ricadute sulle essenziali attività del sistema Paese. Anche per questo, lo stato di salute di una Nazione passa attraverso il suo tipo di approccio, di conoscenza e competenza del digitale e attraverso la sua capacità di resistenza e resilienza da ogni tipo di strategia digitale aggressiva.

In tale ottica, il quinto dominio, o spazio cibernetico, è divenuto il luogo virtuale più ambito per dimostrare l'egemonia dei singoli Stati e un luogo non luogo dove, al posto dei campi di battaglia, si combattono guerre di potere.

Data la crucialità della tecnologia, ormai, in ogni ambito delle attività umane, è fin troppo evidente che occorre un profondo ripensamento, nel nostro Paese, della scuola, dei suoi programmi e delle sue ambizioni, che dovrebbero essere, da sempre, quelle di formare nel miglior modo possibile, le generazioni future.

Incentivare lo studio delle materie STEM, per formare professionisti abili nella gestione della tecnologia, è il migliore investimento che il Paese possa fare per mettersi al passo coi tempi e con l'Europa, che intanto corre verso il futuro. In questo moto di rivoluzione globale, molte sono le sfide aperte tra Uomo e Macchina, a cui si deve accompagnare, oltreché una solida preparazione ingegneristica, una profonda e larga riflessione, nonché una raffinata capacità critica per discernere le opportunità dai pericoli che la tecnologia pone costantemente all'uomo.

L'intelligenza artificiale, è proprio una di queste difficili sfide per l'uomo, perché capace di ottimizzare le sue attività, ma anche di renderlo strumento e non attore dell'innovazione.

Solo con una solida base culturale, che affonda le proprie radici nella tradizione del sapere assimilato e sedimentato nei secoli, si può comprendere e studiare il nuovo, traendone il meglio. In conclusione, il fattore umano non può e non deve prescindere nell'uso della tecnologia che, senza l'intelligenza umana non avrebbe modo di esistere, mentre l'impegno ad un utilizzo consapevole e responsabile dell'innovazione, deve farsi garanzia di un pensiero critico, mai assoggettato allo strapotere di una digitalizzazione cannibale e indifferenziata.

AI – Domande e risposte facili facili

L'AI per la creazione e manipolazione di testi, immagini e suoni

A cura di Gianpiero Cozzolino

Cosa può fare l'AI per i testi?

Abbiamo già citato in precedenza l'utilizzo dell'intelligenza artificiale nelle traduzioni automatiche ed istantanee, ma ovviamente ci sono e ci saranno molte altre applicazioni linguistiche che prenderanno forma.

Rispetto ai sistemi di traduzione automatica "tradizionali", l'intelligenza artificiale ha il grande vantaggio di riuscire ad usare il contesto per rendere la traduzione più precisa, raggiungendo un livello che può costituire una buona base in molti casi, ma comunque senza rappresentare ancora una reale alternativa dove serve accuratezza assoluta.

L'AI è anche in grado di effettuare con buoni risultati il lavoro di sintetizzare un testo lungo, o al contrario di sviluppare una traccia in un elaborato più lungo, fermo restando la necessità di una verifica "umana".

Uno dei rischi che questa tecnologia porta è l'abuso in ambito scolastico e universitario, rendendo ancora più evidente l'impoverimento delle capacità linguistiche delle nuove generazioni.

Cosa può fare l'AI per le immagini?

L'elaborazione avanzata delle immagini non è certo una novità, nel cinema la correzione digitale di colori o luminosità o gli effetti speciali sono apparsi negli anni '90 del secolo scorso. Tuttavia, in questo campo l'AI può rappresentare un ulteriore salto di qualità, soprattutto nel campo delle correzioni e del restauro di immagini sia statiche che in movimento, rendendo il risultato finale più naturale rispetto a quanto era possibile ottenere precedentemente.

Ma il campo in cui si va maggiormente affermando l'uso dell'AI è quello di generazione di immagini completamente nuove partendo da sommarie descrizioni, con risultati decisamente notevoli; il che comporta il rischio di avere immagini talmente realistiche da non poter essere distinte da quelle vere, "documentando" avvenimenti che non sono mai avvenuti. Clamorosi, in questo senso, sono i casi di "deep fake", ossia la sostituzione dei volti in un video, generando filmati in cui personaggi pubblici fanno dichiarazioni mai realmente nemmeno pensate, o addirittura sembrano comparire in film porno.

E comunque, anche in questo caso, la generazione di nuove opere visive comporta gli stessi problemi relativi al copyright che vedevamo prima per i testi.

Cosa può fare l'AI per i suoni?

Nel mondo dell'audio, possiamo trasportare gli stessi utilizzi e gli stessi rischi e problemi appena visti per le immagini: correzioni, effetti speciali, restauri, generazione di nuove musiche e suoni, nonché (novità degli ultimi tempi) la sintesi vocale, ossia la generazione del parlato, o persino del canto, con la voce di una specifica persona, permettendo la sostituzione della voce ai personaggi pubblici; esistono quindi già esempi di deep fake vocale, come per esempio far "cantare" ad un cantante morto da tempo l'ultimo successo appena uscito, con la sua voce e il suo stile.

Esiste anche la singolare e divertente applicazione del riconoscimento di un'opera musicale, partendo da un breve estratto o da un'esecuzione approssimata, come per esempio canticchiarla.

Ma quindi l'AI sostituirà gli artisti ed i produttori?

Effettivamente esistono anche tentativi di generazione di opere "artistiche", siano esse di testi (poesia o prosa, testi di canzoni, sceneggiature o dialoghi per film), di immagini (brevi film, quadri digitali), che di suoni (musica); ma in questi casi si pongono diversi problemi relativi ai dati utilizzati per l'addestramento: le opere così generate possono essere considerate dei plagi? E possono essere poi sottoposte a loro volta a copyright, e se sì, chi può essere considerato l'autore? E l'utilizzo di opere soggette a copyright nella base dati di addestramento, ne comporta la violazione? Queste domande non sono teoriche, le prime cause sono già state intentate negli Stati Uniti; il problema è che praticamente in tutto il mondo manca la legislazione sulla materia.

Che ne penso?

Vedo, nell'AI e nella possibilità di avere "energia circolare" (l'AI consuma e tanto!!), un nuovo approccio sulla generazione di contenuti, già oggi vediamo la generazione di contenuti per gruppi omogenei, uomini da 35 a 40 anni sposati che vivono a nord di Roma, oppure tutti quelli che nell'ultimo mese hanno ricercato, "finale Champions" su un motore di ricerca; fra pochissimo ogni pubblicità che vedremo sarà stata creata per noi, testi, musica ed immagini, per essere sempre più permeante, insomma convincente a comprare questo o quello.

Ma sarà anche un'occasione fantastica, di poter scrivere e pubblicare la commedia ironica che da sempre volevamo scrivere ma per motivi di tempo non abbiamo più fatto, sarà fantastico poter creare il film di azione che ci rappresenta, dove potremmo con le facce dei nostri amici compiere epiche avventure modello Jumanji, dove tutto è possibile; ed infine potremmo cantare bene anzi benissimo senza nessuna pecca o errore di intonazione, l'AutoTune sarà un residuato di qualcosa di vecchio, hahaha!!! sei proprio un vecchio algoritmo gli direbbe l'AI, bene per le nostre orecchie, ma il karaoke dal vivo senza AI sarà una vera sfida per i più coraggiosi.

Sulla proprietà intellettuale dovremmo fare un salto in avanti, ma molto in avanti, a mio parere se tutto fosse a disposizione di tutti non sarebbe una brutta cosa; pensate al mare, a una bella spiaggia, ad un fantastico tramonto, paghiamo forse i diritti al creatore dell'universo?

CYBER Think Tank ASSINTEL

WEBINAR

Il Cyber Risk in produzione

La security OT partendo dalla base: mettere in sicurezza macchine e impianti

Relatori

Carlo Wolter

Sergio Cazzaniga

Mario Testino

31 gennaio

12:00 - 13:00

Per info scrivi a:

segreteria@assintel.it

Perché il manufacturing è un Top Target per il cybercrime

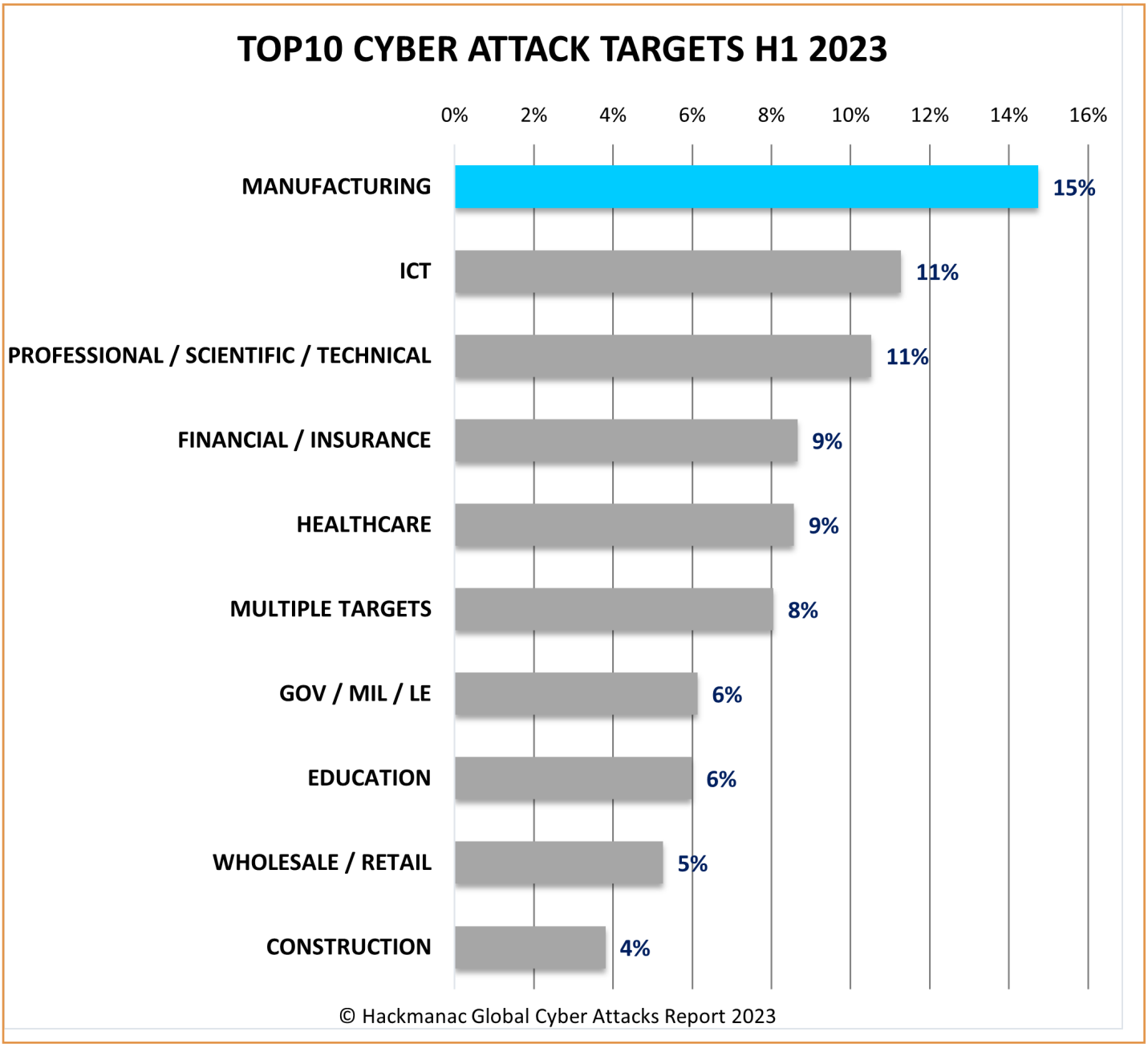
A cura di Sofia Scozzari

Negli ultimi due anni abbiamo visto crescere fortemente i cyber attacchi verso il settore del Manufacturing, fino a vederlo diventare il principale bersaglio del cybercrime nel primo semestre del 2023.

In base ai nostri dati, gli incidenti verso questo settore sono infatti passati dal 5% del totale nel 2022 al 15% nei primi sei mesi dell'anno, una tendenza certamente molto significativa.

Anche il recente rapporto "IBM Security X-Force Threat Intelligence 2023" rileva che, per il secondo anno consecutivo, il settore manifatturiero si conferma come il più colpito da attacchi informatici.

Questa tendenza mette in luce una crescente preoccupazione riguardo la capacità dell'industria di proteggere efficacemente le proprie risorse e le operazioni vitali.



Fattori che rendono il Manufacturing un bersaglio ambito dai criminali

Le minacce informatiche stanno diventando una problematica più che mai pressante, in conseguenza della crescente dipendenza dai sistemi IT per mantenere il funzionamento delle linee produttive.

Oltre ad essere aumentata la superficie di attacco complessiva, i cyber criminali, servendosi di tecniche sempre più sofisticate e perfezionate, riescono a compromettere i sistemi delle vittime con maggiore efficacia, mirando ad interrompere i processi produttivi in modo da amplificare significativamente il loro impatto, principalmente (ma non solo) con finalità estorsive.

Perché l'industria manifatturiera rimane un bersaglio privilegiato per la criminalità informatica?

La risposta risiede in una serie di fattori chiave:

- Il Manufacturing ha una bassa tolleranza per i tempi di inattività: i cyber criminali sanno di poter approfittare della situazione e soprattutto che il tasso di successo delle loro estorsioni verso questo settore è molto alto. Purtroppo, molto spesso i produttori sotto attacco preferiscono pagare il riscatto, creando un circolo vizioso;
- È un obiettivo di alto valore: le aziende manifatturiere possiedono proprietà intellettuale di valore oltre che dati sensibili e questo le rende obiettivi lucrativi per i criminali informatici anche per finalità di sottrazione di progetti, tecniche e informazioni su processi produttivi;
- Gli aspetti di sicurezza informatica non sono considerati una priorità: concentrandosi prevalentemente sul processo produttivo, che ne rappresenta il core business, le industrie tendono a non considerarsi potenziali vittime da parte del cyber crimine, spesso ignorando le dimensioni della loro superficie di attacco;
- La Supply Chain amplifica di rischi: la catena di fornitura è un ambito difficile da controllare e può esporre a notevoli rischi di cyber security. Per questa ragione un attacco riuscito verso il Manufacturing può causare danni enormi, che si ripercuotono a cascata non solo sugli impianti e sui processi propri, ma anche sulle organizzazioni della Supply Chain, andando ad ampliare la portata dell'incidente. Inoltre, si stima che più ampio è il numero di vittime coinvolte da un attacco, più è probabile che il bersaglio primario finisca per pagare il riscatto, il che rappresenta un ulteriore incentivo per gli attaccanti.
- È un settore che fa largo uso di componenti smart e IoT: queste tipologie di dispositivi sono spesso inadeguati dal punto di vista della cyber security e questo aumenta i rischi di violazione della privacy o della protezione dei dati.

Principali minacce per il Manufacturing

Il primo passo per mitigare questi rischi è comprendere le principali tipologie di minacce a cui i produttori sono maggiormente esposti:

- Ransomware ed estorsioni informatiche: I ransomware sono attualmente la principale minaccia cyber. L'obiettivo dei cyber criminali è bloccare i sistemi cifrando sistemi e dati critici della vittima, andando a causare ritardi nella produzione e perdite finanziarie per l'azienda, in modo che la loro richiesta di riscatto abbia più probabilità di essere accolta.
- Furto di proprietà intellettuale: I produttori investono molto in ricerca e sviluppo e i criminali, che ne sono consapevoli, prendono di mira la proprietà intellettuale di valore, i dati sensibili, le informazioni sui progetti e i processi di produzione.
- Attacchi alla/dalla supply chain: Le catena di fornitura può causare l'introduzione di malware, vulnerabilità o componenti compromessi nei processi di produzione, causando l'interruzione delle operazioni, oppure

un attacco subito può propagarsi alle organizzazioni della propria supply chain, creando danni di natura legale, economica e reputazionale.

- Negligenza di dipendenti o collaboratori: I dipendenti non consapevoli dei rischi e delle minacce informatiche attuali o non istruiti in maniera adeguata sulle pratiche di sicurezza informatica dell'azienda possono involontariamente facilitare il successo degli attacchi informatici. L'impreparazione del fattore umano rappresenta un elemento assolutamente critico, ampiamente sfruttato dai criminali.

Come incrementare la Cyber Security nel Manufacturing

Per migliorare le strategie di difesa del settore e difendersi in modo efficace dai crescenti assalti del cybercrime è necessario un approccio multidisciplinare.

a) Valutare correttamente il Rischio informatico

Il processo di Risk Assessment deve includere l'identificazione delle vulnerabilità, la valutazione dei potenziali rischi sia per le operazioni di produzione che per quelle corporate, in particolare in caso di attacco informatico e la chiara valutazione del valore degli asset dell'azienda (dati, processi e sistemi critici).

b) Implementare solide misure di Cyber Security

Investire in infrastrutture e processi di cybersecurity adeguati è a questo punto un imperativo. Allo stesso tempo è necessario stabilire e rinforzare le policy di sicurezza che si occupino del controllo degli accessi, della protezione dei dati e dei sistemi, e della risposta agli incidenti informatici, anche considerando che il fatto tempo è il principale moltiplicatore di danno in questi contesti.

c) Security By Design

Progettare tenendo conto degli aspetti di Cyber Security è un processo meno dispendioso, sia in termini di tempo che economici, dell'implementazione di soluzioni a posteriori, e risulta più efficace.

d) Non dimenticare la Supply Chain

Pur avendo adeguato le misure di sicurezza dell'azienda, la Supply Chain può rivelarsi un punto di ingresso per le minacce cyber. Valutare e migliorare le pratiche di sicurezza informatica di fornitori e partner riduce il rischio che non si introducano in azienda vulnerabilità dovute alla catena di fornitura. Anche gli aspetti legali e contrattuali devono essere indirizzati correttamente per contribuire a mitigare i rischi residui.

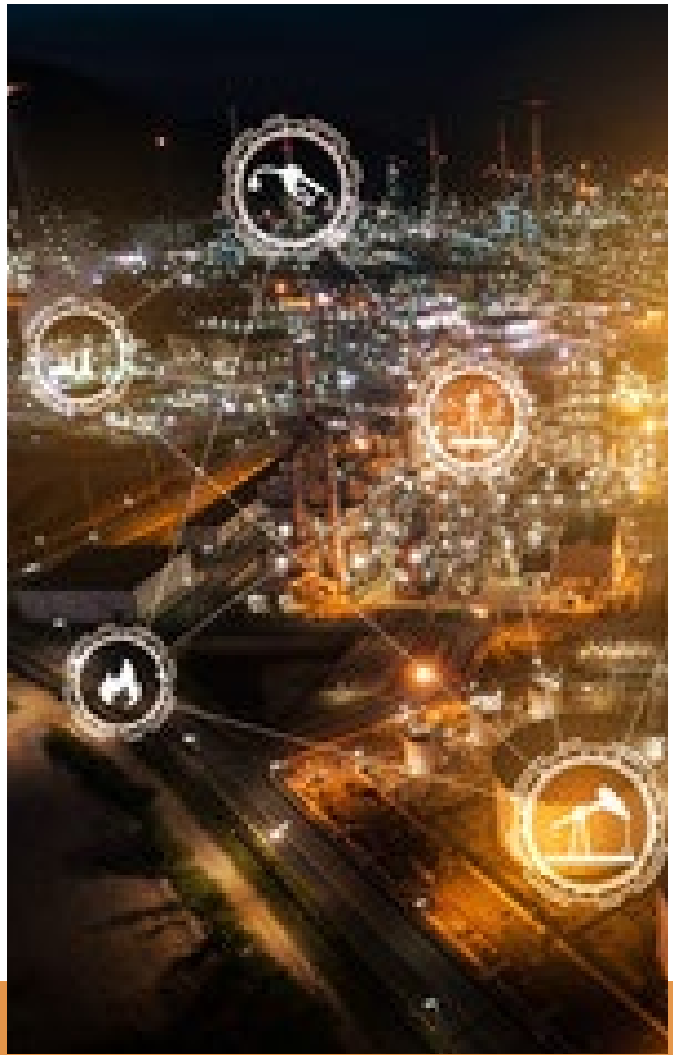
e) Formazione e sensibilizzazione dei dipendenti

È necessario formare regolarmente e sensibilizzare dipendenti e collaboratori per educarli sull'importanza della sicurezza informatica e su come identificare e rispondere alle minacce cyber nell'ambito delle policy aziendali.

f) Rimanere informati sulle minacce

Tenersi al passo con l'evoluzione delle minacce e delle tendenze in materia di sicurezza informatica rappresenta un grande vantaggio quando si tratta di ottimizzare la propria strategia di Cyber Security. A questo proposito è utile l'iscrizione ai feed di intelligence sulle minacce e la collaborazione con i colleghi del settore per condividere informazioni sulle minacce emergenti e sulle più adeguate misure di sicurezza.

Considerando che il Manufacturing, come si evince dai dati più recenti, è diventato un bersaglio facile e redditizio per il cyber crimine, l'unica soluzione è aumentare la resilienza, sia delle singole organizzazioni che del settore nel suo complesso, rendendolo meno appetibile, come è già avvenuto in altri ambiti, più maturi da questo punto di vista, quali ad esempio quello bancario. Osservando le tendenze in atto, raccomandiamo di affrontare e gestire questi rischi al più presto.



La sicurezza delle terze parti

L'attuale panorama normativo è adeguato e sostenibile?

A cura di Gabriele Faggioli

Non passa giorno e convegno senza che si parli delle terze parti come di un elemento di insicurezza.

Le statistiche (e le cronache ne sono testimoni) ci dicono che troppo spesso le terze parti sono il punto di ingresso da cui i criminali entrano per sferrare un attacco.

Come si vede dalla figura che segue nel 2021 l'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano ha pubblicato una survey da cui si rileva che su 151 grandi imprese intervistate il 24% aveva dichiarato di aver subito negli ultimi 12 mesi (quindi nel corso del 2020) un incidente di sicurezza legato alle terze parti.

Se da un lato quindi le terze parti possono essere considerate, in taluni casi, un fattore di insicurezza, è pur vero che gli investimenti che possono porre in essere, se parliamo di player primari, sono esponenziali rispetto a quanto può permettersi singolarmente qualunque azienda e pubblica amministrazione.

Per comprendere al meglio questa affermazione basti considerare i seguenti dati:

- Nel 2022 la spesa italiana in sicurezza informatica si è attestata (Fonte Osservatorio Cybersecurity & Data Protection del Politecnico di Milano) in poco meno di due miliardi di euro
- Nell'agosto 2021 Microsoft e Google hanno dichiarato al Presidente Biden che in 5 anni avrebbero speso 30 miliardi di dollari in cybersecurity (tra gli altri: https://www.wired.it/internet/web/2021/08/26/cybersecurity-biden-miliardi-microsoft-google-apple-ibm-amazon/.

Parliamo di cinque anni in cui, ogni anno, due aziende per quanto immense spenderanno, complessivamente, tre volte ciò che spende tutta l'Italia!

Davanti a questi numeri bisogna chiedersi a chi possa convenire restare su infrastrutture e applicazioni gestite internamente (per quanto magari oggetto di outsourcing), a rischio costante di obsolescenza, senza possibilità di investimenti ripetitivi e massicci, senza capacità di pianificazione, senza conoscenza di quanto costerà manutenere e difendere un complesso di tecnologie,

una superficie di attacco, sempre più ampie e sempre più costose, sempre più insicure, aperte, soggette a continue necessità di upgrade tecnologico e funzionale per restare competitive ma comunque soggette a continue vulnerabilità.

In un contesto di questo tipo, il legislatore chiede ripetutamente che ogni impresa e pubblica amministrazione che intenda fruire di terze parti analizzi il livello di compliance e di cybersecurity dei propri fornitori.

Per fare due esempi:

- in applicazione del GDPR i clienti devono valutare se il livello di sicurezza del fornitore con cui intendono contrattualizzare la collaborazione è adeguato o meno
- la normativa bancaria (e in particolare la regolamentazione EBA in materia di esternalizzazioni e il Regolamento DORA) prevede fra l'altro che:

  i. nella fase precontrattuale il cliente valuti i rischi ed effettui la due diligence del fornitore;

  ii. prima di stipulare un accordo contrattuale per l'utilizzo di servizi ICT le entità finanziarie devono identificare e valutare tutti i rischi pertinenti relativi all'accordo contrattuale;

  iii. nell'effettuare la valutazione dei rischi prima dell'esternalizzazione e durante il monitoraggio continuo della performance del fornitore di servizi, gli enti e gli istituti di pagamento devono: definire e stabilire un adeguato livello di protezione della riservatezza dei dati, di continuità delle attività esternalizzate nonché di integrità e tracciabilità dei dati e dei sistemi nell'ambito della prevista esternalizzazione.

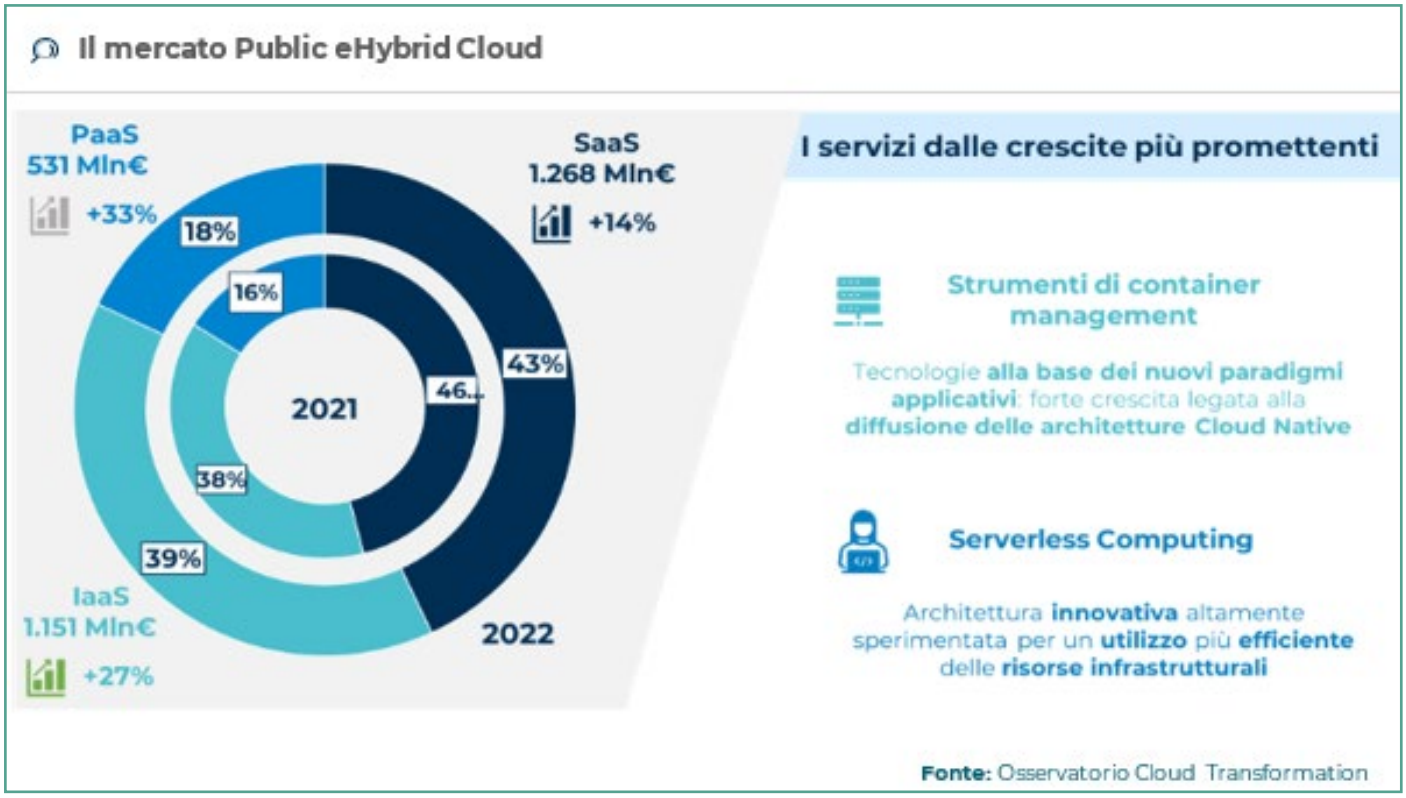
Come si può agevolmente constatare, di fatto, si chiede a tutti i clienti di valutare il livello di sicurezza di ogni fornitore, di valutare se le sue misure di sicurezza sono adeguate e poi di tenere costantemente monitorato durante la durata del contratto il fornitore stesso.

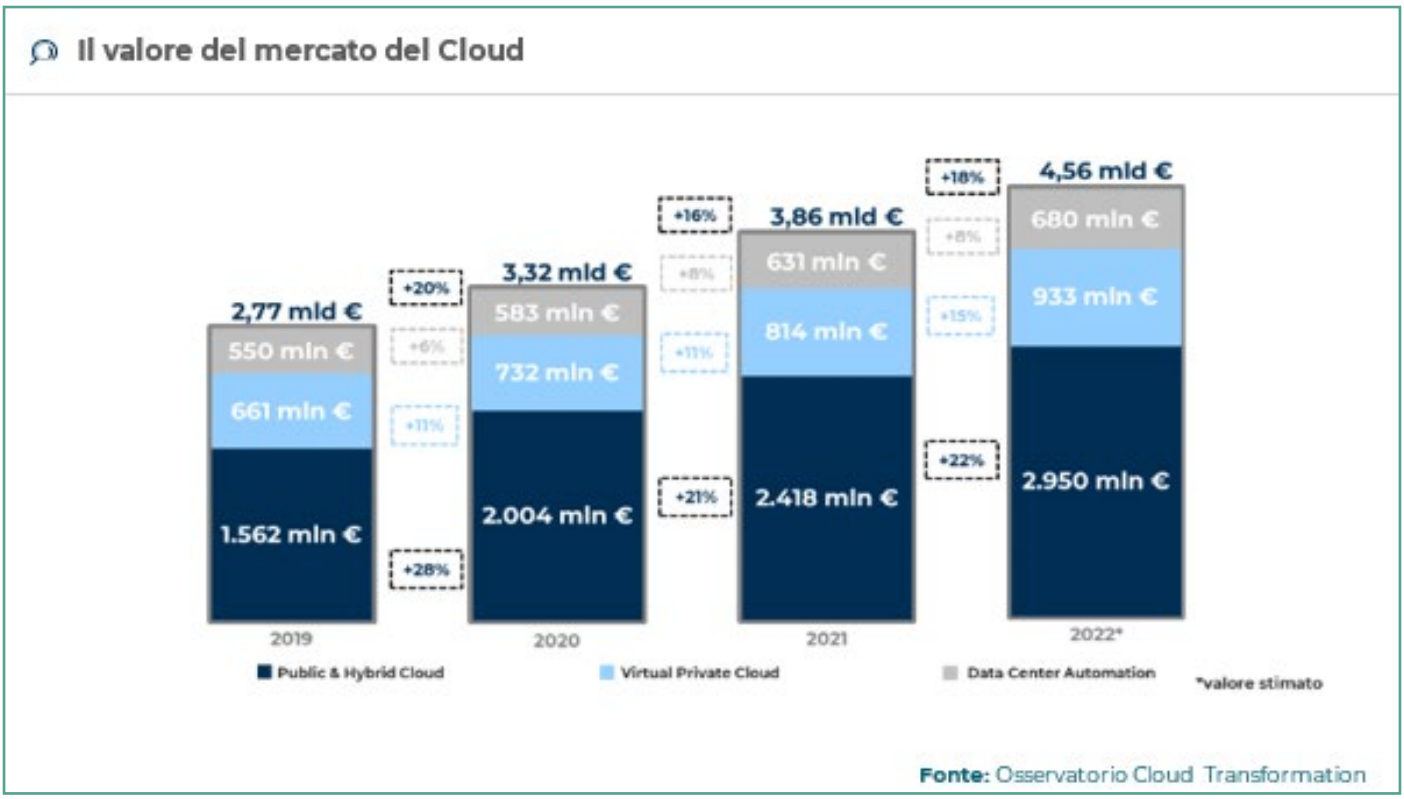
È (ancora) sensato come approccio?

Diamo uno sguardo al mercato italiano del cloud computing per provare a dare una risposta.

Nella figura che segue possiamo vedere come i servizi infrastrutturali sono cresciuti nel 22 rispetto al 21 del 27% mentre i servizi SaaS del 14%. Addirittura maggiore (seppur con una fetta complessiva di fatturato minore) la crescita del platform as-a-service.

In tutta evidenza i servizi di cloud computing crescono enormemente, da anni, come si può constatare dalla figura che segue nella prossima pagina.





In questi dati è forse possibile trovare una risposta.

Il mercato sta andando, sia per l'interesse dei fornitori che per le esigenze dei clienti, verso un modello cloud first sempre più diffuso.

Questa traiettoria evolutiva porterà aziende e pubbliche amministrazioni di tutte le dimensioni a usare sempre di più servizi standardizzati, offerti in modelli fortemente scalabili e uniformi.

Interi settori di mercato useranno sempre più spessi i medesimi fornitori perché è presumibile che aumenti la concentrazione e quindi la convenienza di usare le stesse terze parti che potranno offrire sempre più servizi competitivi, tecnologicamente avanzati, funzionali e sicuri.

In questo scenario quale sarebbe il senso normativo di costringere tutti a valutare i medesimi servizi tutti uguali?

In attesa di una, auspicabile, evoluzione normativa (alcuni passi sono stati fatti come con il cybersecurity act ma siamo ben lungi da una modifica sostanziale del panorama normativo) occorre fare i conti con gli obblighi attuali.

In questa ottica è utile che i fornitori che mirano ad avere (o che hanno) importanti fette di mercato, soprattutto se uniformi, siano in grado di mettere a disposizione documentazione standard completa, e di facile comprensione, ad illustrazione di tutte le politiche di compliance e di cybersecurity poste in essere permettendo ai clienti un facile accesso alle informazioni e quindi una accelerazione del percorso di valutazione (e di monitoraggio).

L'obiettivo non deve essere quello di diminuire l'attenzione dei clienti sull'importanza della sicurezza delle terze parti, deve invece essere quello di rafforzare la responsabilità dei fornitori con politiche di accentramento delle valutazioni e con diritto di accesso per tutti alle valutazioni stesse.

L'accesso alle tecnologie non dovrebbe comportare sforzi supplementari che ben pochi si possono permettere e che paradossalmente rischiano di creare sfiducia e disapplicazione delle norme per evidenti eccessi di costi indotti.

Bisogna mirare alla sicurezza reale anziché incentivare politiche di gestione aziendale che mirano prevalentemente ad evitare le sanzioni senza una reale sostanza pratica.

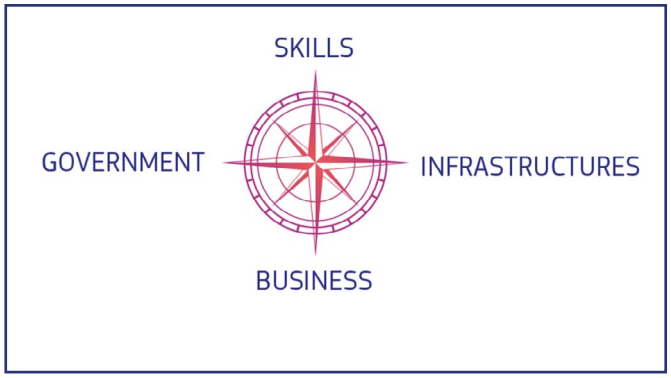
E il mercato, in tutta evidenza, sta ancora una volta anticipando il legislatore.

L’impegno dell’Europa nello sviluppo delle competenze ICT e la loro rilevanza in ambito cybersecurity

A cura di Valentina Sapuppo

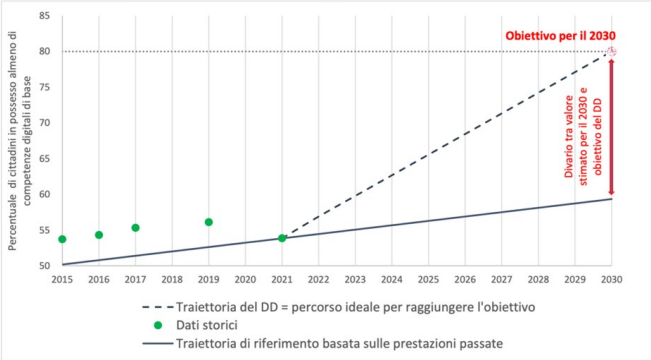
1. Europe’s Digital Decade is your Digital Decade

Il progetto per la costruzione della Decade Digitale Europea è stato presentato con la Comunicazione della Commissione che stabilisce le traiettorie previste a livello di Unione per gli obiettivi digitali (https://digital-strategy.ec.europa.eu/en/library/communication-establishing-union-level-projected-trajectories-digital-targets), quale guida per la trasformazione digitale dell’Europa a favore del cittadino. L’obiettivo principale perseguito è quello di dare più potere alle imprese e alle persone, per costruire un futuro più sostenibile per l’essere umano.



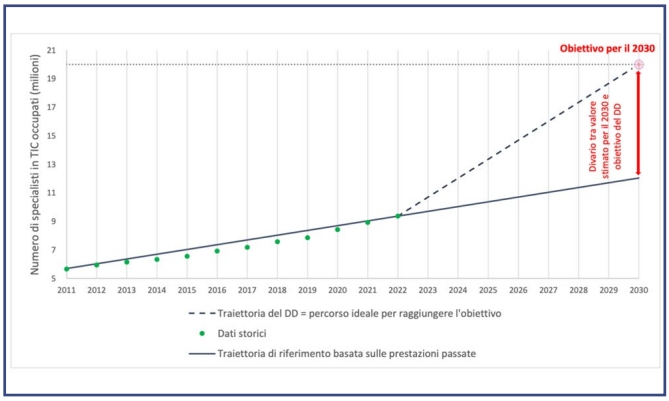
Sulla scorta della Bussola Digitale 2030, che ha delineato la via da seguire per lo sviluppo dell’economia e delle società digitalizzate, e della cooperazione strutturata tra Istituzioni europee e Stati membri, si continua a lavorare tutti insieme verso gli obiettivi digitali prefissati, costruendo tabelle di marcia strategiche verso il Path to the Digital Decade to deliver the EU’s digital transformation by 2030 (https://ec.europa.eu/commission/presscorner/detail/en/ip_21_4630), al fine di sviluppare competenze, infrastrutture e servizi, in linea con i principi digitali europei, rinforzando sempre di più il quadro di governance europeo.

Dalla Comunicazione della Commissione che stabilisce le tendenze previste a livello di Unione per gli obiettivi digitali pubblicata nel settembre 2023 (https://digital-strategy.ec.europa.eu/en/library/communication-establishing-union-level-projected-trajectories-digital-targets), che accompagna il primo Report della decade digitale europea e che descrive “lo scenario di ‘status quo’, basandosi su dati osservati in passato”, emerge che, nonostante l’impegno profuso dal 2021, è necessario ancora compiere uno sforzo importante per colmare il gap registrato nello sviluppo delle competenze digitali.

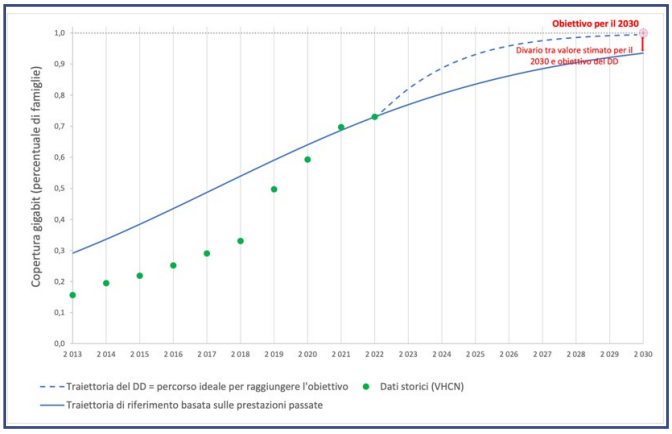


“Nonostante la crescita sostenuta degli ultimi 10 anni, nel 2022 gli specialisti in ICT erano 9,37 milioni, pari al 4,6 % del totale degli occupati e poco meno di 11 milioni al di sotto dell’obiettivo per il 2030. Negli ultimi due anni la tendenza del numero di specialisti in ICT ha registrato un’accelerazione, con una crescita media annua più elevata rispetto al decennio precedente (6,0 % tra il 2020 e il 2022 e 4,2 % tra il 2011 e il 2019). Per conseguire l’obiettivo del decennio digitale, la tendenza positiva degli ultimi due anni dovrebbe essere ulteriormente accelerata. Nel 2022 poco meno del 19% del totale degli specialisti occupati nel settore delle ICT era costituito da donne. Nell’ultimo decennio la percentuale di uomini è rimasta costantemente superiore di circa 60 punti percentuali alla percentuale di donne, quest’ultima compresa tra il

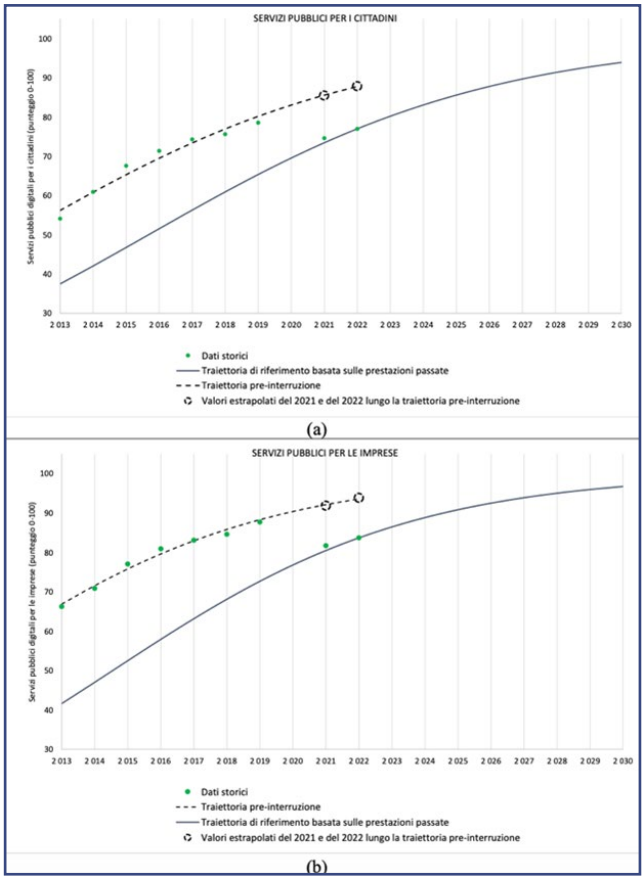
16% e il 19% e quella degli uomini tra l'81% e l'84%." (https://digital-strategy.ec.europa.eu/en/library/communication-establishing-union-level-projected-trajectories-digital-targets)



Ma dalla Comunicazione della Commissione emergono altre evidenze circa lo sviluppo delle infrastrutture digitali e della connettività. Infatti, "oltre al potenziamento delle reti di accesso alla fibra, saranno necessari ulteriori investimenti in hardware e software. […] Negli ultimi anni, sulla base dei dati disponibili, sembra sia stato registrato un aumento significativo della copertura 5G, dove il valore dell'UE per tale ICP ha raggiunto l'81,2% nel 2022. Alcuni Stati membri hanno persino comunicato valori prossimi al 100 % o che raggiungono il 100%." (https://digital-strategy.ec.europa.eu/en/library/communication-establishing-union-level-projected-trajectories-digital-targets)



Alla luce di ciò è chiaro che c'è ancora molto da fare anche per la digitalizzazione delle imprese, per le quali sono stati stanziati 24 miliardi di euro, e per la digitalizzazione dei servizi pubblici sia per i cittadini e per le imprese, in merito al quale si riscontra un grande divario tra i singoli Stati membri a causa del quale non siamo ancora arrivati a raggiungere l'obiettivo di fornire un sistema transfrontaliero migliore per il quale - si spera - il Regolamento eIDAS dia il supporto necessario.

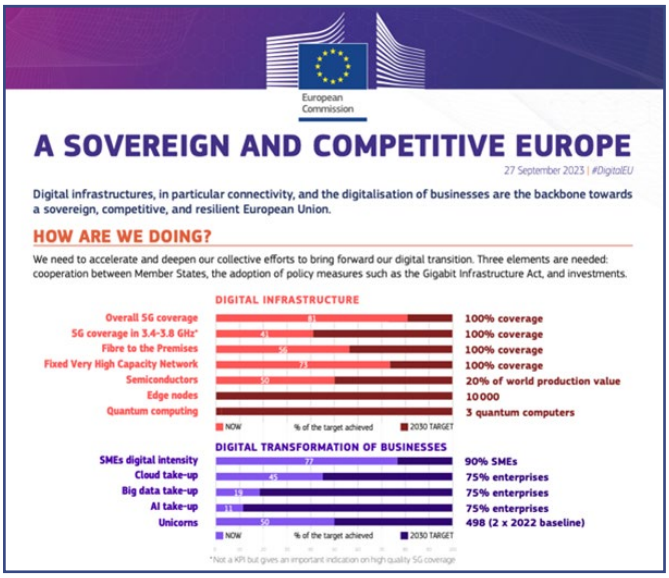


2. Il primo Report sullo stato del Decennio Digitale Europeo

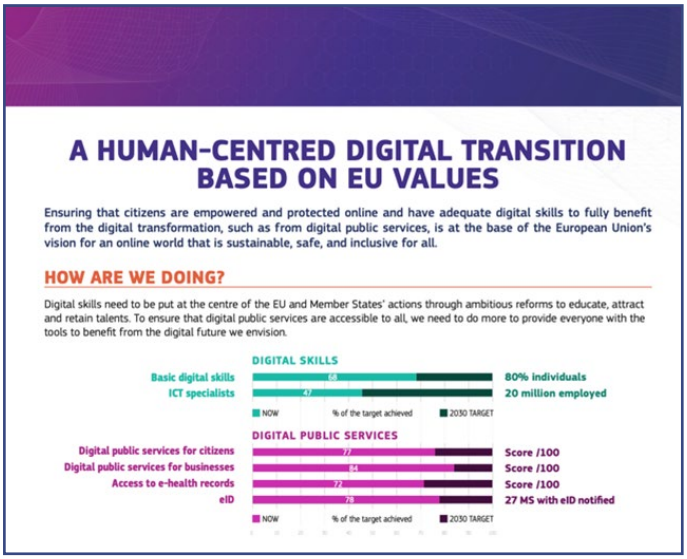
Il primo Report sullo stato del Decennio Digitale Europeo fa il punto sui progressi dell'UE verso una trasformazione digitale di successo come stabilito nel programma politico del decennio digitale 2030 e "fornisce uno sguardo completo sui progressi verso il raggiungimento della trasformazione digitale per potenziare un'UE più digitalmente sovrana, resiliente e competitiva. Comprende una valutazione delle prestazioni dell'UE verso gli obiettivi e gli obiettivi dell'Europa per il 2030 concentrandosi su quattro pilastri principali: competenze digitali, infrastrutture digitali, digitalizzazione delle imprese, compreso l'uso dell'intelligenza artificiale (AI) e digitalizzazione dei servizi pubblici. Comprende anche il monitoraggio della Dichiarazione europea sui diritti e i principi digitali, che riflette l'impegno dell'UE per una trasformazione digitale sicura, sicura e sostenibile, mettendo al centro le persone." (https://digital-strategy.ec.europa.eu/en/news/first-report-state-digital-decade-calls-collective-action-shape-digital-transition)

Come chiarito anche dalla Comunicazione della Commissione, è necessario spingere ancor di più sugli sforzi collettivi, per il tramite dell'accelerazione delle misure politiche e degli investimenti strutturali. Infatti, "il successo del Decennio digitale sarà fondamentale per la futura prosperità dell'UE. La realizzazione del programma del Decennio digitale dell'UE potrebbe sbloccare un valore economico di oltre 2,8 trilioni di euro, pari al 21%

dell'economia attuale dell'UE." (https://digital-strategy.ec.europa.eu/en/library/sovereign-and-competitive-europe-factsheet)



Inoltre, per quello che risulta dal primo Report sullo stato del Decennio Digitale Europeo, risulta di necessaria importanza "garantire che i cittadini siano responsabilizzati e protetti online e che dispongano di competenze digitali adeguate a beneficiare appieno della trasformazione digitale, ad esempio dei servizi pubblici digitali, è alla base della visione dell'Unione europea per un mondo online che sia sostenibile, sicuro e inclusivo per tutti. Le competenze digitali devono essere messe al centro delle azioni dell'UE e degli Stati membri attraverso riforme ambiziose per formare, attrarre e trattenere i talenti. Per garantire che i servizi pubblici digitali siano accessibili a tutti, dobbiamo fare di più per fornire a tutti gli strumenti per beneficiare del futuro digitale che immaginiamo." (https://digital-strategy.ec.europa.eu/en/library/sovereign-and-competitive-europe-factsheet)



Il Report dedica una grande attenzione verso le raccomandazioni per gli Stati membri, confezionati come singoli allegati, tenuto conto anche delle risultanze del monitoraggio aventi ad oggetto lo stato dell'arte dell'attuazione della Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, firmata il 15 dicembre 2022 dalla presidente della Commissione europea Ursula von der Leyen (https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7683), insieme alla presidente del Parlamento europeo Roberta Metsola e al primo ministro ceco Petr Fiala per la presidenza a rotazione del Consiglio. (https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade)

"L'Italia ha un potenziale digitale non sfruttato che può contribuire ulteriormente agli sforzi collettivi per raggiungere gli obiettivi del Decennio Digitale dell'UE. Date le dimensioni dell'economia italiana e della sua popolazione, gli sforzi attuali e futuri potranno contribuire in modo significativo. Negli ultimi anni, l'Italia ha compiuto progressi importanti in termini di infrastrutture, ma si colloca al di sotto della media europea per quanto riguarda le competenze e alcuni aspetti della digitalizzazione dei servizi pubblici. Le strategie adottate in materia di cloud, blockchain, IA e, recentemente, di cybersecurity, insieme alle riforme e agli investimenti nell'ambito del piano di Piano di ripresa e resilienza, creano un quadro solido per realizzare una trasformazione digitale sostenibile e inclusiva. L'Italia sta collaborando con gli altri Stati membri per esplorare la possibilità di creare un Consorzio europeo per le infrastrutture digitali - EDIC per la creazione dell'Accademia europea delle competenze di cybersecurity."

Tenuto conto del fatto che la trasformazione digitale colpisce ogni aspetto della vita delle persone, con la Dichiarazione europea sui diritti e i principi digitali per il decennio digitale del 2022 (https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7683) si realizza il primo passo verso un'Europa sovrana e competitiva, il cui cuore pulsante è l'essere umano. Ciò emerge anche da quanto dichiarato dalla presidente Ursula von der Leyen, e cioè che la Dichiarazione "riflette il nostro obiettivo condiviso di una trasformazione digitale che metta le persone al primo posto. I diritti proposti nella nostra Dichiarazione sono garantiti per tutti nell'UE, online come offline. E i principi digitali sanciti nella Dichiarazione ci guideranno nel nostro lavoro su tutte le nuove iniziative".

In questo contesto, l'European Cybersecurity Competence Centre and Network – ECCC (https://cybersecurity-centre.europa.eu/index_en), svolgerà un ruolo chiave nel conseguimento degli ambiziosi obiettivi in materia di cybersecuirity nei programmi Digital Europe e Horizon Europe. L'ECCC, infatti, che avrà sede a Bucarest (https://cybersecurity-centre.europa.eu/about-us_en), "mira ad aumentare le capacità e la competitività dell'Europa in materia di cybersicurezza, collaborando con una rete di centri nazionali di coordinamento – NCC. […] Questo ecosistema rafforzerà le capacità della comunità

tecnologica della cybersicurezza, proteggerà la nostra economia e la nostra società dagli attacchi informatici, manterrà l'eccellenza della ricerca e rafforzerà la competitività dell'industria dell'UE in questo settore."

3. ENISA: il quadro europeo delle competenze in materia di cybersecurity - ECSF

"La sicurezza dell'Unione europea non può essere garantita senza la sua risorsa più preziosa: i suoi cittadini. L'UE ha urgentemente bisogno di professionisti con capacità e competenze per prevenire, individuare, scoraggiare e difendere l'UE dagli attacchi informatici. Nel 2022, la carenza di professionisti della sicurezza informatica nell'UE era compresa tra 260.000 e 500.000, mentre il fabbisogno di forza lavoro della sicurezza informatica nell'UE era stimato a 883.000 professionisti. Inoltre, le donne rappresentano solo il 20% dei laureati in cybersicurezza e il 19% degli specialisti in tecnologie dell'informazione e della comunicazione." (https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy)

Nel 2022 sono stati presentati, durante la prima conferenza tenutasi in Grecia dal titolo Cybersecurity Skills - Building a Cybersecurity Workforce presentations (https://www.enisa.europa.eu/events/european-cybersecurity-skills-framework-ecsf-2022/cybersecurity-skills-building-a-cybersecurity-workforce-event-presentations), il European Cybersecurity Skills Framework Role Profiles (https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles) e il European Cybersecurity Skills Framework - ECSF - User Manual (https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf).

Quello che è importante, nel nostro contesto di analisi circa l'impegno dell'Europa nello sviluppo delle competenze ICT e della loro rilevanza nel mondo cybersecurity è che l'ECSF viene descritto quale "il punto di riferimento dell'UE per la definizione e la valutazione delle competenze rilevanti, come definito nella Cybersecurity Skills Academy, un'iniziativa politica europea" presentata dalla Commissione nell'aprile 2023 e "che mira a riunire le iniziative esistenti sulle competenze informatiche e a migliorarne il coordinamento, con l'obiettivo di colmare il divario di talenti nel campo della sicurezza informatica e di aumentare la competitività, la crescita e la resilienza dell'UE." (https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy - https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework)

Infatti, grazie all'ECSF - European Cybersecurity Skills Framework, il Ad-Hoc Working Group on the European Cybersecurity Skills Framework (2023-2025) (https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework/adhoc_wg_calls_skills_2023) di ENISA definisce i 12 profili professionali che descrivono i ruoli legati alla information security. L'obiettivo dell'ECSF è, soprattutto, quello di fornire "una comprensione dei ruoli, delle competenze, delle abilità e delle conoscenze pertinenti maggiormente richieste nella sicurezza informatica". (https://digital-strategy.ec.europa.eu/en/policies/digital-principles) e, in particolare (https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework):

- "l'uso della ECSF garantisce una terminologia comune e una comprensione condivisa tra la domanda (posto di lavoro, reclutamento) e l'offerta (qualificazione, formazione) di professionisti della cybersecurity in tutta l'UE.
- L'ECSF sostiene l'identificazione delle competenze critiche richieste dal punto di vista della forza lavoro. Consente ai fornitori di programmi di apprendimento di sostenere lo sviluppo di questo insieme critico di competenze e aiuta i decisori politici a sostenere iniziative mirate per mitigare le lacune identificate nelle competenze.
- Il quadro facilita la comprensione dei principali ruoli professionali della sicurezza informatica e delle competenze essenziali che richiedono, comprese le competenze trasversali, insieme agli aspetti legislativi (se presenti). In particolare, consente ai non esperti e ai dipartimenti delle risorse umane di comprendere i requisiti per la pianificazione delle risorse, il reclutamento e la pianificazione della carriera nel supportare la sicurezza informatica.

- Il quadro promuove l'armonizzazione nell'istruzione, nella formazione e nello sviluppo della forza lavoro sulla sicurezza informatica. Allo stesso tempo, questa lingua europea comune nel contesto delle competenze e dei ruoli di sicurezza informatica si collega bene con l'intero ambito professionale dell'ICT.
- La ECSF contribuisce a realizzare una protezione rafforzata contro gli attacchi informatici e a garantire la sicurezza dei sistemi IT nella società. Fornisce una struttura standard e consulenza su come implementare lo sviluppo delle capacità all'interno della forza lavoro europea impegnata nella sicurezza informatica."

Nonostante lo slancio propositivo, tuttavia, riteniamo importante riportare alcuni dubbi affrontati della presentazione dell'ECF nel febbraio 2023. "Rimangono però ancora alcune domande: La valutazione delle competenze aiuterà effettivamente l'occupabilità e la professionalizzazione? Le certificazioni professionali e l'accreditamento da parte degli enti di formazione contribuiscono a garantire un livello comune elevato di sicurezza informatica? Il riconoscimento reciproco dei certificati professionali migliorerà lo sviluppo professionale garantendo comunque elevati standard di qualità? Quale sarà il ruolo degli enti pubblici degli Stati membri nel coordinamento di questo panorama?" (https://www.enisa.europa.eu/events/webinar-assessing-cyber-skills-on-the-basis-of-the-ecsf)

Inoltre, ENISA si è preoccupata di sviluppare il Cybersecurity Higher Education Database "il più grande catalogo di programmi accademici sulla sicurezza informatica nei paesi dell'UE e dell'EFTA" (https://www.enisa.europa.eu/topics/education/cyberhead#/), in cui sono presenti diversi master e corsi di laurea e, tra questi ultimi, l'unico offerto online e gratuitamente è il Bachelor of Business Administration, Degree programme in Business Information Technology, Cyber Security dell'Università di scienze applicate della Finlandia (https://www.laurea.fi/en/degree_programmes/business-management-and-information-technology/bit-cyber-security/#courses) – per chi fosse interessato il prossimo application period è fissato dal 3 al 17 gennaio 2024.

Crediamo che il tema trattato in questo approfondimento possa essere di interesse per tutti gli addetti ai lavori, soprattutto in vista della necessità di 'forza lavoro' per il panorama europeo alla luce dei nuovi risvolti portati dagli emendamenti proposti dalla Commissione il 18 aprile 2023 in merito all'EU Cyber Security Act (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0208).

CYBER
Think Tank
ASSINTEL

Bibliografia e sitografia

1. https://ncses.nsf.gov/pubs/nsf23315/

2. https://www.osservatoriosocialis.it/2022/02/23/donne-stem-scienza-genere/

3. https://www.conibambini.org/wp-content/uploads/2022/01/STEM-una-sfida-per-lItalia.pdf

4. Aa. Vv., Guidelines 01/2023 on Article 37 Law Enforcement Directive, in European Data Protection Board, 2023.

5. Aa. Vv., Applicazione del GDPR ai casi transfrontalieri: EDPB e GEPD sulla proposta di regolamento, in Diritto Bancario, 22 settembre 2023.

6. Redazione Dimt, EDPB adotta linee guida sui trasferimenti di dati soggetti a adeguate garanzie ai sensi della Direttiva sulla Polizia e la Giustizia Penale, in Diritto, Mercato e Tecnologia, 29 settembre 2023.

7. Ruocco, Data Privacy Framework: arriva il via libera anche dell'EDPB, con alcune precisazioni, in Cybersecurity360, 21 luglio 2023.

CYBER MAGAZINE

Gennaio
2024

CYBER
Think Tank
ASSINTEL

Contattaci:

segreteria@assintel.it
www.assintel.it