CYBER MAGAZINE

CYBER Think Tank ASSINTEL

Settembre - Ottobre 2023

SPECIAL INTERVIEW ◆ SPECIAL INTERVIEW ◆ SPECIAL INTERVIEW ◆ SPECIAL INTERVIEW ◆ SPECIAL INTERVIEW ◆ SPECIAL INTERVIEW

Gianni Riotta

Giornalista, scrittore, conduttore televisivo, direttore del TG1 e del Sole 24 Ore

INTERVISTE SPECIALI

Mariarosaria Taddeo

Professoressa di Etica Digitale e Tecnologie della Difesa presso l'università di Oxford.

SPECIAL INTERVIEW ◆ SPECIAL INTERVIEW ◆ SPECIAL INTERVIEW ◆ SPECIAL INTERVIEW ◆ SPECIAL INTERVIEW ◆ SPECIAL INTERVIEW

Cyber Think Tank Assintel

Cyber Think Tank Assintel

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.

CYBER Think Tank ASSINTEL

Unisci le competenze per un futuro digitale sicuro!

Prossimo Incontro

15 novembre

Ore 14:30

Per info scrivi a: **segreteria@assintel.it**

COORDINATORE:
Pierguido Iezzi

COMITATO SCIENTIFICO:
Antonio Assandri, Gianpiero Cozzolino, Vittorio Orefice

REDAZIONE:
Federico Giberti, Melissa Keysomi, Daniela Grossi, Elisa Buonocore

CYBER THINK TANK ASSINTEL

INDICE

INTERVISTE SPECIALI

WEBINAR

Perché la PMI è un target dei Criminal Hacker?

11 Dicembre

12:00- 13:00

Relatori:

Sofia Scozzari

Cristiano Cafferata

Riccardo Modena

CYBER Think Tank ASSINTEL

Per info scrivi a:

segreteria@assintel.it

INDICE

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

Settembre - Ottobre 2023

Gentili lettori,

dopo la meritata pausa estiva, sono lieto di presentare l'ultimo numero del Cyber Magazine del Cyber Think Tank di Assintel.
Questa edizione presenta un'ampia gamma di articoli redatti da alcuni dei massimi esperti del settore, che esploreranno argomenti di grande rilevanza nel campo della cyber e della tecnologia digitale.
Con l'avvicinarsi dell'autunno, vi invitiamo a intraprendere un viaggio informativo che vi condurrà attraverso temi quali il Digital Operational Resilience Act (DORA), Intelligenza Artificiale, la sicurezza della catena di approvvigionamento e molto altro.
Questo numero offre un'opportunità unica per approfondire la complessità di questi argomenti e comprendere l'importanza di una solida strategia di sicurezza cyber.
Gli articoli presentati coprono una vasta gamma di temi; dalla governance dell'IA all'evoluzione del panorama regolamentare cyber, offrendo una panoramica completa delle sfide e delle opportunità che il mondo digitale ci presenta.
Siamo entusiasti di condividere con voi questa ricca selezione di articoli, nella speranza che possano offrirvi nuove prospettive e stimolare ulteriormente il vostro interesse per la cyber security e l'innovazione tecnologica.

Grazie per essere con noi in questo viaggio e buona lettura!

Pierguido Iezzi

IA: tra miti da sfatare e prospettive reali

Intervista alla Prof. Mariarosaria Taddeo a cura di Federico Giberti

Mariarosaria Taddeo è Professoressa di Etica Digitale e Tecnologie della Difesa presso l'università di Oxford. È anche Direttrice del Programma del Dottorato in Informazione, Comunicazione e Scienze Sociali presso l'Oxford Internet Institute e Fellow di Etica presso l'Alan Turing Institute. Il suo lavoro recente si concentra sull'etica e la governance delle tecnologie digitali, e spazia dalla progettazione di misure di governance per sfruttare l'intelligenza artificiale (IA) fino a affrontare le sfide etiche legate all'uso delle tecnologie di difesa nella cyber, all'etica della sicurezza informatica e alla governance dei conflitti cibernetici. Ha pubblicato oltre 150 articoli in questa area, concentrandosi su argomenti come tecnologie digitali affidabili, governance dell'innovazione digitale, governance etica dell'IA per la difesa nazionale, etica della sicurezza informatica. Il suo lavoro è stato pubblicato in importanti riviste come Nature, Nature Machine Intelligence, Science e Science Robotics.

L'Intelligenza Artificiale (IA) è una forza motrice per l'innovazione tecnologica e il progresso economico. Argomento padroneggiato da pochi sino al recente passato, grazie all'approdo di *large language model* fruibili liberamente da tutti in rete, questa tecnologia è da mesi oramai entrata nel flusso del *main stream*. Naturalmente attirando opinioni divergenti, fautori e censori e una lunga scia di speculazioni e misinformazione.

Per dirimere alcune delle aree più grige e discusse di questa tecnologia, ne abbiamo parlato con Mariarosaria Taddeo, *Professor of Digital Ethics and Defence Technologies presso l'Università di Oxford.*

Professoressa Taddeo, nell'attuale dibattito sull'Intelligenza Artificiale ci sono preoccupazioni riguardo alla sua potenziale minaccia esistenziale per l'umanità; è il classico allarmismo dettato dalla paura del nuovo che avanza?

"Non è una minaccia, almeno non nei termini in cui è stata descritta da alcuni. La paura che l'Intelligenza Artificiale possa diventare intelligente come un essere vivente è infondata, sconfina nella fantascienza.

Questo non vuol dire che l'IA non ponga dei rischi concreti, che è importante identificare tempestivamente per cercare di limitare. Focalizzarsi sui cosìdetti rischi esistenziali non solo è una distrazione inutile che rischia di rallentare gli sforzi per capire questi rischi, ma ha anche l'effetto di polarizzare il dibattito su usi e governance dell'IA. L'IA, con il digitale, è la cifra delle nostre società. Un dibattito pubblico informato, non polarizzato, è cruciale per arrivare a definire misure di governance che rispecchino i nostri valori.

Nel periodo di massimo fervore mediatico sull'Intelligenza Artificiale, è uscito uno studio di Goldman Sachs che annunciava – entro il 2030 – la scomparsa di 300 milioni di posti di lavoro a causa della tecnologia IA, è realistico fare queste previsioni?

La valutazione del numero di posti di lavoro che saranno persi o guadagnati a causa dell'IA richiede una modellizzazione estremamente accurata di un fenomeno complesso.

Foto: https://rosariataddeo.net/

Nel migliore dei casi le stime sono approssimative. Il tema del lavoro è senz'altro importante, ma per capire implicazioni e veridicità di stime come quella che mi ha citato possiamo attingere ad un altro esempio che ha fatto molto discutere: i veicoli a guida autonoma, anch'essi al centro di molte discussioni. Una delle professioni che si riteneva più a rischio in US nello scorso decennio per via dell'IA era quella degli autotrasportatori. Si credeva ad un certo punto che si sarebbero persi tra i 2 e 3 milioni di posti di lavoro in questo settore in US. Un'analisi relativamente recente (pubblicata su *Harvard Business Review*) mostra che i numeri sono molto più contenuti se consideriamo in dettaglio questa professione. Un autista svolge molte altre mansioni oltre a guidare un veicolo. Si occupa anche del carico e dello scarico della merce, firma i documenti necessari e gestisce varie attività correlate. In altre parole, il lavoro di un autista non può essere ridotto ad un singolo compito, guidare un camion, e coinvolge una serie di compiti complessi che le macchine al momento non possono eseguire. Quindi, le previsioni che indicano la scomparsa di questi posti di lavoro devono essere prese con cautela. È importante notare che, sebbene l'IA possa cambiare il modo in cui svolgiamo alcune attività professionali, non significa necessariamente la completa sostituzione degli esseri umani. Potrebbe comportare la trasformazione delle attività professionali, ma non necessariamente la loro estinzione. Quindi, mentre è importante considerare il potenziale impatto dell'IA sul lavoro, non dovremmo adottare un approccio allarmistico. La realtà è molto più complessa di quanto possano suggerire stime più o meno precise, e i meccanismi coinvolti sono difficili da modellare con precisione.

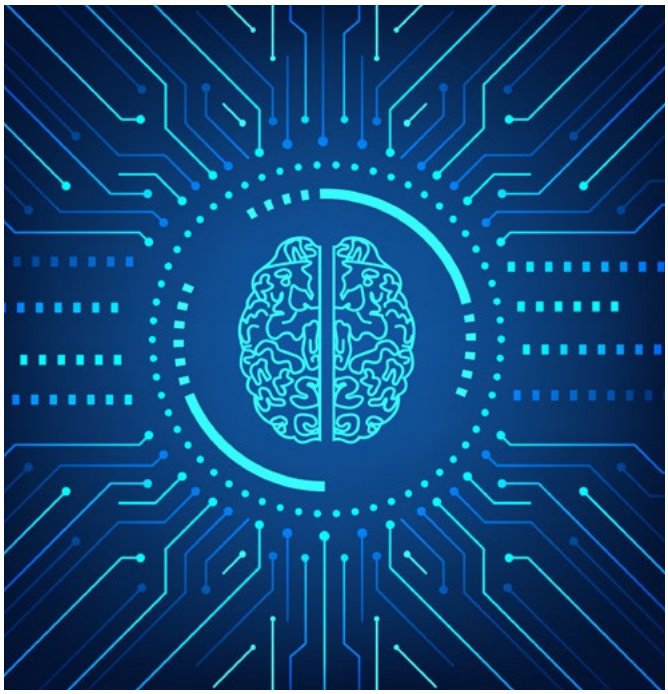
Altro tema "caldo" è stato quello della possibilità concreta che gli esseri umani non rivestano più il ruolo del "decisore" nei processi grazie all'introduzione di algoritmi più efficaci. Come valuta questo timore?

Qui dobbiamo fare una precisazione, utilizziamo già l'IA per prendere molte decisioni al posto nostro. Per esempio, pensiamo agli algoritmi che contribuiscono a definire i risultati di ricerche su Internet o alle decisioni di assunzione prese con l'aiuto dell'IA. Un esempio noto è quello di Amazon, che utilizzava un sistema IA per il processo di selezione del personale e ha scoperto che l'IA tendeva a discriminare le donne a favore degli uomini, suscitando preoccupazione pubblica.

La paura che l'Intelligenza Artificiale possa diventare intelligente come un essere vivente è infondata, sconfina nella fantascienza.

ve a compiti specifici e limitati. Nel caso dell'assunzione, l'IA potrebbe essere coinvolta solo in alcune fasi del processo, ma non sovrintende a tutto il processo di selezione o gestisce tutte le funzioni. A mio avviso le questioni sono due; quali compiti deleghiamo alle macchine e che processi (p.e. di audit) abbiamo per capire quando e perché l'uso dell'IA nei processi decisionali porta a risultati indesiderati.

La sfida, attualmente, sta nel comprendere come le attività professionali potrebbero evolversi in futuro. Dovremo adattare la nostra formazione per preparare i professionisti a lavorare in un ambiente in cui l'IA è un membro del gruppo di lavoro. Diventa quindi importante che professionisti, in diversi ambiti, capiscano come utilizzare l'IA in modo etico e responsabile, magari attraverso delle certificazioni. Oltretutto dovremo affrontare anche le questioni relative alla discriminazione e alla sicurezza dell'IA, poiché le macchine possono essere vulnerabili agli attacchi o produrre risultati non etici se non gestite correttamente. La sfida è trovare un equilibrio tra le capacità delle macchine e le competenze umane, in modo che gli esseri umani possano rimanere al controllo e contribuire in modo produttivo, mantenendo un ruolo centrale nei processi decisionali.



Abbiamo parlato in apertura del "circus" mediatico che ha accompagnato un po' tutto il dibattito sull'IA. Però al momento, apparentemente, sembra che i player siano principalmente privati, è il momento che le istituzioni prendano una posizione?

È una questione molto interessante perché c'è bisogno di una governance per allineare la progettazione, sviluppo e uso di sistemi IA con i valori delle nostre società. Questo è un compito che spetta alle istituzioni. La governance dell'IA deve avere l'obbiettivo di creare un ambiente favorevole all'innovazione - fornire incentivi, finan-

ziamenti, e supportare l'ecosistema di startup attraverso incubatori e altre iniziative, definire misure per trattenere i talenti – ma deve anche definire criteri per bilanciare interessi legittimi ma opposti. Consideriamo per esempio il caso dell'*IA generative*, ChatGPT in particolare: da un lato abbiamo un forte fattore di innovazione, un sistema IA che potrebbe aumentare la produttività di tutti noi, dall'altro abbiamo la necessità di proteggere il *copyright* dei dati usati per allenare questo modello. Oppure, da un lato un tecnologia che ci permette di scrivere testi molto velocemente, dall'altro il rischio che ci inondi di disinformazione mettendo a rischio il dibattito pubblico e i processi democratici (si pensi all'impatto delle cosiddette *fake news* sul referendum per la Brexit). È innegabile il ruolo del legislatore in questo processo come garante dello sviluppo etico e sicuro dell'IA. Le istituzioni pubbliche hanno il dovere di definire le regole che disciplinano cosa e come può essere sviluppato, come l'IA può essere utilizzato. Per esempio, consideriamo l'importante impatto ambientale dell'IA, soprattutto dei modelli generativi; è essenziale che i legislatori intervengano per regolamentare questo settore e garantire che le aziende rispettino gli standard ambientali. C'è bisogno di definire e anche espandere uno spazio per l'innovazione, ma questo spazio non può essere una sorta di "*Far West*" senza regole, dobbiamo invece stabilire un quadro normativo che guidi e regoli lo sviluppo tecnologico in modo sostenibile e responsabile. In caso contrario, rischiamo di perdere serie sfide ambientali e sociali e anche di rallentare l'innovazione. Perché se le nuove tecnologie producono risultati che le nostre società trovano inaccettabili, allora non saranno adottate e non ci sarà innovazione.

L'unione Europea ha mosso un primo passo tramite il suo *AI ACT*, la direzione è giusta?

Io credo che sia l'inizio di un sentiero sicuramente tortuoso, ma corretto. Ritengo che regolamentare non significhi solo limitare, ma anche dare una direzione a queste innovazioni.

L'Unione europea ha già sviluppato con successo dei framework regolamentativi, come il GDPR, il DSA e il DMA, che regolamentano servizi digitali e concorrenza.

Considerati tutti insieme questi acts definiscono un framework regolamentativo finalizzato ad assicurare che lo sviluppo e l'uso dell'IA nei confini EU avvenga nel rispetto dei nostri valori. Non dimentichiamoci che l'EU è stata la prima a definire un *framework* regolamentativo articolato per la goverance del digitale e che nel farlo si posta in una posizione di *leadership* internazionale.

Per concludere, cosa dire a chi si è già immaginato scenari da Matrix o spettri di un HAL 9000? Sono il passo successivo?

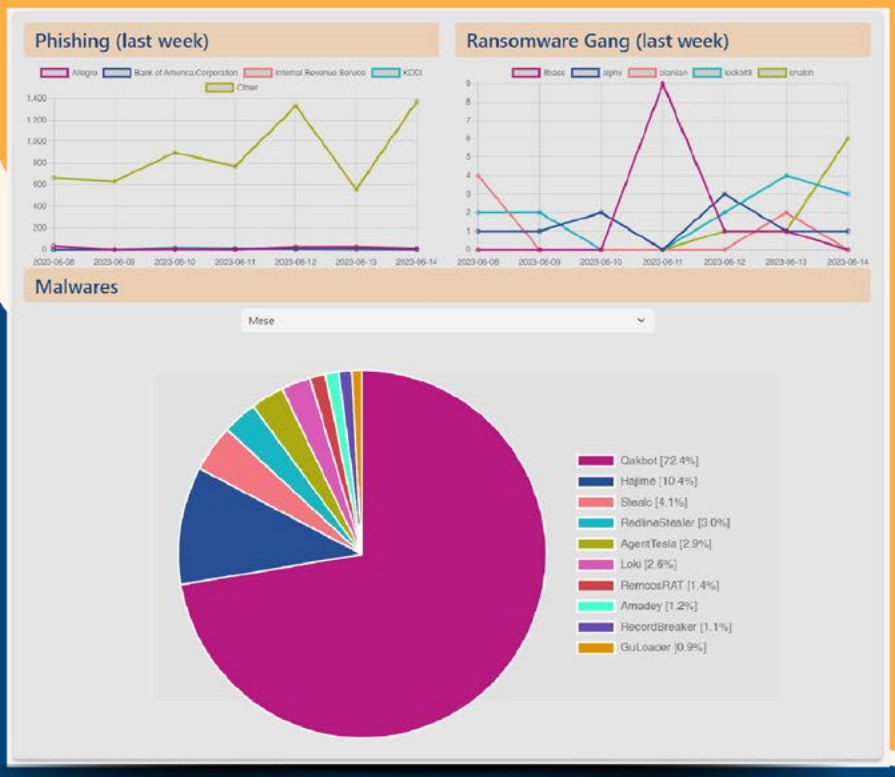
Direi che anch'io vorrei avere la versione aggiornata di HAL 9000 sul mio cellulare, ma che, per quanto ho potuto vedere e studiare, non ci siamo ancora. Perché l'IA che sviluppiamo, anche i modelli generati, non è fatta di altro che di potenti calcolatori capaci di fare calcoli statistici molto complessi. Non ci sono intenzioni, non ci sono idee, non ci sono emozioni, non c'è nulla di tutto questo. L'IA – in un certo senso - è così come ci appare.

Cyber Think Tank Assintel

CYBER Think Tank ASSINTEL

Threat Infosharing

Garantire agli Associati Assintel un servizio di early warning sulle minacce e rischi cyber giornalieri.



Per info scrivi a: segreteria@assintel.it

L’IA come l’elettricità cambierà la nostra vita

Intervista a Gianni Riotta a cura di Massimiliano Cannata

Giornalista, scrittore, conduttore televisivo, direttore del TG1 e del Sole 24 Ore, inviato, Riotta è da sempre un attento osservatori delle fenomenologie del cambiamento, che interpreta esercitando un ottimismo razionale, e un metodo attendo di verifica delle fonti da cronista di razza. In questa intervista vengono presi in esame i tanti risvolti sociali, economici e lavorativi che la rivoluzione dell’IA sta determinando in ogni angolo del pianeta. Dobbiamo imparare a regolare “la macchina del caos” per usare la definizione di Max Fisher, cercando di studiare a fondo il potere degli algoritmi e l’influenza che il loro uso diffuso potrà avere per gli equilibri della democrazia . Il recente caso del New York Time che cita in giudizio chatgpt per l’uso indebito dei propri contenuti giornalistici solleva degli interrogativi che attengono non solo al diritto d’autore, ma più in generale al disallineamento che si registra tra i percorsi evolutivi della tecno-scienza e i progressi della ricerca giuridica .

Direttore Riotta, lei è stato tra i primi ad occuparsi delle trasformazioni apportate dal digitale, tema cui ha dedicato la tesi di laurea alla Columbia University, Come giudica l’esplosione che sta avendo l’intelligenza artificiale?

Siamo di fronte a una vera grande rivoluzione. Nel corso dei miei studi ho avuto modo di conoscere i padri dell’IA, sarebbe stato difficile anche per loro prevedere gli sviluppi cui saremmo andati incontro. Va detto che c’è stata una fase in cui si era anche assistito a uno stop, adesso in forza della capacità di generare linguaggi si sta espandendo con rapidità. Come è stato per l’elettricità imporrà una mutazione profonda del nostro modo di studiare, di lavorare, in una parola di vivere.

Né apocalittici né integrati

Quale approccio è giusto tenere rispetto al vento del cambiamento? Il sociologo Mario Morcellini, ricordando la nota contrapposizione tra “apocalittici” e “integrati”, suggeriva di aderire a una nuova categoria, quella degli “impegnati”. Qual è il suo parere in merito?

“Apocalittici e integrati” è un libro di Umberto Eco del 1964. Il grande intellettuale aveva già risposto a questo dilemma con lucidità. Settanta anni dopo leggiamo sui giornali che l’IA porterà conflitti, ruberà il lavoro, per poi il giorno dopo attribuire a questa applicazione doti salvifiche. In verità nessuno può sapere il futuro. Pensiamo a quanto avvenuto con la fissione nucleare. Come è noto fu sperimentata alla fine degli anni trenta. Nel terribile agosto del ‘45 con lo sganciamento della bomba atomica, su Hiroshima e Nagasaki il mondo assistette alla prima applicazione distruttiva di questa scoperta. Per vedere la prima lampadina elettrica alimentata con il nucleare, bisognerà aspettare il 1957, ben dodici anni. Arrivando all’attualità registriamo che i tedeschi hanno bloccato l’utilizzazione del nucleare, in ragione del fatto che non si riesce a controllarne l’impiego in maniera sicura e indolore. Stesso ragionamento vale per l’intelligenza artificiale, non si possono dare letture univoche, superficiali e sommarie delle scoperte della scienza e della tecnologia. Tutti

Foto: Stefano Montesi - Corbis via Getty Images

quelli che scrivono cosa ci attende, non hanno la più pallida idea di come saremo tra qualche anno.

Rimane il fatto che la contrapposizione disorienta l'opinione pubblica…?

Certamente. Quello che servirebbe è un approccio più pragmatico, più cauto, meno propagandistico. Occorre ragionare e fare un passo alla volta, mentre per adesso vedo un dibattito urlato e, quel che è peggio, sconclusionato.

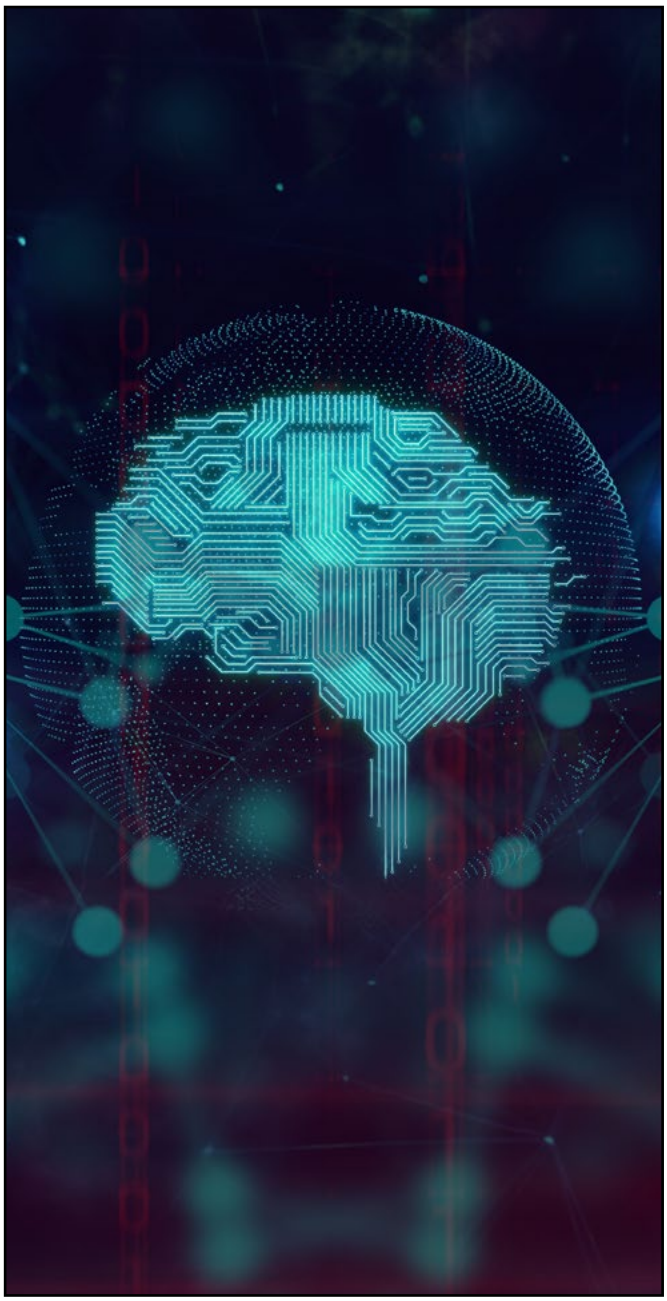
In un commento apparso su Repubblica, insiste sulla necessità di definire regole europee per l'IA. In concreto cosa vuol dire?

Come per tutte le innovazioni, anche l'IA va regolata, non possiamo lasciare mano libera alle grandi piattaforme di gestire la raccolta dei dati senza alcuna verifica. Quali algoritmi vengono usati, come vengono usati, come vengono distribuiti , sono questioni cruciali che devono trovare una regimentazione giuridica. Il vero problema è che la legge sull'intelligenza artificiale, rischia di essere già vecchia, quando verrà approvata. Il Parlamento dell'Unione si è impegnato a vararla prima delle prossime elezioni, intanto però la tecnologia va avanti. A novembre dello scorso anno è arrivato chat GPT 4, ma siamo andati già molto oltre...

Il rapporto tra i tempi della scienza e delle applicazioni tecnologiche e la ricerca giuridica sono disallineati. Non è una novità. Sono tanti i casi che si possono richiamare, forse il più eclatante riguarda lo stop imposto dal Garante della Privacy a Chat GPT, che ha fatto parlare di misura draconiana e di oscurantismo. Che idea si è fatto?

Mentre tutto il mondo sta andando in una direzione, questo "sgambetto" all'italiana rimane difficile da giustificare. Bastava connettersi a un "server open" per aggirare un divieto, che ha avuto il risultato di danneggiare molte start up italiane e alcuni centri di ricerca. Con quel provvedimento ci siamo tirati addosso il giudizio di paese "luddista", conservatore, antitecnologico. La riapertura che è seguita, con le presunte garanzie fornite da Open AI, che da cronista avrei preferito leggere in un documento ufficiale per capirne lo spirito e il significato, sa in realtà di un passo indietro. L'istituzione ha insomma tardivamente capito che aveva preso un grosso abbaglio e si è ricreduta.

Per le aziende un "salto" culturale decisivo



Nel corso de *"La Repubblica delle idee"* evento che si è svolto a Bologna Lei ha moderato un dibattito sul "lavoro come specchio del cambiamento". Cosa sta succedendo alle organizzazioni produttive, non rischiano di farsi travolgere dalla rivoluzione in atto?

Il salto da gestire sarà incredibile. Muta il lavoro dei professori nelle scuole che certo non potranno dare agli studenti come compito la classica ricerca da fare a casa, magari con l'ausilio delle gloriose enciclopedia che ormai non sfoglia più nessuno. Ma anche per avvocati, ingegneri, manager, giornalisti stanno mutando i tempi e i modi di gestire e concepire il lavoro. Dipenderà molto dal modello economico che adotteremo. Vogliamo aderire al paradigma di un capitalismo selvaggio, motore di diseguaglianze e di forti tensioni sociali o piuttosto, dimostrando maggiore equilibrio e ragionevolezza, ci impegneremo per affermare un modello di IA e di sviluppo tecnologico sostenibile? Sarà questo il banco di prova del futuro più immediato.

Lei è direttore della scuola di Giornalismo della LUISS, dove ha messo in campo un progetto di avanguardia. Di che cosa si tratta?

Gli studenti hanno creato una rivista utilizzando gli algoritmi, sperimentando un'attività redazionale mediata dall'innovazione tecnologica originale e stimolante. Quello che abbiamo soprattutto testato è il mutamento della professione. Non si tratta di consegnare o appaltare il giornalismo ai fornitori di tecnologia o di algoritmi, ma di guardare in faccia la trasformazione che sta avvenendo, nella consultazione e nel confronto delle fonti, ma anche nei linguaggi con cui un cronista deve raccontare la realtà.

Credo che non bisogna arretrare rispetto al nuovo, piuttosto rilanciare interrogativi e il senso profondo delle domande che deve animare la curiosità del cronista, oggi come ieri. Perché non ci interroghiamo per esempio a sufficienza sul fatto che non ci sono piattaforme europee? Per quale ragione i giornalisti italiani hanno guardato con distacco prima l'evoluzione di Internet e dei social e oggi quella della IA, che fa parte ormai della nostra strumentazione quotidiana?

Che risposta si è dato?

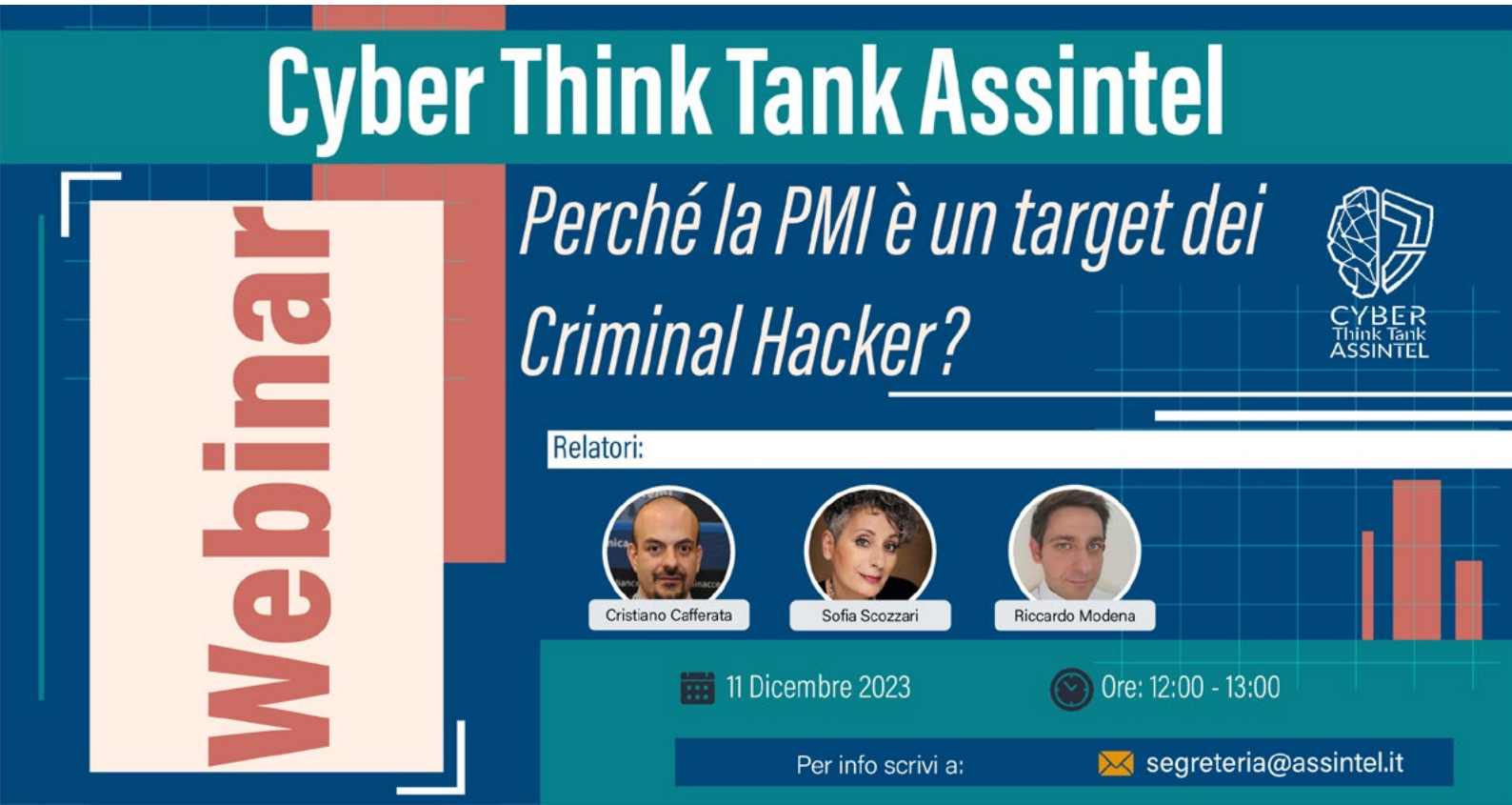
Quando ero direttore del TG1 ho voluto una rubrica: "TG1 sei tu" selezionando dei video realizzati dai nostri ascoltatori. Il messaggio era chiaro: dobbiamo dialogare con tutti, perché oggi videomaker e cronisti di assalto ne abbiamo in ogni angolo di strada, basta avere un telefonino e filmare quello che avviene.

Non commettiamo ancora una volta l'errore di quel celebre giornalista che disse che Internet era un moda cattiva che sarebbe passata presto. Purtroppo, però, non vedo ancora il giornalismo professionale di casa nostra pronto a superare questo gap culturale, che ha già caratterizzato il dibattito pubblico in occasione della "prima" rivoluzione digitale, quella apportata dal telefonino e da Internet diffuso.

La sicurezza arma contro le fake news!

Vorrei chiudere la nostra conversazione con una riflessione sulla sicurezza. Questione divenuta centrale in ogni ambito della vita quotidiana, e che chiama in causa chi si occupa, in particolare, di gestire il flusso delle informazione. Il fenomeno *fake news* preoccupa non poco. Come arginarlo?

Alla LUISS, opera un hub contro la disinformazione che coordino insieme alla professoressa Livia Di Giovanni. Stiamo parlando di una tematica di frontiera, come dimostra la creazione di una task force europea finalizzata a contrastare quella che Max Fischer in un saggio da poco tradotto in Italia a cura del direttore de l'Inchiesta Christian Rocca *La macchina del caos*. Gli studiosi sono sempre più attenti ad analizzare la forza politica dei social. Non è un caso perchè Troll come si è visto con l'alluvione in Emilia e Robot stanno condizionando il percorso della storia, modificando anche il modo di fare la guerra, come si sta vedendo bene in Ucraina. Torna in primo piano ancora la riflessione sull'IA, che sarà certo l'arma della propaganda e della disinformazione anche nel prossimo appuntamento elettorale ma, e lo voglio sperare con convinzione, sarà anche la nostra arma per smascherare hacker e impostori che ormai si annidano a tutte le latitudini.



Wetwar: il paradosso del domani

A cura di Pierguido Iezzi

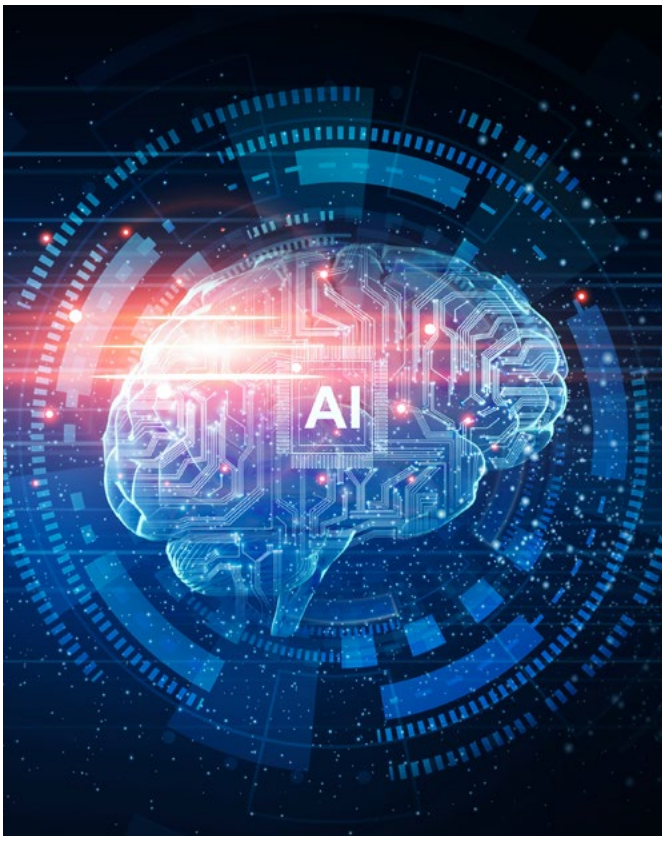
In un'epoca dove sfortunatamente lo spettro della guerra sembra essere sempre più presente, nessun dominio (terra, mare, aria, spazio e – come forse più interessa a noi – cyber) sembra non essere stato toccato dalla mano invisibile del cambiamento.

Questo contesto operativo di multidominio[1] è sicuramente un sistema complesso, in cui le singole variazioni che agiscono lo modificano portandolo ad un nuovo stato, diverso da quello inziale. In tale sistema complesso, i domini, le dimensioni degli effetti (fisica, virtuale e cognitiva), i sistemi (politico, militare, economico, sociale, informativo e infrastrutturale) e gli ulteriori ambienti (informativo ed elettromagnetico) concorrono a generare un mix di gangli, in cui tutti gli aspetti sono legati da una serie di interrelazioni attraverso una serie di nodi collocati su più piani differenti.

Pertanto, particolare rilevanza assume la competizione nella dimensione cognitiva (Cognitive Warfare) che, nella sua dimensione intangibile, prende di mira ideologie, valori e società attraverso un uso sempre più esteso di mezzi di comunicazione, nuove soluzioni tecnologiche e la crescente attenzione militare al settore delle neuroscienze e alle sue applicazioni.

Il "campo di battaglia", in questo caso, è proprio quello della mente umana. Come teorizzato in ambiente scientifico prima e militare poi; il nostro cervello può essere condizionato e "aggredito" in tre modi.

1. **Influenza:** Quest'area si concentra su strumenti e metodologie per influenzare e manipolare il pensiero umano attraverso la manipolazione di informazioni, percezioni e schemi culturali. Questi strumenti operano spesso attraverso l'ambiente digitale e le reti sociali, utilizzando tecnologie di persuasione interattiva per sviluppare strategie di disinformazione.
2. **Interferenza:** Quest'area riguarda strumenti e tecnologie che operano direttamente sul cervello umano, influenzando le dinamiche fisiologiche e biochimiche per interferire con i processi cognitivi. Questi strumenti possono essere utilizzati per migliorare o degradare specifiche funzioni cerebrali. Inoltre, possono includere sostanze chimiche, impulsi elettrici e onde elettromagnetiche che agiscono sui processi cognitivi.



3. **Alterazione:** Quest'area si concentra sulle tecnologie che consentono l'interazione tra il cervello umano e le macchine, con lo scopo di migliorare le capacità cognitive umane o sfruttare le vulnerabilità a fini offensivi. Queste tecnologie vanno dalla realtà virtua-

Il "campo di battaglia", in questo caso, è proprio quello della mente umana.

le/aumentata alle interfacce cervello-macchina (BCI) e cervello-cervello (B2BI), fino alle possibili soluzioni di ibridazione più avanzate, come il modello Cyborg.

È proprio quest'ultimo punto che presenta le più grandi incognite e – forse – i più grandi pericoli. In questo scenario, un esempio è rappresentato dalla recente autorizzazione della Food and Drug Administration alla start-up *Neuralink*, di proprietà di Elon Musk, che testerà su un campione umano volontario, una nuova tecnologia in grado di far interagire direttamente il cervello con il computer, facendoci assistere ad un processo di evoluzione tangibile d'ibridazione uomo-macchina. In estrema sintesi, stiamo assistendo ad una nascita di micro-cervelli in vitro, ognuno contenente circa 800mila neuroni derivati da cellule staminali umane, capaci di interagire tramite un sistema di elettrodi, stimolando l'input visivo. Un esempio di questa nuova ibridazione la potremmo trovare applicata in diversi ambiti, come in quello militare attraverso l'impiego di super soldati (Next Generation Soldiers) con capacità fisiche e cognitive aumentate; muscoli più forti, udito migliore e vista più acuta, permettendogli di controllare droni e sistemi d'arma con il solo pensiero. Tutte potenzialità acquisite senza la necessità di ricorrere ad una chirurgia invasiva, e con l'obiettivo finale di arrivare ad una comunicazione wireless ad alta risoluzione tra mente e macchina.

Queste strategie possono essere utilizzate in vari contesti, inclusi conflitti militari, campagne di disinformazione, manipolazione delle opinioni pubbliche e altro ancora. È importante essere consapevoli di queste potenziali minacce e sviluppare meccanismi di difesa appropriati per proteggere la mente umana da manipolazioni indesiderate.

A breve termine, sarà questo il nuovo campo di battaglia dove si confronteranno le superpotenze globali per il controllo del pianeta, con Stati Uniti e Cina che più di altre hanno investito nell'Intelligenza Artificiale e nelle biotecnologie avanzate. Tale scenario evidenza come la linea tra uomo e macchina si stia assottigliando e sovrapponendo sempre più marcatamente, proiettandoci in un'era futura in cui materia biologica e artificiale si fonderanno per creare individui potenziati.

Le predette argomentazioni non possono essere più considerate fantascienza, ma una vera e propria realtà, che ci traghetta verso un'ulteriore nuova dimensione, quella della cosiddetta "wetwar" termine che deriva da "wetware" utilizzato per la prima volta dallo scrittore Rudy Rucker per riferirsi a sistemi viventi o componenti di essi utilizzati per processare o archiviare informazioni.

Il "wetware", come spiega il neurosicenziato Miguel Nicoleis, "rappresenta l'integrazione di sistemi biologici e artificiali per estendere le capacità umane". Al contrario, con il termine wetwar ci si riferisce ad una guerra condotta attraverso soldati potenziati, finanche con l'obiettivo di far interagire in tempo reale la mente umana con l'IA. Questa convergenza a cui stiamo assistendo tra biologia e tecnologia può, quindi, comportare implicazioni profonde sia in ambito militare che in quello della sicurezza. Nello specifico, se da un lato questa tecnologia fornisce la capacità di interfacciare direttamente il cervello con i sistemi informatici, migliorando notevolmente l'efficienza e la velocità del processo decisionale, dall'altro rende il cervello un potenziale bersaglio, determinando così un fronte di rischio, attraverso cyber attacchi. Questa nuova corsa alle armi, non più nucleari ma biotecnologiche, rischia di mutare per sempre il destino dell'umanità, che potrebbero comportare cambiamenti epocali anche negli equilibri geopolitici globali.

Il Digital Operational Resilience Act (DORA)

A cura di Ranieri Razzante

Il 27 dicembre 2022 è stato pubblicato in Gazzetta Ufficiale il Regolamento 2022/25541/UE del Parlamento Europeo e del Consiglio del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e denominato *Digital Operational Resilience Act* (c.d. DORA).

I destinatari del testo, entrato in vigore su tutto il territorio europeo il 17 gennaio 2023, saranno tenuti all'adempimento degli obblighi ivi previsti entro il 17 gennaio 2025.

La disciplina rappresenta un momento di svolta per l'Unione Europea che, decidendo di abbracciare la transizione digitale nonché di agevolarla attraverso una serie di misure specifiche, è intervenuta con il c.d. "Pacchetto Europeo sulla Finanza Digitale", di cui fanno parte, oltre alla normativa in analisi: il Regolamento 2023/1114/UE sui mercati delle cripto-attività, c.d. Regolamento MiCA (*Markets in Crypto-assets Regulation*); il Regolamento 2022/858/UE relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito ("DLT").

In prima istanza, al fine di fornire un quadro completo, è necessario specificare cosa si intenda per "resilienza operativa digitale", ovvero «la capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi TIC, l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza dei sistemi informatici e di rete utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità, anche in occasione di perturbazioni».

Nello specifico, il DORA introduce un quadro operativo digitale semplificato in tutto il settore finanziario dell'UE, con lo scopo di minimizzare, prevenire e mitigare i rischi informatici, nonché il rischio cyber, per i servizi finanziari, e di contribuire alla sicurezza informatica adeguata al rischio dei fornitori, fortificando la loro resilienza contro le minacce poste dalle tecnologie dell'informazione e della comunicazione.

Gli obiettivi del provvedimento, stabiliti all'art. 1 dello stesso, concernono specifici vincoli applicabili alle entità finanziarie – quali, ad esempio, *test* di resilienza operativa digitale, condivisione di dati e di informazioni in relazione alle vulnerabilità e alle minacce informatiche, o anche misure relative alla solida gestione dei rischi informatici derivanti da terzi – e relativi agli accordi contrattuali stipulati tra fornitori terzi di servizi TIC ed entità finanziarie. A tal proposito, secondo l'art. 2, il disposto si rivolge a determinati enti – come quelli creditizi, istituti di pagamento, prestatori di servizi di informazione sui conti, istituti di moneta elettronica, imprese di investimento, depositari centrali di titoli o imprese di assicurazione e di riassicurazione – ed a fornitori terzi di servizi TIC, ovvero «servizi digitali e di dati forniti attraverso sistemi di TIC a uno o più utenti interni o esterni su base continuativa, inclusi *l'hardware* come servizio e i servizi *hardware*, comprendenti la fornitura di assistenza tecnica mediante aggiornamenti di *software* e *firmware* da parte del fornitore dell'*hardware*, esclusi i servizi telefonici analogici tradizionali».

Tali soggetti sono tenuti a predisporre un quadro di gestione e di controllo interno che sia solido, esaustivo e adeguatamente documentato, al fine di garantire una gestione efficace e prudente di tutti i rischi informatici in maniera rapida, efficiente ed esaustiva, assicurando un elevato livello di resilienza operativa digitale. Essi devono altresì:

- stabilire i requisiti volti all'armonizzazione delle regole di gestione dei rischi relativi alle tecnologie ICT;
- creare un ICT *Risk Management Framework*;
- definire una strategia di resilienza digitale in materia di *business continuity* e *disaster recovery*;
- classificare gli incidenti e le minacce informatiche in

base alla criticità dei servizi a rischio;

- creare un sistema di segnalazione degli incidenti informatici, attuando un processo di monitoraggio, registrazione e gestione costante;
- svolgere *test* di resilienza operativa digitale, secondo un approccio *risk-based*;
- prevedere protocolli di *information sharing*, con l'obiettivo di incoraggiare lo scambio di informazioni.

In merito agli obblighi degli enti, rileva una ulteriore peculiarità: il vincolo per gli enti di test di resilienza operativa digitale che devono essere effettuati da soggetti indipendenti, interni o esterni.

Dunque, si comprende come la resilienza operativa non sia solo un punto di arrivo legislativo e regolamentare, ma anche un punto di partenza per la costruzione di modelli operativi più solidi e più efficaci al fine di offrire adeguate tutele ai consumatori e costruire una più salda reputazione del settore finanziario.

Da ultimo, per quanto concerne l'ambito sanzionatorio, il DORA stabilisce un sistema differenziato di responsabilità delle autorità di vigilanza su base istituzionale per garantire il rispetto del Regolamento. Queste sono invitate a cooperare tra loro; difatti la norma stabilisce ampi poteri di vigilanza, indagine e sanzionatori a beneficio di queste, con lo scopo di garantire l'adempimento dei loro doveri. Si richiede, quindi, agli Stati membri dell'Unione europea di stabilire sanzioni e rimedi amministrativi adeguati per le violazioni.

Risulta evidente come le nuove disposizioni intendano sottolineare la particolare sensibilità del Legislatore europeo verso l'ambito delle strategie di *cybersecurity*. Non rimane che auspicare una reattiva adesione da parte degli *stakeholders* coinvolti a vario titolo, atteso che l'individuazione di rischi comuni e la disposizione di politiche condivise rappresenta l'approccio più efficace nell'ambito del sistema finanziario integrato europeo.

L’evoluzione del panorama regolamentare cyber e l’avvento della Direttiva NIS2 nel settore delle telecomunicazioni

A cura di Milena Antonella Rizzi

La crescente estensione della proiezione digitale delle Istituzioni, delle imprese, della pubblica amministrazione e dei singoli cittadini ha progressivamente fatto emergere una sempre maggiore esigenza di protezione dalle minacce informatiche contribuendo ad elevare la consapevolezza della rilevanza strategica della resilienza cyber a livello unionale e nazionale.

La notevole accelerazione impressa dall’Unione Europea all’evoluzione della regolazione, anche a supporto della strategia Unionale di cybersecurity, ha visto l’introduzione di una moltitudine di prescrizioni attraverso l’adozione della Direttiva Network and Information Systems (NIS) nel 2016 e del Cyber Security Act (CSA) nel 2019, l’istituzione del Centro di competenza in cybersicurezza (ECCC) nel 2021, l’adozione del Regolamento Digital Operational Resilience Act (DORA) e della Direttiva NIS2 nel 2022, cui si aggiunge la prossima conclusione del negoziato sul Cyber Resilience Act (CRA) e l’imminente avvio di quello inerente al Cyber Solidarity Act (CSoA) ed alla revisione del citato CSA.

Tale ingente produzione normativa ha contribuito ad ulteriormente stimolare, a livello nazionale, il dibattito sulla necessità di dotare il Paese di una cornice normativa a protezione della sicurezza cibernetica degli asset strategici che ha condotto, nel 2019, all’istituzione dell Perimetro di sicurezza nazionale cibernetica (PSNC) nonché, più di recente, ai regolamenti e ai decreti attuativi previsti dall’articolo 33-septies del D.L. 172/2012 per la messa in sicurezza delle infrastrutture digitali e dei servizi digitali per la Pubblica Amministrazione.

In tale percorso evolutivo e di crescente consapevolezza della non più procrastinabile esigenza di investire nel potenziamento delle misure di sicurezza cibernetica per l’innalzamento del livello della resilienza nello specifico settore, particolare rilevanza ha assunto la riorganizzazione dell’architettura nazionale cyber introdotta dal D.L. 82/2021 che – razionalizzando le iniziative volte a rafforzare costantemente la postura e la resilienza cyber del nostro Paese e dell’Unione – ha istituito l’Agenzia per la Cybersicurezza Nazionale (ACN) ed ha creato le condizioni per favorire, a livello nazionale, la coerenza normativa, regolamentare e applicativa nello spazio cibernetico.

Proprio in tale ottica ACN, nel contesto dello sviluppo delle iniziative regolamentari cyber e della loro attuazione, coltiva una costante interlocuzione con i soggetti e gli attori dei settori vigilati ai sensi dell’articolata e complessa soprarichiamata normativa, al fine di fornire supporto nel percorso di implementazione delle misure di sicurezza e nella conduzione dell’attività di compliance, formale e sostanziale, alle prescrizioni nazionali ed Unionali.

Con riferimento a queste ultime e, in particolare, a quelle dettate dalla Direttiva NIS1, recepite con il decreto legislativo n. 65/2018, e dalla Direttiva NIS2 in corso di recepimento, occorre evidenziare il ruolo attribuito ad ACN dalla nuova architettura istituzionale, che l’ha individuata quale Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, a tutela dell’unità giuridica dell’ordinamento, competente altresì all’accertamento delle violazioni e all’irrogazione delle sanzioni amministrative previste in materia.

Come noto, la Direttiva NIS2 prevede l’ampliamento del suo ambito di applicazione in cui sono inclusi anche la

pubblica amministrazione centrale (lasciando discrezionalità agli Stati membri di inserire gli enti locali in base all'assetto istituzionale), le piccole e microimprese (se operano in settori chiave per la società) e, indipendentemente dalle dimensioni, fornitori di servizi di comunicazione elettronica e di reti di comunicazione elettronica, giungendo a interessare 18 settori distinti in altamente critici (energia, trasporti, bancario, infrastrutture dei mercati finanziari, sanitario, acqua potabile, acque reflue, infrastrutture digitali, gestione dei servizi TIC business-to-business, pubblica amministrazione, spazio) e critici (servizi postali e di corriere, gestione dei rifiuti, fabbricazione, produzione e distribuzione di sostanze chimiche, produzione, trasformazione e distribuzione di alimenti, manifatturiero, fornitori di servizi digitali, ricerca).

La nuova Direttiva introduce inoltre un approccio «all-hazards» alla cybersicurezza, che considera cioè tutte le minacce, includendo profili di sicurezza fisica per la protezione del perimetro delle reti e dei sistemi informativi in raccordo con la collegata Direttiva sulla resilienza delle infrastrutture critiche ed amplia la definizione di incidente includendovi anche quelli capaci di compromette la "disponibilità", la "autenticità", la "integrità" o la "riservatezza" di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, non limitandosi, dunque, solo a quelli che hanno un impatto rilevante sulla "continuità" dei servizi essenziali prestati con conseguente, prevedibile, considerevole aumento delle notifiche di incidente.

Il recepimento della Direttiva NIS2 produrrà un significativo impatto anche sugli operatori TELCO, a seguito della loro inclusione all'interno del settore delle infrastrutture digitali, la cui regolamentazione, anche in materia di integrità delle reti, risiede nel ben consolidato Codice Europeo delle Comunicazioni Elettroniche (EECC), novellato nel 2018 per adattare il codice alle nuove realtà tecnologiche e di mercato e recepito dal D.Lgs. 207/2021, che tra l'altro estende il suo ambito di applicazione anche ai cd. servizi di comunicazione interpersonali indipendenti dal numero (Number-Independent Interpersonal Communication Services – NI-ICS) come WhatsApp e la posta elettronica.

In particolare, la Direttiva NIS2, nell'assorbire le previsioni in materia di integrità delle reti dell'EECC – ad oggi disciplinate a livello nazionale dal decreto ministeriale adottato dal MIMIT (a quel tempo MISE) il 18 dicembre 2018, cd. DM Telco – a favore di una maggior armonizzazione e orizzontalità della disciplina cyber, postula la realizzazione di un articolato quadro di cooperazione Unionale per la supervisione, la gestione degli incidenti e delle crisi cyber, l'esercizio di poteri regolamentari, ispettivi e sanzionatori rafforzati per assicurare l'implementazione degli obblighi di notifica di incidente e di adozione delle misure di sicurezza.

Ciò potrebbe anche comportare riallineamenti nella governance nazionale del settore TELCO negli Stati membri, con un rafforzamento del ruolo delle autorità cyber, nonché una rimodulazione e armonizzazione della regolamentazione, rispetto a quanto già sviluppato per i settori già oggetto della Direttiva NIS1.

In tale quadro normativo in costante evoluzione altro fattore da tenere in debita considerazione concerne l'attività di recepimento della Direttiva Resilience of Critical Entities (CER) del 2022, il cui combinato disposto con la citata NIS2, come si è detto, pone in capo alle Autorità competenti NIS designate a livello nazionale anche la responsabilità di definire obblighi relativi alla resilienza e sicurezza fisica delle infrastrutture critiche del settore delle infrastrutture digitali.

Ne consegue che le novità introdotte a livello Unionale, unitamente al previsto aggiornamento del quadro regolamentare del Perimetro che investiranno anche il settore TELCO, indirizzeranno nei prossimi mesi le attività di regolamentazione e adattamento della disciplina nazionale cyber. In tale ottica, l'accentramento dei poteri regolatori nell'Agenzia consentirà di agevolare, laddove possibile, l'individuazione di soluzioni armoniche e coerenti tra le diverse discipline, nonché rispettose e adeguate alle specificità settoriali.

L'Agenzia è estremamente sensibile a questo tema, caro alla sostanziale totalità dei soggetti vigilati, inerente alla frammentazione e stratificazione della disciplina cyber nazionale e sovranazionale.

Al riguardo, proprio nell'ottica di mitigare tale criticità, dal 2016 la definizione delle misure di sicurezza a livello nazionale è incardinata nel Framework Nazionale per la Cyber Security e la Data Protection[1] , basato sull'analogo Framework di cybersicurezza del National Institute of Standards and Technology (NIST), uno strumento operativo che consente di organizzare funzionalmente le misure di sicurezza che un'organizzazione può implementare.

L'uso di tale strumento di supporto, che ha già registrato una forte adozione a livello nazionale anche al di fuori del contesto della compliance normativa, potrà essere proseguito anche nella regolamentazione discendente dalla NIS2, in coerenza con la disciplina PSNC, ovvero anche per il settore TELCO, consentendo ai soggetti di ricondurre i requisiti delle diverse discipline a un unico indice generale.

Considerato, inoltre, che la descrizione dei requisiti non impone implementazioni specifiche ma consente, in genere, al soggetto di adottare la migliore pratica ritenuta più opportuna sulla base di una analisi del rischio, tale approccio agevola lo sforzo di compliance, specie in fase di transizione da un diverso modello di regolamentazione.

Al contempo, la definizione di strumenti che rafforzino la postura di cybersicurezza dell'Italia individuando l'opportuno bilanciamento rispetto agli oneri, non può prescindere dal coinvolgimento del settore produttivo.

Con questo spirito, nel contesto dell'attuazione del Perimetro di sicurezza nazionale cibernetica (PSNC), l'Agenzia ha avviato da aprile scorso un ciclo di incontri con tutte le organizzazioni pubbliche e private soggette alla disciplina.

Tale attività, è occasione anche per ricevere dal tessuto industriale riscontri circa le difficoltà attuative e prospettive evolutive della disciplina cyber nazionale. Con specifico riferimento al recepimento della Direttiva NIS2, sono in via di programmazione incontri con le Amministrazioni competenti per i settori della Direttiva NIS2, a partire dalle Autorità di settore, nonché con le associazioni datoriali. Queste iniziative saranno proficue per acquisire gli elementi utili a proporre un recepimento della Direttiva e una regolamentazione coerente con le specificità settoriali.

Tali attività, prodromiche alla costituzione dei tavoli settoriali previsti dalla Strategia Nazionale di Cybersicurezza, scaturiscono dalla postura di ascolto dell'Agenzia nei confronti del settore pubblico e privato necessaria per assicurare il dovuto supporto ai soggetti vigilati per una compiuta attuazione della disciplina cyber nazionale. Ciò anche al fine di incrementare il patrimonio informativo in vista dell'adozione di ulteriori iniziative normative finalizzate a rafforzare maggiormente la cornice di sicurezza cibernetica del Paese.

CYBER
Think Tank
ASSINTEL

Sfruttare le sinergie tra Intelligenza Artificiale e Cybersecurity: uno studio dell'ENISA

A cura di Vittorio Calaprice

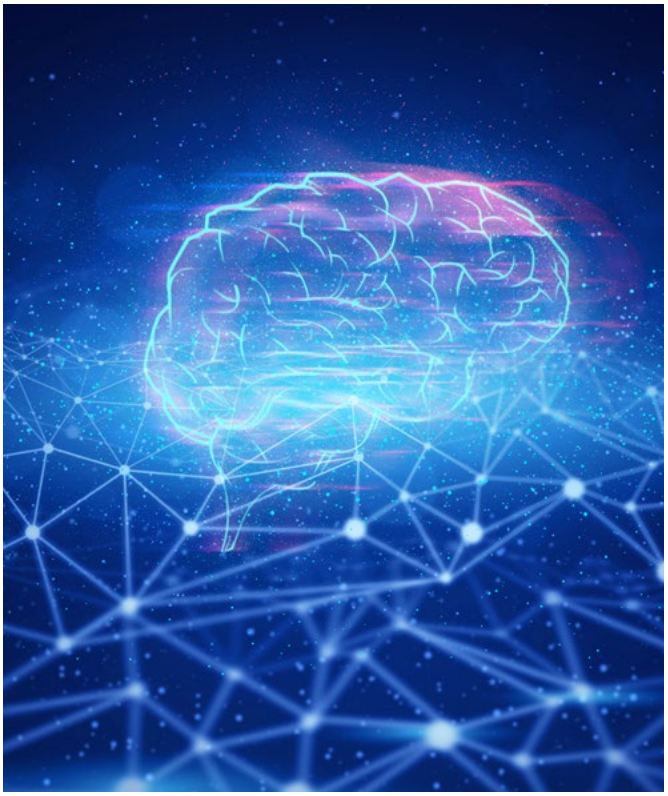
L'Intelligenza Artificiale e la Cybersecurity sono due settori che influenzano oramai in maniera pervasiva ogni aspetto della vita umana.

La loro interconnessione è diventata un'area di interesse scientifico sempre più forte per i ricercatori ed una nuova area di collaborazione tra esperti provenienti da "campi diversi".

Per offrire un quadro sistematico alla materia e studiare le intersezioni tra IA e cybersecurity, l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) ha pubblicato recentemente[2] un documento – denominato "*Artificial Intelligence and Cybersecurity Research*" – che ha preso in considerazione le dimensioni operative dell'IA nei confronti della cybersecurity:

a. l'uso dei sistemi di Intelligenza Artificiale come "servizi criminali" (ovvero una "IA per nuocere");

b. il supporto per la cybersecurity (ovvero una "IA per proteggere").



Come è noto, l'Intelligenza Artificiale sta rivoluzionando il campo della Cybersecurity, migliorando notevolmente la rilevazione, la prevenzione e la risposta alle minacce. Gli algoritmi di *machine learning* (ML, apprendimento automatico) riescono ad analizzare enormi quantità di dati per identificare schemi e comportamenti insoliti che potrebbero indicare un attacco informatico.

I sistemi di IA possono infatti imparare rapidamente dagli incidenti passati, adattando e migliorando i loro meccanismi di difesa in tempo reale.

I sistemi di rilevamento delle minacce – gestiti dall'IA – sono in grado di monitorare agevolmente il traffico di rete, i comportamenti degli utenti e le attività delle applicazioni. Analizzando continuamente i dati, questi sistemi possono individuare anomalie che potrebbero sfuggire ai tradizionali approcci basati su regole.

Questa capacità di rilevare minacce precedentemente sconosciute è cruciale in un panorama dei rischi in evoluzione in cui gli aggressori cambiano costantemente tattiche.

Ad esempio, le istituzioni finanziarie e le piattaforme di e-commerce sfruttano l'IA per combattere le frodi. I modelli di apprendimento automatico imparano a distinguere tra transazioni legittime e fraudolente basandosi sui dati storici. Questi modelli possono identificare schemi sospetti, come comportamenti di acquisto insoliti, contribuendo a prevenire l'accesso non autorizzato e le perdite finanziarie.

La capacità dell'IA di elaborare e analizzare grandi quantità di dati può aiutare i professionisti della Cybersecurity a rimanere un passo avanti rispetto ai criminali informatici.

Al contrario, le stesse funzionalità di intelligenza artificiale possono ugualmente potenziare l'arsenale in mano ai criminali informatici. Si pensi a bot basati sull'intelligenza artificiale che possono lanciare attacchi informatici sofisticati e persistenti: l'IA viene utilizzata per creare attacchi di phishing più efficaci e sofisticati personalizzando le e-mail attraverso dettagli personali raccolti dai social media.

Inoltre, i deepfake, generati dall'intelligenza artificiale,

possono essere utilizzati per commettere frodi o spingere notizie false.

Gli stessi sistemi di intelligenza artificiale possono essere bersaglio di attacchi informatici. Gli aggressori possono manipolare i dati inseriti in un sistema di intelligenza artificiale (avvelenamento dei dati) per influenzarne i risultati. Il rischio di attacchi che comportano l'alterazione dei dati di input per ingannare il sistema di intelligenza artificiale è esponenzialmente cresciuto.

Il documento dell'ENISA su "*Intelligenza artificiale e ricerca sulla cybersecurity*" parte da queste considerazioni per presentare una panoramica sui risultati di 44 progetti di ricerca finanziati dall'Unione europea a partire il 2014.

Lo studio si concentra sulla necessità di un rafforzamento della ricerca e dello sviluppo nel campo dell'IA e della Cybersecurity, favorendo quindi la condivisione dell'intelligence sulle minacce.

Il tema dello sviluppo di competenze qualificate nonché la promozione della cooperazione tra i vari stakeholders appaiono infatti obiettivi strategici da perseguire.

Il documento ENISA evidenzia inoltre l'importanza di stabilire standard giuridici per l'uso dell'IA nella cybersecurity in modo che sia mantenuto un buon equilibrio tra la necessità dell'IA di accedere ai dati e i diritti alla privacy degli individui.

Lo studio formula alcune raccomandazioni per affrontare le sfide attraverso la ricerca scientifica e individua delle aree chiave per guidare gli esperti che guidano la ricerca e lo sviluppo sull'intelligenza artificiale e la sicurezza informatica.

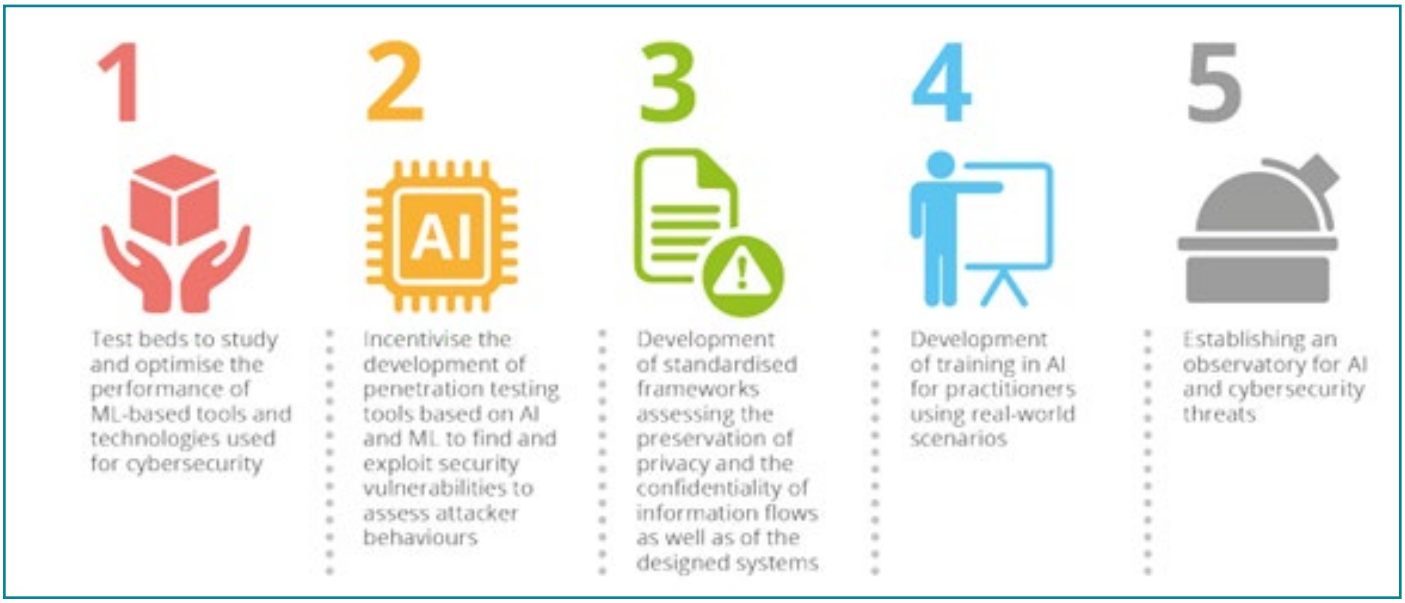
In sintesi, secondo l'ENISA, sono cinque aree di ricerca che stanno offrendo interessanti risultati e per le quali focalizzarsi nel futuro:

1. simulazioni e *testing* per ottimizzare le tecnologie di machine learning (ML);
2. sviluppo di strumenti di "*penetration test*" basati su IA e ML;
3. sviluppo di quadri standardizzati che valutino la tutela della privacy;
4. formazione sull'intelligenza artificiale per professionisti che lavorano nella cybersecurity;
5. creazione di un osservatorio per le minacce all'intelligenza artificiale e alla sicurezza informatica.

L'intersezione tra IA e Cybersecurity presenta un panorama complesso pieno di opportunità e rischi. Il documento dell'ENISA serve a far luce su questo panorama e a orientare la via da seguire.

Man mano che l'IA continuerà a crescere ed evolversi anche le strategie di Cybersecurity dovranno crescere, guidate da ricerche approfondite e in evoluzione con il lavoro dell'ENISA.

Rimane infine aperta la questione fondamentale alla base di questo studio, se gli investimenti nella ricerca e nell'innovazione in materia di cybersecurity sull'IA abbiano consentito all'Europa di compiere progressi in questo settore: le prime indicazioni mostrano che c'è ancora molto lavoro da fare, ma che la strada è stata oramai intrapresa!



Le opinioni espresse nell'articolo sono dell'autore e non rappresentano necessariamente la posizione ufficiale della Commissione europea

C’è vita oltre la firma digitale e la PEC

A cura di Andrea Lisi

Gli strumenti della firma digitale e della posta elettronica certificata sono ormai entrati nelle nostre abitudini aziendali e ne conosciamo bene il significato e le opportunità di utilizzo. Probabilmente non tutti sanno invece che tali strumenti fanno parte di famiglie più grandi: la firma digitale appartiene al genus delle firme elettroniche e la PEC a quella dei servizi elettronici di recapito certificato (SERC).

Effettivamente nell’ordinamento europeo si intrecciano principi fondamentali, come quello di non discriminazione e quello di neutralità tecnologica che a loro volta vanno correttamente interpretati -come vedremo- attraverso l’ausilio del principio di accountability. Tali principi hanno determinato l’opportuna emersione nel mercato digitale di diversi servizi e strumenti utilizzabili per sviluppare rapporti commerciali giuridicamente rilevanti. Ovvio che tali strumenti vadano utilizzati *cum grano salis*, previa valutazione che verifichi di volta in volta se siano adatti alle proprie esigenze.

Ma procediamo con ordine.

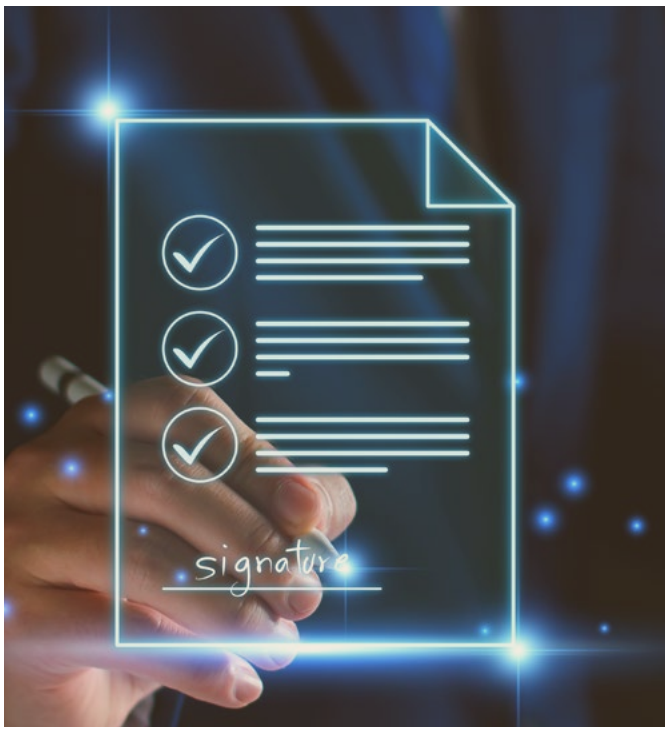
Il valore della firma digitale e delle firme elettroniche qualificate

La piena validità giuridica degli strumenti “tradizionali” della firma digitale e della posta elettronica certificata è oggi ben espressa nel Codice dell’amministrazione digitale (CAD), contenuto nel decreto legislativo 82/2005. In particolare, secondo gli articoli 20 e 21 del CAD la firma digitale, garantendo pienamente sia l’imputabilità giuridica al documento informatico a cui è associata e sia l’integrità, l’immodificabilità e la sicurezza allo stesso, è in grado di assolvere a tutte le funzioni formali e probatorie di una scrittura privata. In poche parole, la firma digitale può essere utilizzata per tutti i contratti informatici e per tutti i documenti per i quali nel nostro ordinamento si preveda il requisito della forma scritta *ad substantiam o ad probationem*. Insomma, la firma digitale garantisce la piena prova della provenienza del documento informatico e dell’immodificabilità del suo contenuto, come un qualsiasi documento cartaceo scritto e sottoscritto.

In realtà, questa valenza formale e probatoria non è una novità ed è prevista nel nostro ordinamento nazionale dalla fine degli anni ’90. Le novità normative in merito alle firme elettroniche sono effettivamente derivate dalle necessità del mercato elettronico, ben individuate dal legislatore europeo nei principi sopra richiamati di neutralità tecnologica e non discriminazione. E così il CAD negli ultimi anni, alla luce delle nuove esigenze europee attualmente ricomprese nel regolamento eIDAS[4], ha dovuto piano piano adattarsi a questo necessario cambiamento allargando così le maglie del giuridicamente rilevante ai tanti nuovi strumenti offerti dal mercato, con un approccio più neutrale dal punto di vista tecnologico.

Oggi il CAD accoglie la firma digitale[5] nel genus delle firme elettroniche qualificate, di cui quindi la firma digitale costituisce una species tecnologicamente orientata, dovendo rispettare precisi standard internazionali. Quindi, come la firma digitale, anche tutte le firme elettroniche qualificate godono della piena validità giuridica e sono in grado di garantirla a qualsiasi documento informatico a cui sono associate.

Tale valenza formale e probatoria è dovuta non alla tecnologia utilizzata, ma a una serie di controlli e verifiche sui dispositivi sicuri utilizzati e sui certificati qualificati emessi da particolari soggetti, i prestatori di servizi qualificati (a loro volta vigilati da autorità di controllo statali[6]).



Il valore delle altre firme elettroniche

In realtà, secondo il CAD la forma scritta digitale, con effetti paragonabili alle firme elettroniche qualificate, deve essere garantita a qualsiasi firma elettronica avanzata (FEA), cioè, una qualsiasi tipologia di firma elettronica che sia connessa unicamente al firmatario, sia idonea a identificare il firmatario, sia creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo e sia collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati[7]. Tali caratteristiche devono essere in qualche modo documentate, secondo quanto previsto attualmente dal DPCM 22 febbraio 2013.[8] Tale necessaria documentazione servirà, in caso di contestazioni giudiziali, a dimostrane le caratteristiche di firma elettronica avanzata, proprio secondo quel principio di accountability che anima la materia. Inoltre, sempre secondo il CAD, se il documento informatico è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore comunque soddisfa i requisiti della forma scritta, come la FEA. Si tratta della cosiddetta "firma SPID"[9].

Infine, secondo il CAD – in piena aderenza con quanto preteso da eIDAS[10] – deve riconoscersi valore giuridico a qualsiasi altra tipologia di firma elettronica[11] che consenta al documento informatico di garantire quelle caratteristiche di sicurezza, integrità, immodificabilità e riconducibilità all'autore che gli consentano di assicurare comunque una forma scritta digitale. Sarà un giudice di volta in volta a doverlo valutare, verificando – con l'aiuto di esperti – la documentazione tecnica a corredo e le caratteristiche proprie del sistema di firma. Come credo risulti evidente, in quest'ultima categoria possono rientrare sistemi completamente diversi di autenticazione informatica, certificazione di transazioni digitali on line, sistemi di trasmissione elettronica.

Sostanzialmente la firma digitale è una species contenuta nelle firme elettroniche qualificate, le quali a loro volta sono uno species del genus firma elettronica avanzata, che a sua volta rientra nella vasta area delle firme elettroniche cosiddette semplici (FES), in una delicata gradazione formale e probatoria prevista nel CAD (spesso affidata alla discrezionalità di un giudice).

Cosa pretende eIDAS per le firme elettroniche, i sigilli e i servizi di recapito certificato

Il Regolamento UE 910/2014 è chiaro nel garantire effetti giuridici a tutti i documenti elettronici, le firme, i sigilli elettronici e i servizi elettronici di recapito certificato, secondo i fondamentali principi di neutralità tecnologica e non discriminazione che favoriscono usabilità e verificabilità di diversi strumenti informatici sul territorio europeo. Eppure, ancora oggi alcune Authority, tanti giuristi e molti operatori sembrano non accorgersene[12].

eIDAs recita: "a una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate". Così come "a un sigillo elettronico non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per i sigilli elettronici qualificati". Stesso approccio per i SERC. "Ai dati inviati e ricevuti mediante un servizio elettronico di recapito certificato non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della loro forma elettronica o perché non soddisfano i requisiti del servizio elettronico di recapito certificato qualificato".

È senz'altro possibile, quindi, prevedere *ex lege* nel nostro ordinamento nazionale determinati effetti giuridici raggiunti in modo diretto e immediato (*in re ipsa*) attraverso strumenti o servizi qualificati, ma non ci possono essere discriminazioni per gli altri similari strumenti o servizi non qualificati presenti sul mercato, i quali – se raggiungono determinati risultati (di integrità, affidabilità, sicurezza) in modo diverso, vanno sempre accettati in giudizio e valutati da un giudice di volta in volta. E qualsiasi legge o regolamento (più o meno speciale), comunicazione (peraltro in molti casi introdotti nel nostro ordinamento per ignoranza e/o violando l'iter di approvazione previsto dall'eIDAS) vanno disapplicati, se incompatibili con i fondamentali principi di neutralità tecnologica e non discriminazione.

Ci piaccia o no, dobbiamo semplicemente prendere atto di questa impostazione UE che prevale su qualsiasi disposizione contraria nel nostro ordinamento. Quindi, accanto a firme digitali e PEC - che restano senz'altro sistemi robusti e affidabili, i quali consentono di validare la sottoscrizione e la trasmissione di documenti informatici garantendo comunque livelli di usabilità e accessibilità sempre più ampi - possono essere utilizzati tanti altri sistemi di firma o di trasmissione, sviluppati da fornitori del mercato digitale e in grado di assolvere funzioni simili e coprire esigenze svariate. Vanno analizzati con attenzione e verificati giuridicamente in base alle proprie esigenze, anche attraverso un'appropriata analisi del rischio.

Questa flessibilità giuridica va avvertita, quindi, da tutti gli operatori commerciali e i professionisti come una preziosa opportunità in grado di far adattare pienamente il mercato digitale alle nostre esigenze aziendali.

Cyber Think Tank Assintel

CYBER
Think Tank
ASSINTEL

Prossimo Incontro:

15 novembre
Ore 14:30

Valori:

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

Per info scrivi a: segreteria@assintel.it

Cyber Resilience Act: forte accelerazione dell'UE sulla sicurezza ma con tante questioni ancora aperte

A cura di Sebastiano Toffaletti

Gli ultimi mesi del 2023 potrebbero portare all'adozione del Cyber Resilience Act, o almeno ad un compromesso politico in seno alle istituzioni dell'UE. La Spagna, che detiene la presidenza del consiglio fino alla fine dell'anno, è determinata a chiudere la negoziazione sotto il proprio mandato.

Il Cyber Resilience Act, nel gergo CRA, completa la direttiva NIS2 nel promuovere nuovi livelli di sicurezza informatica non solo per le infrastrutture digitali, ma anche per i prodotti hardware e oggetti telematici per la casa. Fatta esclusione per apparecchiature medicali, aviazione e settore automobilistico, qualunque dispositivo connesso, come elettrodomestici smart, telecamere per la sorveglianza, televisori o giocattoli dovrà dimostrare un livello di riferimento di sicurezza.

Nelle intenzioni del legislatore europeo il sistema di marcatura e label dei prodotti promuoverà consapevolezza da parte dei consumatori e renderà i produttori responsabili della sicurezza dei loro prodotti. Sin dallo sviluppo e progettazione di nuovi prodotti, i fabbricanti dovranno integrare la capacità di rispondere a requisiti minimi sicurezza.

Anche una volta immessi sul mercato, i prodotti dovranno continuare a garantire protezione contro attacchi informatici e l'obbligo di fornire aggiornamenti di sicurezza durante tutto il ciclo di vita del prodotto. Le istituzioni UE non hanno ancora trovato del tutto una linea condivisa sull'obbligo a fornire aggiornamenti di sicurezza. Sarà molto interessante seguire la negoziazione politica, in quanto la questione potrebbe avere impatti importanti sui fabbricanti europei, ma non solo. Pensiamo in particolare a tutti quei prodotti, specie provenienti dalla Cina, la cui vita utile viene volutamente ridotta dal fabbricante semplicemente rendendo obsoleto il software. Al momento della redazione di questo articolo, esistono ancora posizioni contrapposte tra Commissione, Parlamento e Consiglio UE. Mentre la Commissione, finora sostenuta dai paesi membri, vuole fissare a 5 anni il periodo minimo in cui il fabbricate è tenuto a fornire aggiornamenti, la lobby dei grandi produttori per lo più extra europei ha fatto pressione sul parlamento riuscendo ad inserire la possibilità di accorciare il periodo a discrezione del fabbricante.

L'immissione sul mercato UE di prodotti soggetti al Cyber Resilience Actt prevederà la classificazione in base al rischio, da cui discendono requisiti diversi a seconda della classe. I prodotti considerati "critici" saranno soggetti a norme armonizzate e a controlli di terze parti indipendenti. Rientrano in questa categoria, ad esempio, i gestori di password, la interfacce di rete, i cripto-processori sicuri, le Smart card, i lettori e i token.

In linea con una diffusa sensibilità verso gli interessi della Piccola e Media Impresa, vero motore del sistema economico non solo italiano ma di tutti i paesi dell'Unione, Il Cyber Resilience Act riconosce l'importanza di coinvolgere attivamente le PMI nel processo decisionale, garantendo che queste imprese ricevano il supporto necessario per adattarsi alle nuove normative.

La European DIGITAL SME Alliance, l'associazione che a livello europeo maggiormente presidia gli interessi delle PMI soprattutto negli ambiti relativi al digitale tra cui la sicurezza informatica, sostiene il CRA e l'armonizzazione dei requisiti di sicurezza informatica. Tuttavia, l'Alleanza ha chiesto maggiore attenzione al potenziale impatto del CRA sulle PMI, affinché ricevano orientamenti chiari e risorse finanziarie per facilitare la conformità con la nuova legge. Per stimolare l'innovazione, l´Alleanza ha inoltre chiesto il supporto della Commissione europea attraverso finanziamenti, assistenza tecnica e collabo-

razione tra le parti interessate. L'attuazione richiederà infatti uno sforzo collettivo da parte di tutti gli attori coinvolti. La Commissione europea dovrebbe istituire programmi in collaborazione con l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) ed altri organismi di cybersecurity per offrire supporto, assistenza tecnica e sostegno finanziario alle PMI nell'affrontare i nuovi requisiti regolamentari.

Il successo del CRA risiede dunque nell'empowerment delle PMI. Queste imprese devono essere rappresentate nei comitati di standardizzazione per adattare le norme alle loro esigenze specifiche e garantire che i requisiti tecnici siano adeguati alle realtà più piccole. L'istituzione di meccanismi strutturati di consultazione consentirebbe loro di fornire contributi su aspetti chiave del Cyber Resilience Act, come standard, linee guida e strumenti di sostegno finanziario.

Alcune questioni rimango ancora aperte e ci si aspetta facciano parte delle negoziazioni presiedute dalla Spagna nel Consiglio UE, con la Commissione e con il Parlamento. Anche l'Italia ha un ruolo centrale in questo processo, o almeno ce l'ha il deputato europeo Nicola Danti, eletto nelle lista della Lega, il quale presiede la commissione parlamentare incaricata.

Tra le questioni ancora non affrontate, per facilitare l'adozione da parte delle PMI è auspicabile che i legislatori forniscano una lista di metodologie e quadri riconosciuti come riferimento, semplificando così il processo decisionale per le aziende più piccole.

Rimane ancora da chiarire se il legislatore intenda estendere il campo di applicazione oltre che ai prodotti connessi anche ai servizi post vendita cioè il mercato dei servizi secondari legati ai dati generati dai prodotti smart. Inoltre, al fine di evitare o almeno ridurre le inevitabili discrepanze di attuazione tra Stati membri, e quindi prevenire concorrenza sleale tra aziende, è necessario creare un sistema centralizzato gestito dalla Commissione europea o da ENISA per armonizzare le metodologie e i tempi delle valutazioni del rischio.

In aggiunta a quanto sopra, la European DIGITAL SME Alliance ha spesso insistito sulla necessita di regolamentare la capacità dei fabbricanti di imporre protocolli di sicurezza che limitano l'accesso indipendente di terze parti ai loro dispositivi. Tali restrizioni ledono da un lato il "diritto alla riparazione" per gli utenti e limitano la concorrenza di imprese indipendenti nel mercato post vendita. Allo stesso modo è importante mantenere l'obbligo di fornire aggiornamenti di sicurezza per l'intero ciclo di vita dei prodotti, o almeno 5 anni, e di evitare "sconti" alle aziende che desiderano accorciarlo.

Una questione ancora osteggiata fieramente da molte aziende extra europee, specie BigTech, è l'obbligo per i fabbricanti di comunicare ad ENISA, piuttosto che alle agenzie nazionali, l'esistenza di vulnerabilità, includendo potenzialmente anche quelle non ancora risolte. Queste aziende mettono l'accento sui rischi che una diffusione di tali vulnerabilità potrebbe generare. Si può però rispondere che esse devono probabilmente molto al valore dei loro brand, più che alla qualità dei loro prodotti, e quindi temono di dover ammettere di non essere sempre all'altezza della tale reputazione.

Altra questione ancora aperta è la possibile esclusione del Software Libero e Open Source, quanto meno se utilizzato a scopo non commerciale. L'obbligo di estendere la conformità ai fornitori di componenti è considerato molto oneroso, se non addirittura impossibile da affrontare, per chi sviluppa in ecosistemi altamente distribuiti come l'Open Source.

Come spesso accade, sebbene il processo legislativo sia ormai giunto alla conclusione, le questioni più spinose sono ancora irrisolte. I prossimi mesi ci diranno cosa deciderà l'UE, quali interessi nazionali avranno ottenuto le migliori condizioni e quali aziende saranno penalizzate o ne avranno un beneficio. Tutti, certamente, dovranno mettere la sicurezza tra le loro priorità.

Cybersecurity, non possiamo più fare a meno di un approccio manageriale. Anche nelle PMI

A cura di Alessandro Manfredini

Il mondo moderno, fortemente digitalizzato, è costantemente sottoposto a un'ampia gamma di minacce informatiche e anche l'Italia non fa eccezione. Al contrario, nel 2022 il nostro Paese è stato il più colpito in Europa da attacchi di tipo ransomware e questo impone a tutti noi – e più in generale a tutti gli imprenditori, compreso chi guida una PMI – una profonda riflessione sulla cybersecurity e sulla sua gestione.

Per comodità di lettura, provo a procedere per punti.

1. Una minaccia crescente

Che gli investimenti in sicurezza cibernetica siano quanto mai necessari, lo dicono i numeri.

Il numero di attacchi informatici in Italia è cresciuto in modo preoccupante nel 2022, con un aumento del 138%, raggiungendo quota 13.000 attacchi all'anno. La Polizia Postale ha segnalato una "proliferazione di gruppi ostili" con un incremento del 78% dei sospettati. A dicembre, gli attacchi rilevati sono stati pari a 12.947, più del doppio rispetto all'anno precedente. Questo trend allarmante continua ad aumentare nel corso del 2023.

In particolare, l'Italia e le sue imprese e pubbliche amministrazioni sembrano essere vulnerabili ai ransomware, un tipo di attacco informatico in cui i cybercriminali infiltrano un virus che "sequestra" i dati delle vittime e li rilascia solo in cambio di un riscatto. Una fattispecie che nel 2022 e nel 2023 abbiamo più volte visto in azione nel nostro Paese.

Il primo argine di difesa, per le aziende, è la valutazione delle vulnerabilità presenti nei sistemi informatici. Fragilità che devono essere indicizzate per priorità e progressivamente mitigate, al fine di minimizzare gli impatti sull'operatività e sulla sicurezza dei dati in possesso delle imprese.

Anche in questo caso, il primo passo è culturale.

2. La Sicurezza al 100% è un'utopia

È fondamentale, infatti, comprendere che la sicurezza al 100% è un obiettivo inarrivabile. La sicurezza informatica è un processo continuo, e ogni volta che ci si avvicina a un obiettivo, questo si sposta sempre più lontano. Pertanto, le aziende devono organizzarsi per minimizzare gli effetti delle vulnerabilità dei sistemi informatici, che possono emergere nel tempo. La cooperazione tra aziende, enti di ricerca, formazione e istituzioni regolamentari può aumentare notevolmente la consapevolezza e la sicurezza del nostro "sistema" digitale.

3. La gestione manageriale della cybersecurity

La sicurezza informatica non è, dunque, solo una questione tecnologica ma richiede un approccio manageriale. È fondamentale focalizzarsi sulle priorità e redigere documenti tecnici che definiscano chiaramente i requisiti tecnici da implementare. Non bisogna cadere nella trappola di lasciarsi guidare ciecamente dai fornitori di prodotti e servizi di sicurezza informatica, ma è essenziale avere un controllo attivo e una visione strategica della propria cybersecurity.

In conclusione, la cybersecurity è diventata una priorità inderogabile per tutte le aziende, indipendentemente dalle loro dimensioni. L'Italia deve fare fronte alle sfide crescenti delle minacce informatiche e allo stesso tempo cogliere le opportunità che una gestione avanzata della cybersecurity può offrire. Solo attraverso l'investimento nella formazione, la collaborazione tra le aziende e una gestione manageriale della cybersecurity, potremo proteggere i nostri dati, le nostre operazioni e la nostra economia digitale.

4. Accrescere le professionalità

In un contesto in cui gli attacchi informatici sono sempre più sofisticati e diffusi, è essenziale investire nella professionalità nel settore della gestione dei rischi di cybersecurity. Questo investimento passa attraverso la formazione e l'acquisizione di competenze avanzate. Ma qui si apre un problema, soprattutto nell'ordine delle priorità di settori fondamentali come il manifatturiero e la piccola e media industria.

Se guardiamo agli ultimi dati diffusi dal sistema Excelsior-Unioncamere, infatti, tra settembre e novembre le imprese prevedono di assumere circa 1,4 milioni di persone. Di queste, soltanto 20mila sono tecnici informatici, esperti di telecomunicazioni e di sicurezza delle reti. Un dato che non può né deve essere sottovalutato, poiché racconta di un difetto di percezione dell'importanza di questo settore. Questione di costi e di priorità, si dirà, appunto. Ma il problema resta. Le piccole e medie imprese, infatti, sono spesso inserite all'interno di una supply chain che vede come primo anello aziende grandi e grandissime, impegnate a gestire servizi spesso strategici. La sicurezza dell'intera catena diventa dunque essenziale.

Ecco perché la miglior soluzioni per le PMI potrebbe essere quella di sviluppare forme consortili per migliorare le loro capacità di fronteggiare le minacce informatiche, provando così ad abbattere i costi e superare ostacoli oggettivi come la mancanza di risorse professionali, organizzative e tecniche necessarie.

La cybersecurity è diventata una priorità inderogabile per tutte le aziende, indipendentemente dalle loro dimensioni.

I costi inutili della compliance e della security. La necessità di un approccio maggiormente efficiente

A cura di Gabriele Faggioli

Aziende e pubbliche amministrazioni, perlomeno le più dimensionate e le più attente alle evoluzioni normative, sono ormai abituate da anni a fare i conti con la necessità di dare attuazione a normative che impongono modelli organizzativi, procedure, analisi di rischi, analisi di sicurezza, valutazione dei rischi residui, comunicazioni alle Autorità di controllo e tanti altri adempimenti che perseguono finalità assolutamente virtuose: la corretta, etica e sicura conduzione dell'attività di impresa (e delle attività pubbliche).

A fronte di un obiettivo così importante, tuttavia, è venuto il momento di fare un po' di riflessione sulla opportunità di ragionare in chiave di razionalizzazione normativa e di knowledge sharing o di economia di scala strumentale a ridurre gli sprechi.

Facciamo un esempio: migliaia di aziende, a volte centinaia di migliaia, usano gli stessi servizi esternalizzati in ambito ICT.

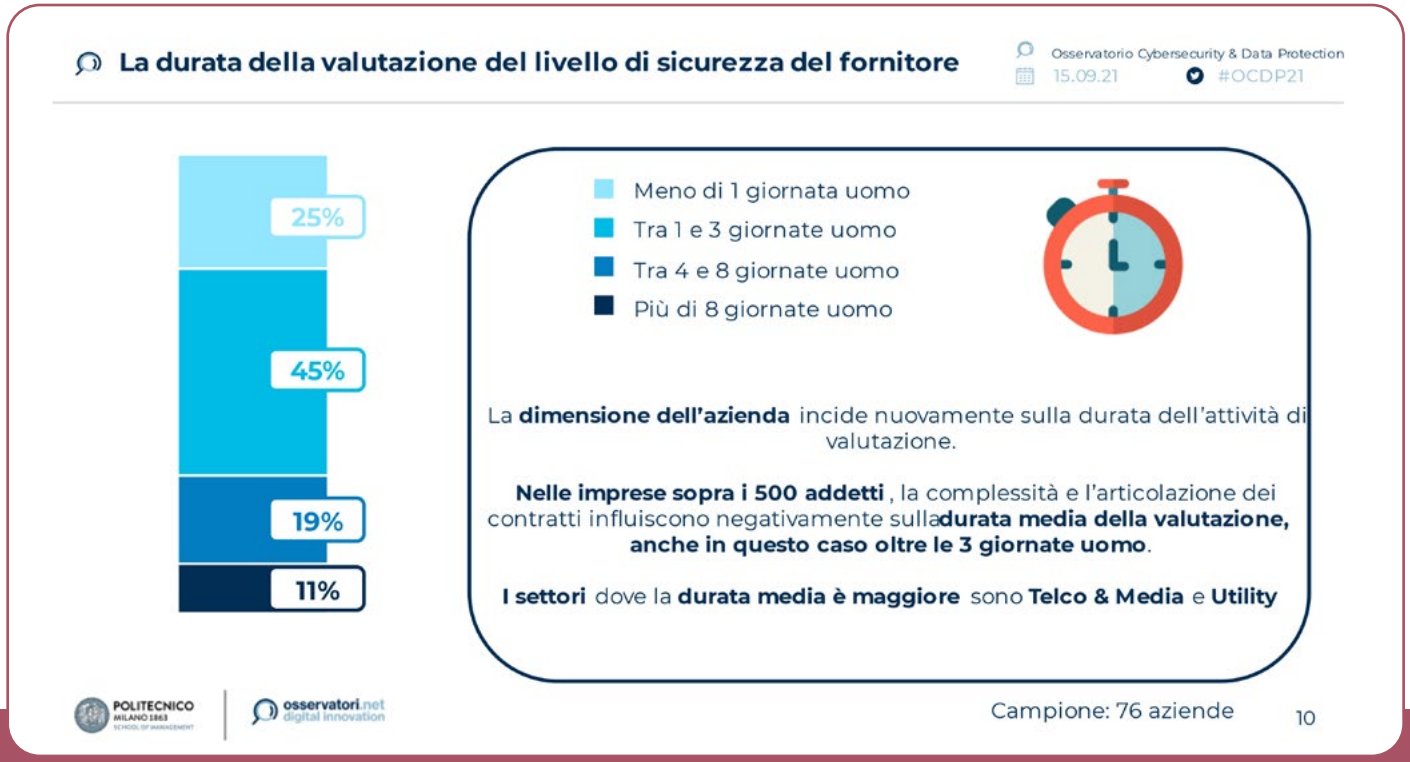
A volte interi comparti utilizzano gli stessi fornitori a cui esternalizzano le stesse attività e a tale scopo vengono usati gli stessi sistemi con le stesse misure di sicurezza.

Anche se è vero che differenti aziende possono fare diverse valutazioni di rischio sullo stesso servizio per moltissimi motivi, è pur vero che questo non vale in tantissimi casi in cui le realtà sottostanti fanno la stessa identica attività, hanno medesime dimensioni e i servizi su cui si appoggiano sono spesso commodity dove un fornitore serio, preparato e che fa gli investimenti opportuni viene in genere considerato adeguato da tutti (o quasi tutti) i clienti.

Se questo è vero, c'è da chiedersi a cosa serva moltiplicare per migliaia di volte la valutazione di un fornitore quando basterebbe, per fare un esempio, mettere a fattor comune la valutazione di una Autorità indipendente o di un cliente di riferimento per un intero settore di mercato lasciando libere le altre imprese di scegliere fra utilizzare la valutazione terza o farsela autonomamente.

Secondo una ricerca del Politecnico di Milano il numero di giornate/uomo necessario per valutare il livello di compliance normativa (data protection) di un fornitore di un servizio di cloud computing può arrivare a valere oltre 8 giornate uomo.

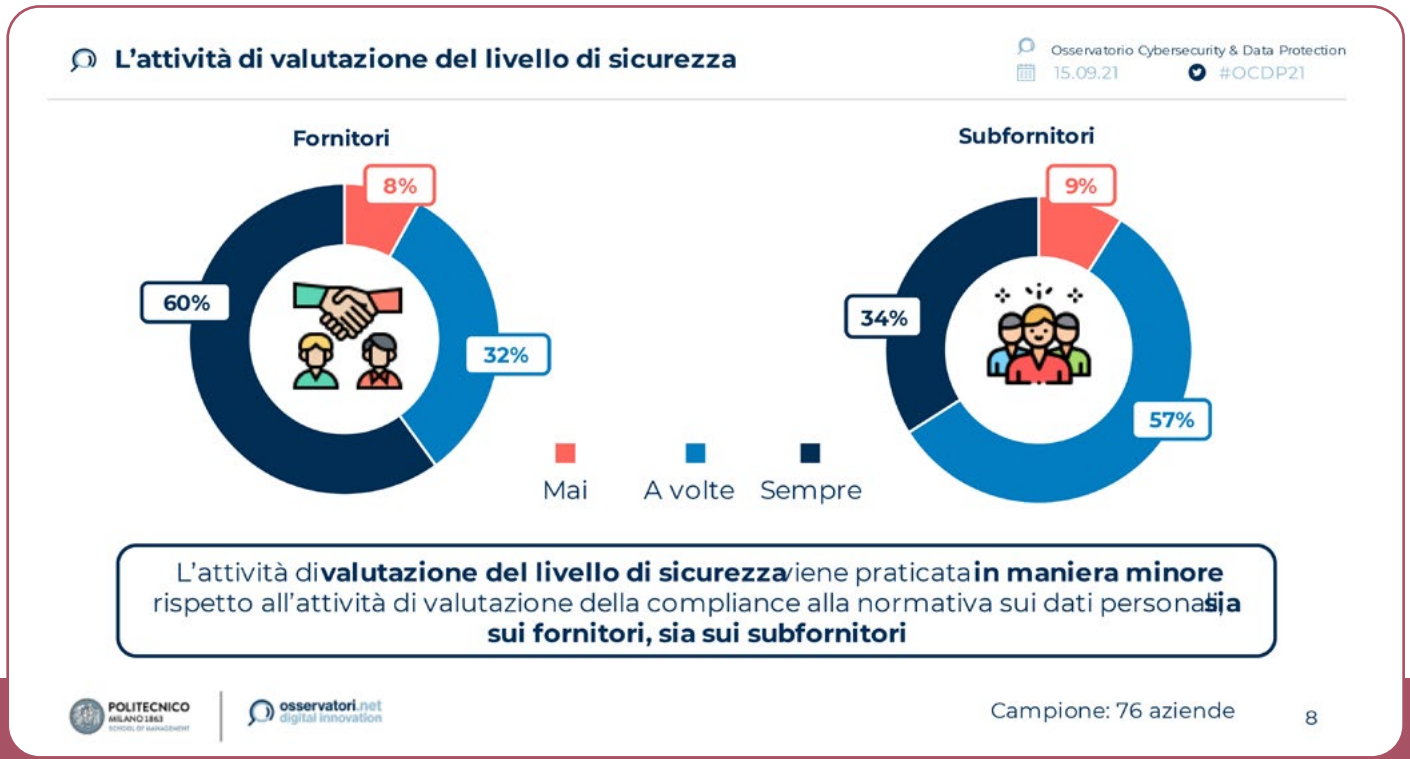
Lo stesso dicasi per la valutazione del livello di sicurezza.



In altre parole, le aziende o pubbliche amministrazioni che decidono di fare quello che devono, cioè valutare il livello di compliance normativa e di cyber-sicurezza di ogni fornitore dovrebbero investire una media di 6/8 giorni uomo, cifra da moltiplicare per il numero di fornitori!

Si tratta in tutta evidenza di un numero elevatissimo che porta a una conclusione ovvia: non tutti i clienti valutano tutti i fornitori anche per la complessità della catena di fornitura.

Come si evince dai dati del Politecnico di Milano il 40% delle aziende intervistate non valuta tutti i fornitori e addirittura il due terzi non valuta tutti si subfornitori.



È facile condannare questi comportamenti ma bisogna rendersi conto dei costi e dell'effort, in termini di giornate/uomo, che queste attività comportano.

Non tutte le aziende e pubbliche amministrazioni si possono permettere questi oneri e non tutte hanno le competenze e le risorse per adempiere agli obblighi normativi che sempre più numerosi e complessi (e a volte disomogenei) impongono sovra strutture organizzative e attività ad altissima specializzazione.

Nel caso che abbiamo fatto sarebbe quindi estremamente utile una scelta normativa radicale che permettesse a tutti i clienti di accedere a una valutazione di parte terza per evitare la moltiplicazione infinita delle stesse valutazione che spesso comportano il giungere a una stessa identica valutazioni anche solo perché un fornitore offre un servizio in una certa modalità e non accetta di modificarlo per un cliente singolo.

Ma l'esempio serve solo per comprendere un ambito dove una scelta normativa potrebbe aiutare imprese e pubbliche amministrazioni a non sprecare soldi in attività utili ma già svolte da altri, e quindi acquisibili come *know how* che diventano spreco di risorse quando impongono la replica delle stesse azioni.

Un identico discorso si potrebbe fare per gli standard, che sempre più numerosi vengono imposti alle aziende e che potrebbero essere razionalizzati o per gli obblighi di notifica alle Autorità che talvolta pretendono tempi diversi e contenuti non identici con quindi extra oneri non indifferenti.

Si deve considerare che i costi per l'aggiornamento tecnologico e la cybersecurity tenderanno a salire e solo poche imprese e pubbliche amministrazioni se li potranno permettere.

Fare economia di scala, mettere a fattor comune le conoscenze, trovare la via anche normativa per razionalizzare gli adempimenti è fondamentale sia per evitare sprechi in un'era di risorse scarse (in ogni caso sprecare risorse è sempre sbagliato), sia per indirizzare gli sforzi in direzioni produttive.

Oggi si chiede ad ogni organizzazione di aver competenze estremamente differenziate in molteplici settori della conoscenza del tutto accessori rispetto al core business, ma non è detto che questa sia la scelta migliore e, anzi, è venuto il momento di iniziare a comprendere se questo sia un modello a tendere sostenibile.

CYBER
Think Tank
ASSINTEL

Supply Chain Security: rischi e soluzioni

A cura di Sofia Scozzari

Gli attacchi alla catena di approvvigionamento rappresentano una minaccia crescente e sempre più sofisticata.

Prendendo di mira la complessa rete di relazioni tra le organizzazioni e i loro fornitori e clienti, questa tipologia di attacchi negli ultimi anni ha dimostrato con quale facilità gli aggressori possono aumentare drasticamente l'impatto di un singolo incidente avvantaggiandosi della compromissione di un'unica vittima per violare anche tutte le entità correlate.

Comprendere i rischi e le implicazioni della Supply Chain Security è quindi cruciale per mantenere ed aumentare la sicurezza e la resilienza dell'intera catena di business.

I principali rischi della Supply Chain

Gli attacchi alla Supply Chain sfruttano le relazioni di trust di un'organizzazione, che includono i partner esterni e i software di terze parti.

I principali rischi di questo ambito riguardano:

- **Data leak:** ovvero fughe di informazioni che avvengono sia a causa di attacchi esterni che interni. I cyber criminali possono utilizzare diverse tecniche, come ad esempio phishing, social engineering o lo sfruttamento di vulnerabilità pre-esistenti, per raccogliere informazioni utili a violare successivamente i sistemi. D'altra parte, anche dipendenti o manager possono divulgare informazioni sensibili, inconsapevolmente o meno, apportando un grave danno all'azienda. È importante ricordare che l'eventuale sottrazione di dati da parte di cyber criminali può implicare anche informazioni e documentazione relativa o di proprietà di clienti e fornitori.
- **Data breach:** ovvero violazioni che si verificano quando un cyber criminale o un utente malintenzionato si infiltra in un sistema informatico a cui non dovrebbe avere accesso senza autorizzazione. L'obiettivo è spesso quello di causare danni ai sistemi, attraverso l'eliminazione, la duplicazione e la corruzione dei dati, oppure di ottenere qualche tipo di vantaggio, la sottrazione di dati o la possibilità di installare del malware utile a future operazioni criminali.
- **Malware:** ovvero codice malevolo in grado di apportare danni ai sistemi informatici di un'azienda. Negli ultimi anni vengono particolarmente sfruttati i ransomware, che consentono ai cyber criminali di chiedere un riscatto per ripristinare il funzionamento dei sistemi infettati. Ma esistono ulteriori tipologie che possono mettere a rischio l'azienda, come trojan o backdoor, spyware, wiper, etc. I malware, inoltre, possono anche essere pre-installati su componenti hardware, rendendone più complicata la rilevazione.
- **Codice vulnerabile:** lo sviluppo di web application e apps si basa comunemente su numerose librerie di terze parti, e non sempre gli sviluppatori hanno una visibilità completa sul codice che finiscono per includere nelle loro applicazioni. Se una libreria di terze parti contiene vulnerabilità sfruttabili o backdoor, un cyber criminale può sfruttare questa problematica per danneggiare l'organizzazione e i suoi clienti e fornitori. Le vulnerabilità zero-day, inoltre, hanno l'aggravante di non essere ancora note ai produttori; quindi, non esistono patch o aggiornamenti in grado di mitigarle. Fino a quando i produttori non sono in grado di rilasciare appositi aggiornamenti per risolvere la situazione, i software risultano esposti alla problematica e questo può causare danni ingenti.
- **Denial of service:** se gli attaccanti lanciano un attacco DDoS (Distributed Denial of Service) contro i sistemi di un'organizzazione, questo può avere ripercussioni gravi, come l'incapacità di accedere a servizi critici, ma può anche interrompere le operazioni di clienti e fornitori.
- **Partner compromessi:** spesso le organizzazioni consentono a terze parti di accedere alle loro reti e sistemi. Se il partner in questione è stato in qualche modo compromesso, questa relazione di fiducia può essere sfruttata da un cyber criminale per ottenere un accesso fraudolento ai sistemi dell'organizzazione. Inoltre, l'organizzazione può essere messa a rischio anche nel caso in cui i fornitori utilizzino pratiche di sicurezza delle informazioni scadenti o non adeguate.

Gli incidenti più famosi

Giugno 2023 – MOVEit

Questo attacco alla Supply Chain ha preso di mira gli utenti di MOVEit, un Managed File Transfer (MFT) software di proprietà dell'azienda statunitense Progress Software. MOVEit è stato progettato per trasferire file sensibili in modo sicuro ed è particolarmente popolare negli Stati Uniti.

Gli attaccanti sono riusciti a compromettere più di 620 organizzazioni, e tra queste se ne annoverano alcune molto note come BBC, British Airways, Ernst & Young, Boots e Aer Lingus.

I dati personali identificabili (PII) che sono stati divulgati a seguito dell'attacco includono documenti di identità, indirizzi, date di nascita e numeri di assicurazione nazionale.

Da allora è stato rilasciato un aggiornamento e l'Agenzia per la Sicurezza e l'Infrastruttura Cibernetica degli Stati Uniti (CISA) ha emesso un avviso, raccomandando urgentemente agli utenti di installare l'aggiornamento per prevenire ulteriori violazioni.

Il gruppo ransomware Cl0p è stato collegato all'attacco e ha sfruttato le interfacce web esposte (EWI) di MOVEit per causare danni significativi.

Le EWI possono rappresentare un'importante minaccia per la sicurezza, in quanto, se lasciate incustodite, queste interfacce possono essere manipolate da potenziali aggressori per estrarre dati sensibili o infiltrare malware nei sistemi.

Questo incidente ha mostrato quanto rapidamente si possa fare escalation di un attacco alla Supply Chain e come anche piccoli fornitori possano avere un impatto rilevante su grandi aziende e multinazionali.

Dicembre 2021 – Log4j

Alla fine del 2021, Log4j, una logging utility basata su Java, è stata vittima di una vulnerabilità zero-day, chiamata Log4Shell, che ha messo a rischio milioni di dispositivi in tutto il mondo.

Creato dalla Apache Software Foundation, Log4j è un software open-source che registra informazioni diagnostiche sui sistemi e le comunica agli utenti e agli amministratori.

Tuttavia, nel dicembre 2021, la vulnerabilità zero-day Log4Shell ha permesso ai cyber criminali di penetrare nei sistemi, rubare dati, collezionare credenziali di accesso e installare ulteriori malware.

Poiché Log4j è utilizzato da un vasto numero di individui e organizzazioni, questo incidente ha esposto un numero straordinario di utenti e aziende al rischio di attacchi.

Tra le vittime anche il Ministero della Difesa del Belgio, che ha rivelato un attacco ai suoi sistemi a metà dicembre, e la piattaforma crypto vietnamita Onus, che utilizzava una versione vulnerabile di Log4j.

Luglio 2021 – Kaseya

Avvenuto a luglio 2021, questo attacco è stato attribuito a REvil (o Sodinokibi), un gruppo di cybercriminali con base in Russia.

REvil è un noto gruppo ransomware-as-a-service (RaaS) responsabile di numerosi attacchi di alto profilo a varie organizzazioni in tutto il mondo.

Kaseya è invece un'azienda leader nella gestione IT per MSP (Managed Service Providers) e PMI con sedi in 10 paesi. Tra le funzionalità che offre, VSA (Virtual System Administrator), uno strumento unificato di monitoraggio e gestione remota per l'amministrazione di reti ed endpoint.

Nel corso dell'incidente, REvil ha sfruttato una vulnerabilità zero-day proprio di VSA, per distribuire ransomware a numerose aziende di servizi gestiti ed ai loro clienti, causando gravi interruzioni di servizio e perdite finanziarie notevoli per le organizzazioni colpite.

Si stima che l'impatto di questo incidente abbia colpito tra le 800 e le 1.500 aziende di piccole e medie dimensioni, che potrebbero aver subito una compromissione tramite il proprio MSP.

Dicembre 2020 – SolarWinds

SolarWinds è una nota software house americana che distribuisce una soluzione per supportare le aziende nella gestione delle proprie reti, dei sistemi e delle infrastrutture informatiche.

Avvenuto a fine 2020, l'attacco a SolarWinds è stato attribuito a un gruppo di cyber criminali di alto profilo sponsorizzati dalla Russia noto come APT29 o Cozy Bear.

Si ritiene che questo gruppo sia collegato al Servizio di intelligence estera della Federazione Russa (SVR).

L'incidente ha coinvolto la compromissione del software Orion di SolarWinds, che è stato successivamente utilizzato per distribuire una backdoor maligna (SUNBURST) a numerose organizzazioni.

Tra le vittime di SolarWinds, numerose agenzie governative degli Stati Uniti e un numero ingente di aziende private.

Gli attaccanti si sono avvantaggiati di questa backdoor per accedere a dati sensibili, condurre attività di spionaggio e mantenere una presenza persistente nelle reti attaccate.

Quali soluzioni?

Come abbiamo visto, gli attacchi alla Supply Chain rappresentano una significativa minaccia per le aziende di tutte le dimensioni e settori che può avere impatti drammatici.

Comprendere la natura di questa minaccia, oltre che un approccio proattivo nella gestione dei rischi, è prioritario.

Inoltre, una serie di misure preventive e best practice è utile nel ridimensionamento degli impatti:

- **Meno è meglio:** il principio del minimo privilegio stabilisce che gli utenti, le applicazioni ed i sistemi, dovrebbero essere gestiti con gli accessi e le autorizzazioni strettamente necessarie per il loro ruolo. Ridurre l'accesso di default limita i danni che un'applicazione o un fornitore compromesso possono causare all'organizzazione. L'accesso privilegiato, soprattutto quando si ha a che fare con sistemi sensibili, dovrebbe sempre essere ridotto al minimo per limitare i rischi di compromissione. Se non è possibile evitarlo, è fondamentale che l'accesso concesso ai fornitori o ad altre parti della catena di approvvigionamento a questi sistemi, sia strettamente monitorato e controllato.
- **Implementazione di un framework di "zero trust":** questo approccio assume che ogni richiesta di accesso non sia autorizzata fino a quando le credenziali non vengano approvate. Il framework "zero trust" combina diverse tecniche per ridurre i danni di eventuali compromissioni alla catena di approvvigionamento. Con questo approccio, anche se un cyber criminale riuscisse a superare le misure di sicurezza lungo la Supply Chain, i danni che potrebbe causare sarebbero circoscritti in quanto godrebbe di autorizzazioni limitate.
- **Segmentazione della rete:** è utile per la suddivisione di una rete in più segmenti in base allo scopo e al livello di trust degli utenti che autorizzati all'accesso. La segmentazione della rete rende più difficile per un attaccante muoversi all'interno della rete aziendale senza essere rilevato.
- **DevSecOps:** questo approccio promuove l'integrazione della sicurezza nel ciclo di sviluppo. Tenendo in considerazione le minacce della sicurezza informatica fin dalla definizione del processo di sviluppo del codice, è possibile identificare potenzialmente e rimediare alle vulnerabilità della catena di approvvigionamento prima che le applicazioni raggiungano la produzione.
- **Analisi della composizione del software (SCA):** questa attività identifica automaticamente le dipendenze all'interno di un'applicazione. Eseguire l'SCA consente di mantenere una buona visibilità sull'utilizzo del codice da parte di terze parti e di monitorarlo per identificare eventuali vulnerabilità o backdoor.

- **Identificazione delle minacce:** principio che prevede la ricerca proattiva di minacce e vulnerabilità nei sistemi dell'azienda. Questa attività può contribuire non solo ad identificare e risolvere tempestivamente nuove vulnerabilità che impattano i sistemi, ma anche a riconoscere eventuali violazioni della catena di approvvigionamento.
- **Non dimenticare le minacce interne:** molte problematiche legate alla sicurezza informatica sono causate da errori umani o da una mancata consapevolezza su rischi e minacce. Spesso non si tratta di azioni di natura maliziosa ma frutto di errori o disattenzioni. Ciononostante, possono avere gravi conseguenze, sia per l'azienda che per tutta la sua catena di approvvigionamento. A questo proposito è utile associare una formazione specifica di consapevolezza sulle minacce informatiche per tutto il personale con le apposite soluzioni tecnologiche per la rilevazione delle problematiche e degli accessi fraudolenti anche all'interno dell'organizzazione, non dando per scontato che i rischi possano arrivare solo dall'esterno.
- **Aspettarsi il peggio:** è buona norma supporre che il peggio possa accadere (ed essere preparati!), piuttosto che dare per scontato che attacchi del genere avvengano solo ad altri. Presumendo che una violazione possa avvenire, è necessario mettere in atto strategie di difesa efficaci e più propense a rimanere aggiornate nei confronti di una minaccia reale.

CYBER
Think Tank
ASSINTEL

Quinto dominio. “Il nuovo spazio da conquistare”

A cura di William Nonnis

La guerra russo/ucraina sta dimostrando come la tecnologia, al nostro tempo, sia determinante a tal punto per gli esiti delle singole battaglie e dell’intero conflitto, da essere oggi l’arma più potente a disposizione delle nazioni.

Gli stessi rumor delle ultime ore, riguardo allo spegnimento della rete di comunicazioni satellitari Starlink, da parte del proprietario Elon Musk - utilizzata dagli ucraini per tentare di abbattere con i droni la flotta russa, nel mare che bagna la Crimea - per evitare il rischio di una guerra nucleare, raccontano bene l’importanza strategica dell’innovazione tecnologica.

In tale contesto, assume considerevole rilevanza il quinto dominio, vale a dire lo spazio cibernetico, rappresentante una nuova tipologia di dominio per le operazioni militari e belliche, in aggiunta ai quattro domini canonici, quelli cioè di terra, mare, aria e spazio.

A differenza del dominio spaziale, il cyberspace non ha una geo specificità, trattandosi di uno spazio virtuale in cui gli Stati più tecnologizzati svolgono un ventaglio di attività digitali, legate all’informazione e alla comunicazione, inerenti al warfare.

Si tratta quindi di una sofisiticata pratica di intelligence per la cybersecurity delle singole nazioni, ma anche per attacchi che vanno dalla manipolazione delle informazioni, alla propaganda, allo spionaggio, all’hackivismo fino al terrorismo e al sostegno dell’aggressione cinetica, quella, cioè effettivamente giocata sul campo.

Le strategie offensive che nascono dal ciberspazio, hanno una capacità dannosa che nel tempo sta aumentando la propria efficacia, per l’azione sinergica di più fattori.

Innanzitutto ciò è dovuto al fatto che le Infrastrutture Critiche di ogni Paese, intendendo con ciò la logistica della catena produttiva e distributiva alimentare; il comparto energetico; le risorse idriche; i servizi sanitari; le telecomunicazioni e il trasporto con tutta la sua rete viaria, possono essere i bersagli ideali per piegare un intero Stato, senza l’uso di una sola arma.

Inoltre, gli zettabyte di dati personali, molto spesso anche sensibili, che circolano in Rete, hanno una loro potentissima vulnerabilità, che si estende dal singolo indivi

duo alle aziende erogatrici di servizi, capace di procurare danni alla comunità, anche ingenti.

Comprendendo la nevralgica centralità che le Infrastrutture Critiche e le informazioni sensibili svolgono all’interno di uno Stato, si comprenderà anche come la sua sovranità in campo internazionale, venga riconosciuta in base alla capacità di difesa e di resilienza dagli attacchi provenienti dal Cyberspazio.

Già dal 2016 il Parlamento Europeo con il progetto per la direttiva NIS (National and Information Security), ha posto la prima pietra per una strategia legislativa in ambito di sicurezza informatica.

Con essa infatti si sono stabilite una serie di norme volte a garantire un elevato livello di sicurezza nei servizi di società delle informazioni all’interno dell’ UE, dando responsabilità di attuazione della direttiva nei singoli Paesi membri, ai rispettivi governi nazionali.

Con tale direttiva si è inteso migliorare la prevenzione e la gestione degli incidenti di sicurezza informatica (CSIRT), grazie alla presenza in ogni nazione, di squadre di pronto intervento informatico (altrimenti dette CERT), cooperanti tra loro e attive anche nel settore pri-

vato, poiché tutti i tipi di operatori di servizi essenziali e i fornitori di servizi digitali devono essere coperti da CSIRT designati.

Con il trascorrere degli anni, l'esponenziale crescita delle minacce informatiche provenienti dal cyberspazio, ha indotto a un riesame della direttiva NIS per renderla più efficace e performante, iter che si è concluso a gennaio 2023 con l'entrata in vigore della NIS2, anche se gli Stati membri avranno tempo fino ad ottobre 2024 per integrare le disposizioni nel loro diritto nazionale.

Ma non è finita, perché l'UE tenta di correre dietro all'innovazione tecnologica, con proposte di legge e progetti atti ad arginare le criticità difensive e contenere i possibili danni provenienti dal cyberspazio, che incombono ormai come minaccia costante, sia in ogni singolo Paese membro che in tutta la zona UE.

Per questo, la presidente della Commissione Ursula von der Leyen ha annunciato una proposta, già dal 2021, di un'unità congiunta per il ciberspazio a livello unitario europeo.

Tale tassello, nel quadro della cybersecurity nella'UE, costituisce un elemento cardine, per il progetto di rinforzo, su scala globale, dell'economia e del benessere sociale di tutti i cittadini europei.

Grazie alla piattaforma di Unità Congiunta per il Cyberspazio, si intende assicurare una risposta univoca e coordinata dell'Europa unita, alle crisi e agli incidenti informatici su vasta scala, così da offrire una pronta assistenza nella fase di contenimento e di ripresa da tali attacchi.

Infatti, nell'UE e nei singoli Stati membri, molti potrebbero essere i bersagli tali da provocare una crisi, in ambiti e situazioni completamente differenti, ma nonostante la contingenza del singolo caso, le tipologie di minacce sono spesso comuni.

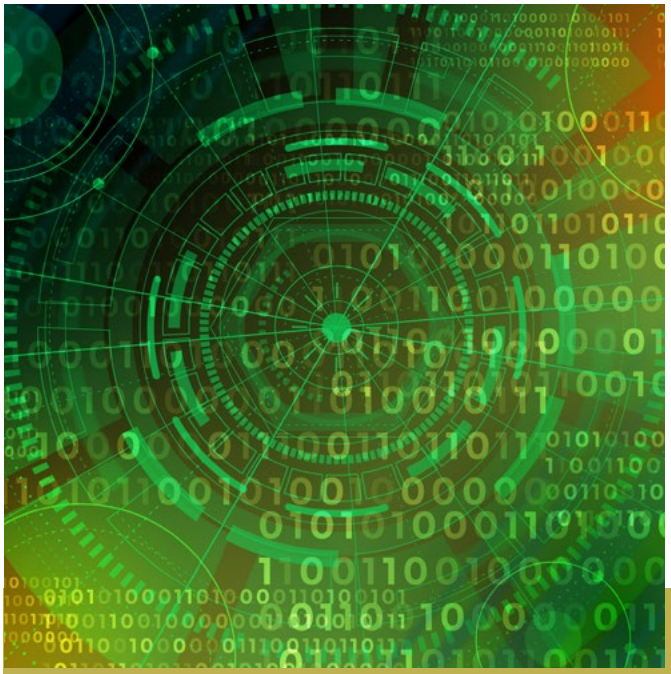
Da ciò, dunque, l'esigenza di un'unica regia per il coordinamento, la cooperazione e la condivisione di conoscenze e competenze specifiche, nonché per un piano comune di sistemi di pre-allerta.

In un'ottica ancora più vasta, anche la NATO sta lavorando alacremente, negli ultimi quindici anni, alla sicurezza cibernetica, concentrandosi, come da sua vocazione specifica, alla cyber defence, avendo ben compreso come un attacco cibernetico sia in grado di provocare danni paragonabili a quelli di un attacco armato, e quindi diventare un caso di difesa collettiva ai sensi dell'articolo 5 del Trattato di Washington.

La guerra Uomo/Macchina purtroppo è solo agli albori e, sul crinale in cui si è, chissà se la capacità umana di guidare responsabilmente e con consapevolezza la tecnologia, potrà avere la meglio sulla mastodontica macchina digitale.

La tecnologia, creata per trovare soluzioni, e quindi condurre ad un progresso largo e distribuito, foriero di benessere per tutti, sta mostrando ora l'altra faccia, quella capace con un semplice click di dichiarare guerra all'umanità.

Vedremo se l'uomo, tornando all'idea principe che ha mosso la storia della sua evoluzione, ossia di porre se stesso al centro di tutta la sua attività, sarà in grado di sottrarsi dal giogo della supremazia tecnologica che ora lo governa e, grazie ad un uso fortemente etico dello strumento digitale, di riprenderne la guida, per il beneficio dell'intera umanità.



WEBINAR

RISK 360:

come le PMI possono gestire i rischi Cyber e privacy

23 novembre

12:00- 13:00

Relatori:

Davide Giribaldi

Enzo Veiluva

Federico Brenzone

CYBER Think Tank ASSINTEL

Per info scrivi a:

segreteria@assintel.it

Governance Cybersecurity & Cloud Computing

A cura di Valentina Sapuppo

Introduzione

Il Cloud Computing è la chiave della digitalizzazione moderna ed è così importante tanto che si trova al centro della regolamentazione europea in materia di Cybersecurity nella strategia per lo sviluppo del "*Digital Europe Programme for Europe's Digital Transition and Cybersecurity*" – DEP 2023/2024.

Tuttavia, a fronte delle note difficoltà incontrate dalle aziende che hanno scelto di immettersi nella via dell'accreditamento per l'ottenimento dei finanziamenti europei, è bene fare chiarezza sull'importanza di scelte di business orientate alla Governance Cybersecurity & Cloud Computing, tenuto conto dei principali Framework presenti sul mercato internazionale.

Perché è importante orientare il business alla Governance

Al fine di sviluppare indirizzi strategici adeguati e definiti sulla base dei risultati attesi, l'Industria 4.0 deve aver chiaro in quale contesto opera, i propri obiettivi di business e quali sono le aspettative delle parti interessate. Chiaramente, non può esserci attività industriale a rischio zero e per questo, data la forte digitalizzazione dei processi e del mondo moderno, per aiutare le organizzazioni a comprendere, ridurre e comunicare, internamente e esternamente, sul rischio di sicurezza informatica, già dal 2014 il National Institute of Standard and Technology - NIST ha dato vita al CSF Core, poi aggiornato nel 2018, a cui si è ispirato anche il modello italiano.

Quest'anno, con lo scopo di chiarire come "*affrontare le sfide attuali e future della sicurezza informatica e per rendere più facile per le organizzazioni l'uso del Framework*", il framework è stato aggiornato nella sua nuova versione, il NIST Cybersecurity Framework (CSF o Framework) V. 2.0, la cui bozza è posta all'attenzione degli stakeholders, i quali dovranno fornire i propri feedback entro il 4 novembre 2023.

FONTE: *https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters*

Il nuovo CSF Versione 2.0 implementa una nuova funzione, la più importante: la *Governance*. Si prende atto, pertanto, della fondamentale importanza di "s*tabilire e monitorare la strategia, le aspettative e le politiche di gestione del rischio di sicurezza informatica dell'Organizzazione*", prima ancora di attivare i controlli delle classiche funzioni Identify, *Protect, Detect, Respond* e *Recover*.

Nella funzione di governo del rischio cyber, "*che copre il modo in cui un'organizzazione può prendere ed eseguire le proprie decisioni interne per sostenere la sua strategia di sicurezza informatica*", il NIST dimostra di implementare la già nota struttura dei framework internazionali ISO/IEC, poiché scandaglia minuziosamente i punti dell'HLS – *Hight Level Structure*, ossia contesto, gestione del rischio di Business e della Supply Chain, ruoli e responsabilità, politiche, processi, procedure e controlli. La nuova versione, che definisce inoltre i modelli di *Shared Responsibility Model* da tenere a mente per la sottoscrizione dei contratti di servizi con i fornitori di servizi Cloud, si applica a tutti i tipi di ambienti tecnologici, dai sistemi di Intelligenza Artificiale - IA a quelli strutturati in Cloud Computing. La Governance Cloud Computing, infatti, è presente in tutte le funzioni del CSF 2.0 e nei relativi controlli.

Tuttavia, è necessario fare un ulteriore sforzo quando si persegue l'obiettivo di *governare* il Cloud Computing. Infatti, l'Open Group ha definito i 5 principi di Governance del Cloud Computing, da adottare e applicare nell'intero il ciclo di vita del Cloud:

1. Conformità con le politiche e gli standard: gli standard cloud dovrebbero essere aperti, coerenti e complementari agli standard prevalenti nel settore e adottati dall'azienda.

2. Gli obiettivi aziendali devono guidare la strategia del cloud: la strategia del cloud aziendale dovrebbe essere parte integrante della strategia aziendale e IT complessiva guidata sia dagli obiettivi "business of the business" che "business of IT" per l'azienda.

3. Contratti di collaborazione tra gli stakeholders dell'ecosistema cloud: una chiara serie di regole e accordi che definiscono l'interazione tra le parti interessate è essenziale per consentire la loro sana coesistenza all'interno dell'ecosistema cloud.

4. Aderenza ai processi di gestione del cambiamento: il cambiamento dovrebbe essere esercitato e applicato in modo coerente e standardizzato in tutti i componenti dell'ecosistema cloud dell'azienda.

5. Applicazione dei processi di vitalità per ottenere un miglioramento continuo: i processi di governance del cloud computing devono monitorare dinamicamente gli eventi che innescano miglioramenti continui.

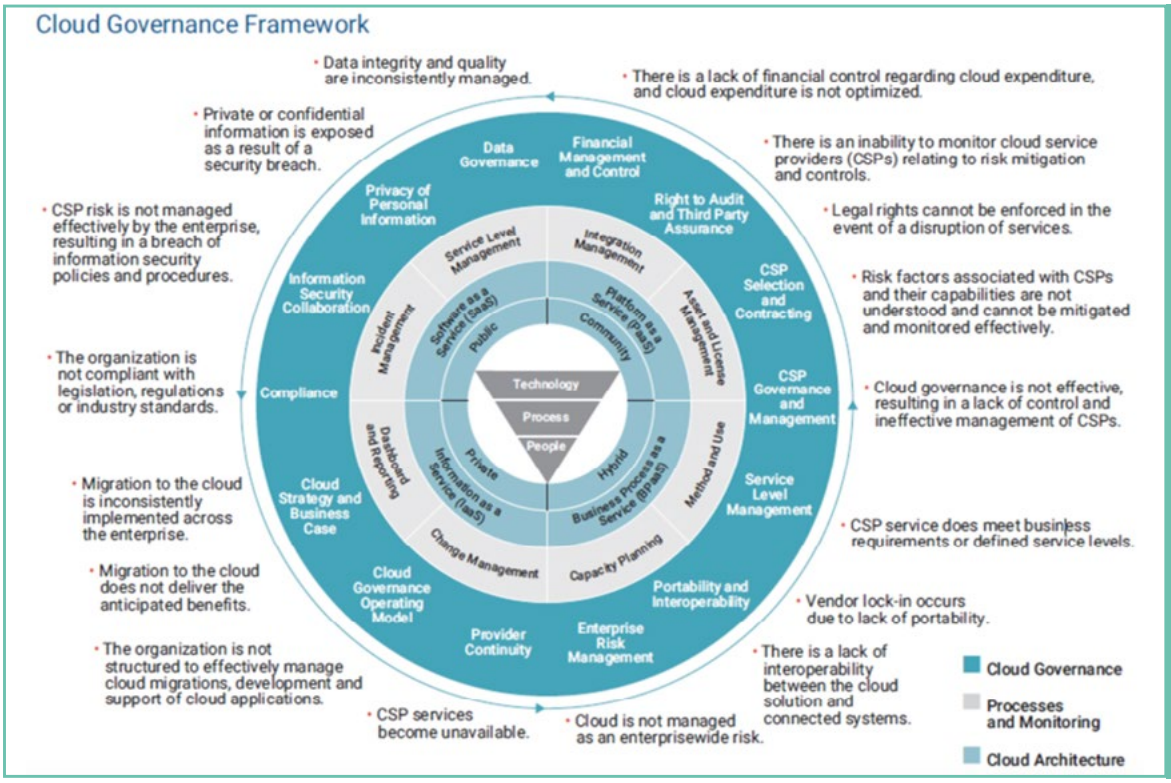
Una volta compresi, fissati e implementati tali principi, l'Industria 4.0 deve definire, quale sottoinsieme delle scelte di Business Management, un quadro di Cloud Governance in linea con gli obiettivi prefissati e i KPI della sicurezza informatica.

I Principali Framework Cloud Computing

Le Industrie 4.0 hanno la necessità di identificare e misurare qualsiasi tipologia di rischio, da quello finanziario, creditizio, legale, normativo a quello reputazionale al fine di sviluppare nuove strategie di gestione, riduzione e mitigazione del rischio.

A livello internazionale, sono già presenti diversi Framework che definiscono la Governance del Cloud Computing. Da ISACA a Cloud Security Alliance – CSA, passando per ISO/IEC, notiamo che il ventaglio di opzioni per le aziende che vogliono entrare nella *Nuvola* (o che scelgono di farne parte come Cloud Service Provider – CSP) sono diverse e la scelta, probabilmente, verte su quello che è maggiormente integrabile con eventuali certificazioni già ottenute in punto di qualità [ISO/IEC 9001:2015] e di sicurezza delle informazioni [ISO/IEC 27001: 2022].

Nel mondo ISACA la Governance è definita come "*il processo con cui un'Organizzazione assicura che esigenze, condizioni e opzioni degli stakeholder siano valutate per raggiungere obiettivi equilibrati e concordati. […] Il cloud computing influisce pesantemente sulla governance, perché introduce un nuovo modello di business, nuove tecnologie che richiedono tipi di controlli e processi sconosciuti e nuove terze parti nell'ecosistema IT.*" Infatti, il Cloud Governance Framework di ISACA traduce un ambiente interoperante con le varie componenti IT, poiché prende in considerazione situazioni di digitalizzazio-



FONTE: https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/redefining-enterprise-cloud-technology-governance

ne che comportano la migrazione dei servizi *in house* negli spazi di *storage* forniti da un CSP – *Cloud Service Provider*. Sono presenti 14 aree di Governance Cloud principali, la cui portata può mutare a seconda del tipo di servizio Cloud implementato - SaaS, IaaS o PaaS – e che sono rappresentate dal cerchio esterno dell'immagine riportata.

I cerchi più interni definiscono propriamente le varie sfumature dei processi in base al tipo di architettura Cloud scelta e, quindi, in linea con il c.d. *Shared Responsibility Model*, già ben noto al mondo di Cloud Security Alliance - CSA.

Nel mondo ISO/IEC, invece, sono due gli standard che traducono le tecniche di sicurezza per la Governance del Cloud Computing:

- ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

In questo Framework sono definite le linee guida per i controlli di sicurezza delle informazioni applicabili alla fornitura e all'uso dei servizi Cloud basati sulla SOA della ISO/IEC 27002, dimostrando come anche in questo contesto la Governance Cloud sia un di cui della Governance IT.

- ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

In questo Framework, invece, il focus è sul c.d. Cloud Pubblico e sono definiti controlli, obiettivi e linee guida che vanno ad arricchire ulteriormente i controlli della SOA della ISO/IEC 27002, in linea con le esigenze di tutela dei dati personali delle persone fisiche.

Inoltre, secondo gli esperti di Cloud Security Alliance - CSA si ritiene sia una scelta migliore occuparsi della Governance e poi delle questioni di Cybersecurity. Secondo tale inquadramento, sono forniti diversi strumenti che consentono di migliorare la Governance Cloud e dimostrare alle Industrie 4.0 di essere compliant. Tra questi, CSA offre il Consensus Assessments Initiative Questionnaire – CAIQ, il questionario di base – composto da 261 domande - per realizzare l'autovalutazione STAR Level 1, dal 20 1 combinato nella versione 4.0 con la Cloud Controls Matrix – CCM, strutturata su 197 obiettivi di controllo sviluppati in 17 domini relativi agli aspetti chiave della tecnologia cloud e che può essere utilizzato dalle aziende come strumento di self assessment sistematico. La versione 4.0 è prettamente orientata al Security Shared Responsibility Model – SSRM.

Il CSA STAR di livello 2, invece, che consente alle organizzazioni di basarsi su altre certificazioni e standard di settore per renderli specifici per il cloud, oggi è stato identificato come uno dei requisiti di sicurezza previsti per la nuova qualificazione dei servizi Cloud per la PA italiana. Infatti, la Cloud Control Matrix - CCM di CSA integrerà le caratteristiche di sicurezza del Framework Nazionale per la Cybersecurity e Data Protection, ambito di competenza dell'Agenzia per la Cybersicurezza Nazionale - ACN.

Sono diverse le attività di ricerca e sviluppo che gli esperti presenti in Cloud Security Alliance - CSA portano avanti. Tra questi, il gruppo di lavoro di sulla Governance SaaS ha proceduto a sviluppare la *SaaS Governance Best Practice for SaaS Customers*, così da definire i meccanismi per garantire la sicurezza dei dati dei clienti e la resilienza dell'infrastruttura Cloud SaaS. Ciò in quanto "*Il SaaS richiede una diversa mentalità di governance della sicurezza" anche alla luce del fatto che "a causa della forte pressione competitiva nel mercato SaaS di oggi, la sicurezza troppo spesso non è una priorità assoluta per i fornitori SaaS, specialmente per i fornitori più piccoli che potrebbero non avere le competenze di sicurezza necessarie per identificare e gestire i rischi che potrebbero avere un impatto sui clienti cloud e sulle operazioni del fornitore di cloud.*" Tutti i Cloud Service Provider – CSP che soddisfino i requisiti previsti, possono fare richiesta per essere inseriti nel CSA Trusted Cloud Providers, un registro pubblicamente accessibile armonizzato con la

Cloud Controls Matrix – CCM. Come affermato dalle parole degli esperti "*il programma STAR facilita efficacemente una migliore relazione tra i fornitori di cloud e gli utenti del cloud: questo è un aspetto unico che non può essere replicato da altri schemi di sicurezza del cloud*". Inoltre, "la certificazione CSA STAR è un framework di garanzia, che consente ai fornitori di servizi cloud di incorporare controlli di sicurezza specifici per il cloud. Il modello di maturità si concentra continuamente sull'affrontare il rischio mutevole di questa tecnologia, che si allinea con l'impegno di BSI ad aiutare i clienti a rendere l'eccellenza un'abitudine."

Conclusioni

La difficoltà di implementazione dei sistemi di Cloud Computing è data dal fatto l'Industria 4.0 deve procedere ad amalgamare tali tecnologie le già note aree di Governance IT, tenuto conto anche della la normativa vigente. Ciò in quanto l'utilizzo dei servizi di Cloud Computing, siano essi *in house* o *in pay as a service*, non garantisce automaticamente la tutela della sicurezza delle informazioni e, pertanto, sarebbe necessario sviluppare una infrastruttura che consenta ai Cloud Service Provider e ai Cloud Service Consumer – CSC di fuggire scenari di rischio - come quelli che potrebbero portare a dei Data Breach – davvero molto rischiosi anche in punto di violazione della normativa portata dal Regolamento 679/2016 – GDPR. Infatti, le Industrie 4.0 che operano nel mondo della Data Driven Economy si pongono pienamente nella qualità di titolari delle attività di trattamento di dati personali in Europa e nel mondo in tutti quei casi in cui siano esse stesse a decidere che i dati debbano essere trattati su piattaforme Cloud. Pertanto, alla luce delle nuove esigenze di Governance orientate al miglioramento continuo e all'osservanza di leggi e regolamenti, l'adozione di corrette scelte di Cloud Governance consentirà all'Industria 4.0 una migliore Data Governance e Data Quality, entro un perimetro cybersecuritario forte e resiliente. Inoltre, è necessario che ruoli e responsabilità tra il Cloud Service Provider – CSP e il Cloud Service Customer – CSC siano chiaramente definiti nei contratti di servizi – siano essi *Service life cycle management* - SLM o le *Service-level agreement* - SLA - in tal modo inquadrando già a monte una parte del rischio che dovrà essere gestito per il tramite di un Security Shared Responsibility Model – SSRM.

AI – Domande e risposte facili facili. L'AI per l'interazione con gli umani

A cura di Gianpiero Cozzolino

Iniziamo con delle definizioni, che ci aiuteranno:

- **VERO:** che rappresenta un fatto o una situazione fedelmente, tale quale è
- **REALE:** che è, che esiste veramente, effettivamente e concretamente
- **FALSO:** ciò che è falso, che non corrisponde a verità
- **IRREALE:** privo di realtà, di esistenza effettiva, che è fuori della realtà o la supera

Teniamoli in mente sempre quando ci approcciamo a materie che non bene conosciamo

Quando l'AI è diventata uno strumento di uso comune?

I sistemi che fanno uso delle tecniche di intelligenza artificiale, la più comune delle quali è l'apprendimento, sono entrati nelle nostre vite quando la potenza di calcolo necessaria ha raggiunto costi ragionevoli. Una delle prime applicazioni è stata quella dei risponditori automatici usati soprattutto nell'ambito nel supporto agli utenti/clienti di servizi. Poi il progresso ha portato i comandi vocali, ossia la possibilità di impartire comandi ad un sistema usando la nostra voce invece di mouse, tastiera e schermi touch, "liberandoci" quindi le mani. La naturale conseguenza è stata quella dell'avvento degli assistenti digitali, appunto comandati dalla voce e che rispondono sempre con la voce, ovviamente virtuale (in termini tecnici, "sintetizzata"). Ecco, quindi, i vari "Ehi, Siri", "chiama mamma", "che temperatura c'è oggi a Roma?", e ovviamente vari scherzi come facevamo al telefono molti anni fa, più o meno riusciti...

In realtà, le capacità degli assistenti virtuali o dei risponditori automatici sono abbastanza limitate: eseguire comandi e dare risposte semplici e/o ripetitive. Ultimamente si sono affermati strumenti apparentemente più avanzati, cioè in grado di fornire risposte complesse (al momento però si usano interfacce scritte tipo chat, non vocali), o in grado di effettuare traduzioni praticamente in qualsiasi lingua.

Ma questi strumenti sono affidabili?

Il problema dell'affidabilità è strettamente legato alla quantità e qualità dei dati usati per l'apprendimento: maggiore è la quantità e la qualità, maggiore sarà anche l'affidabilità dello strumento. Per fare un esempio, le traduzioni potranno essere piuttosto affidabili per lingue molto usate e per argomenti comuni, mentre saranno inevitabilmente meno affidabili per lingue poco usate e argomenti di nicchia.

Oggi, possiamo affermare che il riconoscimento del "comando" (sia esso scritto o vocale) risulta abbastanza affidabile, mentre lo è decisamente meno la generazione della risposta. Questo accade perché i modelli linguistici non sono basati su una vera comprensione (come erroneamente viene fatto credere), ma solo su una distribuzione probabilistica dell'ordine delle parole: in pratica, vengono scelte in sequenza le parole più probabili sulla base delle distribuzioni delle parole nei testi "assimilati". Ci sono quindi ambiti (es. la matematica o i linguaggi di programmazione dove esistono regole molto precise, per cui le distribuzioni probabilistiche sono, anch'esse, molto precise e quindi il risultato è quasi deterministico) mentre ci sono altri ambiti dove non esistono regole precise, le cui distribuzioni probabilistiche sono molto ampie e i cui risultati sono sostanzialmente casuali. Risultati casuali significa, semplicemente, risposte quasi sempre imprecise o sbagliate.

Quali altri problemi possano comportare?

Ovviamente, bassa affidabilità dovrebbe corrispondere a generare una bassa fiducia in questi strumenti, ma ciò si scontra col mito che i computer hanno sempre ragione.

L'approccio che si dovrebbe usare nell'utilizzo di questi strumenti è quello guidato dal rischio (come infatti prevede la legislazione europea in via di definizione): più è elevato l'impatto sulle persone o sulla società che deriva dall'utilizzo dell'intelligenza artificiale, più restrittivi devono essere i vincoli di affidabilità imposti. Credo sia evidente a tutti come affidare il verdetto di colpevolezza o meno per un crimine, e la conseguente condanna, ad un giudice virtuale non possa che spaventare, almeno finché l'affidabilità non raggiunga almeno quella dei giudici in carne ed ossa.

Ed infatti, uno dei problemi fondamentali che ci si pone è: di chi è la responsabilità giuridica delle scelte basate sulle risposte di un sistema di intelligenza artificiale? Dell'utilizzatore? Del programmatore? Di chi ha curato l'addestramento o dei dati utilizzati? Se ritenete che questi dubbi siano inutili o esagerati, pensate al caso in cui la risposta del sistema di AI riguardi voi personalmente: "chi è Tizio?", "conviene licenziare Caio o Sempronio?", "dove abita Pinco Pallino?", e che, in caso di errore, non sappiate con chi far valere le vostre ragioni.

Un altro aspetto rilevante: siamo in grado di capire come il sistema è arrivato a dare una certa risposta invece di un'altra? Quest'ultima domanda è importante perché possiamo, è vero, affidare ad un umano il controllo della risposta, ma nei casi in cui non esiste una risposta palesemente giusta o sbagliata, tale controllo umano è a sua volta affidabile nella misura in cui è in grado di capire come il sistema abbia fornito quella risposta.

Che ne penso?

La parte linguistica del nostro cervello è sicuramente legata al nostro vocabolario, che, anche se veramente ampio non copre neanche una infinitesima parte di un qualsiasi translator, che per anni ha letto e ascoltato miliardi di persone, in tutte le lingue e dialetti del globo, basterà che queste nuove AI possano entrarne in possesso, di che volume di dati parliamo? di oltre 5000 linguaggi che di media hanno circa 500 mila parole, un paio di miliardi parole che messe insieme dalla struttura linguistica, produrranno un insieme infinito di frasi.

Cosa ne verrà fuori:

Creare nuovi concetti? Ogni parola al posto giusto, con pieno significato…

Una mono lingua globale? useremo una lingua unica con 5 miliardi di termini…

Oppure una lingua che capiranno solo fra AI? Beh!!! fra loro che possono…

Oggi non sappiamo più se dall'altra parte di una chat c'è una AI o una persona VERA e REALE, fra pochissimo tempo, oltre a risponderci testualmente le vedremo anche in carne ed ossa (4k di streaming si avvicinano tanto al nostro concetto di REALE), ci daranno supporto a tutte le nostre esigenze e ci guideranno nelle scelte della nostra vita.

La sfida: la ricerca della VERITÀ in una piena libertà di informazioni fra REALE ed IRREALE.

Affrontare le Nuove Sfide della Cyber-security: NIS2 e gli Operatori di Tele-comunicazioni

A cura di Alessio Fasano

L'avvento delle telecomunicazioni ha rivoluzionato il nostro modo di comunicare e di interagire con il mondo. Viviamo ormai in un mondo in cui oggetti e persone sono costantemente connessi, tuttavia, questa crescente dipendenza dalla connettività digitale ha portato con sé una serie di nuove sfide, tra cui la minaccia costante di attacchi informatici. Per affrontare questa crescente minaccia, l'Unione europea ha introdotto la direttiva NIS (Network and Information Systems Directive) nel 2016. Tuttavia, con il rapido sviluppo delle tecnologie e delle minacce cibernetiche, è diventato necessario un aggiornamento sostanziale, che ha portato alla creazione della versione aggiornata della direttiva, la NIS2. Il tema è articolato e sicuramente presenta delle complessità ed in questo breve articolo esamineremo la direttiva senza alcuna velleità di completezza ed esaustività, volendo però soffermarci sull'impatto che la direttiva avrà in particolare sugli operatori di telecomunicazioni.

La NIS2, ufficialmente nota come il Regolamento sulla Resilienza Digitale e di Mercato (DMRR), è la versione aggiornata e migliorata della direttiva NIS. Questa nuova normativa è stata proposta dalla Commissione Europea nel dicembre 2020 come parte della Strategia Digitale Europea. Uno degli obiettivi principali di NIS2 è rafforzare la resilienza delle infrastrutture digitali dell'Unione europea e migliorare la sua capacità di far fronte alle minacce informatiche. Vediamo nello specifico come ciò influenzerà gli operatori di telecomunicazioni.

L'Impatto di NIS2 sugli Operatori di Telecomunicazioni

1. **Allargamento del Campo di Applicazione:** la NIS2 amplia il campo di applicazione rispetto alla direttiva NIS. Oltre agli operatori di servizi essenziali (OSE), includerà anche i fornitori di servizi digitali (DSP), il che significa che molti altri operatori di telecomunicazioni rientreranno in questa categoria. Questo allargamento comporta nuove responsabilità e obblighi.
2. **Gestione del Rischio:** la NIS2 pone una maggiore enfasi sulla gestione del rischio. Gli operatori di telecomunicazioni dovranno valutare e gestire i rischi per i propri sistemi informativi e di rete in modo più efficace. Questo richiederà una valutazione continua delle minacce e una risposta rapida a potenziali violazioni.
3. **Requisiti di Notifica degli Incidenti:** la direttiva NIS2 mantiene i requisiti di notifica degli incidenti, introducendo alcune modifiche significative. Gli operatori di telecomunicazioni dovranno notificare gli incidenti entro un breve lasso di tempo e con criteri di notifica più rigorosi. Ciò pone una pressione maggiore sulla capacità di rilevare e rispondere alle violazioni in modo tempestivo.
4. **Collaborazione tra Stati Membri:** la NIS2 promuove la collaborazione tra gli Stati membri dell'UE nella gestione delle minacce informatiche. Si prevede la creazione di un Centro Europeo per la Competenza in Sicurezza Informatica (ECCC) e una Rete di Centri Nazionali di Coordinamento (CNC) per facilitare la cooperazione nell'affrontare le minacce cibernetiche transnazionali.
5. **Valutazione della Catena di Fornitura:** con l'aumento delle minacce alla catena di approvvigionamento, la direttiva NIS2 richiede agli operatori di telecomunicazioni di valutare e mitigare i rischi cibernetici nella loro catena di fornitura. Questo è fondamentale per prevenire attacchi alla catena di approvvigionamento che potrebbero comprometterne la sicurezza.

Affrontare le Sfide e Sfruttare le Opportunità

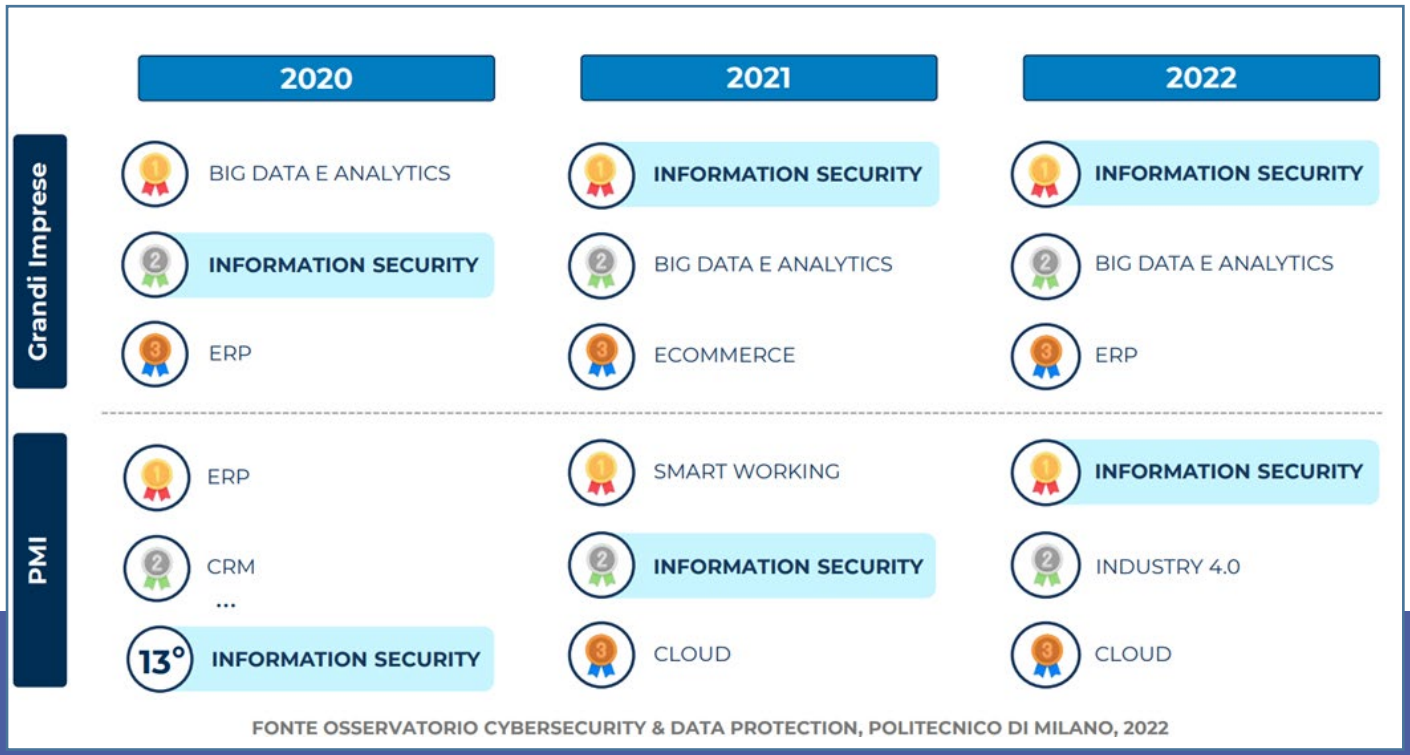
Sebbene la NIS2 rappresenti una sfida per gli operatori di telecomunicazioni, richiedendo ulteriori importanti investimenti per la sua attuazione, offre anche significative opportunità:

1. **Miglioramento della Sicurezza:** l'adozione delle pratiche di gestione del rischio e delle misure di sicurezza richieste dalla NIS2 migliorerà la sicurezza delle reti e dei dati dei clienti, aumentando la fiducia nei servizi offerti e consolidando le relazioni commerciali
2. **Conformità Normativa:** gli operatori di telecomunicazioni che si conformeranno alla NIS2 dimostreranno il loro impegno verso la sicurezza cibernetica, il che risulterà un vantaggio competitivo ed un fattore abilitante per vincere le grandi sfide di mercato ed offrire servizi alla Pubblica Amministrazione.
3. **Collaborazione:** la cooperazione tra operatori di telecomunicazioni, autorità di regolamentazione e altri attori del settore può porterà ad una migliore condivisione delle informazioni e delle best practice da utilizzare nelle politiche di difesa cibernetica.

Se già per le grandi imprese, gli investimenti per l'Information Security, sono ormai ai primi posti di spesa, l'allargamento della NIS2 consoliderà questa tendenza anche nelle PMI, che rientreranno nella catena di approvvigionamento delle big company.

È evidente che la NIS2 rappresenterà una tappa importante nell'evoluzione della normativa sulla sicurezza informatica in Europa e gli operatori di telecomunicazioni dovranno adeguarsi ai nuovi obblighi e alle nuove sfide, cogliendo l'opportunità di migliorare la sicurezza delle loro infrastrutture e dei dati dei clienti. La cooperazione tra operatori, autorità di regolamentazione e altri soggetti sarà essenziale per affrontare le minacce informatiche in modo sempre più efficace.

In questo mondo sempre più connesso, la sicurezza delle telecomunicazioni è fondamentale per proteggere l'infrastruttura digitale e la privacy dei cittadini europei. Le nostre aziende, in particolare gli operatori di telecomunicazioni, sono quotidianamente in prima linea per vincere questa che ormai è chiaro a tutti essere una battaglia cibernetica.



**fonte: Rapporto sulla filiera delle Telecomunicazioni in Italia – Edizione 202 – Asstel*

Terrorismo e tecnologia: i nuovi strumenti di attacco. Dalla comunicazione alla (dis)informazione

A cura di Marco Santarelli

Secondo il report Digital 2023 di We Are Social, 5.16 miliardi di persone, ossia oltre il 64% della popolazione globale, hanno oggi accesso a Internet, il 2% in più rispetto al 2022. Di questi, almeno 4.76 miliardi sono anche utenti social, ossia il 3% in più rispetto alla precedente rilevazione. Dall'avvento di Facebook e delle altre piattaforme social che si sono susseguite in questi ultimi anni, ci sono stati diversi cambiamenti che hanno riguardato aspetto, regole e modalità di utilizzo. Anche se il primo social network in assoluto è stato ufficialmente Six Degrees, lanciato in USA nel 1997 per creare profili, elencare i propri amici e navigare in questi elenchi, è la piattaforma firmata da Mark Zuckenberg nel 2004 quella considerata la prima a raggiungere una posizione dominante rispetto alle altre. Nati per comunicare tra utenti, i social network hanno poi man mano sostituito, o almeno ci stanno provando, i mass media consolidati come televisione, radio e stampa cartacea. Basti pensare a TikTok, piattaforma figlia della cinese ByteDance e basata sulla condivisione di video, che nel 2022 ha ricevuto più visite addirittura di Google e i cui video sono stati più guardati a livello di numero di minuti rispetto a quelli di YouTube. Questo esempio dimostra che i social network si stanno trasformando, se non lo hanno già fatto, nel punto di riferimento, oltre che per la comunicazione, anche per l'informazione globale a tutto tondo. Informazione, che, purtroppo, spesso si converte in disinformazione e nelle cosiddette fake news sfruttate per diffondere notizie false con obiettivi malevoli e pericolosi o che viene sfruttata per l'organizzazione di azioni criminali terroristiche.

Nel frattempo, si sta facendo strada anche un altro tipo di attacco, quello attraverso i droni, probabilmente tra le armi più preoccupanti del futuro, insieme agli attacchi batteriologici.

I divieti social nel mondo

Sono diversi i casi nel mondo di paesi che hanno deciso negli ultimi tempi di vietare l'utilizzo di determinati social media per le preoccupazioni legate alla disinformazione e all'impatto negativo sulla giovane popolazione. Ultimo tra tutti la Somalia, che ha bandito a fine agosto TikTok e Telegram, insieme al sito di scommesse online 1XBet, dichiarando, tramite il MOCT, Ministero delle Comunicazioni e della Tecnologia, di lavorare per preservare la cultura della società somala, dato che sono i dispositivi di telecomunicazione e internet a influenzare gli stili di vita e a favorire le cattive abitudini. L'annuncio del MOCT recita così: "Si è ritenuto importante chiudere TikTok, Telegram e le attrezzature da gioco 1XBet, che hanno avuto un impatto sui giovani somali, causando la morte di alcuni di loro […] Il ministro delle comunicazioni ordina alle aziende Internet di fermare le applicazioni sopra menzionate, che terroristi e gruppi immorali utilizzano per diffondere immagini orribili costanti e disinformazione al pubblico". Il divieto di utilizzare queste app potrebbe essere legato anche all'adozione di criptovalute nel Paese, come in altri paesi africani, ma molte giurisdizioni globali ritengono che le criptovalute siano associate a rischi di finanziamento del terrorismo.

Anche l'Iran aveva bannato Telegram, ora riammesso, per timori sulla sicurezza e sui dati personali dei suoi utenti, così come il Brasile l'ha temporaneamente sospeso mesi fa a causa di un'indagine in corso su un gruppo di neonazisti che incitavano attacchi scolastici. E prima ancora, per citarne alcuni, la Danimarca con un divieto per ragioni di cybersicurezza, l'Olanda, che ne aveva sconsigliato l'utilizzo, la maggior parte dei paesi USA, Canada, India, Afghanistan, mentre Pakistan, Bangladesh, Indonesia, Armenia e Azerbaijan hanno sospeso temporaneamente l'app per controlli su contenuti non graditi ai governi.

Il terrorismo dal basso: l'esempio Telegram

Fondato da Nikolaj e Pavel Durov dieci anni fa, Telegram è subito diventata, come molti pensano, un'alternativa più sicura a WhatsApp, soprattutto grazie al fatto che utilizza un sistema di crittografia per proteggere la privacy dei messaggi. Si aggiunge anche la quasi totale assenza di censura, di controlli e soprattutto di collaborazione con le autorità, motivi che lo hanno reso celebre tra i gruppi e le persone malintenzionate. Infatti, i servizi di Telegram di messaggistica istantanea e broadcasting sono basati su un cloud erogato dalla società Telegram LLC, con sede a Dubai. Non è possibile, quindi, rivolgere richieste alla società in assenza di rogatoria internazionale.

I fratelli fondatori di Telegram, che hanno fondato un popolare social network russo, VKontakte, hanno lanciato poi questa piattaforma nel periodo in cui gli alleati del Cremlino hanno preso il controllo di Vkontakte. Pavel Durov ha dichiarato nel 2014 al New York Times che Telegram è stato concepito dal desiderio di avere una piattaforma di comunicazione libera e sicura fuori dalle mani dello Stato russo. Infatti, l'applicazione è stata fondamentale, ad esempio, in nazioni come la Bielorussia, in cui è stata sfruttata per le proteste per le elezioni del 2020 e come la Cina per le manifestazioni del lockdown dovuto al Covid-19.

Rispetto ad altre piattaforme apparentemente più utilizzate, come Whatsapp perché con un numero maggiore di utenti, 2 miliardi al mese rispetto ai 700 milioni di Telegram, quest'ultima è, però, la piattaforma favorita, come già anticipato, da attivisti, truffatori di cryptovalute, spacciatori, terroristi, estremisti, cospirazionisti. Gratuita e leggera come le altre app di messaggistica, Telegram promette un sistema di alta privacy e anticensura e, pertanto, finisce nelle mani di determinate categorie di utenti. Molto spesso, l'unico modo per ottenere informazioni è infiltrarsi nei gruppi e monitorare dall'interno le informazioni e i dati scambiati. Avere il servizio in cloud significa anche che tutte le conversazioni e gli allegati multimediali vengono salvati online e sono accessibili da qualsiasi dispositivo da cui effettuiamo l'accesso; in più, non impatta sulla memoria interna del nostro dispositivo. È anche possibile creare chat segrete, in cui le conversazioni si autodistruggono.

La forza di Telegram, al di là della classica crittografia end-to-end, che protegge i messaggi da qualsiasi parte esterna che voglia accedervi e che troviamo anche in altre piattaforme, è che permette anche agli utenti deplorati altrove di avere voce e crearsi un pubblico di sostenitori, con una moderazione dei contenuti non vincolante, eccetto per quelli di pornografia illegale ed espliciti appelli pubblici alla violenza. In più, Telegram, rispetto alle altre piattaforme, funziona maggiormente ad invito in canali specifici, cosa che rende più complicato l'accesso ad accademici, giornalisti o forze dell'ordine in generale. Solo per il mercato grigio delle pillole abortive su Telegram sono stati trovati 200 canali pubblici contenenti 47.000 messaggi, ma, proprio per il funzionamento a invito della piattaforma, è stato quasi impossibile risalire a chi vendeva prodotti farmaceutici legittimi e quali organizzazioni erano prestanome o truffe.

Per contrastare la diffusione di materiale estremista, Telegram sta collaborando con Etidal, il Centro globale per la lotta all'ideologia estremista, e di recente è stata effettuata la rimozione di 7 milioni di post e messaggi e la chiusura di 1.500 canali, per un totale di 28 milioni di canali estremisti chiusi da febbraio 2022. Un esempio eclatante di quanto il fenomeno sia diffuso ce lo dà la giornata del 18 aprile scorso, che ha registrato un picco della diffusione di contenuti da parte di al-Qaeda di 615.000 articoli. Il fondatore Pavel Durov, che durante un'intervista nel settembre del 2015 ha ribadito che il tema della privacy su Telegram è caro alla piattaforma ed è più importante rispetto alle nostre preoccupazioni sulla sicurezza, è stato smentito solo un paio di mesi dopo a seguito dell'attentato di Parigi al Bataclan e altre zone della capitale francese, con un pesante bilancio di morti e feriti, dato che lo strumento per organizzare e coordinare le azioni terroristiche, come è emerso dalle indagini, è stato proprio Telegram.

Altra funzionalità che permette al social di facilitare la propaganda terroristica è rappresentata dai bot, che pubblicano, diffondono e rispondono in maniera automatica alle chat 24 ore su 24, garantendo a organizzazioni criminali terroristiche la copertura di propaganda di cui hanno bisogno.

Il terrorismo dall'alto: i droni

Dal 2001, anno dell'attacco alle Twin Towers di New York, che ha rappresentato un attacco all'Occidente intero, il terrorismo ha subito una vera e propria evoluzione, diventando sempre più creativo e imprevedibile e giocato su campi di battaglia "invisibili", come il web, o sopra le nostre teste, attraverso strumenti tecnologici come i droni.

I droni sono "aeromobili a pilotaggio remoto" (APR), velivoli pilotati da un computer di bordo o da un pilota che li guida da remoto con un radiocomando, anche classificati come sistemi a pilotaggio remoto (SAPR). Questi strumenti rappresentano una reale minaccia per le infrastrutture critiche, dato che possono essere utilizzati per attaccare dighe o centrali nucleari dall'alto oppure possono essere sfruttati anche per mettere in crisi i sistemi di navigazione di droni altrui, come è accaduto in passato ad alcuni Predators in volo sull'Iraq, i cui video non criptati sono stati intercettati dal gruppo ribelle Kata'ib Hezbollah, sostenuto dall'Iran.

Il primo attacco nella storia che ha utilizzato il drone come arma c'è stato il 7 ottobre 2001, giorno dell'invasione dell'Afghanistan da parte degli USA e degli alleati, che ha rovesciato il regime talebano. Il Il drone, un Predator armato, aveva come obiettivo il mullah Mohammad Omar, leader supremo del gruppo, e, sorvolando sulla provincia meridionale di Kandahar, la cosiddetta capitale dei talebani, ha invece colpito, con due missili Hellfire, un gruppo di afghani, ma non lui. Il mullah Omar è, infatti, morto per cause naturali una decina di anni dopo all'interno di un nascondiglio a poca distanza da una base tentacolare degli Stati Uniti. E nel cercare di scovarlo e ucciderlo sono state seminate tante vittime civili.

Vent'anni dopo l'attacco effettuato con i droni dagli USA contro Kabul, a seguito della ritirata ufficiale delle ultime truppe USA e della coalizione NATO dall'Afghanistan nell'agosto 2021, e la ripresa al comando delle forze talebane con a capo il leader talebano di spicco nella rete Haqqani, ala militare del gruppo, sulla cui testa gli Stati Uniti dieci anni fa avevano affisso una taglia da cinque milioni di dollari e che, tra l'altro, gli stessi USA credevano di aver ucciso tramite attacchi di droni. In questo attacco morì una famiglia di dieci civili, tra i quali un'interprete per gli Stati Uniti in Afghanistan e sette bambini. Un attacco, quindi, fallimentare, da parte dell'amministrazione Biden e non solo, visto che molto spesso, già in passato, gli attacchi da parte americana sono avvenuti in zone rurali, in cui poi era difficile svolgere le dovute verifiche. In questo caso, l'attacco era stato rivolto alla capitale afghana, su luoghi a cui tutti avevano accesso, da giornalisti a investigatori.

Oggi, i droni sono diventati alleati della resistenza ucraina contro la Russia e in particolare i droni di consumo rappresentano strumenti cruciali per osservare l'artiglieria e dirigere il fuoco verso il nemico, dopo averne individuato la posizione esatta. Lo sviluppo di questi strumenti diventati militari, soprattutto con il conflitto russo-ucraino in corso, ha subito una forte impennata negli ultimi, basti pensare che l'Ucraina, ad esempio, possiede sistemi di caccia con droni forniti di piccoli radar e veicoli aerei senza pilota, alimentati da intelligenza artificiale, della Fortem Technologies, con sede nello Utah, programmati per individuare i droni nemici, che vengono disattivati dagli UAV sparando reti contro di loro, senza che vi sia l'intervento dell'uomo. E poi Israele, paese all'avanguardia dal punto di vista tecnologico, con droni dotati di intelligenza artificiale, gli Harpy, esportati da anni e capaci di distruggere i radar e sostare al di sopra di quelli antiaerei per nove ore in attesa che si accendano, la Cina con l'elicottero senza pilota chiamato Blowfish-3, e ancora la Russia con il drone subacqueo AI a propulsione nucleare, Poseidon, ancora in fase di progettazione, e i Paesi Bassi con i loro test su un robot terrestre dotato di una mitragliatrice calibro 50.

CYBER
Think Tank
ASSINTEL

Insieme difendiam il futuro digitale!

CYBER THINK TANK ASSINTEL

Prossimo incontro

15 Novembre
Ore 14:30

Bibliografia e sitografia

1. Cognitive_Warfare_Ed.2023, Ministero della Difesa

2. Sviluppato dal Consorzio Interuniversitario Nazionale per l'Informatica (CINI) e dal Centro di Ricerca di Cyber Intelligence and Information Security (CIS) Sapienza, con il supporto del Dipartimento delle Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio dei ministri e in collaborazione, tra l'altro, con il Garante per la protezione dei dati personali (GPDP).

3. https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research

4. Regolamento UE in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno che abroga la direttiva 1999/93/CE.

5. Secondo la definizione contenuta nel CAD la firma digitale è infatti un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. Mentre secondo il regolamento eIDAS la firma elettronica qualificata è una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche.

6. In Italia AgID (Agenzia per l'Italia Digitale).

7. Così articolo 26 eIDAS

8. Che contiene le Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali. Tale decreto, in realtà, meriterebbe un corposo aggiornamento per attualizzarlo con le ultime novità di eIDAS (di cui peraltro si sta discutendo in ambito europeo per una sua nuova versione).

9. La regolamentazione AgiD di tale tipologia di firma on line è stata affidata alla determinazione n. 157/2020 del 23 marzo 2020.

10. L'art. 25 di eIDAS ricorda, infatti, che a una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate.

11. Secondo eiDAS, per firma elettronica deve intendersi qualsiasi tipologia di dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.

12. Mi permetto in proposito di consigliare la lettura di un breve articolo scritto a quattro mani con il Collega Luigi Foglia dal titolo "La FES è davvero inutilizzabile in ambito fiscale e tributario?", pubblicato su anorc.eu alla pagina: https://anorc.eu/attivita/la-fes-e-davvero-inutilizzabile-in-ambito-fiscale-e-tributario/.

CYBER MAGAZINE

Settembre - Ottobre
2023

CYBER
Think Tank
ASSINTEL

Cyber Think Tank Assintel

Contattaci:

segreteria@assintel.it
www.assintel.it