CYBER MAGAZINE

CYBER Think Tank ASSINTEL

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

Novembre 2024

Cyber Think Tank Assintel

CYBER
Think Tank
ASSINTEL

Hai idee per un mondo digitale più sicuro?

Il nostro cyber think tank ti aspetta!

Collabora, crea e proteggi insieme a noi!

Prossimo Incontro

27 Novembre

14:00 - 15:30

Per Info:
segreteria@assintel.it

CYBER THINK TANK ASSINTEL

INDICE

CYBER Think Tank ASSINTEL

WEBINAR

TPRM:

Third Party Risk Management

Dicembre 2024

12:00 - 13:00

Moderatore:

Ranieri Razzante

Relatori:

Enzo Veiluva

Federico Brenzone

Per info scrivi a:
segreteria@assintel.it

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

NOVEMBRE 2024

Carissimi lettori,

Benvenuti in questa nuova edizione del Cyber Magazine!

Apriamo le pagine di questo numero con una riflessione fondamentale, che spero vi accompagni durante la lettura e oltre: la resilienza è la chiave per affrontare le sfide del nostro tempo digitale.

Ogni giorno, affrontiamo un panorama cyber sempre più articolato, dove le minacce non solo evolvono, ma si adattano con rapidità sorprendente. Il dark web prospera come un ecosistema in perenne mutazione, l’Intelligenza Artificiale diventa tanto una risorsa quanto un’arma, e i confini tra reale e virtuale si confondono, creando un contesto di vulnerabilità diffusa.

Ma c’è un altro lato della medaglia. Proprio in questa complessità risiede la nostra opportunità di costruire qualcosa di più solido: un futuro digitale basato su valori di sicurezza, collaborazione e sostenibilità. Resilienza non significa solo saper resistere. Significa essere pronti al cambiamento, imparare dagli errori, e sviluppare strategie che anticipino il domani.

In questo numero troverete contributi preziosi per comprendere le sfide e cogliere le opportunità del mondo digitale. Dalla governance dell’Intelligenza Artificiale alla sostenibilità nella cybersecurity, fino alle implicazioni geopolitiche delle nuove tecnologie, ogni articolo è un tassello che arricchisce il mosaico della conoscenza.

Il messaggio che desidero lanciare è semplice: non possiamo permetterci di essere spettatori passivi. Il progresso digitale richiede il nostro contributo attivo. Come individui, come aziende, come sistema Paese, dobbiamo investire non solo in tecnologie avanzate, ma anche nella formazione delle persone, nel consolidamento di reti collaborative e nella costruzione di un’etica che metta al centro la protezione dell’essere umano e delle sue libertà.

Vi invito a sfogliare queste pagine con curiosità e spirito critico. Troverete spunti, analisi e proposte per affrontare con consapevolezza il presente e prepararci a un futuro che è sempre più vicino. Insieme possiamo trasformare le sfide in opportunità, perché la resilienza non è solo una qualità: è una scelta, una visione, una responsabilità condivisa.

Grazie per essere parte di questa comunità.

Buona lettura!

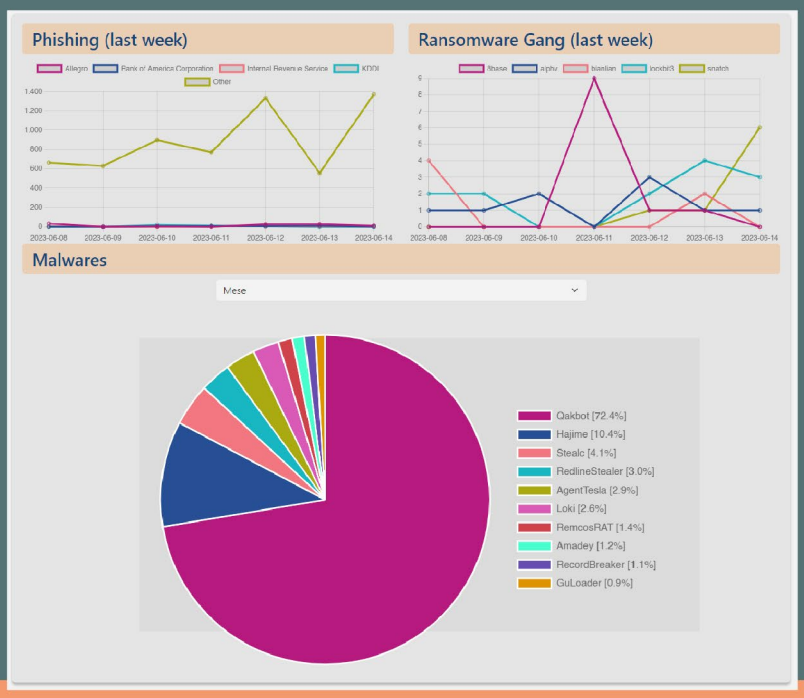
Pierguido Iezzi

CYBER Think Tank ASSINTEL

Threat Infosharing

CYBER Think Tank ASSINTEL

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



Per info scrivi a:

segreteria@assintel.it

Intervista a Padre Benanti

Quale governance per l'IA

Un'ipotesi di dialogo tra etica, scienza e tecnologia

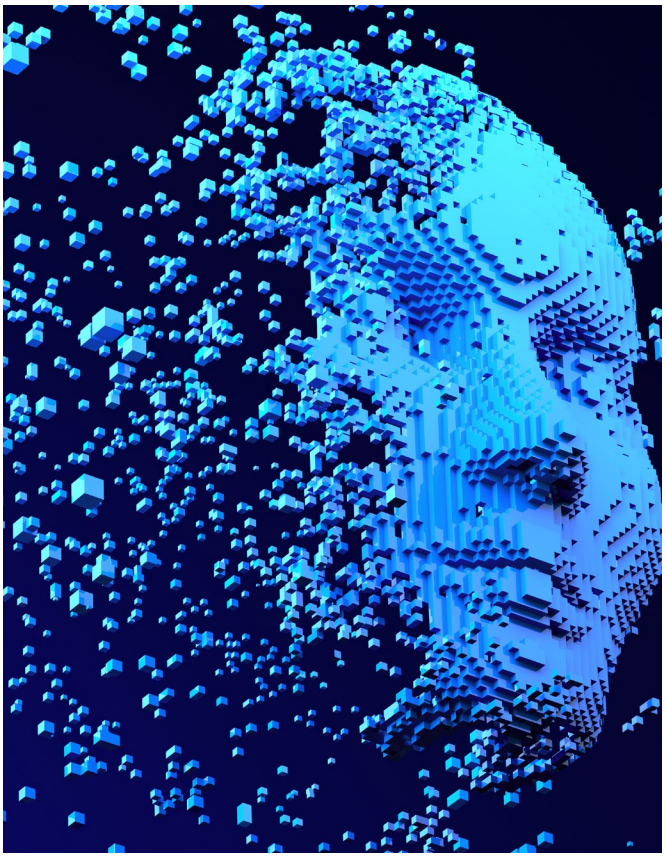
A cura di Massimiliano Cannata

Benvenuti nel post umano, dove macchine intelligenti parlano con noi e meglio di noi, dove il virtuale è una categoria dell'essere, dove viviamo la rete in una dimensione omeopatica, senza una distinzione tra dentro e fuori. Siamo all'alba di un nuovo mondo? Difficile dirlo. Neanche Colombo all'alba del 3 agosto del 1949 dopo aver allestito le tre caravelle poteva immaginare la portata della rivoluzione che avrebbe innescato. Le sue mappe geografiche erano lacunose, anche le nostre mappe cognitive lo sono. Il grande navigatore agognava la meta, sicuro che durante il percorso avrebbe aggiornato la cartografia senza farsi disorientare. La nostra condizione è la stessa, camminiamo verso l'ignoto, non sappiamo la catena di implicazioni che l'uso dei potenti strumenti del digitale comporterà, intanto stiamo andiamo. Per governare la paura, istintiva e incomprimibile possiamo solo tentare di aumentare il grado di conoscenza di cui disponiamo.

Lo sviluppo e la diffusione delle intelligenze artificiali ha cambiato il nostro modo di essere nel mondo, oltre ai nostri processi conoscitivi. La svolta non è solo di natura tecnica, ma spirituale e filosofica. Tornano di attualità grandi interrogativi che hanno segnato l'evoluzione del pensiero occidentale. Ne abbiamo parlato con Padre Paolo Benanti, teologo, specializzato in bioetica e nel rapporto tra teologia morale, bioingegneria e neuroscienze. Consigliere del Papa consulente della presidenza del Consiglio sullo sviluppo dell'IA tra le voci più ascoltate del pianeta, ha appena pubblicato insieme al filosofo Sebastiano Maffettone "Noi e la macchina", edito da Luiss University Press.

Padre Benanti di IA si parla ormai in tutti i consessi, dal G7 che ha visto per la prima volta la partecipazione di un Papa, all'Onu, il tema rimbalza sollecitando una molteplicità di letture. Il Pontefice nel documento "IA e sapienza del cuore: per una comunicazione pienamente umana" ha chiesto ai capi di governo del pianeta l'applicazione dei principi dell'etica all'intelligenza delle macchine. Da che cosa è dettata l'universalità di questo interesse che attraversa discipline, professioni, campi del sapere?

Innanzi tutto va detto che esiste, ed ha un profondo radicamento storico, una cultura ecclesiale che si pone il problema di essere fermento per la società, cercando di rispondere a una profonda domanda di senso oggi molto diffusa. Mi pare dunque legittimo, oltre che necessario, che l'impegno del Papa possa andare in questa direzione. Non dobbiamo stupirci se il tema dell'IA sta condizionando di fatto le agende dei governi e le strategie aziendali a tutti i livelli. Provo a fare un passo indietro per rispondere più compitamente alla sua sollecitazione, risalendo agli anni difficili del secondo conflitto mondiale. In quel momento sono state, infatti, poste le premesse che hanno portato a qualcosa di irripetibile: il mondo che ci circonda non è più quella di una volta. Nei celebri Bell Labs non è stata, infatti, solo ridefinita la realtà dell'informazione, perché è stato introdotto un componente essenziale il transistor, la cui diffusione massiva avrebbe cambiato per sempre la natura degli oggetti intorno a noi.



Soffermiamoci su questo passaggio cruciale. Per capirci: dobbiamo fare i conti con un "salto ontologico", che Byung-chul Han, filosofo di Seul, pensatore tra i più influenti del Pianeta, definisce in un recente saggio come il "regno delle non-cose" (ed. Einaudi ndr,)?

Significa che dovremo imparare a gestire un nuovo potere, ne parlerò in uno studio di prossima pubblicazione: il potere computazionale. La realtà è definita dal software. L'auto è l'emblema di questa trasformazione. Divenuta una commodity, non negoziamo il suo acquisto, possediamo solo la licenza d'uso. Il vecchio diritto romano associava tre attribuzioni alla proprietà degli oggetti: usus, abusus e fructus. Possiamo, una volta acquistato, usare a nostro piacimento lo smart phone, ma lo sfruttamento dei dati che convergono su quel bene, che sia un cellulare o un'auto è solo parzialmente e temporaneamente appannaggio nostro. Il cambio di prospettiva è molto profondo perché di fatto sta mutando la catena di potere all'interno del mondo.

Che cosa ha comportato e soprattutto che cosa comporterà la "transistorizzazione" della realtà?

Che la realtà è ormai definita dal software. Se in un negozio oggi per un motivo qualsiasi la connettività viene meno cambia la natura di quel luogo. Pensiamo, per fare un esempio molto familiare, a un supermercato, se privo di connessione non sarà possibile fare nessuna transazione, né verificare quello che c'è in magazzino. Se un ransomware, cosa che avviene sempre più spesso, si insinua nei sistemi IT di un ospedale, si arrestano le sale operatorie, si congelano pratiche mediche e terapie, con le conseguenze del caso. Inoltre se il è il software che definisce la realtà, quest'ultima diventa una commodity del software, colui che lo possiede definisce gli oggetti che ci troviamo di fronte.

Detto in sintesi: un software sofisticato come la IA può molto semplicemente cambiare il controllo e la percezione stessa che abbiamo del mondo che ci circonda. Non a caso si parla sempre più sovente di software defined reality.

Il software "anima del mondo"

Quella che Lei sta tratteggiando è una rivoluzione profonda che ha una duplice matrice: tecno-scientifica e filosofico- epistemologica. Per governare l'innovazione senza pregiudizi, con equilibrio razionale, con capacità di analisi Servirebbe, come ha scritto in un fortunato pamphlet di alcuni anni fa

Tòmas Maldonado l'esercizio di una "critica della ragione informatica", quale scandaglio utile per andare al fondo dei problemi, senza alimentare spettri di superficie. Siamo fronti ad affrontare la sfida?

"Non ci può essere una risposta univoca alla domanda: l'IA è un bene o un male. UnA cosa è certa: dobbiamo fare i conti con questo salto ontologico, perché questo è il territorio entro cui ci muoviamo. Siamo di fronte a un'altra specie di sapiens che abita il pianeta, ecco perché la comprensione di questa macchina diventa particolarmente impegnativa. Ma questo non deve spaventarci. Se ormai l'"anima del mondo" è data dal software, il tesoro che muove economia e società è rappresentato dai dati e dalle informazioni. Per questa ragione l'IA si è spostata dai tavoli degli ingegneri ed è arrivata a investire tutti gli ambiti strategici dell'economia e della politica. Quello che dobbiamo affrontare (mi riferisco in particolare alla nostra Europa che ha sperimentato il disastro del totalitarismo) è un nuovo inizio, una nuova età dei diritti per usare la celebre definizione di Norberto Bobbio. Bisogna, in atri termini, cominciare a maturare una coscienza giuridica, che ci permetta di proteggere l'individuo nel divenire di un eco-sistema segnato dalla tecnologia.

Siamo dentro la sfera che Stefano Rodotà definiva "corpo elettronico", dove reale e virtuale si mescolano. In questo orizzonte la persona va tutelata nel suo profilo fisico e immateriale. Lavoro improbo per i giuristi, non crede?

Non solo per loro. L'individuo deve relazionarsi con la sua estensione digitale, sempre più articolata in virtù del prepotente sviluppo delle applicazioni della tecno-scienza. Dobbiamo cercare di "addomesticare" questa nuova potente tecnologia all'interno di un sistema sociale che crede nella mediazione del potere democratico. Se vediamo il progresso normativo passi avanti ne sono stati fatti. Il GDPR è stata per esempio una grande conquista, ma siamo già oltre. La questione che si apre oggi riguarda i dati aziendali, che sono le informazioni prodotte dai processi produttivi. Nella definizione delle norme il legislatore dovrà tenere conto del mutato scenario. Bisognerà espandere l'IA ACT alla tutela integrale del consumatore, guardando agli ambiti di privatezza e alla sfera sensibile che si intreccia con la dimensione professionale che ci realizza nelle organizzazioni industriali.

La società della "sorveglianza"

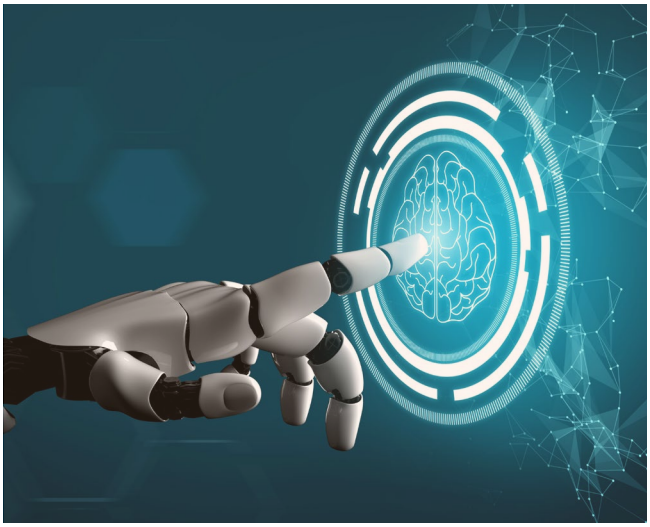
Molte aziende che appaiono molto "disinvolte" nell'utilizzazione dell'algoritmo per osservare comportamenti, mansioni e ruoli dei dipendenti. Sono aspetti della società della sorveglianza che generano paure nella collettività. E' questo il progresso che le macchine intelligenti dovrebbero garantirci?

Faccio riferimento all'"l'IA ACT per dare un risposta. La normativa vieta l'uso di meccanismi come il riconoscimento facciale per leggere lo stato emotivo della persona, ma non impone nessun alt alla possibilità di valutare la performance e il rendimento, con strumenti quali i copilot che tracciano l'efficacia efficienza di ogni attore dell'organizzazione. Si fa strada una logica nuova che attiene a una diversa concezione del lavoro, ormai focalizzato sulla performance individuale. Vacilla il "noi" per dare spazio alla predominanza dell'io, i legami di solidarietà che sostanziano l'azione del sindacato e dei corpi intermedi appaiono chiaramente slabbrati. L'intelligenza collettiva che dovrebbe sostanziare la rete, evapora in una prospettiva che, dietro il miraggio di maggiori guadagni, si preoccupa solo del destino individuale. Deriva molto pericolosa, che trova una corrispondenza inquietante nella platformizzazione del lavoro, che è un feno-

meno emergente, che rappresenta la nuova frontiera di analisi e di studio, che dovrebbe sollecitare corpi intermedi e sindacati, oltre alle istituzioni. Rispetto a tutto questo non si può rimanere inerti, mentre si staglia un orizzonte che riguarda la cultura del lavoro oltre che la difesa dei diritti che va presidiato e che impegnerà le menti più illuminate, quelle che si dimostreranno realmente capaci di uno sguardo profetico.

Etica e sviluppo tecnologico. Vorrei chiudere la nostra conversazione toccando questo delicato nesso, cui Lei faceva riferimento all'inizio. Vengono necessariamente in mente le preoccupazioni espresse negli ultimi scritti di Emanuele Severino. Si tratta di timori infondati?

Probabilmente Severino è stato troppo tranchant nella manifestazione di alcuni pareri e posizioni sull'argomento. In realtà noi sappiamo che la tecnologia non è solo cieca volontà di potenza ma anche strumento eccezionale di risposta alle domande che l'uomo si fa, da quando è apparso sulla terra, sulla realtà che ci circonda. L'uomo che nel passato si è sentito minacciato dalla realtà, ha fatto uno strumento che si chiama fucile. Quel fucile non è solo uno strumento di offesa, ma è anche uno strumento ermeneutico, che mi fa vedere il mondo diviso tra amici e nemici. Ecco che entra in gioco l'artefatto tecnologico, come risposta a una domanda sulla realtà. Solo se vedo la domanda che sta dietro l'artefatto potrò avere un rapporto etico con l'artefatto. Definire un codice etico vuol dire in conclusione proprio questo: far risuonare la domanda dal produttore al consumatore in ogni istante, affinché quella domanda non risulti soffocata con indifferenza e superficialità.



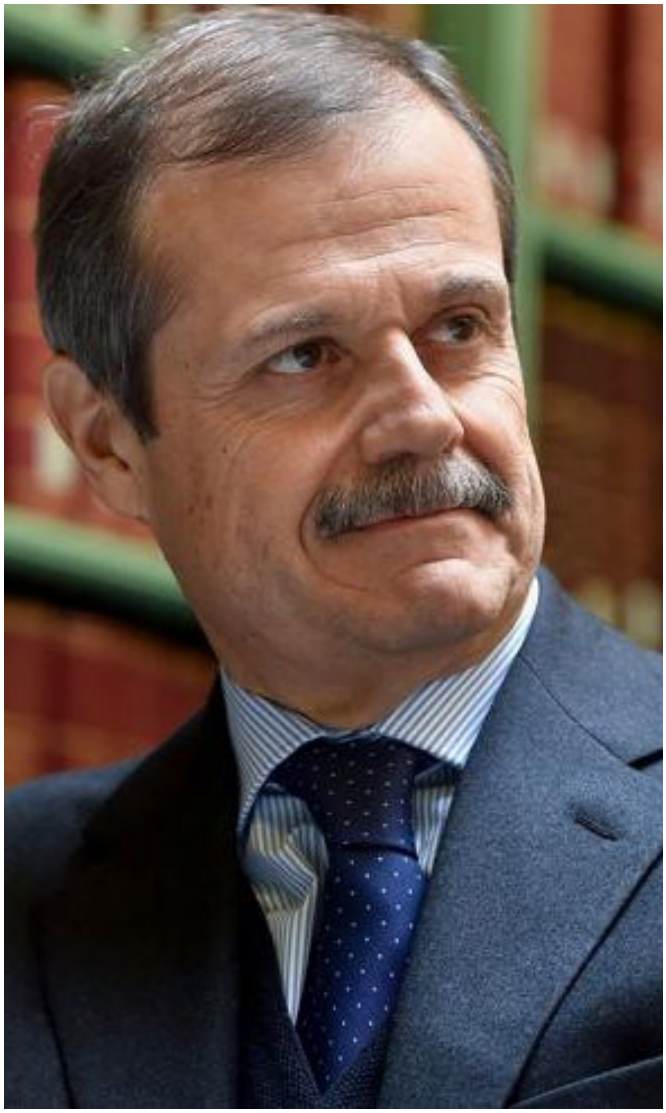
Ritorno al futuro: le nuove minacce tra tecnologia e geopolitica

*A colloquio con l'ambasciatore **Giampiero Massolo** per analizzare il mutamento delle sfide globali, dalla guerra in Ucraina all'influenza delle Big Tech, passando per il futuro dell'Europa tra autonomia strategica e cyberwarfare.*

Giampiero Massolo è un diplomatico italiano, già Segretario generale del Ministero degli Affari Esteri. Attualmente è Presidente di Mundys (ex Atlantia), ruolo che ricopre dall'aprile del 2022. In precedenza ha ricoperto per quattro anni l'incarico di Presidente di Fincantieri e di Direttore generale del Dipartimento delle informazioni e della Sicurezza (DIS). Da 2017 al 2024 è stato inoltre Presidente dell'Istituto per gli Studi di Politica Internazionale (ISPI).

Ambasciatore, negli ultimi anni ci siamo concentrati su minacce asimmetriche come il terrorismo e il cyberwarfare. Con la guerra in Ucraina e le tensioni in Medio Oriente, siamo tornati ai conflitti convenzionali. Qual è la sua opinione su questo ritorno alle minacce tradizionali?

In realtà, le minacce tradizionali non sono mai del tutto scomparse. Abbiamo creduto che la globalizzazione potesse eliminare o almeno ridimensionare i rischi legati ai confini e alla guerra convenzionale, ma gli eventi recenti, come quelli in Ucraina e in Medio Oriente, ci ricordano che queste minacce esistono ancora e sono rilevanti. Tuttavia, oggi queste minacce tradizionali si sovrappongono e coesistono con quelle asimmetriche, come il terrorismo jihadista, gli attacchi cyber, e i rischi derivanti dalla tecnologia. Ci troviamo quindi in una situazione molto più complessa. La deterrenza tradizionale – quella fondata sull'equilibrio del terrore nucleare o sulla superiorità militare convenzionale – non funziona più come in passato, poiché le minacce si sono moltiplicate e diversificate. Quello che stiamo osservando, in particolare con il conflitto in Ucraina, è che lo scontro diretto, il conflitto "classico", ha ancora un impatto devastante. Eppure, in parallelo, siamo costretti a considerare le implicazioni della guerra cyber, dell'informazione e dei nuovi equilibri geopolitici che non si basano più solamente sulla forza militare, ma anche su fattori economici e tecnologici. In questo contesto, la Cina e la Russia hanno giocato un ruolo importante nel risvegliare questo ritorno alla guerra tradizionale, pur continuando a sfruttare le armi della disinformazione e del cyberwarfare.



A proposito di Europa, cosa dovrebbe fare per affrontare questa crescente complessità nelle minacce e nelle sfide?

L'Europa deve inevitabilmente ripensare e ridefinire la propria strategia di difesa, partendo dal potenziamento delle proprie capacità industriali e tecnologiche, perché una delle lezioni principali di questi anni è che senza sovranità tecnologica e capacità produttiva, non si è in grado di difendersi o di avere un ruolo autonomo nella scena internazionale. Il contesto globale ci impone di prendere delle decisioni rapide: la rivalità tra Stati Uniti e Cina non è più soltanto economica, è anche strategica, e questo costringe l'Europa a fare delle scelte. La Cina ha un ruolo centrale nell'industria tecnologica e nelle infrastrutture energetiche e molte nazioni si trovano di fronte a un dilemma: scegliere tra tecnologia cinese, meno costosa ma più rischiosa dal punto di vista della sicurezza, e quella occidentale, che è spesso più costosa e regolamentata, ma più sicura. Ma c'è un altro problema fondamentale per l'Europa: il rapporto con gli Stati Uniti. Negli ultimi anni, la dipendenza europea dall'ombrello protettivo americano si è ridotta, ma non abbastanza da garantire una vera autonomia strategica. Per diventare un attore rilevante nel nuovo ordine globale, l'Europa deve investire nella propria difesa, nella ricerca tecnologica, e nelle infrastrutture critiche, soprattutto nel settore digitale e della produzione di semiconduttori. Solo così potrà evitare di rimanere ai margini del confronto tra le grandi potenze.

Un tema di grande attualità è la crescente influenza delle grandi aziende tecnologiche. Come vede la governance del digitale e la crescente potenza delle Big Tech?

La potenza delle grandi aziende tecnologiche è ormai una realtà globale, e gli Stati stanno cercando di trovare risposte. Da un lato, abbiamo modelli come quello cinese, in cui il governo esercita un controllo diretto e centralizzato sulle aziende tecnologiche. Dall'altro, l'Europa sta cercando di imporre regole e regolamenti per contenere e bilanciare il potere delle Big Tech. In mezzo ci sono gli Stati Uniti, che invece lasciano maggiore libertà alle grandi aziende private, permettendo loro di dominare il panorama tecnologico e digitale. Nel complesso, ci troviamo in una fase di transizione in cui gli Stati stanno perdendo sovranità in certi settori, soprattutto quello tecnologico e dei dati, e le grandi aziende stanno assumendo un ruolo sempre più centrale nella regolamentazione e gestione di infrastrutture vitali. Questi giganti non si limitano a dominare il mercato, ma controllano anche enormi quantità di dati sensibili, che possono influenzare le economie, le società, e perfino la politica. La sfida, soprattutto per l'Europa, è quella di creare un quadro normativo che protegga i cittadini e la sovranità nazionale, senza però ostacolare l'innovazione.

Per diventare un attore rilevante nel nuovo ordine globale, l'Europa deve investire nella propria difesa, nella ricerca tecnologica, e nelle infrastrutture critiche, soprattutto nel settore digitale e della produzione di semiconduttori.

Cambiando prospettiva, parlando di dinamiche economiche, come sta cambiando il rapporto tra capitale e lavoro nell'era digitale?

Stiamo assistendo a una redistribuzione del potere economico tra capitale e lavoro. Il capitale, soprattutto quello tecnologico, ha acquisito una forza enorme. Le grandi aziende tech, che operano su scala globale, generano profitti enormi con un numero relativamente limitato di lavoratori, molti dei quali altamente qualificati. Allo stes-

so tempo, il lavoro meno qualificato è sempre più vulnerabile, in quanto viene sostituito da processi automatizzati o da algoritmi. La transizione tecnologica ha quindi accelerato questa polarizzazione economica: da un lato, le élite tecnologiche e finanziarie accumulano ricchezza e potere; dall'altro, i lavoratori meno qualificati vedono ridursi le loro prospettive di carriera e di reddito. Questo squilibrio tra capitale e lavoro è una delle sfide più urgenti che dobbiamo affrontare. Non solo per ragioni di equità sociale, ma anche per la stabilità delle nostre democrazie.

Parlando di tecnologia, stiamo assistendo a progressi enormi in settori come l'Intelligenza Artificiale e il Quantum Computing. Questi sviluppi possono diventare anche armi?

Senza alcun dubbio. L'Intelligenza Artificiale, per esempio, ha il potenziale per trasformare molteplici settori, dall'economia alla sanità, migliorando la vita di milioni di persone. Ma allo stesso tempo, può essere utilizzata in ambito militare per sviluppare armi autonome, sistemi di sorveglianza avanzati, o addirittura per creare disinformazione su larga scala. Lo stesso vale per il Quantum Computing, che può rivoluzionare la crittografia, rendendo obsoleti gli attuali sistemi di sicurezza, ma potrebbe anche essere utilizzato per violare dati sensibili a livello globale. In sostanza, la tecnologia moderna è sia un bene pubblico che una potenziale minaccia. E come tutte le innovazioni, dipende da come viene utilizzata e dalle regole che vengono stabilite per controllarla. La sfida sarà quella di trovare un equilibrio tra il progresso e la sicurezza, tra la libertà di innovare e la necessità di proteggere la società dalle conseguenze negative dell'uso improprio della tecnologia.

Uno degli aspetti più discussi è il cyberwarfare. Come mai non ha avuto un ruolo decisivo nei conflitti recenti, nonostante le previsioni?

Il cyberwarfare è una minaccia costante e presente, ma non ha ancora avuto il ruolo centrale che ci si poteva aspettare. La ragione è duplice. Da un lato, ci sono stati vari attacchi cibernetici a infrastrutture critiche, che hanno causato danni economici e politici, ma non al livello di un conflitto su larga scala. Dall'altro lato, esiste un'enorme preoccupazione per il rischio di escalation. Un attacco cyber che colpisce infrastrutture critiche – ad esempio, una rete elettrica o un sistema sanitario – potrebbe scatenare una risposta imprevedibile e potenzialmente devastante. Inoltre, a differenza delle armi tradizionali, la deterrenza non funziona nel cyberspazio. Non ci sono accordi internazionali che regolino il cyberwarfare in modo efficace, e questo rende il tutto molto più pericoloso e meno prevedibile. Molti Stati preferiscono utilizzare il cyberwarfare come arma di pressione o di disturbo, piuttosto che rischiare un conflitto su larga scala. Tuttavia, non dobbiamo sottovalutare il potenziale distruttivo del cyberwarfare, che potrebbe in futuro diventare un'arma decisiva in conflitti internazionali.

Alla luce di queste considerazioni, l'Europa è pronta a fronteggiare queste minacce o è troppo dipendente da altri?

L'Europa purtroppo è ancora dipendente, soprattutto dal punto di vista tecnologico. Siamo diventati, in un certo senso, una potenza economica ma non una potenza strategica. Questo è evidente quando guardiamo alla nostra dipendenza dalle tecnologie americane o cinesi, sia nel campo dell'energia, che in quello delle telecomunicazioni o della sicurezza digitale. Abbiamo fatto molti progressi, ma c'è ancora molto da fare. Il vero problema è la mancanza di una visione comune tra i Paesi europei. Ognuno tende a perseguire i propri interessi nazionali, piuttosto che lavorare insieme per una difesa comune e una strategia tecnologica condivisa. Se l'Europa vuole davvero affrontare le sfide future, dovrà investire nella sua autonomia strategica, rafforzando le proprie capacità nel settore della difesa, della ricerca scientifica e dell'innovazione tecnologica. Altrimenti, rischiamo di diventare sempre più irrilevanti nello scenario globale.

CYBER
Think Tank
ASSINTEL

LA CYBER PER TUTTI

ISTRUZIONI SEMPLICI PER QUESTIONI COMPLESSE

CYBER Think Tank ASSINTEL

ASSINTEL ASSOCIAZIONE NAZIONALE IMPRESE ICT

Consigli per creare una password "inviolabile"

Con l'accrescersi delle violazioni dei dati e degli attacchi di ingegneria sociale, una ***password sicura*** è la prima linea di difesa.

1 Non usare informazioni personali

2 Usare caratteri speciali

3 Usare almeno 12 caratteri

4 Usare password differenti per differenti account

5 Cambiare password regolarmente (almeno ogni 90 giorni)

6 Non condividere le password e non scriverle su POST-IT

7 Abilitare, se possibile, l'autenticazione a due fattori

8 Disabilitare "Ricordare Password?" sui motori di ricerca

9 Evitare frasi di senso compiuto o ad uso comune

10 Non memorizzare password nel browser

Queste password possono essere craccate in 0.00 secondi per cui affrettiamoci a cambiarle!

123456	Password
Ciao	1111111

Qui per restare: come il dark web continua a prosperare

A cura di Pierguido Iezzi

Anche se molti ne hanno annunciato la fine, il dark web non solo è ancora vivo, ma si evolve in un pericolo sempre più complesso. Nel primo semestre del 2024, il cybercrime ha raggiunto livelli allarmanti: quasi un milione di avvisi di compromissione dati sono stati inviati, segnando un incremento del 10% rispetto ai sei mesi precedenti. Dietro le quinte di internet, nel cuore di queste reti oscure, si accumulano dati e vulnerabilità che i criminali digitali sfruttano con precisione chirurgica. L'Italia, posizionata al quinto posto per furto di e-mail e password e al settimo per esposizione di indirizzi e-mail, non è estranea a questo fenomeno: il 36,8% degli italiani ha ricevuto un alert per la sottrazione dei propri dati.

Mentre la percezione del dark web può variare tra un immaginario di rischio e mistero, in realtà rappresenta un sistema molto più strutturato e devastante. Si stima che entro il 2028 questo mercato nero raggiungerà un valore di 1,3 miliardi di dollari, crescendo a un tasso annuo del 22,3%. Questo ecosistema è attivo e in continua espansione, con Tor che ospita circa 30.000 siti e oltre 2,5 milioni di visitatori stimati al giorno. Si tratta di una rete di interazioni illecite, dove beni e servizi proibiti alimentano un'economia clandestina che non accenna a ridursi. Il dark web, infatti, si è rivelato un ambiente resiliente e "adattivo": gli sforzi per smantellarlo spesso portano a un rafforzamento dei suoi meccanismi di difesa e anonimato. Ogni chiusura di un mercato porta all'apertura di una nuova piattaforma, più sicura e più difficile da rintracciare. Al suo interno, i dati personali sono la merce più preziosa: pacchetti completi che includono e-mail, indirizzi, numeri di telefono e informazioni bancarie consentono di orchestrare frodi mirate. È proprio l'abbondanza di queste informazioni dettagliate che ha permesso ai cybercriminali di affinare le loro tecniche, rendendo gli attacchi sempre più sofisticati.

Carding e Identity Leak: il boom delle credenziali compromesse

Tra le attività più redditizie del dark web c'è il carding, ossia il commercio di carte di credito rubate. A seguito di attacchi e furti sistematici, milioni di numeri di carte finiscono nelle mani di criminali. Queste carte, vendute a prezzi che oscillano tra 7 e 15 dollari, vengono acquistate da soggetti che, a loro volta, le utilizzano per clonazioni o spese fraudolente. L'impatto della vendita di carte di credito si avverte a più livelli. Da una parte, gli utenti devono far fronte a un furto che spesso si traduce in danni economici rilevanti. Dall'altra, le aziende e i gestori di sistemi di pagamento devono confrontarsi con un problema sempre più strutturale, investendo risorse ingenti per contenere la minaccia.

Phishing e Malware-as-a-Service

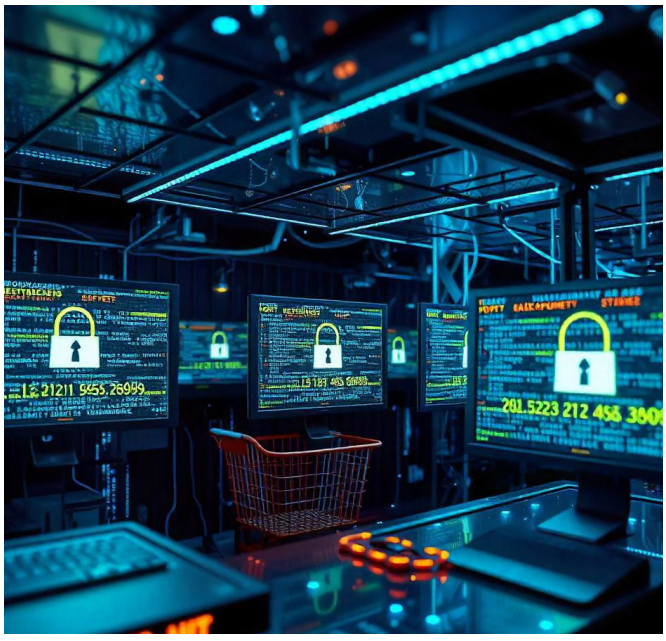
Un altro settore in espansione è il malware-as-a-service. Qui, criminali di diverso livello di competenza possono acquistare kit pronti all'uso per lanciare attacchi in maniera autonoma. Strumenti di phishing e malware come i famigerati zero-click exploit permettono di compromettere i dispositivi senza bisogno di interazione della vittima: basta un messaggio, ed è già troppo tardi. Tra i malware di punta, troviamo Psoglav, ransomware che opera senza connessione internet, rendendo difficile il suo rilevamento. Questi malware vengono distribuiti anche in modalità ransomware-as-a-service (RaaS), un modello che permette ai meno esperti di noleggiare strumenti di attacco, pagando i creatori con una percentuale del riscatto ottenuto. Ogni attacco che va a segno finanzia nuovi sviluppi e un'ulteriore diffusione del ransomware, con un circolo vizioso che crea una minaccia pervasiva e particolarmente difficile da arginare.

Futuro e strategie di difesa

La sopravvivenza del dark web e la sua trasformazione in un mercato iper-specializzato e globale dimostrano quanto sia necessario un approccio integrato alla sicurezza digitale. La sola tecnologia, per quanto avanzata, non può garantire la protezione necessaria. La resilienza del dark web e l'astuzia dei suoi utilizzatori richiedono una combinazione di misure di difesa proattive, controllo costante dei dati e una formazione che coinvolga anche il singolo utente.

In futuro, la crescita del dark web sarà probabilmente accompagnata dall'aumento delle normative internazionali volte a contrastare questi fenomeni. Tuttavia, il fattore umano, che da solo è responsabile del 90% degli attacchi informatici, resta una delle vulnerabilità più difficili da risolvere. La conoscenza delle tecniche di attacco e l'adozione di sistemi di autenticazione avanzati sono le basi di una difesa efficace. Il dark web non è mai stato così potente: dai market di identità rubate ai ransomware su larga scala, fino agli exploit zero-day, la rete oscura rappresenta oggi una minaccia in continua evoluzione. Con milioni di visitatori giornalieri e un'ampia gamma di servizi disponibili, sembra improbabile che questa economia illegale possa essere smantellata in tempi brevi.

menti principali per chi vuole tutelarsi: senza un'adeguata conoscenza del rischio, gli attacchi continueranno a colpire, trovando nella negligenza delle vittime il loro punto di forza.



"Il dark web rappresenta oggi una minaccia in continua evoluzione: dai market di identità rubate ai ransomware su larga scala".

Fatturazione elettronica: la chiave per l'armonizzazione digitale e la sicurezza economica in Europa

A cura di Danilo Cattaneo

In Italia, la fatturazione elettronica è diventata obbligatoria per la Pubblica Amministrazione in due fasi: dal 6 giugno 2014 per le amministrazioni centrali e dal 31 marzo 2015 per quelle locali. Dal 1° gennaio 2019, l'obbligo è stato esteso anche alle transazioni tra aziende (B2B), posizionando l'Italia ai vertici europei nell'adozione di questo strumento digitale. Il Sistema di Interscambio (SdI) gestisce circa 260 milioni di fatture all'anno tra privati e Pubbliche Amministrazioni.

L'introduzione obbligatoria della fatturazione elettronica in Italia ha generato rilevanti vantaggi economici e operativi. Secondo l'Osservatorio del Politecnico di Milano, nel primo anno di obbligo sono state trasmesse 2,09 miliardi di fatture elettroniche, coinvolgendo 3,9 milioni di imprese. Questo ha permesso di identificare e bloccare falsi crediti IVA per un valore di 945 milioni di euro, con un incremento del 3,6% nei versamenti IVA rispetto all'anno precedente. La digitalizzazione delle fatture ha migliorato l'efficienza, riducendo tempi e costi di gestione, migliorando la qualità dei processi aziendali e facilitando lo sviluppo dell'eCommerce B2B, che ha raggiunto un valore di 410 miliardi di euro, pari al 19% del fatturato complessivo tra imprese.

Questi risultati dimostrano che la fatturazione elettronica è uno strumento cruciale per contrastare l'evasione fiscale e rafforzare la sicurezza economica del Paese. Inoltre, ha imposto anche alle Partite IVA con fatturati inferiori a 25.000 euro l'adozione del sistema digitale, con l'unica eccezione dei medici, per ragioni di privacy.

Nonostante l'alta adozione della fatturazione elettronica, il livello di digitalizzazione complessivo delle imprese italiane rimane moderato. Secondo il Digital Economy and Society Index (DESI) della Commissione Europea, l'Italia si posiziona al decimo posto per l'adozione di tecnologie digitali da parte delle PMI, con il 60,70% delle aziende che utilizza strumenti digitali quotidianamente. Al vertice della classifica si trovano Finlandia, Svezia e Paesi Bassi.

La fatturazione elettronica rappresenta una leva fondamentale per la digitalizzazione delle PMI, ma la sua trasformazione in una pratica consolidata richiede una maggiore consapevolezza e maturità tecnologica da par-

te del management aziendale. La normativa, da sola, non è sufficiente a generare un cambiamento duraturo.

A livello europeo, la Commissione Europea ha promosso varie iniziative per rendere la fatturazione elettronica uno standard nelle transazioni commerciali, ma il quadro normativo rimane eterogeneo. In Spagna, la normativa definitiva è attesa per il 2026, in Francia l'obbligo scatterà a fine 2026, mentre in Germania sarà operativo dal 2025 solo per le fatture in ricezione, estendendosi anche all'invio dal 2027. Portogallo e Danimarca partiranno tra il 2024 e il 2025.

I grandi provider di servizi fiduciari digitali (QTSP) collaborano attivamente con i legislatori per facilitare gli aggiornamenti normativi in Europa. Tavoli di lavoro come il TAG (Technology Advisory Group) e il progetto "ViDA - VAT in the Digital Age" dell'Unione Europea, insieme a forum nazionali come il Forum E-Invoicing, mirano ad armonizzare i linguaggi di fatturazione tra i Paesi membri. Reti come Peppol svolgono un ruolo fondamentale nella standardizzazione dello scambio di documenti di trasporto e fatture elettroniche tra aziende di Paesi diversi.

Oltre a migliorare l'efficienza operativa e la trasparenza delle transazioni, la fatturazione elettronica è anche un potente strumento di cybersecurity. La digitalizzazione riduce il rischio di frodi e falsificazioni, garantendo maggiore sicurezza nella gestione dei dati finanziari. Inoltre, l'adozione di standard elevati per la trasmissione e l'archiviazione delle fatture elettroniche protegge le informazioni sensibili delle aziende.

L'Italia, insieme all'Europa, ha scelto la strada della fatturazione elettronica per migliorare la lotta all'evasione fiscale e rafforzare la sicurezza economica. La digitalizzazione delle transazioni commerciali permette un controllo più tempestivo e accurato delle operazioni finanziarie, riducendo le opportunità di evasione e incrementando le entrate fiscali. Questo contribuisce a rafforzare la stabilità economica e a creare un ambiente imprenditoriale più sicuro e trasparente.

Sebbene l'Italia sia all'avanguardia nel settore della fatturazione elettronica, il percorso verso una piena digitalizzazione delle transazioni quotidiane è ancora lungo. L'armonizzazione a livello europeo presenta altrettante sfide, ma con la collaborazione tra governi, aziende e fornitori di servizi digitali, è possibile raggiungere un alto livello di integrazione e sicurezza, a vantaggio della crescita economica e della competitività del continente.

Oltre a migliorare l'efficienza operativa e la trasparenza delle transazioni, la fatturazione elettronica è anche un potente strumento di cybersecurity.

Non solo obblighi: la Direttiva NIS2 come leva di sicurezza e vantaggio competitivo per le imprese italiane

A cura di Andrea Monti

Con l'introduzione della Direttiva NIS2 (Network and Information Security Directive) e del Decreto Legislativo 138/2024, l'Italia e l'Europa si preparano a elevare in maniera significativa la difesa delle infrastrutture critiche e dei servizi essenziali dai crescenti rischi informatici. Si tratta di una normativa ambiziosa, pensata per un'epoca in cui i dati e i sistemi digitali sono diventati l'ossatura di ogni attività, da quelle industriali a quelle finanziarie, passando per i settori dei trasporti e della sanità. Con questa direttiva, l'Unione Europea intende delineare un quadro di requisiti e pratiche standardizzate che possano garantire, in tutta l'area comunitaria, un livello omogeneo di sicurezza e resilienza digitale. A tal riguardo, il Decreto Legislativo 138/2024 ha formalizzato anche in Italia le disposizioni previste dalla NIS2, segnando un passaggio fondamentale per almeno 1.500 aziende attive in settori nevralgici come energia, telecomunicazioni, finanza, sanità e trasporti, tutte realtà strategiche e quindi più esposte al rischio di attacco. Questa cifra rappresenta una stima delle imprese che, operando in settori cosiddetti "essenziali" o "importanti", rientrano tra i soggetti obbligati a rispettare le nuove norme.

Ma qual è il reale scopo della NIS2? Come dichiarato dalla Commissione Europea stessa, l'obiettivo primario è quello di garantire una protezione uniforme e robusta per le reti e le informazioni, prevenendo i rischi di disservizi che potrebbero portare a conseguenze economiche e sociali su vasta scala. Parafrasando Margrethe Vestager - vicepresidente esecutiva per un'Europa pronta per l'era digitale – oggi sappiamo che una delle principali sfide è la necessità di proteggere la nostra infrastruttura digitale dalle minacce in costante evoluzione. Con la NIS2, non solo si rendono obbligatori standard più elevati di sicurezza, ma vengono create delle reti di protezione interconnesse e coordinate, in cui ogni Stato membro diventa un anello forte di una catena solida. In un mondo digitale caratterizzato da continue sfide e pericoli, la posta in gioco non è solo la difesa dei dati aziendali o il funzionamento regolare dei sistemi, ma anche – e soprattutto – la fiducia dei consumatori e la stabilità delle economie nazionali. La sicurezza informatica, dunque, cessa di essere un semplice strumento di difesa e diventa una componente fondamentale della reputazione e della competitività di ogni azienda, come affermato da numerosi analisti. Questa direttiva introduce standard che impongono alle imprese di attuare un approccio alla sicurezza strutturato e sistematico, in cui la resilienza e la proattività devono essere garantite a livello organizzativo.

Le principali scadenze e gli obblighi di conformità

La normativa italiana ha imposto scadenze precise per il percorso di conformità alla NIS2, suddiviso in diverse tappe fondamentali. Entro il 17 gennaio 2025, le organizzazioni che operano nei settori individuati dalla direttiva devono stabilire la propria appartenenza ai gruppi di soggetti "essenziali" o "importanti" e registrarsi sulla piattaforma dell'Agenzia per la Cybersicurezza Nazionale (ACN). La registrazione costituisce il primo passo verso la conformità e serve a monitorare il perimetro di attuazione della direttiva, affinché si possa avere un quadro accurato e aggiornato dei settori e delle entità più esposte a potenziali minacce informatiche. Dopo la registrazione, l'ACN procederà a verificare entro il 15 aprile 2025 l'inclusione delle aziende nel perimetro di sicurezza NIS2. L'adozione di tali misure rappresenta un cambiamento radicale rispetto al passato, poiché ora esiste un ente dedicato che controlla e gestisce, a livello nazionale, le pratiche di conformità alla cybersecurity per settori strategici. Le aziende dovranno successivamente rispettare la scadenza del 1° gennaio 2026, data entro cui sarà necessario adottare processi formali e documentati per la gestione degli incidenti di sicurezza, un'area che si estende dalla rilevazione alla notifica tempestiva di eventuali attacchi.

In questo quadro, il monitoraggio delle minacce diventa fondamentale. La NIS2 richiede alle aziende di mantenere aggiornato il proprio profilo di sicurezza, con report periodici sulla piattaforma dell'ACN, indicando le misure adottate per garantire protezione e continuità dei servizi essenziali. Tali aggiornamenti dovranno essere parte di una strategia di compliance costante, che permetta alle aziende di essere pronte a rispondere in modo tempestivo ed efficace in caso di attacco. Infine, per l'ottobre 2026, tutte le aziende dovranno dimostrare di aver raggiunto un livello di sicurezza che consenta loro di prevenire, rilevare e mitigare i rischi con un approccio coordinato e strutturato. Tale scadenza segna un punto di arrivo che, tuttavia, non rappresenta un semplice obiettivo di conformità, ma piuttosto una soglia minima

che ogni azienda sarà tenuta a mantenere e migliorare nel tempo.

Gli strumenti per adeguarsi alla NIS2: misure tecniche e organizzative

Essere conformi alla NIS2 richiede non solo la semplice implementazione di misure tecniche, ma un approccio integrato che combini tecnologia, formazione e monitoraggio continuo. Le aziende italiane possono allinearsi agli standard della direttiva attraverso alcune strategie e pratiche specifiche:

1. Cyber Threat Intelligence (CTI)

La CTI è un insieme di processi che permette di raccogliere, analizzare e interpretare informazioni sulle minacce per identificare e prevenire potenziali attacchi. Adottare soluzioni CTI avanzate consente alle aziende di anticipare le minacce emergenti e reagire in modo proattivo. Questo approccio permette di rilevare rapidamente le criticità, proteggendo l'azienda dai rischi legati a un attacco su vasta scala.

2. Security Information and Event Management (SIEM) e Security Orchestration, Automation, and Response (SOAR)

I sistemi SIEM offrono una panoramica completa degli eventi di sicurezza all'interno dell'infrastruttura IT aziendale, analizzando e correlando dati provenienti da diverse fonti. L'integrazione con SOAR automatizza il processo di risposta agli incidenti, riducendo al minimo il tempo di reazione e migliorando l'efficacia della gestione della sicurezza.

3. Audit periodici e gestione della supply chain

Un aspetto cruciale della NIS2 è la protezione delle catene di fornitura, che spesso rappresentano uno dei punti deboli nelle difese aziendali. Attraverso un programma di Third Party Risk Management (TPRM), le aziende possono valutare e monitorare la sicurezza dei propri fornitori e partner. Gli audit periodici, inoltre, permettono di mantenere elevati standard di sicurezza lungo tutta la filiera produttiva e distributiva.

4. Formazione continua del personale

La NIS2 richiede che il personale aziendale sia consapevole dei rischi informatici e sappia come agire di fronte a un potenziale incidente. La formazione è una componente essenziale per rafforzare la cosiddetta "cyber hygiene" all'interno dell'organizzazione. Simulazioni di attacco come il phishing testing, per esempio, rappresentano strumenti efficaci per sensibilizzare i dipendenti e per preparare l'azienda a reagire prontamente.

5. Implementazione di Business Continuity Plans (BCP)

La resilienza operativa è un elemento cruciale della NIS2. Le aziende devono essere in grado di garantire continuità anche in caso di attacco, e per questo la direttiva prevede l'adozione di piani di Business Continuity e Disaster Recovery. Avere protocolli ben definiti per la risposta agli incidenti e la ripresa delle attività è essenziale per ridurre al minimo l'impatto di eventuali attacchi.

Un nuovo paradigma di sicurezza per il futuro

La NIS2 non si limita a imporre un insieme di regole: essa vuole trasformare la sicurezza informatica in un pilastro della competitività e dell'affidabilità delle aziende europee. Una tappa cruciale per creare un'Europa più sicura, dove la cybersecurity non sia vista come un costo, ma come un investimento strategico. Adeguarsi a questa direttiva significa per le aziende italiane non solo mitigare i rischi, ma anche costruire una reputazione di affidabilità e sicurezza in un mercato dove la cybersecurity è ormai un valore imprescindibile. Le imprese che sapranno conformarsi alla NIS2 e adottare una cultura della sicurezza integrata a tutti i livelli potranno emergere come leader nel proprio settore, capaci di garantire protezione e continuità operativa anche nelle condizioni più difficili. Con una prospettiva di crescita basata sulla sicurezza e sulla resilienza, le aziende italiane potranno guardare al futuro con la consapevolezza di essere pronte a fronteggiare le sfide del mondo digitale.

LA CYBER PER TUTTI
ISTRUZIONI SEMPLICI PER QUESTIONI COMPLESSE

Deepfake: sfide e soluzioni per contrastare una delle più insidiose minacce emergenti

A cura di Fabio Ugoste

Negli ultimi anni, lo scenario delle minacce cyber (il cosiddetto cyber threat-landscape) è diventato sempre più complesso e sofisticato. Facendo leva su tecniche e strumenti resi disponibili dalla sempre più rapida innovazione tecnologica, i cybercriminali hanno perfezionato le loro tecniche offensive per sferrare attacchi informatici con fini malevoli: un esempio è l'utilizzo dell'intelligenza artificiale (AI).

Una delle minacce più insidiose e difficili da contrastare, tra quelle che sfruttano, l'intelligenza artificiale è quella detta deepfake. Questa tecnica rappresenterà una sfida crescente nei prossimi anni, come evidenziato nella recente pubblicazione di ENISA sulle prospettive delle minacce informatiche per il 2030.

Il termine deepfake deriva dalla combinazione del concetto di "deep learning", la tecnologia alla base dell'apprendimento automatico dei sistemi informatici, e "fake", poiché gli algoritmi impiegati mirano ad emulare input reali per creare contenuti multimediali contraffatti. L'intelligenza artificiale generativa, addestrata su contenuti multimediali reali reperiti da fonti reali e legittime, può produrre video, immagini e file audio così realistici da rendere sfidante per gli utenti la distinzione tra ciò che è un contenuto digitale originale da ciò che è deepfake (o finto).

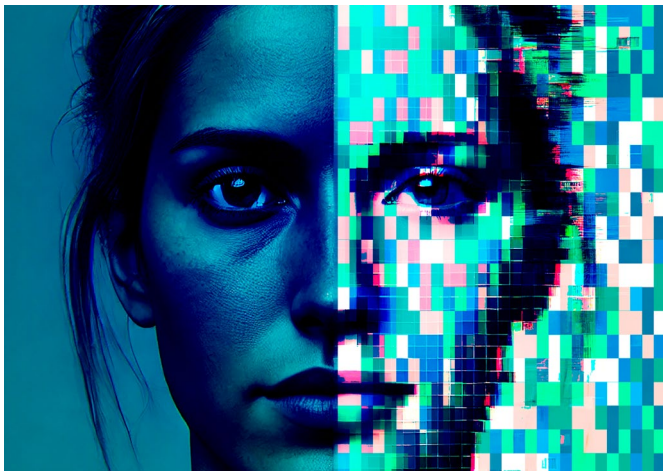
I contenuti fraudolenti così' creati vengono poi diffusi tramite e-mail, messaggi istantanei, social media e videochiamate, e utilizzati per diffondere notizie false o per cercare di portare a termine truffe ai danni di aziende e persone, richiedendo, per lo più, l'esecuzione di transazioni di denaro.

Le istituzioni finanziarie sono tra i bersagli più frequenti di questi attacchi, soprattutto a causa delle ingenti somme di denaro che movimentano giornalmente e della mole di dati in loro possesso. In questo contesto, focalizzandoci sul mondo bancario e finanziario, i deepfake vengono utilizzati principalmente per perpetrare truffe bancarie, ma possono essere usati anche per diffondere informazioni false al fine di compromettere la reputazione aziendale e creare turbative sui mercati.

Recentemente, ci sono stati tentativi di truffa in cui gli hacker hanno utilizzato la tecnica del deepfake per impersonare il CEO di un'azienda, richiedendo l'esecuzione di operazioni di pagamento urgenti e riservate, sfruttando canali di contatto non aziendali (per esempio, contattando i collaboratori tramite messaggistica istantanea), ingannando così il personale aziendale e inducendolo a compiere trasferimenti di denaro verso IBAN fraudolenti. Questi attacchi sono solitamente mirati e richiedono un'analisi approfondita del tessuto aziendale prima di essere portati a termine. Ciò che rende realistico e credibile il deepfake non è solo la tecnologia impiegata per produrlo, ma anche la profonda conoscenza che gli hacker riescono ad ottenere rispetto all'ambiente aziendale.

Questa attenta analisi fondata sull'osservazione del potenziale target contribuisce ad aumentare la probabilità che le vittime cadano nel tentativo di truffa, rendendo così efficaci le tecniche di manipolazione psicologica, note come social engineering, il cui scopo è, in sintesi, instaurare nella vittima un senso di fiducia nei confronti del truffatore.

Al fine di contrastare questi fenomeni, è assolutamente necessario che aziende e istituzioni investano in tecnologie avanzate e programmi di sensibilizzazione e formazione fornendo alle persone gli strumenti utili a riconoscere queste minacce. Oltre a ciò, è necessario migliorare i processi aziendali, creando meccanismi procedurali di controllo e sistemi tecnico-organizzativi, che possano garantire un adeguato livello di sicurezza. Queste diverse forme di prevenzione e controllo contribuiscono a mitigare i potenziali grandi rischi derivanti dall'innovazione tecnologica.



Infatti, se da un lato l'evoluzione tecnologica può introdurre nuove minacce, dall'altro può fornire le tecniche di difesa.

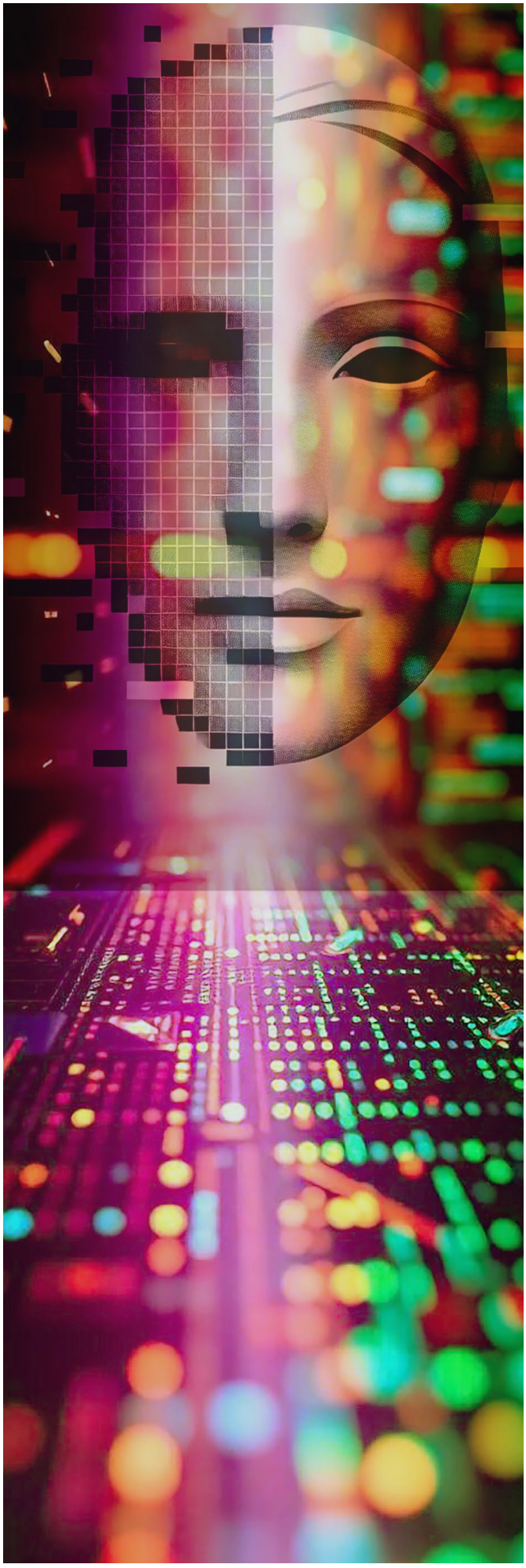
In particolare, l'AI può essere utilizzata per esaminare la qualità dei contenuti multimediali per scorgere tracce di manipolazione: per esempio analisi delle risoluzioni video o delle condizioni ambientali o ancora dei dettagli visivi, permette di individuare possibili alterazioni nella qualità, luminosità e nei particolari delle immagini.

Oltre a ciò, è altrettanto fondamentale strutturare processi aziendali lineari e ben comprensibili che mettano i dipendenti nelle migliori condizioni per contrastare i deepfake. L'organizzazione deve favorire la chiarezza e la consapevolezza tra tutti gli attori coinvolti nei processi, riducendo le ambiguità che potrebbero essere sfruttate dagli attaccanti per i loro scopi malevoli. Infatti, processi chiari e ben definiti permettono la loro corretta applicazione anche in situazioni di urgenza, prevenendo il rischio di raggiri tramite richieste ingannevoli da parte di falsi superiori gerarchici che mirano ad utilizzare strumenti al di fuori della consuetudine aziendale (es. utilizzo di messaggistica istantanea). Per questo motivo, i processi di controllo devono prevedere l'esecuzione di determinate operazioni esclusivamente tramite strumenti aziendali; ad esempio, i dipendenti devono avere chiaro che è sconsigliato/vietato dare seguito a richieste di esecuzione di operazioni, tipicamente di pagamento, effettuate su canali alternativi a quelli aziendalmente previsti.

I dipendenti devono quindi essere preparati a identificare richieste sospette ed a verificare l'autenticità delle comunicazioni, soprattutto quando queste avvengono tramite telefonate o strumenti di messaggistica istantanea (in generale canali non usuali). Ad esempio, di recente, un manager di una nota casa automobilistica, sospettando un tentativo di deepfake, ha smascherato una impersonificazione del CEO ponendo una domanda personale al suo interlocutore. Questo ha indotto i malintenzionati a desistere dall'attacco.

La formazione sui rischi e sulle modalità per riconoscere i deepfake, incluse le simulazioni di attacchi che utilizzano questa tecnica, deve quindi diventare parte integrante dei programmi di sviluppo della cultura relativa alla sicurezza informatica e, più in generale, alla sicurezza all'interno delle organizzazioni.

È assolutamente necessario che aziende e istituzioni investano in tecnologie avanzate e programmi di sensibilizzazione e formazione fornendo alle persone gli strumenti utili a riconoscere queste minacce.



CYBER
Think Tank
ASSINTEL

WEBINAR

Cybersecurity per PMI: soluzioni efficaci e sostenibili

Relatori:

Fabio Zanoli

Marco Scognamiglio

Riccardo Paglia

29 Novembre

12:00 - 13:00

Per info scrivi a:

segreteria@assintel.it

IA e finanza

A cura di Ranieri Razzante

Le applicazioni dell'IA (Intelligenza Artificiale), nel settore finanziario e bancario sono molteplici. Tra le principali rientrano sicuramente i modelli di scoring per il rischio di credito, il marketing, il contrasto alle frodi nell'ambito delle transaction banking, i sistemi di gestione dei rischi operativi.

L'uso dell'IA da parte degli operatori di mercato sta portando ad una serie di cambiamenti che avranno un forte impatto:

- sulle Autorità, le quali dovranno rivedere gli strumenti di vigilanza e di prevenzione del rischio;
- sulla clientela, attraverso la modifica delle modalità di acquisto (c.d. customer journey).

Notevole impatto, infine, sarà registrato sulla produttività degli operatori attraverso la modifica ragionata dei processi produttivi.

I dati che emergono dal rapporto OCSE 2023 sugli investimenti in venture capital relativi all'Intelligenza Artificiale mostrano che Stati Uniti e Cina risultano essere i due Paesi più attivi, seguiti da Giappone ed Europa. Si osserva come le imprese italiane siano ancora indietro rispetto alla media europea.

Il settore finanziario svolge un ruolo molto rilevante nell'applicazione di soluzioni relative all'IA, sia a livello internazionale che domestico. In particolare, l'indagine fintech svolta dalla Banca d'Italia nel 2023 mostra come gli investimenti per l'innovazione siano in continua crescita. I progetti basati su IA sono aumentati in termini di spesa, grazie alle applicazioni per il c.d. digital lending (prestito digitale).

Le banche italiane utilizzano principalmente due modalità operative in materia: il rafforzamento delle strategie in ambito informatico e la ricerca di accordi con società informatiche primarie, volti alla realizzazione di infrastrutture.

Le potenzialità offerte dall'applicazione di soluzioni basate su modelli di IA consentono di adottare decisioni più rapide, attenuando le asimmetrie informative, risparmiare sui tempi e sui costi, migliorare le offerte per la clientela. È proprio questo che spinge gli operatori ad utilizzare questi modelli, che vanno necessariamente bilanciati ed integrati dalla valutazione dei rischi.

La Banca d'Italia è ben consapevole delle potenzialità dell'Intelligenza Artificiale, sia in termini di funzioni che di impatto sul sistema economico. L'attività della Banca d'Italia si sviluppa principalmente lungo tre assi.

In primo luogo, essa fornisce supporto tecnico al Governo nei negoziati in corso sulla normazione in materia di Intelligenza Artificiale. Uno dei punti più complessi riguarda i cc.dd. "modelli fondamentali" di tipo generativo. L'Autorità vede con favore l'ampliamento delle garanzie per la tutela dei diritti e l'attività antiriciclaggio.

In secondo luogo, la Banca d'Italia promuove l'attività dei facilitatori dell'innovazione. Sono stati sviluppati tre canali di dialogo con il mercato: il Canale Fintech, Milano Hub e la Sandbox regolamentare.

Da ultimo, la necessità di "conformità digitale" evidenzia un ambito di crescente importanza pratica e teorica, ovvero l'implementazione delle nuove tecnologie che sta influenzando i sistemi di compliance, con particolare riguardo ai modelli di organizzazione e gestione definiti nel D. Lgs. 231/2001 (noti anche come MOG: modelli di organizzazione, gestione e controllo).

Nello specifico, nel mondo aziendale, il termine “conformità digitale” si riferisce all’utilizzo delle tecnologie di intelligenza artificiale, in particolare a quella applicata ai Big Data. Questo tipo di tecnologia, legata al regno digitale, ha raccolto un notevole interesse per le sue profonde implicazioni sociali.

I processi decisionali (governance), la valutazione preventiva del rischio (gestione del rischio) e l’adozione di comportamenti conformi sono interconnessi. Sebbene questi strumenti operino su differenti livelli e richiedano diversi gradi di implementazione, a seconda della tipologia di azienda o di attività, nessuno può essere trascurato quando si analizza l’impatto della digitalizzazione.

Le soluzioni basate sull’Intelligenza Artificiale introducono significativi challenge nei modi finora conosciuti di organizzare e gestire il sistema finanziario. L’IA arricchisce le opportunità di business e gli strumenti messi a disposizione per gli operatori, a condizione che sappiano gestire i rischi in modo adeguato. È appena il caso di ricordare, infatti, che “adeguatezza” e “proporzionalità” sono i paradigmi classici dell’organizzazione delle imprese bancarie e del settore finanziario.

La Banca d’Italia assume il ruolo di promuovere e agevolare la trasformazione del sistema finanziario, nel rispetto del principio fondamentale di una governance consapevole del rischio. Un dialogo costruttivo con tutti gli operatori su un tema così complesso è condizione necessaria per favorire una buona innovazione tecnologica capace di realizzare le proprie potenzialità non solo per il mondo finanziario, ma anche per l’intera comunità nazionale.

Una rapida (e, in verità, già testata) applicazione nella prevenzione del rischio di credito, in quello di riciclaggio, delle frodi e dell’investment banking sono le evidenze empiriche che indubbiamente sono già consistenti in materia.

Il settore finanziario svolge un ruolo molto rilevante nell’applicazione di soluzioni relative all’ IA, sia a livello internazionale che domestico.

Sostenibilità e cybersecurity

A cura di Sofia Scozzari

Nel panorama digitale attuale, due temi stanno acquisendo crescente rilevanza e si collocano tra le principali priorità per le aziende a livello globale: la Sostenibilità, particolarmente inquadrata nel contesto ESG (Environmental, Social, and Governance), e la Cyber Security, non più relegata alla sola protezione di dati e sistemi, ma inevitabilmente intrecciata con tutti gli aspetti della nostra vita sempre più connessa.

Sebbene possano sembrare due ambiti distinti e distanti tra loro, un'analisi più approfondita può rivelare interessanti punti di contatto e opportunità di integrazione.

Punti di contatto tra Sostenibilità e Cyber Security

Sostenibilità e Cybersecurity operano in ambiti apparentemente diversi, ma esistono significative aree di sovrapposizione che possono essere sfruttate per creare strategie più integrate ed incisive:

- **Governance:** Sia le iniziative ESG che la Cyber Security richiedono un forte impegno da parte del management aziendale che, in entrambi i casi, deve definire una strategia chiara, risorse dedicate e una cultura aziendale che ne sostenga l'implementazione e la continuità.
- **Gestione del rischio:** ESG e Cyber Security mirano a mitigare rischi aziendali, sebbene di natura diversa: mentre la Sostenibilità si focalizza su rischi ambientali, sociali e di governance, la Cyber Security si occupa della protezione degli asset aziendali dalle minacce digitali.
- **Compliance:** Entrambi gli ambiti sono soggetti a normative in continua evoluzione. La conformità agli standard ESG e di sicurezza informatica è ormai cruciale, non solo per non incorrere in sanzioni, ma anche per incrementare la reputazione aziendale e la fiducia degli stakeholder.
- **Resilienza:** Sia Cyber Security che Sostenibilità mirano a garantire la resilienza a lungo termine. Mentre, infatti, la Sostenibilità cerca di proteggere l'ambiente e le comunità per le future generazioni, una strategia di Cyber security efficace, oltre all'implementazione di misure difensive, deve includere anche piani per garantire una risposta adeguata e tempestiva in caso di incidenti o attacchi informatici.
- **Reputazione aziendale:** Una violazione dei dati può compromettere la reputazione di un'azienda al pari di uno scandalo ambientale o sociale. Gestire efficacemente entrambi gli aspetti è fondamentale per mantenere la fiducia di clienti, investitori e partner.
- **Trasparenza e Responsabilità:** La trasparenza nelle pratiche aziendali e la responsabilità rappresentano valori chiave sia per la Sostenibilità che per la Cyber Security, necessari per costruire e mantenere la fiducia degli stakeholder.

Carenze della cybersecurity in termini di Sostenibilità

Nonostante i punti in comune, la Cyber Security necessita di maggiori interventi per allinearsi ulteriormente con i principi di Sostenibilità in particolare nei seguenti ambiti:

- **Consumo Energetico:** I data center necessari alle infrastrutture IT consumano enormi quantità di energia. Questi consumi possono avere un impatto ambientale significativo, in particolare se l'energia proviene da fonti non rinnovabili, e incidono significativamente sulle emissioni di carbonio. Inoltre, l'utilizzo sempre più diffuso di Intelligenza Artificiale contribuisce a peggiorare l'impronta ambientale, a causa delle enormi risorse che comporta, sia in termini energetici che di acqua necessaria ai sistemi di raffreddamento dei data center.
- **Ciclo di Vita delle Tecnologie:** I dispositivi IT hanno un ciclo di vita breve, in particolare nella Cyber Security, che porta a frequenti aggiornamenti e sostituzioni. Questo contribuisce all'accumulo di rifiuti elettronici (e-waste), che rappresenta una delle moderne sfide ambientali più sentite.
- **Materiali e Risorse:** La produzione di dispositivi IT richiede l'estrazione di materiali rari e risorse naturali, che possono avere impatti ambientali significativi.
- **Uso inefficiente delle risorse hardware:** Spesso i dispositivi hardware non vengono utilizzati al massimo della loro capacità, portando a un utilizzo inefficiente delle risorse.

L'integrazione tra Cyber Security e Sostenibilità non è solo una necessità, ma rappresenta anche una straordinaria opportunità per le aziende di creare valore aggiunto, rafforzare la resilienza e costruire un vantaggio competitivo duraturo.

Rendere la Cyber Security più sostenibile

Per incorporare i principi ESG nella Cyber Security è necessario agire su tre fronti principali:

1. Tematiche ambientali:

- Efficienza energetica: Ottimizzare l'uso di energia nei data center e nelle infrastrutture IT, oltre che investire in strutture alimentate da energie rinnovabili, può ridurre significativamente l'impatto ambientale delle operazioni di sicurezza.
- **Gestione dei dispositivi hardware:** Promuovere il riciclo, il riutilizzo e lo smaltimento responsabile di hardware obsoleto o compromesso è essenziale per la riduzione dei rifiuti elettronici. Inoltre, è importante non sottostimare i rischi di sicurezza derivanti da pratiche di smaltimento non sicure che può portare alla perdita o al furto di informazioni sensibili.
- **Cloud computing:** Utilizzare provider cloud con forti credenziali di sostenibilità può migliorare sia la sicurezza che l'impatto ambientale.
- **Lavoro remoto sicuro:** Promuovere il lavoro remoto per dipendenti e collaboratori, implementando al tempo stesso pratiche di sicurezza robuste, può ridurre le emissioni legate agli spostamenti mantenendo alti standard di protezione.

2. Tematiche Sociali:

- Inclusività e Accessibilità: Le soluzioni di sicurezza devono essere accessibili e utilizzabili da un pubblico più ampio, includendo disabili e comunità svantaggiate.
- Sensibilizzazione del personale: È fondamentale formare dipendenti e collaboratori sull'importanza della sostenibilità e delle pratiche sicure, sensibilizzandoli sui rischi associati a comportamenti non sostenibili.

3. Tematiche di Governance:

- Aspetti etici: Un approccio etico alla sicurezza informatica implica la protezione contro il furto di identità, la diffusione di fake news e la violazione dei dati personali, tutti aspetti che incidono direttamente sul benessere della società.
- Privacy e Trasparenza: È necessario che le aziende trovino un equilibrio tra la protezione dei dati e la privacy degli utenti e la trasparenza richiesta dalle iniziative ESG, in particolare quando si ha a che fare con rischi informatici.
- Compliance normativa: Un approccio sostenibile alla Cyber Security richiede un adeguamento continuo alle normative in evoluzione e un impegno verso una governance responsabile. Le aziende devono, non solo rispettare le normative vigenti, ma anche anticipare e prepararsi per futuri requisiti, integrando la conformità in ogni aspetto delle loro operazioni.

Conclusioni

L'integrazione tra Cyber Security e Sostenibilità non è solo una necessità, ma rappresenta anche una straordinaria opportunità per le aziende di creare valore aggiunto, rafforzare la resilienza e costruire un vantaggio competitivo duraturo. Inoltre, questa sinergia favorisce una maggiore fiducia da parte degli stakeholder, un elemento cruciale in un mondo sempre più connesso e consapevole delle responsabilità ambientali e sociali.

Le aziende che sapranno combinare efficacemente queste due aree strategiche saranno meglio attrezzate per affrontare le sfide future, garantendo al contempo una crescita sostenibile. Grazie alla collaborazione tra aziende e professionisti del settore per sviluppare soluzioni innovative che uniscano questi due mondi, sarà quindi possibile creare un impatto positivo non solo per il business, ma per la società nel suo complesso, oltre che un futuro più sicuro e sostenibile.

Cybersecurity: quali sono i rischi connessi all'Intelligenza Artificiale?

A cura di Pierluigi Paganini

L'Intelligenza Artificiale (IA) sta trasformando radicalmente ogni aspetto della nostra società, ivi compreso il settore della cybersecurity. L'Intelligenza Artificiale (IA) è fucina di nuove opportunità, ci troviamo dinanzi ad un cambiamento epocale senza precedenti ma che inevitabilmente porta con sé rischi significativi. Le tecnologie basate sull'IA, possono migliorare la capacità di rilevare e rispondere a minacce informatiche, tuttavia esse stesse possono essere utilizzate da varie categorie di attori malevoli, o peggio diventare bersagli di una nuova generazione di offensive mirate.

La principale preoccupazione della comunità di cyber sicurezza è il possibile impiego dell'IA da parte di organizzazioni dedite al cybercrime ed attori Nation-State per sviluppare attacchi sempre più sofisticati e difficili da individuare.

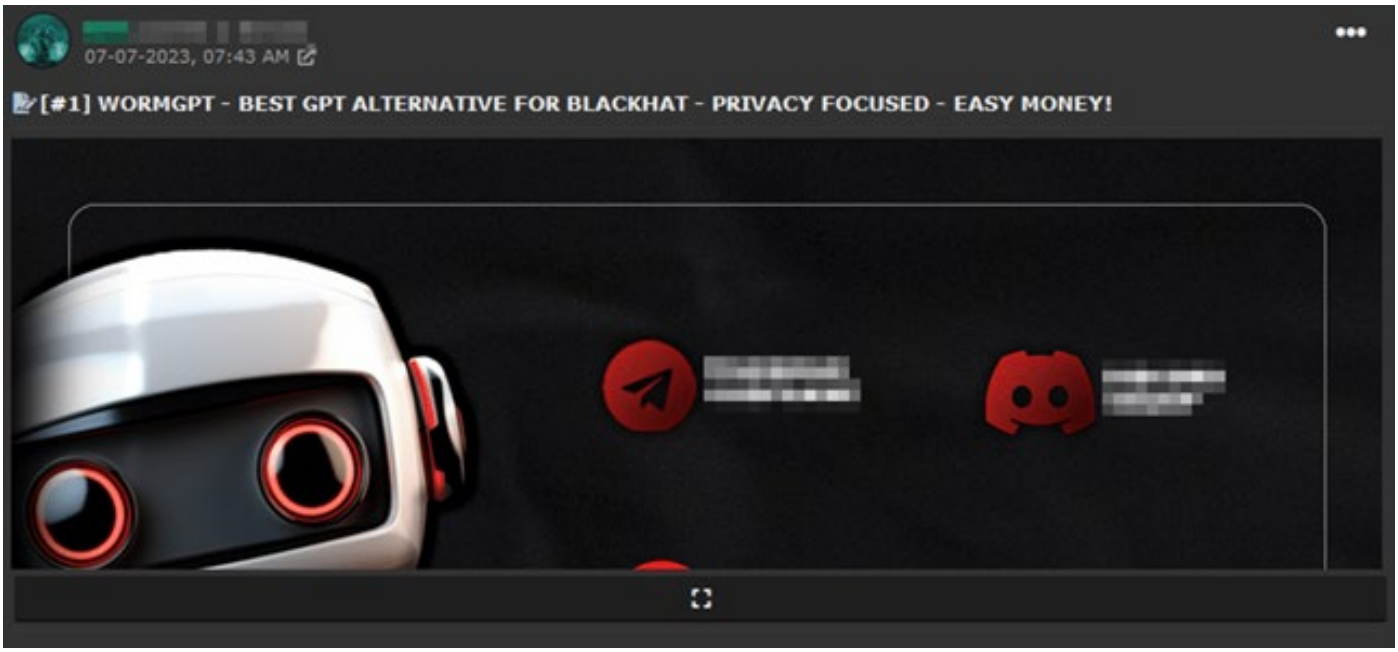
Ad esempio, sistemi basati su intelligenza artificiale generativa possono essere utilizzati da attaccanti con motivazione finanziaria per condurre sofisticate truffe ed attacchi di phishing in grado di eludere gli attuali sistemi di difesa.

Sono già disponibili nell'underground criminale piattaforme per generare condurre campagne di phishing su larga scala. Nel 2022, il Federal Bureau of Investigation (FBI) ha messo in guardia gli utenti in rete dal crescente utilizzo dell'intelligenza artificiale generativa per creare reti di falsi profili sui social media coordinati per ingannare le vittime e sottrarre loro denaro.

Lo scorso anno, nel panorama delle minacce sono state documentate due piattaforme rispettivamente chiamate FraudGpt e WormGpt, utilizzabili per condurre sofisticati attacchi di phishing e Business email compromise (Bec).

Diverse organizzazioni criminali oggi possono contare su piattaforme simili a queste due, che mediante una sottoscrizione al costo di poche centinaia di dollari per mese, consentono loro di organizzare attacchi complessi.

I sistemi basati su Intelligenza Artificiale possono essere utilizzati per automatizzare diverse fasi di un attacco, dalla ricognizione alla compromissione di un sistema obiettivo. L'Intelligenza Artificiale potrebbe essere impiegata per lo sviluppo di codice malevolo e tool di attacco. Diverse ricerche condotte da esperti del settore dimostrano che i modelli di IAG possono essere impiegati per sviluppare varianti di malware in grado di evadere i meccanismi di detection dei principali motori anti-malware.



Sebbene siano diversi i possibili abusi dell'Intelligenza Artificiale da parte degli attaccanti, in un momento storico come questo spaventa l'impiego della tecnologia in campagne di disinformazione.

Un deepfake è un contenuto multimediale, come un video o un'immagine, creato utilizzando l'Intelligenza Artificiale per alterare, sostituire o manipolare in modo realistico il volto, la voce o il corpo di una persona. Esistono numerose piattaforme e servizi offerti dai criminali informatici per la generazione di deepfake in grado di ingannare gli utenti in rete tanto da far sembrare autentici eventi che in realtà non lo sono. I deepfake sono un elemento centrale nelle campagne di disinformazione, così come in frodi finanziarie. Si sono osservati in questi ultimi mesi diversi attacchi basati su deep fake condotti da criminali informatici e attori che operano per conto di governi.

Il governo cinese sta già utilizzando l'Intelligenza Artificiale generativa in campagne di disinformazione per condurre operazioni di influenza contro paesi come gli Stati Uniti e Taiwan, come documentato in un rapporto del Microsoft Threat Analysis Center. Attori riconducibili al governo cinese sono intenti nella creazione di contenuti con l'IAG per manipolare le prossime elezioni negli USA, utilizzando account falsi sui social media per alimentare questioni su temi 'divisivi'.

L'Intelligenza Artificiale (IA) sta trasformando radicalmente ogni aspetto della nostra società, ivi compreso il settore della cybersecurity.

Altro aspetto legato alla diffusione di sistemi basati su IA all'interno della nostra società, è la possibilità che essi stessi siano oggetti di attacchi con conseguenti impatti sul contesto in cui sono impiegati.

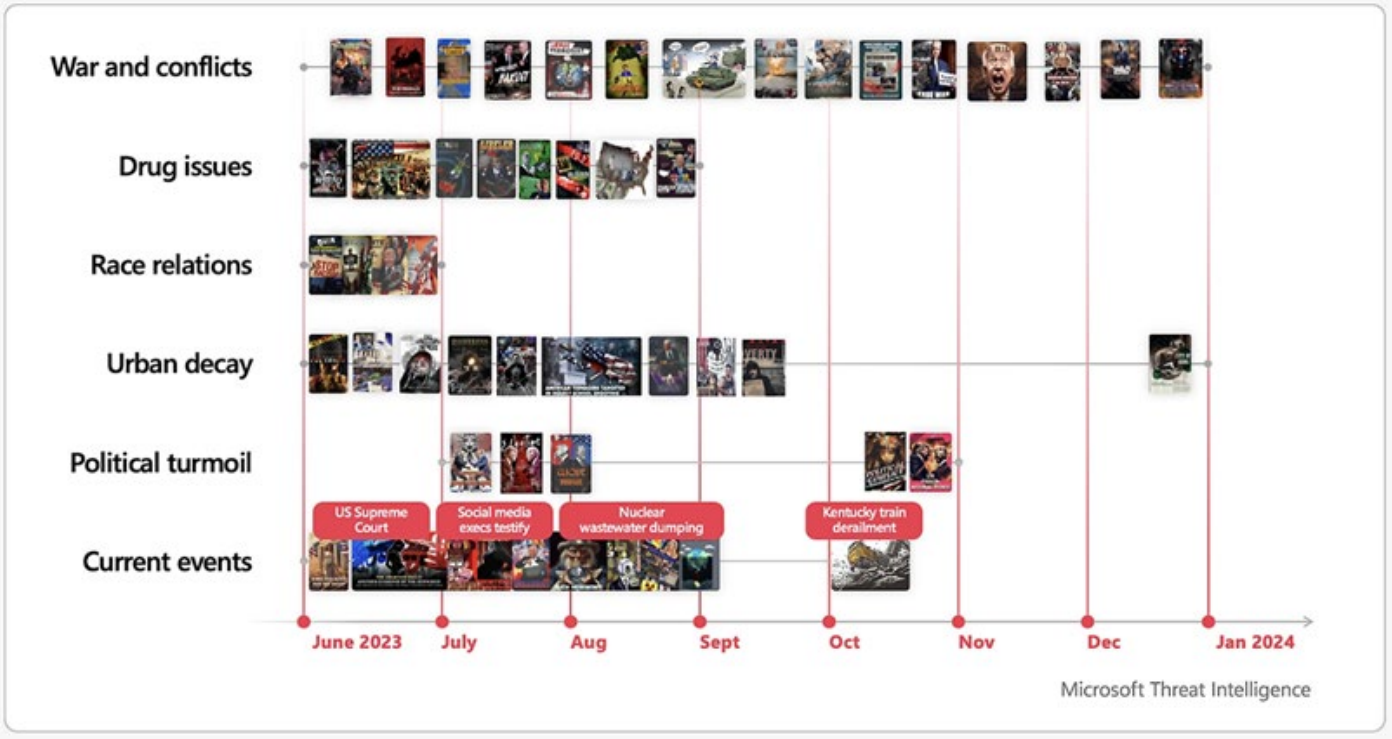
In ambito cyber security un attaccante potrebbe "manipolare" i modelli di machine learning per eludere le difese e compromettere la sicurezza.

Si distinguono attacchi contro i sistemi stessi e gli attacchi ai modelli di Intelligenza Artificiale.

Alla prima categoria appartengono gli attacchi all'infrastruttura su cui si basa un sistema di intelligenza artificiale, ad esempio, alle reti o ai server che lo ospitano, alle comunicazioni tra le componenti e l'accesso non autorizzato ai dati ed al modello stesso. Gli attacchi appartenenti alla seconda categoria sono concepiti per interferire con il modello di IA utilizzato dal sistema. Un attaccante potrebbe manipolare i dataset utilizzati per l'addestramento del modello o modificarne i parametri. Pensiamo ad un sistema di difesa da attacchi cyber, qualora un attaccante riuscisse a fornire false informazioni sugli attacchi nel set di addestramento potrebbe portare il modello a non riconoscere correttamente uno specifico attacco quando questo si verifica.

Esistono poi attacchi di inferenza condotti nel tentativo di ottenere informazioni sensibili dal modello di IA mediante una serie di interrogazioni ad hoc. Questi attacchi potrebbero essere sfruttati per eludere le limitazioni imposte al modello nell'iterazione con gli umani.

In sintesi, un attacco potrebbe riuscire ad avvelenare il modello di Intelligenza Artificiale usato da un sistema colpendo diverse fasi del processo di addestramento,



dalla raccolta dei dati all'addestramento stesso.

Quando si affrontano i rischi connessi all'utilizzo di sistemi basati su IA è necessario affrontare temi come etica e privacy.

Esiste un rischio concreto che sistemi basati su IA possano portare a discriminazioni e violazioni della privacy. Gli algoritmi di IA sono suscettibili a bias, ovvero la possibilità che algoritmi e sistemi di IA possano produrre risultati sistematicamente pregiudizievoli o imprecisi a causa di assunzioni errate nel processo di apprendimento automatico.

Il bias potrebbe portare quindi a decisioni non corrette se i dati utilizzati per addestrare un modello contengono pregiudizi. Questo è particolarmente preoccupante in ambiti come la cybersicurezza, dove una valutazione errata delle minacce può avere conseguenze gravi.

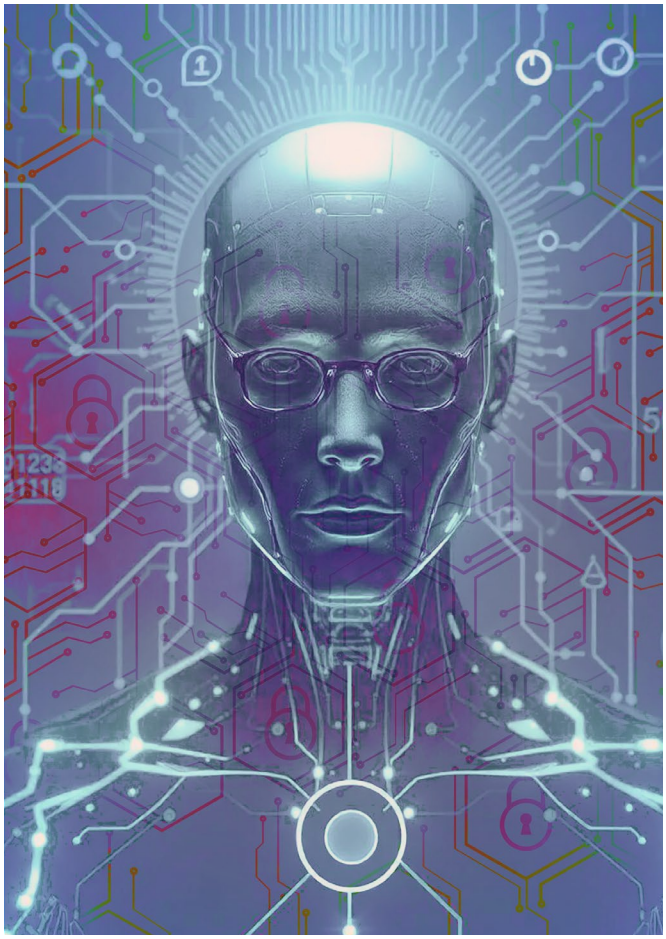
L'adozione massiva di IA in cybersecurity comporta rischi tutt'altro che trascurabili relativi ad una maggiore automazione e persino alla continuità operativa.

Se da un lato, l'IA può ridurre il coinvolgimento umano nella gestione della sicurezza migliorando l'efficienza, è possibile instillare un falso senso di sicurezza. Le organizzazioni potrebbero trascurare l'importanza della componente umana nelle attività di supervisione e valutazione di scelte critiche, aumentando il rischio di attacchi di esposizione alle minacce.

È essenziale che analisti di sicurezza continuino a svolgere un ruolo attivo nella valutazione delle minacce e nella gestione degli incidenti, anche in ambienti in cui vi è una adozione massiva di sistemi basati su IA.

L'integrazione dell'IA nei sistemi di sicurezza può comportare rischi per la continuità operativa. La compromissione di sistemi di IA potrebbe portare a interruzioni significative delle operazioni aziendali. È fondamentale che le organizzazioni implementino piani di continuità e strategie di gestione degli incidenti specifiche per affrontare incidenti legati all'IA.

In conclusione, l'IA è un potente alleato nella lotta contro le minacce informatiche, ma richiede un approccio equilibrato e collaborativo. È fondamentale investire in formazione specializzata, sviluppare tecnologie di sicurezza all'avanguardia e promuovere un dialogo costante tra esperti del settore, policymaker e sviluppatori. Solo così potremo sfruttare appieno i benefici dell'IA, mitigandone i rischi.



Intelligenza Artificiale: prime regole dal Governo e impatti sulle PMI

A cura di Enzo Veiluva

Breve sintesi dei principali aspetti definiti nel DDL del Governo sull'IA e quali impatto per le PMI

Mercoledì 13 marzo il Parlamento Europeo approvava il testo del Regolamento sull'Intelligenza Artificiale (di seguito: Regolamento o AI Act). A poco più di un mese, il Consiglio dei Ministri italiano (23 aprile) approva un disegno di legge per l'introduzione di disposizioni e la delega al Governo in materia di Intelligenza Artificiale, proprio in continuità con l'AI Act.

Questa accelerazione normativa dell'Europa e del Governo Italiano sul tema dell'IA sta a dimostrare quanto sia ritenuto strategico l'argomento, ma al tempo stesso quanto forte sia la preoccupazione dei rischi e dell'evoluzione, se non vengono definiti paletti e regole chiare di utilizzo. E pensare che il tema dell'IA non è recente, la data di nascita ufficiale dell'IA, risale ben al 1956, l'anno del famoso seminario estivo tenutosi presso il Dartmouth College di Hanover (New Hampshire). A 70 anni di distanza da allora il contesto è però totalmente diverso: la digitalizzazione dei nostri dati, l'informatizzazione dei sistemi e dei processi , la profilazione continua a cui siamo sottoposti, i rischi e pericoli del furto d'identità digitale e decisione automatizzata ci portano ad un mondo dove l'uso dell'IA può avvenire esclusivamente in presenza di regole chiare e di tutele !

Ed è proprio su questi temi che si sviluppa il DDL italiano, focalizzandosi sulle opportunità che offrono le nuove tecnologie, ma anche i rischi legati al loro uso improprio, al loro sottoutilizzo o al loro impiego dannoso.

I capi su cui si sviluppano i 26 articoli del DDL prendono in considerazione cinque punti:

1. Finalità e principi.
2. L'uso dell'IA nei settori (sanità, lavoro, giustizia, etc)
3. Strategia del Governo e attività di promozione.
4. La tutela del diritto di autore.
5. Le sanzioni.

Finalità e Principi

Principio sovrano l'IA (ricorda un po' la prima legge sulla robotica): è uno strumento di supporto e non deve pregiudicare in alcun modo i diritti e le libertà dell'essere umano; deve essere sempre garantita e vigilata la correttezza, l'attendibilità, la sicurezza, la qualità, l'appropriatezza e la trasparenza.

L'uso dell'IA non deve quindi creare situazioni di discriminazione e occorre soprattutto porre massima attenzione al suo utilizzo malevolo, presidiando la cybersicurezza lungo tutto il ciclo di vita dei sistemi e dei modelli di Intelligenza Artificiale, secondo un approccio proporzionale e basato sul rischio.

L'uso dell'IA nei vari settori

Alcuni ambiti come la sanità, il lavoro , la ricerca offrono casi utili di applicazione dell'IA, ed il Governo ribadisce, che il tutto deve avvenire sempre nel pieno rispetto del regolamento UE n. 679/2016, da parte dei soggetti autorizzati per legge a trattare dati personali.

I trattamenti di dati sanitari eseguiti da soggetti pubblici e privati senza scopo di lucro per la ricerca e la sperimentazione scientifica nella realizzazione di sistemi di Intelli-

genza Artificiale per finalità terapeutica e farmacologica, sono dichiarati di rilevante interesse pubblico.

Si istituisce una piattaforma di Intelligenza Artificiale per il supporto alle finalità di cura e, in particolare, per l'assistenza territoriale, in capo ad AGENAS (Agenzia Nazionale Sanità), che con proprio provvedimento, specifica i tipi di dati trattati e le operazioni eseguite all'interno della piattaforma, nonché le misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio.

Idem per il l'utilizzo in ambito lavoro vale in primis il principio di equità e non discriminazione, stabilendo che l'utilizzo dei sistemi di IA non può in nessun caso creare situazioni di discriminazione.

Per l'utilizzo dell'IA nel settore dell'attività della pubblica amministrazione la finalità principale è l'efficienza dell'attività amministrativa, come pure nell'amministrazione della giustizia l'utilizzo dell'IA è consentito esclusivamente per finalità strumentali e di supporto, quindi per l'organizzazione e la semplificazione del lavoro giudiziario anche finalizzata all'individuazione di orientamenti interpretativi.

Strategia governativa sull'IA

Il Capo normativo mette subito in chiaro la strategia ed i ruoli del governo sull'IA:

- La strategia nazionale per l'Intelligenza Artificiale è predisposta e aggiornata dalla struttura della Presidenza del Consiglio dei ministri.
- La strategia favorisce la collaborazione tra le amministrazioni pubbliche e i soggetti privati relativamente allo sviluppo e adozione di sistemi di Intelligenza Artificiale.
- l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN) sono Autorità nazionali per l'Intelligenza Artificiale.

Definito che deve stare al timone della regolamentazione e monitoraggio della strategia sull'IA, si passa alla definizione economica degli investimenti, partendo dai 300.000 per ciascuno degli anni 2025 e 2026 per la realizzazione di progetti sperimentali volti all'applicazione dell'Intelligenza Artificiale ai servizi forniti dal Ministero degli affari esteri e della cooperazione internazionale a cittadini e a imprese.

Molto interessante tutto l'art 22 ove il governo pone in previsione percorsi di alfabetizzazione e formazione in materia di utilizzo dei sistemi di Intelligenza Artificiale.

Il diritto di autore

Negli obiettivi del Capo IV è immediato leggere tra le righe la necessità di contrastare i "deepfake", cioè i contenuti audiovisivi che presentano come reali materiali o altri file che riproducono suoni voci e immagini in movimento, generati, modificati o alterati attraverso l'utilizzazione di sistemi di Intelligenza Artificiale. "Qualunque contenuto informativo diffuso da fornitori di servizi audiovisivi che, previa acquisizione del consenso dei titolari dei diritti, sia stato, attraverso l'utilizzo di sistemi di intelligenza artificiale, ovvero, anche parzialmente, modificato o alterato in modo tale da presentare come reali dati, fatti e informazioni che non lo sono, deve essere reso, chiaramente visibile e riconoscibile da parte degli utenti mediante inserimento di un elemento o segno identificativo, anche in filigrana o marcatura incorporata purché chiaramente visibile e riconoscibile, con l'acronimo "IA".

Le sanzioni

Come purtroppo sempre più spesso accade ogni tecnologia innovativa, oltre ad essere utilizzata per scopi

leciti, può essere utilizzata anche per la commissione di reati mirati alla truffa, estorsione, insidia o controllo dell'individuo. Per questo motivo il DDL indica la variazione dell'art. 494 del codice penale al quale si viene ad aggiungere che «La pena è della reclusione da uno a tre anni se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale».

Di pari passo tutti gli articoli, tipicamente legati ai reati informatici (612, 640, 648 nello loro declinazioni bis, ter , quater etc) vengono aggiornati includendo, l'eventuale utilizzo dell'IA per la commissione del reato. Sicuramente quanto qui riportato è solo un accenno della revisione della normativa sostanziale e processuale vigente, che deve essere rivista in merito all'impiego fraudolento dell'IA.

L'Impatto sulle PMI

Detto tutto quanto sopra riportato, quale impatto ne può derivare per le PMI? Considerato in generale che allo stato attuale l'impiego dell'Intelligenza Artificiale, in termini principalmente di analisi e supporto che vanno dagli assistenti virtuali, alla computer vision, all'analisi predittiva passando dalla comprensione di immagini e contenuti può dare benefici a chiunque voglia efficientare attività d'ufficio, di ricerca informazioni o di sviluppo software (chatGPT e copilot insegnano). Doveroso valutare sempre e comunque i rischi di non far debordare il "supporto nel" con la "sostituzione" o la "copiatura" del lavoro da svolgere (la tecnologia al servizio dell'uomo e non viceversa). Per quanto riguarda le opportunità delle PMI, non come fruitori ma come promotori dell'IA, l'art. 21 del DDL ribadisce l'autorizzazione fino all'ammontare di un miliardo di euro l'assunzione di partecipazioni nel capitale di rischio direttamente o indirettamente, di PMI e imprese finalizzate alla creazione e allo sviluppo di campioni nazionali nei settori e nelle tecnologie indicate. E gli ambiti tecnologici su cui cimentarsi sono molteplici a partire dall'Intelligenza Artificiale, alla cybersicurezza e dal quantum computing alle telecomunicazioni e alle tecnologie per queste abilitanti, al fine di favorire lo sviluppo, la crescita e il consolidamento delle imprese operanti in tali settori.

Insomma, un'opportunità assolutamente di riguardo per le PMI, che rappresentano da sempre la spina dorsale dell'economia italiana, di partecipare ancora una volta in prima linea allo sviluppo ed alla crescita di competenze e servizi tecnologici del nostro paese.

CYBER
Think Tank
ASSINTEL

Assintel Cyber Hub

Obiettivo:

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

Uniti per una sicurezza digitale senza confini!

Per info scrivi a:

segreteria@assintel.it

Silos-hacking: infiltrarsi nell'organizzazione per rafforzarla

Superare le barriere, introdursi nei processi ed esfiltrare conoscenze per integrare la sicurezza

A cura di Manuela Italia

Con l'evolversi delle dinamiche sociali, economiche e normative, in un contesto sempre più digitalizzato, la rete di interdipendenze tra i vari attori e fattori nel contesto aziendale è diventata sempre più fitta. In tutte le organizzazioni, ogni elemento, dal più semplice al più strategico, è parte di un ecosistema complesso, dove ogni cambiamento ha ripercussioni a catena.

L'Information Security si muove all'interno di questa rete di interconnessioni sempre più intricata, in cui organizzazioni complesse, funzioni, persone, processi, tecnologie, minacce e normative evolvono costantemente e si influenzano generando un vero e proprio effetto domino sulla postura di sicurezza aziendale.

Secondo un'indagine di PwC*, il 75% dei dirigenti ritiene che la complessità all'interno delle proprie organizzazioni possa creare rischi significativi per la cybersecurity. Questa percezione è ben fondata. Di fronte a questa complessità, l'introduzione di funzioni e processi sempre più specializzati indirizza diverse sfide, mentre ne introduce di nuove. Le aree specializzate, infatti, focalizzandosi sui propri ambiti di competenza ed obiettivi, rischiano di perdere la visione d'insieme, operando in modo frammentato e contribuendo alla formazione di silos operativi. Questo approccio può avere conseguenze dirette sull'efficacia e l'efficienza del sistema di gestione della sicurezza delle informazioni.

- Un esempio particolarmente emblematico e maldipancia quotidiano di ogni Chief Information Security Officer è la mancanza di allineamento tra la funzione di Information Security e le altre aree aziendali su strategie, iniziative e progetti critici. Quando questi vengono avviati senza considerare le implicazioni di sicurezza e le iniziative già in corso, non solo si moltiplicano i costi legati alla cybersecurity*, ma si compromette anche l'efficacia complessiva delle misure esistenti.
- La stessa funzione di Information Security spesso cade nella trappola dell'isolamento. Le strategie cyber sviluppate senza un adeguato input da parte del business e da altre funzioni rilevanti, composte da iniziative focalizzate principalmente ad implementare controlli tecnici standard e processi dedicati, risultano inconsistenti e disconnesse dalle reali esigenze aziendali.
- Un altro caso rilevante si verifica quando diversi team dell'azienda (es. Information Security, Privacy, Physical Security, Business Continuity, Finance) conducono valutazioni dei rischi senza linee guida comuni e coordinamento. Questo approccio genera spesso sovrapposizioni nelle aree di rischio e di controllo di ambito information security e rende difficile rappresentare i rischi in modo coerente e consolidato. A tal proposito, il Ponemon Institute, nel suo "Cost of a Data Breach Report 2021", ha evidenziato come le organizzazioni con un approccio frammentato alla gestione del rischio subiscano in media costi del 51,8% superiori in caso di violazioni dei dati rispetto a quelle con un approccio integrato.

- Le verifiche di audit e compliance rappresentano un altro terreno di sfida. Quando queste vengono definite senza una pianificazione condivisa e basate esclusivamente su requisiti normativi senza contesto, rischiano di diventare ridondanti, time-consuming e di non rispondere alle reali priorità, lasciando indisturbate le vulnerabilità più importanti.

- La disconnessione può estendersi fino alle interazioni tra Information Security e le funzioni che gestiscono gli aspetti legali. L'assenza di un linguaggio comune e la percezione di distanza tra queste funzioni (i tecnici da una parte, gli avvocati dall'altra), unita alla mancanza di dialogo costruttivo con regolatori e istituzioni, potrebbe generare errori nell'interpretazione dei requisiti normativi a svantaggio dell'azienda.

Quelli elencati sono solo alcuni dei fenomeni generati da un approccio a silos, ma gli esempi potrebbero essere molti altri: metriche e indicatori disomogenei, cambiamenti organizzativi definiti senza consultare le aree impattate, fino agli inventari degli asset non condivisi e a campagne di awareness che diffondono messaggi ridondanti e disorganici.

Tra le conseguenze più significative della frammentazione, in primo luogo, vi è **l'incapacità di fornire alla leadership una visione coerente e consolidata,** che porta a processi decisionali incoerenti e inefficaci. In secondo luogo, viene drasticamente limitata **l'efficacia della prevenzione e risposta agli incidenti di sicurezza.** Infine, come evidenziato dal "(ISC)² Cybersecurity Workforce Study", la mentalità a silos contribuisce a generare **culture organizzative malsane,** burnout e squilibrio tra lavoro e vita privata.

Di fronte a queste sfide, è chiaro che l'Information Security, per operare correttamente, necessiti di essere integrata nell'organizzazione in modo armonioso, condividendo obiettivi, processi e risorse con tutta la value chain. Quando questo approccio non è ancora consolidato in azienda, non è esplicitamente incluso nel mandato della funzione, o non viene promosso dalla leadership, è comunque necessario impegnarsi nella promozione di un cambiamento culturale. Per farlo, è fondamentale studiare a fondo il contesto e le dinamiche aziendali, identificare i punti di accesso che possano facilitare un dialogo e procedere con spirito critico, proattività e pazienza, riadattando continuamente le proprie tattiche.

Con l'evolversi delle dinamiche sociali, economiche e normative, in un contesto sempre più digitalizzato, la rete di interdipendenze tra i vari attori e fattori nel contesto aziendale è diventata sempre più fitta.

A tal proposito, framework e standard autorevoli come il NIST Cybersecurity Framework (NIST CSF), lo standard ISO/IEC 27001 e la recente NIS2 Directive forniscono linee guida preziose per una gestione strategica e integrata della sicurezza delle informazioni, favorendo un linguaggio comune tra diversi dipartimenti e facilitando la collaborazione. Il processo di hacking dei silos può essere agevolato dall'adozione di tali standard e normative, accompagnata da sforzi e azioni pratiche che i professionisti del settore devono attuare nella loro operatività quotidiana. Di seguito sono elencate alcune di queste azioni, che possono essere implementate in base al contesto e alle esigenze specifiche di ogni organizzazione:

- Impegno collettivo: la strategia di Information Security deve essere progettata e condivisa su vasta scala. Questo, non solo permette di raccogliere input preziosi, ma crea anche un senso di impegno comune. Cross-department meeting, aggiornamenti periodici e iniziative di comunicazione su strategia e iniziative sono cruciali per mantenere vivo questo impegno e intercettare cambiamenti e informazioni utili.

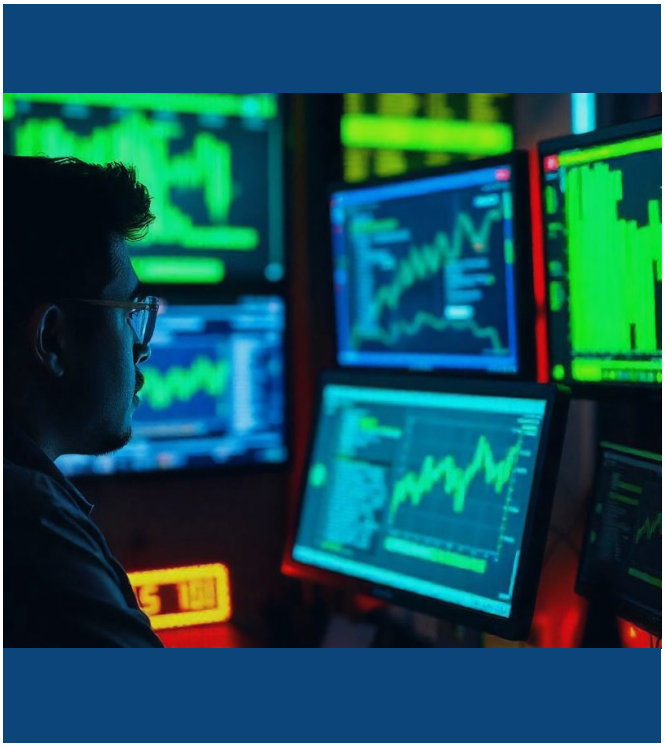
- Un team che include tutti: è fondamentale ripensare e promuovere l'Information Security come una responsabilità distribuita in un team che si estende su tutta l'organizzazione. La mappatura delle intersezioni tra le diverse funzioni aziendali, utilizzando strumenti come le matrici RACI, aiuta ad identificare gap o sovrapposizioni nelle responsabilità. In molti casi, è utile nominare dei "champion" o rivacy, Physical Security e modelli 231"evangelist" all'interno delle funzioni per fornire supporto diretto e diffondere le best practice,

creando un network capillare di competenze che rafforza il sistema complessivo e la sua resilienza.

- Fornire esperienze: le sessioni di formazione tradizionali non sempre sono l'opzione più efficace. Può essere opportuno organizzare iniziative di formazione più coinvolgenti ed esperienziali che favoriscano la partecipazione attiva, come simulazioni di incidenti, workshop e discussioni di case study. L'implementazione di meccanismi di raccolta continua di feedback è utile ad orientare meglio le scelte.

- Operare nel contesto: è fondamentale che i professionisti cybersecurity (e per quanto possibile, anche i fornitori) siano costantemente aggiornati sulla strategia e le principali iniziative aziendali, conoscano i processi, i crown jewels e le normative applicabili. Questo permette di adattare gli sforzi quotidiani al contesto e di gestire al meglio le priorità nel proprio ruolo.

- Parlare la stessa lingua: nel dominio Governance, Risk and Compliance (GRC), è essenziale utilizzare metodologie condivise (es. framework, controlli, owner, tassonomie) e linguaggi comuni, come glossari, su scala aziendale. Diversi assessment, se mappati adeguatamente, possono essere centralizzati in un repository comune a disposizione di più funzioni per la creazione di viste specifiche. Ad esempio, i framework di maturity level assessment sui domini Information Security, Privacy, Physical Security e modelli 231, tipicamente contengono alcuni controlli simili o equivalenti



- Non solo IT: anche le modifiche organizzative, alle procedure operative di business e i nuovi investimenti sono elementi che richiedono un'attenta valutazione degli aspetti di sicurezza. Allo stesso modo, la criticità dei fornitori deve essere valutata tenendo conto dell'impatto che questi hanno sui processi di business. È essenziale instaurare una collaborazione attiva e continua tra Information Security e le funzioni che gestiscono i fornitori e i fornitori stessi per creare un allineamento di intenti basato sul reciproco interesse.

- Alleanze importanti: il panorama normativo di Information Security è in fermento. È richiesto un forte allineamento con le funzioni legali, sia nel linguaggio che nelle prospettive, e una connessione con le specifiche autorità e associazioni di settore.

- Trovare soluzioni: di fronte ad un'esigenza rischiosa, rispondere subito con un NO in nome della policy, senza fornire spiegazioni adeguate, potrebbe rendere la vita del professionista cybersecurity apparentemente semplice. In realtà, questo atteggiamento, oltre a non essere collaborativo, incentiva lo shadow IT, spesso legato alla percezione di policy troppo rigide. Collaborare attivamente con i colleghi per individuare soluzioni pratiche ed equilibrate è una scelta che fa la differenza.

- Trasparenza: la creazione di portali aziendali dedicati all'Information Security, contenenti policy, procedure, linee guida, news, canali dedicati e contatti è un modo efficace per aumentare la trasparenza. L'utilizzo di piattaforme di collaboration e knowledge sharing rafforza ulteriormente la collaborazione tra i team e assicura un accesso rapido e centralizzato alle risorse.

In conclusione, un approccio all'information security sistemico, integrato e capillare, che superi le barriere dei silos, consente alle organizzazioni di destreggiarsi in un panorama di minacce in continua espansione e di reagire rapidamente e in modo coordinato agli attacchi cyber. Per affrontare le sfide attuali e future, è più che mai necessario promuovere una cultura di collaborazione e responsabilità condivisa che conduca ad un posizionamento dell'Information Security non solo come una questione tecnica, ma come un elemento integrato della strategia aziendale, che richiede il coinvolgimento e l'impegno di tutta l'organizzazione. Affinché questo approccio diventi effettivo e sostenibile, è essenziale una leadership forte e competente. Chief Information Security Officer qualificati e dotati di giuste leve e risorse rappresentano un fattore determinante per orientare l'organizzazione verso un modello di sicurezza resiliente e pienamente integrato nella governance e nell'ecosistema aziendale.

Integrare la sostenibilità nella Cybersecurity: un nuovo paradigma per aumentare l'efficienza

A cura di Massimo Ravenna

Negli ultimi anni, il dibattito sul rapporto tra sostenibilità e *cybersecurity* ha assunto un ruolo sempre più rilevante, soprattutto alla luce delle crescenti minacce digitali ad infrastrutture critiche che sono strettamente legate alla sostenibilità, come le reti di energia rinnovabile, l'acqua potabile e la gestione delle risorse ambientali. La cybersecurity è stata fino ad ora vista come un elemento chiave per proteggere queste infrastrutture, ma il legame tra i due ambiti è stato affrontato principalmente in modo unidirezionale: proteggere la sostenibilità attraverso la sicurezza informatica. Tuttavia, un approccio più innovativo potrebbe capovolgere questa visione, mettendo in luce come la sostenibilità possa essere un fattore strategico per migliorare l'efficienza della *cybersecurity* stessa.

Questa nuova prospettiva si fonda sull'idea che i principi della sostenibilità — come la riduzione degli sprechi, l'efficienza nell'uso delle risorse e l'integrazione di tecnologie più verdi — possano essere applicati direttamente alla gestione della sicurezza informatica. Non si tratta semplicemente di rendere "più ecologica" la cybersecurity, ma di utilizzare i driver della sostenibilità per migliorare la resilienza, l'efficienza e la capacità di adattamento dei sistemi di sicurezza. Questo approccio si inserisce perfettamente in contesti di crescente complessità, in cui le minacce informatiche evolvono rapidamente e dove le risorse — tanto energetiche quanto umane — devono essere utilizzate in modo sempre più efficiente.

Uno dei principali contributi alla riflessione su questa nuova visione proviene dal report *"Cybersecurity in ESG"*, che evidenzia come le imprese stiano cercando di integrare i rischi cibernetici all'interno delle loro strategie di sostenibilità e governance. Il report sottolinea che la crescente interconnessione delle infrastrutture critiche, come quelle energetiche, richiede l'adozione di pratiche sostenibili anche nell'ambito della cybersecurity, per assicurare che gli sforzi di decarbonizzazione e riduzione dell'impatto ambientale siano protetti da attacchi sempre più sofisticati. Tuttavia, c'è spazio per andare oltre questa visione difensiva, spostando il focus sulla **sostenibilità come fattore che migliora l'efficacia stessa della cybersecurity.**

Sostenibilità come Fattore di Efficienza nella Cybersecurity

Per comprendere appieno come la sostenibilità possa migliorare la cybersecurity, occorre partire dai principi che la governano. L'efficienza nell'uso delle risorse, la riduzione degli sprechi e la promozione di tecnologie a basso impatto ambientale sono concetti ormai centrali nella gestione aziendale, e questi stessi principi possono essere adattati ai sistemi di sicurezza informatica. Per esempio, l'adozione di pratiche di data minimiza-

tion — un principio fondamentale della protezione dei dati, come sancito dal GDPR — non solo riduce il rischio di attacchi, ma diminuisce anche la quantità di risorse (energia, capacità computazionale) necessarie per gestire

Un altro esempio di come i driver della sostenibilità possano arricchire la cybersecurity è l'ottimizzazione delle infrastrutture. *Data center* efficienti dal punto di vista energetico, sistemi di cloud computing ottimizzati per ridurre l'impronta di carbonio e l'uso di energie rinnovabili per alimentare queste infrastrutture non solo migliorano la sostenibilità complessiva delle operazioni, ma aumentano anche la resilienza della cybersecurity. In situazioni di crisi, sistemi progettati per funzionare con un consumo energetico ridotto sono meno vulnerabili a interruzioni dell'energia, il che può garantire continuità operativa anche durante attacchi su larga scala.

L'Integrazione della Sostenibilità nei Framework di Cybersecurity

Perché la sostenibilità possa effettivamente arricchire la cybersecurity, è necessario integrarla all'interno dei principali framework esistenti. Un esempio concreto è il *NIST Cybersecurity Framework (CSF)*, uno dei più diffusi standard per la gestione della sicurezza informatica. Questo framework si basa su cinque funzioni fondamentali — Identificare, Proteggere, Rilevare, Rispondere, Recuperare — che possono essere ulteriormente potenziate attraverso l'integrazione di controlli specifici di sostenibilità.

Un possibile approccio è l'introduzione di controlli di sostenibilità nelle prime fasi di valutazione del rischio e pianificazione strategica. Ad esempio, durante la fase di Identificazione, le organizzazioni potrebbero considerare non solo i rischi legati alle minacce informatiche, ma anche quelli legati all'efficienza energetica e alla gestione delle risorse dei loro sistemi informativi. Un sistema IT che consuma più energia del necessario non solo è meno sostenibile, ma potrebbe essere anche più vulnerabile, a causa dell'aumento delle superfici d'attacco (es. più server, più connessioni non ottimizzate).

Nella fase di Protezione, l'adozione di tecnologie sostenibili, come il cloud computing ottimizzato o la virtualizzazione dei server, può ridurre l'impatto ambientale, ma allo stesso tempo aumentare l'efficienza e la sicurezza. La capacità di allocare dinamicamente risorse solo quando necessario — una pratica standard nel cloud — significa che i sistemi sono meno esposti a potenziali attacchi derivanti da infrastrutture sovradimensionate o poco utilizzate. Adottare pratiche di "green IT" potrebbe dunque diventare una strategia centrale per ottimizzare la gestione della cybersecurity in modo sostenibile.

Infine, nelle fasi di Recupero e Risposta, l'approccio sostenibile può garantire che le risorse utilizzate per il ripristino delle operazioni in seguito a un attacco siano gestite in modo efficiente. Ad esempio, l'uso di energie rinnovabili per alimentare i data center di backup, insieme a tecnologie di ripristino automatizzate che riducono la necessità di intervento umano, può contribuire a una gestione più rapida e a un minor impatto ambientale durante la fase critica post-attacco.

Esempi di Driver di Sostenibilità nella Cybersecurity

Per concretizzare questo nuovo paradigma, è utile considerare alcuni driver di sostenibilità che possono essere integrati direttamente nei processi di cybersecurity. Uno dei principali e sicuramente più immediati è l'efficienza energetica. Le infrastrutture IT rappresentano una porzione significativa del consumo energetico globale, e la cybersecurity deve necessariamente tener conto di questo aspetto. Ottimizzare i consumi riduce i costi opera-

tivi, ma rende anche i sistemi più agili e resilienti, grazie alla riduzione della complessità e del numero di componenti fisici da proteggere.

Un secondo driver facilmente identificabile è la gestione responsabile dei dati. Minimizzare l'accumulo di dati non necessari non solo riduce il rischio di violazioni, ma anche l'impatto ambientale legato all'archiviazione e alla protezione di dati obsoleti. Questa pratica si allinea perfettamente con i principi della cybersecurity, che si focalizzano sulla protezione dei dati critici e sulla riduzione delle superfici d'attacco.

Infine, un terzo driver è l'uso di tecnologie verdi nei controlli di sicurezza. L'adozione di data center "carbon neutral", alimentati da fonti di energia rinnovabile, garantisce che le operazioni di cybersecurity siano intrinsecamente più resilienti e meno esposte alle interruzioni causate da eventi catastrofici legati ai cambiamenti climatici o ad attacchi mirati alle infrastrutture energetiche tradizionali.

Conclusione

In un contesto in cui le minacce informatiche sono in continua evoluzione e le risorse naturali sono sempre più preziose, l'integrazione della sostenibilità nella cybersecurity rappresenta un nuovo paradigma che può migliorare l'efficienza dei sistemi, ridurre i rischi e garantire un impatto ambientale ridotto. Attraverso l'adozione di driver di sostenibilità come l'efficienza energetica, la gestione responsabile dei dati e l'uso di tecnologie verdi, le aziende possono non solo migliorare la loro sicurezza informatica, ma contribuire attivamente a un futuro più sostenibile.

Incorporare tali principi nei framework di sicurezza come il NIST CSF può fornire alle organizzazioni un vantaggio competitivo, rendendo i loro sistemi più sicuri e resilienti, senza sacrificare l'impegno verso la sostenibilità. La cybersecurity e la sostenibilità, quindi, non devono essere viste come due entità separate, ma come elementi integrati di una strategia più ampia volta a garantire la resilienza e la sicurezza in un mondo sempre più interconnesso.

Mentre il mondo anglosassone, tradizionalmente più avanzato in termini di maturità tecnologica e di cybersecurity, continua a guidare la riflessione in questo ambito, anche in Italia emergono iniziative da seguire con interesse nel prossimo futuro, stanno nascendo Fondazioni ed Associazioni dedicate alla cybersecurity, che collaborano con il mondo accademico e player privati; Queste iniziative rappresentano un importante passo avanti nel promuovere un approccio integrato e sostenibile alla cybersecurity nel contesto italiano, che speriamo possa offrire nuovi spunti di riflessione per le imprese e le istituzioni del nostro Paese.

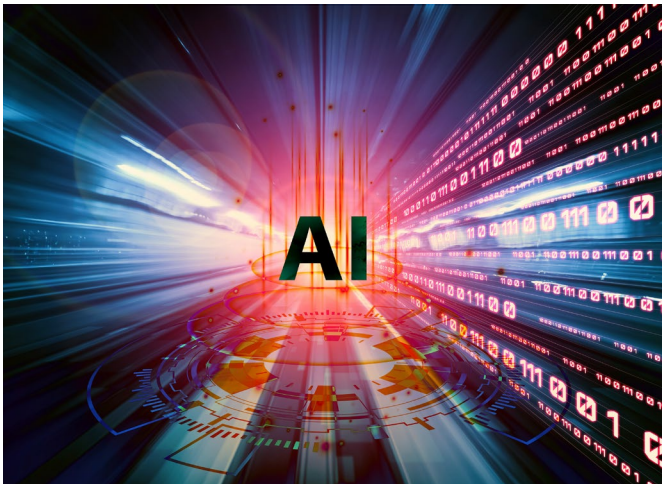
CYBER
Think Tank
ASSINTEL

IA, uno tsunami digitale inarrestabile: siamo pronti ad affrontarlo?

A cura di Ettore Guarnaccia

Le ondate di evoluzione tecnologica hanno sempre trasformato la nostra vita, e l'era dell'informatica ha portato rivoluzioni come il personal computer, Internet, i social media e gli smartphone. Oggi stiamo entrando in una nuova fase di innovazione, con l'intelligenza artificiale (IA) destinata a trasformare profondamente ogni settore della nostra società. Questa nuova ondata tecnologica si preannuncia inarrestabile e incontrollabile, paragonabile a uno tsunami.

Studio l'IA e le reti neurali da tempo e ho approfondito il loro enorme potenziale, ma anche i relativi rischi. Le grandi aziende tecnologiche prevedono che l'IA sostituirà molto presto i tradizionali motori di ricerca e assisterà le persone in moltissime attività, rendendo i processi aziendali più efficienti e redditizi. Tuttavia, come è già successo con Internet, i social media e i dispositivi digitali, non siamo ancora preparati a fronteggiare questa nuova rivoluzione tecnologica. Rischiamo quindi di pagare un prezzo elevato per la nostra mancanza di consapevolezza e formazione. Mustafa Suleyman, ex vicepresidente IA di Google e cofondatore di DeepMind, Geoffrey Hinton, pioniere della ricerca sulle reti neurali di Google, e il nostro Federico Faggin, inventore del microprocessore, profondo studioso delle reti neurali e fondatore di Synaptics, sono solo tre dei tanti esperti che ci avvertono dei rischi legati all'uso irresponsabile dell'IA, privo di supervisione umana ed etica. Non a caso, il World Economic Forum ha posizionato gli effetti avversi della tecnologia IA fra i più preoccupanti rischi globali.



Uno dei problemi principali dell'IA è l'accuratezza. Essendo sistemi probabilistici, le IA non garantiscono risposte sempre corrette, non conoscono la risposta esatta, ma forniscono la più plausibile, basandosi spesso su fonti online non sempre affidabili. Molte fonti, considerate autorevoli, sono contaminate da fake news, propaganda e vincoli dettati dal politically correct. Inoltre, l'uso dell'IA per produrre contenuti potrebbe portare a una sorta di circolo vizioso, in cui le IA creano e consumano contenuti generati da altre IA diventando autoreferenziali, e riducendo la qualità e la genuinità delle informazioni disponibili. Alcuni studi, come quelli svolti di recente da KPMG in collaborazione con l'università australiana del Queensland e da Salesforce, evidenziano che molti utenti ritengono che l'IA sia inaffidabile.

Un altro problema è la trasparenza. Molti utenti non sanno come funzionano i processi interni delle IA, e questo può portare a decisioni incomprensibili e difficilmente spiegabili. Le logiche nascoste potrebbero essere affette da pregiudizi di produttori e sviluppatori, nonché da cortocircuiti ideologici derivanti dall'uso di fonti contrastanti o prive di basi scientifiche e buon senso. E poi c'è il tema della responsabilità delle decisioni e delle azioni dell'IA, in caso di errori e danni è difficile stabilire chi sia responsabile: il produttore, chi l'ha addestrata o chi la utilizza? Inoltre, l'uso di contenuti protetti da copyright per l'addestramento delle IA è oggetto di dispute legali, come dimostra la causa intentata dal New York Times contro OpenAI e Microsoft.

L'IA viene spesso utilizzata in azienda in modo non regolamentato, creando rischi per la sicurezza dei dati aziendali. Uno studio recente di Microsoft e LinkedIn rivela che il 78% dei dipendenti nelle grandi aziende e l'80% nelle PMI utilizza già forme di IA generativa nei processi aziendali. Di conseguenza, ogni giorno dati, contenuti e documenti aziendali riservati vengono inavvertitamente caricati su piattaforme e app IA di terze parti per svariate finalità, all'insaputa dell'azienda, finendo nella disponibilità di soggetti non autorizzati. Al tempo stesso, i dipendenti concedono l'accesso agli strumenti aziendali di collaborazione (come Office 365, Teams, Zoom, ecc.) a soluzioni IA esterne, che ascoltano le videoconferenze in modalità silente e generano automaticamente i verbali degli incontri, inviandoli ai partecipanti. Molti di questi

aspetti hanno indotto grandi realtà come Apple, Amazon, JP Morgan, Goldman Sachs, Citigroup, Deutsche Bank, Walmart, Wells Fargo e Verizon a vietare ai dipendenti l'uso di IA generativa.

I sistemi IA possono essere vulnerabili ad attacchi informatici o manipolazioni dei dati. Ad esempio, casi come il bot Tay di Microsoft, che è stato rapidamente "corrotto" su Twitter fino a indurlo a utilizzare un linguaggio razzista e misogino, o AI Overviews di Google, che ha raccomandato l'uso di colla per far aderire il formaggio alla pizza, mostrano come l'IA possa essere alterata. Inoltre, attacchi di vario tipo (ad esempio XSS, CSRF, SSRF e DoS) e lo sfruttamento di vulnerabilità infrastrutturali o di elementi non protetti della supply chain possono comprometterne il funzionamento, con conseguente interruzione di processi di business critici e numerosi danni per le aziende. Così come l'IA può apportare grandi benefici alla sicurezza preventiva e alle capacità di rilevazione degli attacchi, essa viene utilizzata attivamente dai criminali per produrre nuovi e più efficaci attacchi, ad esempio phishing molto sofisticato attraverso la piattaforma WormGPT e malware in grado di modificare il proprio codice per eludere i sistemi di sicurezza, come dimostrato dal virus polimorfico BlackMamba sviluppato a scopo dimostrativo dai laboratori HYAS.

Oltre ai problemi tecnici, ci sono questioni etiche e sociali legate all'uso dell'IA. Il crescente utilizzo dell'IA in sostituzione di competenze umane potrebbe portare alla perdita di posti di lavoro. Questo rischio è già avvertito in settori come quello cinematografico, dove attori e sceneggiatori hanno scioperato per chiedere regolamentazioni sull'uso dell'IA. Nei prossimi anni, molti mestieri verranno sostituiti dall'IA, aumentando l'efficienza, ma anche mettendo in pericolo il futuro di molte professioni. Un recente studio di Microsoft e LinkedIn rivela che quasi la metà dei professionisti teme che l'IA sostituirà il proprio lavoro, mentre a Londra è già in funzione la prima biglietteria IA virtuale.

Infine, il problema più preoccupante, a mio avviso irrisolvibile, è che l'IA non possiede coscienza, empatia o libero arbitrio, non prova emozioni o sentimenti. In situazioni delicate, come conflitti armati, terrorismo, criminalità o scenari in cui è in gioco la vita delle persone (es. mezzi a guida autonoma o apparecchiature chirurgiche), a fronte di imprevisti l'IA potrebbe agire solo sulla base dei dati disponibili e delle logiche interne, senza considerazioni etiche o morali, senza compassione né intuito né creatività. Questo potrebbe portare a conseguenze devastanti e letali. Un migliaio di esperti hanno persino sottoscritto una lettera aperta per metterci tutti in guardia dal fatto che l'IA potrebbe in futuro diventare una minaccia per l'umanità intera, qualora non venisse adeguatamente controllata.

Per affrontare questa sfida, dobbiamo governare la nuova ondata tecnologica, non subirla passivamente. È indispensabile assicurare una supervisione umana costante sulle azioni e decisioni dell'IA, così come è urgente implementare politiche di sicurezza rigorose. È fondamentale adottare sia un controllo accurato dei dati inseriti dall'utente e delle fonti utilizzate dalle IA, sia un approccio "zero trust" con una netta separazione dei sistemi IA dal resto dell'IT aziendale, per impedire fughe non autorizzate di dati riservati. Solo con un uso etico e consapevole dell'IA potremo evitare le gravi conseguenze che un uso irresponsabile e impreparato potrebbe comportare, al tempo stesso preservando il ruolo unico e insostituibile dell'intelligenza umana.

Uno tsunami non può essere arrestato né impedito, ma è pur sempre possibile cavalcare l'onda.

Il paradigma di Carmine Miano: hacking VS Cyber Threat Intelligence

A cura di Raoul Chiesa

Le recenti cronache hanno visto protagonista il ventitreenne “super hacker” Carmine Miano, in quel di Gela.

Tanto è stato scritto nelle scorse settimane dai media nazionali. “Il più bravo hacker di sempre” intercettava investigatori, Pubblici Ministeri e leggeva le informative e le email che lo vedevano protagonista di indagini e procedimenti penali contro di lui. La realtà dei fatti non è esattamente così e porta, invece, ad un nuovo paradigma della Cybersecurity: i dati sono già stati rubati – spesso all’esterno del c.d. “perimetro aziendale” - e sono reperibili con estrema semplicità. Lo sanno tutti: cybercriminali, Governi (intesi come “State-Sponsored Attack”) e smanettoni di medio livello come nel caso di Carmine Miano… a quanto sembra, gli unici a non saperlo sono proprio le vittime, le aziende, gli enti ed i cittadini.

Un paradigma che gli analisti e gli esperti di CTI (Cyber Threat Intelligence) conoscono molto bene, oramai da diversi anni: le informazioni, i dati necessari a “sferrare un attacco” sono liberamente disponibili sui black forum del Dark e del Deep Web, così come su canali Telegram appositi. Credenziali di accesso, accoppiate “login e password” per sistemi di posta elettronica, connessioni VPN o addirittura verso le Intranet ed i server interni della maggior parte della Pubblica Amministrazione e aziende di piccole, medie e grandi dimensioni.

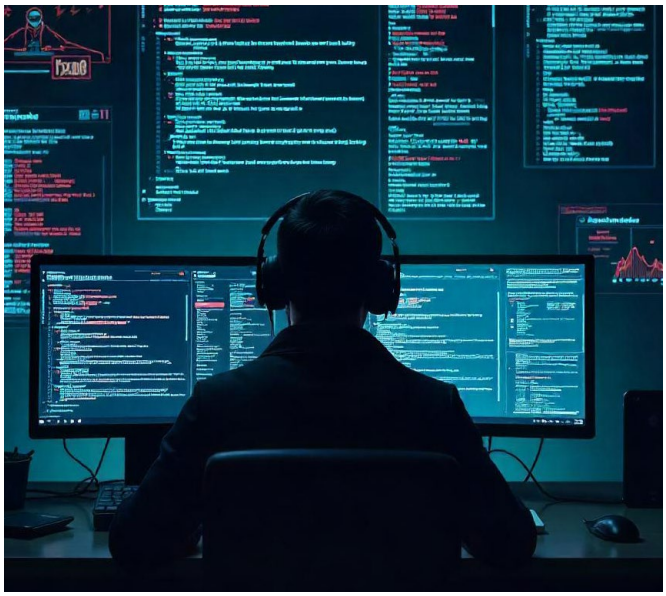
Quasi nessuna organizzazione ne è esente, generando così in questi anni nuovi approcci e nuovi modus operandi nella violazione di asset informatici, spesso intesi come compromissione dell’intera infrastruttura IT e TLC dell’organizzazione vittima. Le informazioni sono presenti, al di fuori del cosiddetto “perimetro aziendale” e, soprattutto, per pochi spicci.

Questo nuovo scenario ha quindi contribuito a creare un modello criminale: per violare un target oggi è sufficiente ottenere i file esfiltrati da PC, smartphone e tablet dei singoli utenti e infettati da malware, cercandoli all’esterno dell’organizzazione che si vuole attaccare.

Carmine Miano è stato paragonato a vere e proprie icone, come Kevin “The Condor” Mitnick, Kevin Poulsen o persino al sottoscritto. Un agente di minaccia, il Miano, così “lamer” da apparire su tutti i quotidiani e siti nazionali ritratto in una foto già divenuta celebre: inquadrato dalle telecamere nascoste installate dagli operativi delle Forze dell’Ordine a casa sua a Roma, nella stanzetta dalla quale lanciava i suoi “attacchi”.

Se però un ventitreenne con medie capacità tecniche ha potuto violare colossi come TIM, Noovle, Telespazio e Leonardo, solo per citare i più noti, ed accedere alle reti informatiche della Guardia di Finanza e di alcune Procure italiane…allora, abbiamo un problema. Non da poco ma, anzi, molto, molto serio.

È il paradigma a cui accennavo poco fa. È davvero sufficiente un TOR Browser, tanto tempo a disposizione e un pugno di accessi a certi specifici forum, per accedere ai dati più sensibili ed agli accessi più ad alto livello del nostro Paese? Purtroppo la risposta è sì.



Questo però è un problema non solo italiano ma, anzi, mondiale. Multinazionali ed Enti governativi di tutte le nazioni subiscono quotidianamente gli stessi danni, le stesse violazioni, le stesse esfiltrazioni di dati. Negli ultimi mesi ho personalmente visto, indagando e “ravanando” tra i dati esfiltrati da centinaia di malware, accessi che permettono il controllo completo di flotte di navi (da crociera, cargo, ecc), agenzie assicurative, banche nazionali e così via.

I motivi per i quali questo accade regolarmente, sino al punto di essere diventato, appunto, un modus operandi dichiarato e ben noto a chi lotta contro il cybercrime ogni giorno, sono principalmente due:

- il solito “fattore umano”, qui inteso però come smart working, utilizzo di PC (asset digitali) personali, ambiente domestico, rapporti relazionali e sociali di famiglia e di amicizia;
- un servizio come la CTI che, se da un lato paga sin dal proprio esordio sul mercato dell’offerta della Cybersecurity il fatto di essere una scienza molto recente, dall’altro vede tra i grandi player pochissimi “veri” fornitori (quelli che detengono i dati) e una moltitudine di piccoli, medi e grandi fornitori di servizi di CTI largamente orientati sul Dark e Deep web; ma giocoforza, e nella quasi totalità dei casi, privi di quei dati “che fanno la differenza”.

Questo porta, per svariate ragioni, ad una quasi totale ignoranza di questi “ecosistemi” e degli attori che li popolano, in un circolo di nutri-consuma dei nostri dati, strategici e personali, da parte dei Seller e dei Buyer del Cybercrime.

Le nostre identità digitali, le nostre informazioni aziendali sono oggetto di continue compravendite “all’ingrosso” così come al dettaglio, permettendo così la più totale violazione delle vite e delle attività professionali . Una specializzazione del fenomeno criminoso estremamente sottovalutata che, anche per questo, causa ogni anno danni immensi e conseguenze incredibilmente costose.

Cosa bisogna quindi fare per prevenire il mega-incidente informatico, il blocco delle aziende per ransomware e gli abusi e frodi contro i cittadini e le imprese del nostro Paese?

Bisogna iniziare a comprendere il paradigma, dando per assunto che “i nostri dati sono giù stati rubati”, e individuando un serio e competente fornitore di CTI per le verifiche del caso. Inoltre, le aziende e gli enti dotati di buon senso dovrebbero stipulare un abbonamento annuale con piattaforme di CTI dedicate e dinamiche, le quali informino in tempo reale le aziende dell’avvenuta compromissione e forniscano le evidenze del caso.

“Le nostre identità digitali, le nostre informazioni aziendali sono oggetto di continue compravendite ‘all’ingrosso’ così come al dettaglio”.

Non è un percorso difficile o complicato, tutt’altro. È soprattutto, invece, un cambio di mindset e modo di porsi verso la lotta al Cybercrime e nel contrasto agli incidenti informatici.

Ritengo sia però giunto davvero il momento di “toglierci il prosciutto dagli occhi” e comprendere come la CTI rappresenti, già oggigiorno, la migliore risorsa possibile per ottenere conferme, o smentite, rispetto alle tante keywords (ab)usate negli ultimi anni quando si parla di Cybersecurity aziendale e a livello Paese: Compliance, Verifiche di terze parti, bollini, certificazioni e chi più ne ha più ne metta.

Stiamo parlando dei nostri dati: il primo passo logico è verificare se ci sono già stati rubati e se addirittura sono in vendita a nostra totale insaputa…non mi sembra così difficile da comprendere ed accettare.

AI – DOMANDE E RISPOSTE FACILI FACILI
L'AI per il mondo educativo

A cura di Gianpiero Cozzolino

Come si utilizza l'AI nel mondo educativo?

Il mondo dell'educazione è uno dei più impattati dall'avvento dell'IA, soprattutto quella della branca "generativa". I docenti possono sfruttarla come supporto per la preparazione delle lezioni, per esempio generando i testi (che siano brevi, come uno script, o estesi, quindi un intero discorso o delle dispense), compiti e verifiche, immagini statiche da utilizzare come illustrazioni di supporto, video sia come supporto illustrativo che come videolezioni, persino presentazioni intere e mappe concettuali. Dall'altra parte, gli studenti la usano primariamente come supporto allo studio, per cercare risorse (sostanzialmente sostituendo il motore di ricerca a cui erano abituati fino a poco tempo fa) e per svolgere i compiti, anche in questo caso generando testi, immagini, video e presentazioni analogamente ai docenti.

Ma non esiste solo l'IA generativa: principalmente si può pensare anche alle IA che effettuano analisi, che possono essere utilizzate come ausilio per velocizzare la correzione delle verifiche e la generazione dei giudizi (nonché stimare il grado generale di insegnamento e apprendimento), oppure alle IA che possono riconoscere se qualche contenuto è stato generato con IA generativa.

Ci sono poi gli strumenti che "riconoscono" qualcosa a partire dal un'immagine (che sia già esistente o sia ciò che inquadra la fotocamera di uno smartphone in quel momento): in ambito scientifico (rocce, piante, animali, il cielo stellato, etc) o artistico (opere d'arte, musica e canzoni, paesaggi, etc), e ciò che ancora non viene riconosciuto prima poi lo sarà.

Nel particolare contesto delle materie artistiche, l'IA può essere non solo un ausilio come prima evidenziato, ma proprio l'oggetto dell'azione educativa: cioè va insegnato ad utilizzarla efficacemente in modo da rappresentare un ulteriore modalità di espressione, sia essa quella finale o come preparazione a tecniche espressive più tradizionali.

Quali sono le ultime attività che vengono supportate con l'IA?

Molto interessanti e particolarmente utili sono i servizi di trascrizione, spesso utilizzati in ambito professionale per tenere i verbali delle riunioni, che invece in ambito educativo possono essere utilizzati per le lezioni (versione tecnologicamente avanzata delle famose "sbobinature" delle lezioni universitarie); così come le traduzioni, in entrambi i "sensi", che possono rendere accessibili le più disparate risorse a quel pubblico più vasto che

non maneggia sufficientemente le lingue; infine, anche la possibilità di riassumere un documento (o anche un video) per estrapolarne gli aspetti principali può facilitare sia l'apprendimento che anche la ricerca di contenuti utili, scremandoli facilmente.

Un ambito certamente da sviluppare è quello degli strumenti che possono affiancare gli studenti che abbiano bisogno di sostegno, per esempio personalizzando il materiale didattico in funzione delle necessità di ognuno, favorendo l'inclusione e potenzialmente riducendo l'abbandono scolastico.

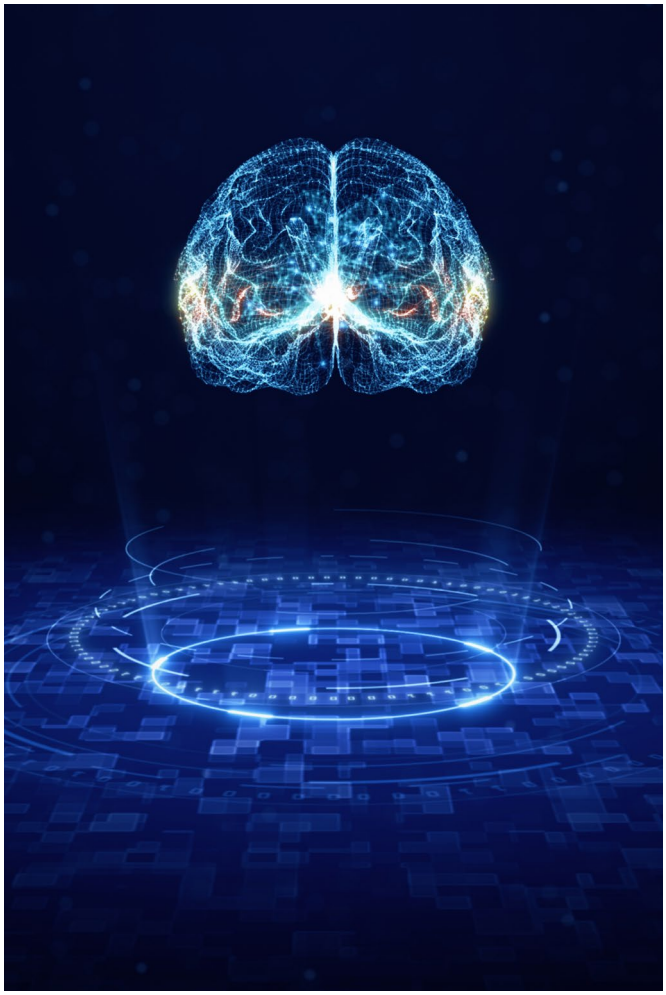
Cosa ne penso?

L'IA, sicuramente, serve a velocizzare una serie di compiti, sempre tenendo presenti tutti i rischi che ciò comporta; più che mai nell'ambito educativo il rischio è l'abuso, perché evidentemente l'imparare comporta impegno e tempistiche minime nel fare le cose in prima persona (non diversamente dagli allenamenti per le attività fisiche). Non va mai dimenticato che il risultato più importante dell'imparare è sviluppare un adeguato senso critico, che permetta di capire quando ci troviamo di fronte a qualcosa di dubbio, e ciò è particolarmente importante proprio con l'IA per via delle "allucinazioni", almeno finché esse non saranno eliminate.

Ciò non riguarda solo gli studenti, anche gli insegnanti non devono abusare delle opportunità degli strumenti di IA, poiché questi sono sostanzialmente impersonali, mentre l'insegnamento, per raggiungere il massimo risultato, dovrebbe sempre essere adattato al contesto specifico degli studenti (in particolare nella valutazione dei singoli).

Peraltro, anche l'IA va imparata, nel senso che è necessario non solo imparare ad utilizzare operativamente gli strumenti, ma anche a capirne i principi di funzionamento e le limitazioni, in modo che l'utilizzo sia consapevole e di conseguenza proficuo.

Concludo evidenziando che questa immane, amorfica, massa di dati diventerà il nostro curriculum fin dai primi mesi di vita, qui ci sarà l'obbligo di addentrarci su come usare i dati, per non catalogare a scaffale l'essere umano.

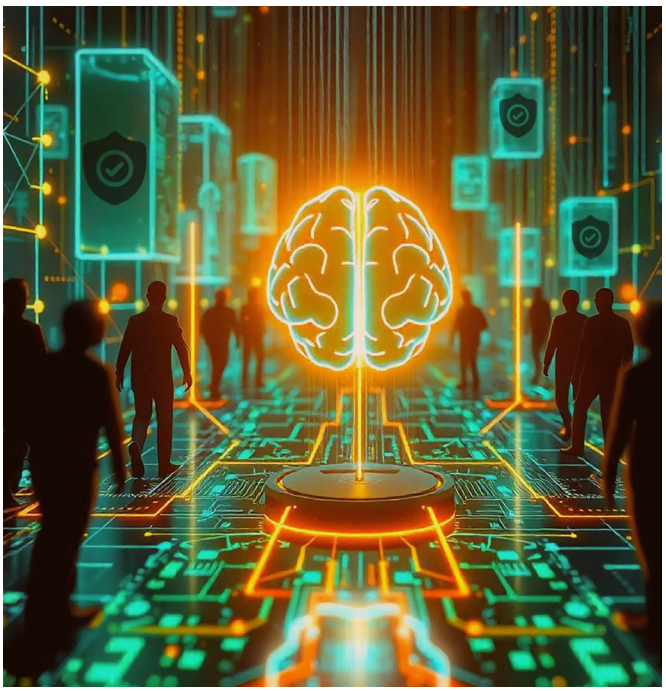


Cybersecurity e Intelligenza Artificiale: L'alleanza necessaria per un futuro digitale sicuro

A cura di Emiliano Marmondi

L'Intelligenza Artificiale (IA) sta rivoluzionando il mondo della tecnologia e non solo. Dalle auto a guida autonoma ai chatbot intelligenti, dalle raccomandazioni personalizzate di acquisto fino alle diagnosi mediche supportate da IA, questa tecnologia è sempre più integrata nella nostra vita quotidiana. Le opportunità create dall'IA sono potenzialmente immense, così come lo sono anche le cyber minacce che grazie alla IA stanno prendendo sempre più piede. L'uso dell'intelligenza artificiale nelle mani sbagliate può essere un'arma a doppio taglio, capace di esporre individui e organizzazioni a nuovi e sofisticati attacchi informatici.

La sicurezza informatica, oggi, non può più fare a meno dell'intelligenza artificiale, ma allo stesso tempo deve essere attrezzata per rispondere alle minacce derivanti dall'uso malevolo dell'IA stessa. A fronte di ciò, il tradizionale approccio alla sicurezza informatica, basato su misure preventive standard come firewall e antivirus, non è più sufficiente. Gli attacchi odierni sono più rapidi, più complessi e più difficili da individuare. Questo ha portato a una crescente domanda di soluzioni di cybersecurity avanzate, che siano in grado di rispondere in tempo reale alle minacce. È qui che l'intelligenza artificiale entra in gioco.



Intelligenza Artificiale e cybersecurity: le potenzialità

L'IA ha il potenziale per rivoluzionare la cybersecurity in molti modi, di seguito riporto solo alcune delle applicazioni principali, che possono essere d'aiuto a chi si occupa quotidianamente di sicurezza informatica:

1. Rilevamento delle minacce in tempo reale: Uno degli aspetti più significativi dell'uso dell'intelligenza artificiale nella cybersecurity è la sua capacità di analizzare grandi quantità di dati in tempo reale e rilevare anomalie. Attraverso l'uso di algoritmi di machine learning e deep learning, l'IA è in grado di riconoscere comportamenti sospetti, che potrebbero indicare un attacco informatico. Le soluzioni basate su IA sono in costante evoluzione e puntano sull'efficacia nell'individuare minacce zero-day e/o altre attacchi "non standard".

2. Automazione delle risposte: tutti noi sappiamo quanto sia importante la capacità e la velocità di risposta quando si tratta di contrastare un attacco informatico. Le soluzioni basate su IA ci possono aiutare non solo a identificare una minaccia in tempo reale, ma possono essere di aiuto per avviare delle risposte automatiche, atte a mitigare l'impatto dell'attacco in corso. Ridurre il tempo di reazione automaticamente abbassa il valore di rischio del potenziale danno. Ad esempio, un sistema di difesa IA può isolare una parte della rete compromessa non appena rileva un comportamento anomalo, può isolare un singolo client oppure può essere di supporto a un servizio SOC (security operations center) per analisi precise dei log.

3. Previsione e prevenzione degli attacchi: Un altro vantaggio dell'IA è la sua capacità predittiva. Attraverso l'analisi di grandi quantità di dati, l'IA può identificare modelli e tendenze che suggeriscono la possibilità di futuri attacchi. In questo modo, le organizzazioni possono adottare misure preventive prima che si verifichi un attacco. L'IA può anche simulare scenari di attacco, aiutando le aziende a testare e rafforzare le loro difese.

4. Gestione delle vulnerabilità: Le reti e i sistemi informatici moderni sono complessi e comprendono una vasta gamma di software e dispositivi. Identificare e correggere tutte le vulnerabilità presenti è un compito arduo e dispendioso in termini di tempo. L'IA può aiutare a identificare le vulnerabilità in modo più efficiente, aiutando nella prioritizzazione dei task da mettere in campo ed analizzando velocemente i potenziali punti deboli che richiedono attenzione immediata.

Tuttavia, l'Intelligenza Artificiale non è solo uno strumento a disposizione dei difensori, ma, purtroppo, anche di potenziali attaccanti. In questi mesi si è potuto notare un aumento consistente degli attacchi che sfruttano l'IA; tra questi il **"Deepfake e manipolazione di contenuti"** ossia video e audio falsificati con l'ausilio dell'Intelligenza Artificiale che possono essere utilizzati per diffondere disinformazione, ricattare persone o manipolare eventi e elezioni governative, etc.

Avendo l'IA a disposizione di molti (direi "on the shelf") anche **gli attacchi automatizzati** più "banali" come il brute force, per esempio, possono essere eseguiti in modo più efficiente e con meno risorse grazie agli algoritmi di machine learning. Gli stessi **ransomware** possono diventare più efficaci, imparando ad evitare i sistemi di difesa e a criptare dati in modo più intelligente e rapido, sfuggendo così alle potenziali misure di remediation.

L'utilizzo della IA in campo della cybersecurity e non solo solleva importanti questioni etiche e normative. Da un lato, l'IA offre molteplici opportunità per migliorare la sicurezza dei sistemi informatici, ma dall'altro presenta rischi legati alla privacy e all'uso scorretto dei dati. I sistemi di IA, per essere efficaci, richiedono grandi quantità di dati per addestrarsi, il che può comportare l'accesso a informazioni sensibili o personali.

Inoltre, esiste il rischio che algoritmi di intelligenza artificiale possano essere distorti o manipolati, portando a decisioni errate o discriminatorie. Questo apre la strada a domande su come regolamentare l'uso dell'IA nella cybersecurity e su chi sia responsabile in caso di errori o violazioni della privacy.

Il futuro della Cybersecurity con l'IA

Guardando al futuro, è chiaro che l'Intelligenza Artificiale giocherà un ruolo sempre più importante nella cybersecurity. Le aziende e le organizzazioni che abbracceranno questa tecnologia saranno meglio equipaggiate per fronteggiare le minacce informatiche in continua evoluzione. Tuttavia, sarà fondamentale un approccio equilibrato, che consideri i benefici dell'IA, ma che, contemporaneamente, metta al centro sempre il professionista con le sue capacità. L'IA dovrà essere sempre di più un potenziatore di queste capacità, considerando anche le sfide etiche e normative che essa porta con sé.

La collaborazione internazionale sarà cruciale per sviluppare standard e normative globali che possano gestire l'uso dell'IA nella cybersecurity. La minaccia informatica è globale e non conosce confini: solo con un approccio concertato sarà possibile sfruttare appieno le potenzialità dell'IA e, allo stesso tempo, proteggere la sicurezza e la privacy degli individui e delle organizzazioni.

Minacce nascoste nei Marketplace: difendersi con le TTP e la Pyramid of Pain

A cura di Martina Fonzo

Negli ultimi anni, gli attacchi informatici ai dispositivi mobili sono diventati sempre più complessi, con malware che riescono a superare i controlli di sicurezza e diffondersi persino attraverso marketplace ufficiali. Gli attori malevoli hanno perfezionato le loro tecniche, usando metodi come la code obfuscation e il dynamic code loading. In pratica, si tratta di mascherare il comportamento dannoso di un'applicazione, che si attiva solo dopo l'installazione, magari attraverso aggiornamenti o moduli scaricabili in seguito. Questo trucco permette ai malware di passare inosservati durante i controlli preliminari, e spesso gli antivirus basati su firme statiche non riescono a individuarli perché il codice dannoso resta dormiente fino al momento giusto.

Un altro problema è l'uso crescente di botnet mobili, reti di dispositivi infetti che gli attori malevoli sfruttano per attacchi su larga scala, furto di dati o la diffusione di altro malware. In Italia, il numero di dispositivi mobili compromessi è in costante aumento, molte volte a causa di applicazioni che sembrano innocue al momento dell'installazione, ma che poi si trasformano in strumenti per scopi malevoli.

Tradizionalmente, una delle tecniche per difendersi da queste minacce è il monitoraggio degli Indicatori di Compromissione (IoC), come indirizzi IP, domini o hash di file sospetti. Tuttavia, il problema con gli IoC è che sono facilmente modificabili. Un attaccante può cambiare velocemente un dominio o un indirizzo IP per evitare di essere rilevato. Questo rende difficile basare l'intera strategia di difesa su questi indicatori, che spesso hanno una durata molto breve.

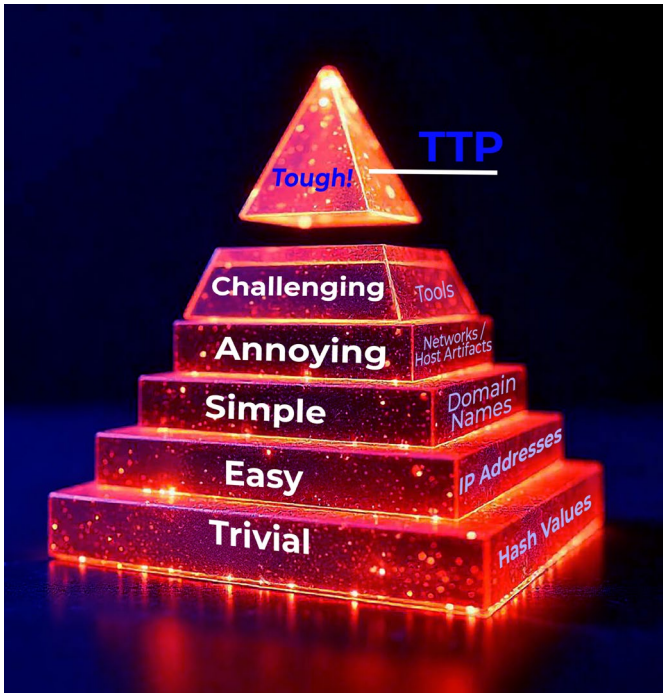
Ed è qui che entra in gioco il concetto della Pyramid of Pain. Secondo questa teoria, più in alto si trova un elemento nella piramide, maggiore è la difficoltà per un attaccante di modificarlo. Gli IoC, che si trovano nella parte bassa della piramide, sono i più facili da cambiare. Ma se saliamo nella piramide, troviamo le Tecniche, Tattiche e Procedure (TTP), ovvero i metodi e le strategie che gli attori malevoli usano per portare a termine un attacco. Cambiare i TTP richiede molto più tempo e impegno rispetto alla semplice modifica di un dominio o di un hash. Questo rende i TTP un bersaglio molto più efficace per chi si occupa di sicurezza.

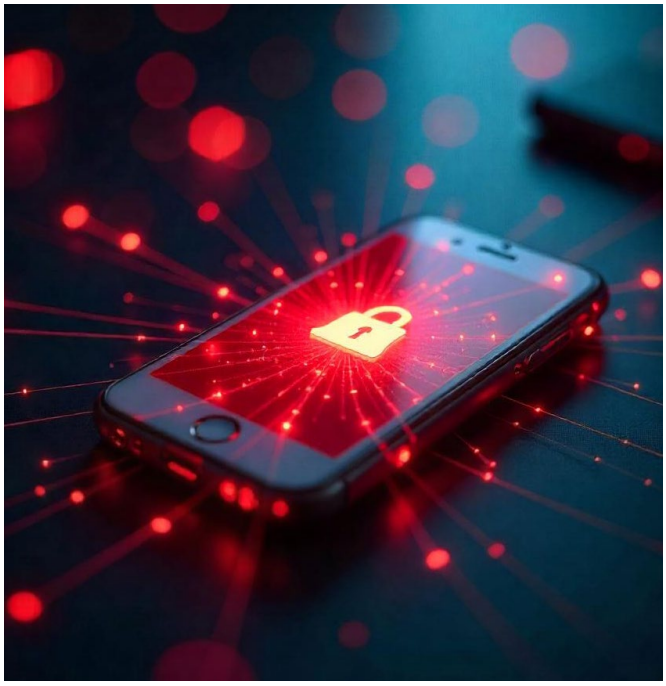
Concentrarsi sui TTP significa costringere l'attaccante a cambiare il suo approccio, una cosa che richiede tempo e risorse. Questo rallenta le operazioni malevole e dà alle difese il tempo necessario per reagire e migliorare la propria capacità di rilevamento. Ad esempio, un malware mobile può cambiare facilmente il dominio del suo server di comando e controllo (C2) per evitare di essere

bloccato, ma il modo in cui comunica con i dispositivi infetti – il protocollo utilizzato o le tecniche di crittografia impiegate – rimane spesso costante. Monitorando questi comportamenti, è possibile individuare la minaccia anche se gli IoC sono cambiati.

La Threat Intelligence è uno strumento fondamentale per questo tipo di analisi. Mentre gli IoC ci danno indicazioni su minacce note, l'analisi dei TTP ci aiuta a comprendere e prevedere il comportamento degli attaccanti, permettendoci di reagire in maniera più efficace. Questo approccio non significa ignorare gli IoC, che restano comunque importanti, ma semplicemente spostare l'attenzione su elementi che richiedono più tempo e fatica agli attaccanti per essere modificati.

In definitiva, per migliorare davvero la sicurezza mobile, dobbiamo andare oltre il semplice monitoraggio degli IoC. Sì, sono utili, ma sono solo il primo livello di difesa. Concentrarsi su elementi più difficili da cambiare, come le TTP, ci permette di avere un vantaggio significativo nel fermare gli attaccanti. La Pyramid of Pain ci insegna che, spingendo un attaccante a dover modificare le sue TTP, possiamo guadagnare tempo prezioso per rafforzare le nostre difese e migliorare la detection. In un panorama di minacce in continua evoluzione, questo approccio ci dà la possibilità di rimanere un passo avanti rispetto agli attacchi.





"La Pyramid of Pain ci insegna che, spingendo un attaccante a dover modificare le sue Tattiche, Tecniche e Procedure (TTP), possiamo guadagnare tempo prezioso per rafforzare le nostre difese".

NIS2 panoramica

A cura di Francesco Tieghi

Il decreto legislativo n. 138 del 4 settembre 2024 ha recepito nel nostro Paese la Direttiva cosiddetta NIS2, pubblicata il che entrerà in vigore il 18 Ottobre. Esso introduce un nuovo quadro normativo per rafforzare la sicurezza informatica nell'Unione Europea. Le aziende coinvolte devono dichiararsi soggette alla normativa entro il 1 Gennaio 2025, mentre i controlli e l'applicazione delle sanzioni partiranno da Marzo 2025. Le sanzioni per chi non rispetta le disposizioni sono pesanti e possono arrivare fino a 10 milioni di euro o al 2% del fatturato globale, proporzionate alla gravità delle infrazioni.

La NIS2 rappresenta un'evoluzione rispetto alla versione precedente, ampliando significativamente il campo d'azione. Oltre ai settori già considerati critici, come energia e trasporti, ora vengono inclusi nuovi ambiti, come la fabbricazione di sostanze chimiche, alimenti, dispositivi medici, computer e autoveicoli. Questo allargamento implica che molte entità, prima non coinvolte, dovranno adottare misure di sicurezza più rigorose per proteggere le loro reti e sistemi informativi.

Le categorie principali coinvolte dalla normativa sono gli Operatori di Servizi Essenziali (OSE), che includono settori chiave come energia, sanità, trasporti e infrastrutture digitali, e i Fornitori di Servizi Digitali (DSP), come piattaforme online e servizi cloud. Entrambe queste categorie devono garantire un alto livello di sicurezza e notificare tempestivamente eventuali incidenti di sicurezza alle autorità competenti.

Con la scadenza fissata per l'1 Gennaio 2026, le aziende hanno circa un anno di tempo per adeguarsi. Il percorso per conformarsi alla NIS2 richiede l'adozione di un approccio strutturato che prevede tre punti chiave:

Strutturazione del team di sicurezza: Non si tratta solo di formazione, ma di creare un team dedicato, con risorse interne o esterne, responsabile delle attività di monitoraggio, rendicontazione e gestione degli incidenti. È essenziale definire ruoli e responsabilità in modo chiaro e preciso.

Gestione degli incidenti e delle notifiche: La rendicontazione degli attacchi e degli incidenti di sicurezza diventa centrale nella strategia di difesa cibernetica. Le autorità competenti devono essere informate tempestivamente, pena ulteriori sanzioni.

Tecnologie per la sicurezza: la NIS2 richiede l'adozione di misure tecniche, operative e organizzative adeguate per proteggere le infrastrutture critiche. Non si scende nei dettagli di ogni attività specifica, ma si raccomanda un approccio "multi-rischio", in grado di proteggere sia l'ambiente digitale che fisico.

Tra le tecnologie da implementare, emerge l'importanza della gestione dei backup e del ripristino dei dati, per assicurare la continuità operativa delle infrastrutture critiche. Le soluzioni più avanzate prevedono l'uso di storage resilienti, come sistemi RAID o distribuiti, e backup su cloud, per proteggere i dati anche da eventi catastrofici o violazioni della sicurezza. Inoltre, l'automazione dei processi di ripristino consente di minimizzare il downtime e riprendere rapidamente le operazioni in caso di interruzioni.

La NIS2 richiede inoltre una maggiore consapevolezza della rete e dei suoi punti deboli. Gli audit di sicurezza e le scansioni periodiche diventano obbligatori, soprattutto in ambienti operativi come le industrie manifatturiere, dove è necessario monitorare costantemente le vulnerabilità.

Le tecnologie di anomaly detection, basate su algoritmi di machine learning, possono rilevare comportamenti anomali o sospetti, prevenendo incidenti prima che compromettano la produzione o la sicurezza delle infrastrutture.

Infine, la continuità operativa è un pilastro essenziale della sicurezza informatica secondo la NIS2. Le aziende devono sviluppare piani di emergenza e ripristino, testati con simulazioni periodiche, per garantire la disponibilità dei servizi essenziali anche in caso di incidenti. L'implementazione di infrastrutture ridondanti e sistemi di failover diventa cruciale per minimizzare i tempi di inattività.

Con l'avvicinarsi della scadenza dell'1 Gennaio 2026, le entità coinvolte devono accelerare l'implementazione delle misure necessarie per conformarsi alla direttiva. L'adozione di tecnologie avanzate per la gestione dei dati, il monitoraggio continuo e la continuità operativa saranno determinanti per garantire la sicurezza e la resilienza delle infrastrutture critiche, riducendo al minimo i rischi di violazioni e interruzioni dei servizi. I fornitori di tecnologie specializzate in sicurezza informatica saranno partner strategici per aiutare le aziende in questo processo di trasformazione e adeguamento.

CYBER
Think Tank
ASSINTEL

Decentralizzazione: la rivoluzione dei dati e non solo

A cura di William Nonnis

Viviamo in un mondo dove tutti, nessuno escluso – cittadini, imprenditori, politici – sono sempre più connessi. Per questo, è importante migliorare le nostre conoscenze usando gli strumenti che la tecnologia ci offre. Imparare a usare il digitale ci rende più sicuri su quello che facciamo, aiutandoci a capire cosa è giusto e cosa no. Anche il presidente Mattarella ha ricordato che le tecnologie, come l'intelligenza artificiale, devono essere al servizio dell'uomo e non il contrario.

Egli ha sottolineato l'importanza di stabilire regole comuni e globali per gestire la tecnologia in modo corretto. Inoltre, il Presidente ha opportunamente posto l'attenzione su chi gestisce le informazioni e su quanto siamo disposti a cedere il controllo dei nostri dati a terzi, spesso a vantaggio di grandi aziende, le cosiddette Big Tech. Queste aziende hanno ormai un enorme potere e influenzano molti aspetti della nostra vita quotidiana.

Per questo motivo, credo che ogni persona debba essere responsabile e consapevole della gestione delle proprie informazioni. È fondamentale essere formati e informati, con l'obiettivo di promuovere la decentralizzazione e la distribuzione delle informazioni, in modo che il controllo non sia concentrato nelle mani di pochi.

La decentralizzazione, intesa come distribuzione delle informazioni e dei poteri decisionali tra più attori anziché concentrarli in un'unica entità centrale, rappresenta un tema di crescente importanza in un'era in cui la gestione dei dati e dei servizi è dominata da grandi aziende tecnologiche. La centralizzazione dei dati e la loro vulnerabilità, come dimostrano i recenti scandali di spionaggio e fuga di informazioni, evidenziano la necessità di un nuovo paradigma. La decentralizzazione offre una risposta innovativa, con benefici che si estendono in vari settori, tra cui quello finanziario e sanitario.

Benefici della decentralizzazione

La decentralizzazione non riguarda solo una migliore gestione dei dati, ma porta con sé un cambiamento culturale. Ogni cittadino avrebbe il controllo diretto delle proprie informazioni, riducendo l'influenza dei colossi tecnologici. Settori come quello finanziario e sanitario, in cui vengono generate e gestite enormi quantità di dati sensibili, trarrebbero grandi benefici da questo nuovo approccio. Grazie alla decentralizzazione, questi settori potrebbero vedere una riduzione delle violazioni della privacy e una maggiore sicurezza nella gestione delle

informazioni personali.

Miglioramento della sicurezza dei dati bancari

L'adozione della decentralizzazione nei servizi bancari potrebbe rappresentare una vera rivoluzione. Attualmente, le grandi aziende tecnologiche, note come GAFAM (Google, Amazon, Facebook, Apple e Microsoft), hanno il controllo delle regole globali sulla gestione delle informazioni. La decentralizzazione propone di restituire ai cittadini il controllo dei propri dati, permettendo loro di monetizzare le informazioni generate, anziché cederle involontariamente a queste aziende.

Questo cambiamento si fonda sul principio della responsabilizzazione individuale e sulla realizzazione del Web 3.0, in cui le informazioni personali diventano beni di valore economico gestiti direttamente dai legittimi proprietari. In questo contesto, la decentralizzazione protegge non solo la privacy, ma anche la dignità degli individui, evitando intrusioni non autorizzate nei loro dati personali, come dimostrato dal recente scandalo che ha coinvolto la Premier Giorgia Meloni e altre figure pubbliche.

Rischi e benefici nella decentralizzazione

Oggi, la gestione di grandi quantità di dati presenta rischi sia per i sistemi centralizzati che per quelli decentralizzati o distribuiti. Tuttavia, quando i dati sono centralizzati, i pericoli sono più significativi, perché tutto ciò che passa attraverso la rete può essere manipolato.

Nel nostro Paese, l'infrastruttura digitale è ancora vulnerabile, e molti sistemi di archiviazione sono facili da violare. Questo rende relativamente semplice rubare informazioni. La centralizzazione dei dati facilita questi problemi, con il rischio che, nella migliore delle ipotesi, qualcuno acceda ai dati per curiosità o, nel peggiore dei casi, li venda per profitto.

Oltre ai problemi legati ai piccoli furti o alle attività criminali, esiste una preoccupazione più grande: in Italia, molti dati sono ancora archiviati senza adeguate protezioni (come la crittografia).

Spesso ci si affida a slogan come "crittografia end-to-end" (ad esempio su WhatsApp), senza capirne realmente il significato. Inoltre, i dispositivi e le app che gestiscono dati sono spesso utilizzati con superficialità, anche da minori che condividono liberamente informazioni in rete.

È quindi necessario educare le persone su come gestire in modo sicuro e responsabile i propri dati. Dobbiamo anche ripensare il sistema centralizzato che, di fatto, non lascia molta scelta a chi non vuole che la propria vita diventi merce di scambio. La protezione dei cittadini online non dovrebbe dipendere dall'etica o dalla competenza degli operatori, ma da un sistema sicuro e inac

cessibile alle minacce esterne. Questo tipo di sicurezza può essere garantito solo dalla decentralizzazione e distribuzione delle informazioni.

La Blockchain decentralizzata/distribuita, una tecnologia che non è soggetta a controlli esterni, offre una soluzione concreta. Con l'arrivo del Web 3, ogni utente può finalmente diventare proprietario dei propri dati, decidendo di mostrare o nascondere informazioni in base alle proprie necessità.

Un esempio concreto dei benefici della blockchain riguarda il settore sanitario. Attualmente, la gestione delle informazioni sensibili è spesso incerta. Con un sistema crittografato basato su blockchain, solo il legittimo proprietario delle informazioni può accedervi. Questo non solo migliora la sicurezza dei dati, ma riduce anche la burocrazia. Ad esempio, un paziente può prenotare visite e ricevere assistenza senza dover essere fisicamente presente, grazie alla certezza delle informazioni condivise.

"La decentralizzazione protegge non solo la privacy, ma anche la dignità degli individui, evitando intrusioni non autorizzate nei loro dati personali".

La Blockchain nella decentralizzazione dei servizi finanziari

La Blockchain, a quindici anni dalla sua introduzione per supportare le transazioni di Bitcoin, è ormai riconosciuta come una tecnologia fondamentale per la decentralizzazione dei servizi finanziari. Il sistema economico attuale si basa sulla fiducia, un concetto che la Blockchain rivoluziona affidandosi a formule matematiche e algoritmi per garantire sicurezza e trasparenza. Lo slogan “don’t trust, verify” sintetizza l’essenza di questa tecnologia, che elimina la necessità di fidarsi di intermediari, offrendo invece certezze concrete.

I vantaggi della Blockchain nei servizi finanziari includono tempi di risposta più rapidi, riduzione della burocrazia e maggiore trasparenza nelle transazioni. Inoltre, l’utilizzo di identità digitali uniche semplifica i controlli incrociati, contribuendo a combattere l’evasione fiscale e la criminalità.

“Non si tratta solo di una migliore gestione dei dati, ma di un cambiamento culturale”.

Riduzione dei rischi di dossieraggio

Come abbiamo visto, la pratica del dossieraggio/spionaggio è una piaga che la decentralizzazione può affrontare con successo. La Blockchain, con la sua struttura distribuita e sicura, protegge i dati personali da occhi indiscreti, contribuendo a un cambiamento culturale in cui ogni individuo è responsabile della propria sicurezza. L’identità digitale e la digitalizzazione dei processi, rese possibili dalla Blockchain, eliminano la possibilità di manipolare o spiare i dati sensibili, garantendo la sicurezza dell’individuo in un contesto globale.

Ostacoli alla decentralizzazione nel sistema bancario

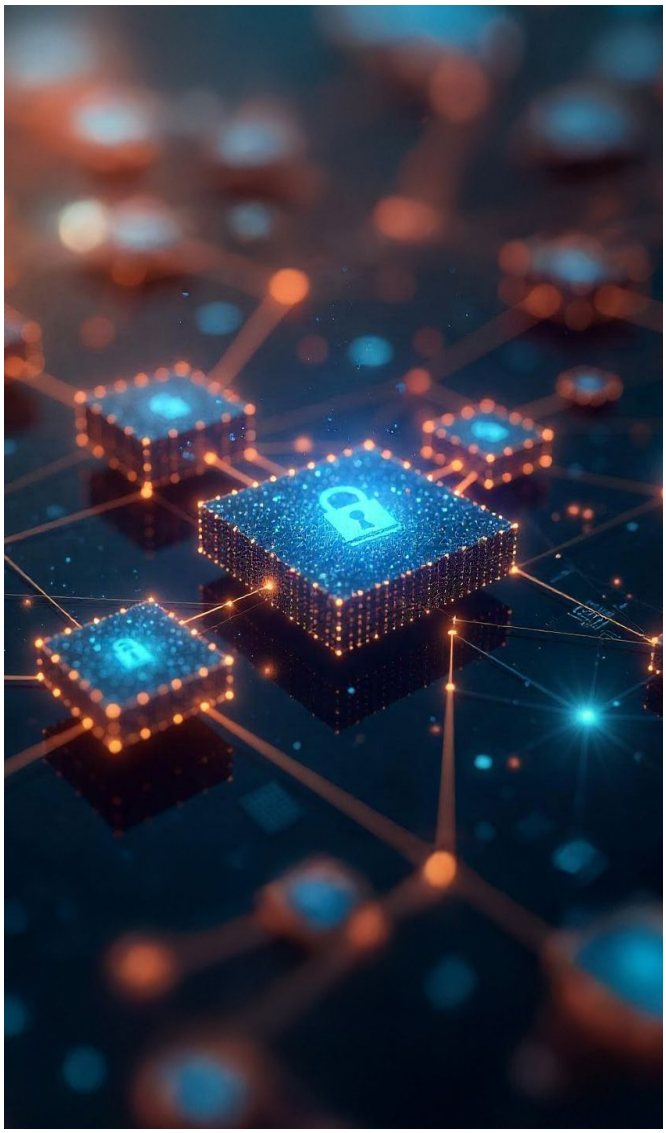
Nonostante i numerosi benefici, la decentralizzazione affronta ostacoli significativi, soprattutto nel sistema bancario italiano. Le banche tradizionali sono ancora fortemente legate a una mentalità centralizzata, dove il controllo è nelle mani di poche entità. Tuttavia, l’evoluzione tecnologica e la crescente digitalizzazione richiedono un cambiamento epocale. Le banche dovranno accettare un ruolo più limitato, fungendo da garanti dei processi tecnologici piuttosto che da controllori assoluti.

Integrazione con le normative europee

Uno dei maggiori ostacoli all’adozione della decentralizzazione è l’integrazione con le normative europee sulla privacy, come il GDPR. Il diritto all’oblio, ad esempio, entra in conflitto con l’immutabilità dei dati nella Blockchain. Tuttavia, la regolamentazione dovrebbe evolversi per supportare le tecnologie decentralizzate, mantenendo un equilibrio tra protezione dei dati e innovazione tecnologica. La rapidità con cui le tecnologie evolvono richiede un adattamento delle normative, per non ostacolare lo sviluppo di nuovi strumenti di gestione dei dati e dei servizi.

Conclusioni

La decentralizzazione rappresenta un’opportunità unica per migliorare la sicurezza, la privacy e l’efficienza dei servizi in vari settori. Sebbene ci siano ostacoli da superare, soprattutto in termini di normative e cambiamenti culturali, la tecnologia Blockchain e la decentralizzazione offrono soluzioni concrete per proteggere le informazioni sensibili e ridurre il potere dei grandi attori tecnologici. Il futuro dei servizi finanziari e della gestione dei dati sarà sempre più decentralizzato, e i benefici per cittadini e imprese saranno tangibili.



NIS2 & DORA: postura e mitigazioni

A cura di Mark Alan Barlow

DORA e NIS2 danno importanza alla Postura di Sicurezza delle aziende. La postura di sicurezza di un'organizzazione è la sua prontezza e capacità di identificare, rispondere e recuperare dalle minacce e dai rischi alla sicurezza.

Una buona strategia per un'azienda sarebbe quella di studiare i Regolamenti NIS2 e DORA e cercare di definire le varie aree e di mappare i requisiti con le varie mitigazioni attualmente in vigore, per poi creare un piano per affrontare le lacune.

Le aree che compongono il NIS2 sono varie, e di seguito sono elencati 10 di questi, riportati nell'articolo 21 del regolamento, che possono essere analizzate per capire la Postura di autovalutazione in termini di conformità e chiudere le gaps:

(a) politiche di analisi del rischio e sicurezza dei sistemi informativi

La direttiva NIS2 si basa sulle fondamenta della precedente direttiva NIS e introduce diverse modifiche e miglioramenti chiave in termini di ambito, struttura e rendicontazione. Ottenere certificazioni e verifiche esterne è un modo per rimanere al passo con le migliori pratiche.

Ecco alcuni suggerimenti:

- Ricercare e mantenere la prestigiosa certificazione ISO/IEC 27001:2022; con questo standard un'azienda si presenta ai propri clienti, fornitori e collaboratori il proprio ISMS (information security management system).
- Stabilire una serie di Regolamenti interni che comprendano la Governance degli accessi, la Politica di backup, la Gestione degli incidenti, etc.
- Ottenere ulteriori certificazioni, quali la Certificazione UNI EN ISO 9001:2015 relativa alla Qualità, la certificazione ISAE3402, etc.
- Stabilire una Roadmap per l'implementazione delle misure di Cyber Security che viene riportata mensilmente alla Direzione.
- Istituire un Comitato Rischi per valutare i rischi, le mitigazioni e i controlli di 2° livello con una struttura organizzativa e i ruoli per gestire i rischi.

(b) gestione degli incidenti

La Direttiva introduce obblighi di comunicazione più stringenti per le entità, imponendo loro di segnalare tempestivamente alle autorità competenti gli incidenti informatici significativi.

Occorrerebbe quindi:

- Sviluppare un regolamento interno specifico sulla gestione degli incidenti e un regolamento interno sul Disaster Recovery e sul BCP.
- Adottare un antivirus con EDR e integrare un SOC esterno con un SIEM.
- Progettare e implementare procedure per la comunicazione e il reporting a tutti gli stakeholder, tra cui Direzione, Clienti, Provider, etc.
- Valutare l'implementazione di uno specifico strumento di incident management per una gestione ancora più efficace ed efficiente.
- Testare la risposta agli incidenti e tracciare le tempistiche in base alle nuove regole.

(c) continuità aziendale, gestione dei backup, disaster recovery e gestione delle crisi

L'attenzione della direttiva alla pianificazione della continuità assicura che le entità siano ben preparate a mantenere la continuità dei servizi critici. Qui occorre:

- Sviluppare una procedura di sistema "Politica di backup" che regoli l'intero processo nel dettaglio.
- Creare una politica di Disaster Recovery / BCP.
- Implementare e mantenere un sistema di backup aggiornato e state-of-the-art (i.e. Snapshot Technology).
- Sviluppare un Piano di Continuità Operativa (BCP) che identifichi i potenziali pericoli che minacciano l'organizzazione e fornisca una struttura che consenta una maggiore reattività.
- Mantenere un Piano di emergenza (CP), il quale si basa sul presupposto che il rischio non può essere totalmente eliminato.
- Promuovere un Disaster Recovery Plan (DRP), che è un sottoinsieme del Contingency Plan e mira a stabilire le modalità di ripristino dei servizi ICT.
- Analizzare le strategie del data center e l'analisi dei livelli Tier.
- Eseguire test multipli su tutti i componenti per garantire la resilienza end-to-end complessiva.

(d) sicurezza della catena di fornitura :relazioni tra fornitori diretti o provider

La direttiva sottolinea l'importanza di valutare e garantire la sicurezza delle catene di fornitura. Le entità sono tenute a valutare le pratiche di sicurezza dei loro fornitori e appaltatori terzi, a stabilire obblighi contrattuali e ad attuare misure per mitigare i potenziali rischi provenienti dalla catena di fornitura.

Qui bisogna:

- Adottare una strategia di gestione della catena di fornitura per fornire una governance adeguata sia a monte che a valle.
- Sviluppare un quadro TPRM, valutando le pratiche di sicurezza dei fornitori terzi.
- Collaborare pienamente con i clienti nelle loro richieste di audit.
- Sforzarsi di realizzare processi centralizzati e controllati in questi termini, al fine di avere informazioni critiche prontamente disponibili.

(e) sicurezza in rete,compresa la gestione e la divulgazione delle vulnerabilità

(f) politiche e procedure relative all'uso della crittografia

La direttiva riconosce la criticità dell'infrastruttura internet di base nel mantenere la stabilità e la sicurezza dei servizi digitali e salvaguardare l'integrità e la disponibilità dei servizi online, nonchè gestire attivamente le vulnerabilità delle proprie reti e sistemi.

Occorrerà quindi:

- Implementare e mantenere i controlli per garantire la sicurezza delle informazioni che transitano sulle reti e per proteggere i servizi da accessi non autorizzati.
- Definire le responsabilità appropriate all'interno dell'organizzazione, stabilire controlli per salvaguardare la riservatezza e l'integrità dei dati in transito su tutte le reti.
- Assicurare una crittografia all'avanguardia dei dati in transito e a riposo in tutta l'organizzazione e tra i sistemi ICT.
- Concentrarsi sulla sicurezza offensiva, conducendo ogni anno molteplici CTI, VA, VS, e PT.
- Utilizzare diversi Red Team e Blue Team.

(g) politiche e procedure per valutare le misure di gestione del rischio di sicurezza informatica

L'implementazione dei requisiti consente alle organizzazioni di identificare, valutare e gestire in modo proattivo i rischi informatici. In tal caso serve:

- Adottare una metodologia di valutazione del rischio, come FMEA (Failure Mode and Effects Analysis), quale metodo proattivo per scoprire potenziali guasti nei processi aziendali al fine di prevenirli o mitigarne gli effetti, scoprendo dove questi potrebbero verificarsi e determinandone l'impatto.
- Estendere la metodologia per includere un'implementazione della valutazione del rischio di processo.
- Estendere la metodologia per includere una capacità e un processo di valutazione del rischio del progetto.
- Estendere la metodologia per includere le analisi di scenario.

(h) pratiche di base di igiene informatica e formazione sulla sicurezza informatica

Garantire buone pratiche di igiene informatica è un aspetto fondamentale. Promuovendo buone pratiche di igiene informatica e Cyber Awareness, bisognerà:

- Organizzare una formazione strutturata nelle aree di CyberSecurity, Data Privacy, Risk Management, Compliance, ecc., per tutto il personale.
- Concentrarsi su attività di formazione sul posto di lavoro, tutoraggio e collaborazioni nei campi della privacy dei dati e della sicurezza informatica per rafforzare la conoscenza.
- Diventare un leader di pensiero e partecipare a iniziative di CyberSecurity, come corsi, webinar, podcast, interviste, pubblicazioni e forum, ecc. anche attraverso collaborazioni con associazioni di categoria, come APSP, Assilea, etc.
- Mantenere un processo di ricerca e raccolta di eventi ICT e informatici, in termini di notizie, avvisi ed eventi, per rimanere sensibili alla mitigazione degli eventi esterni.

(i) human resources security, access control policies and asset management

(j) the use of multi-factor authentication and secured emergency communication

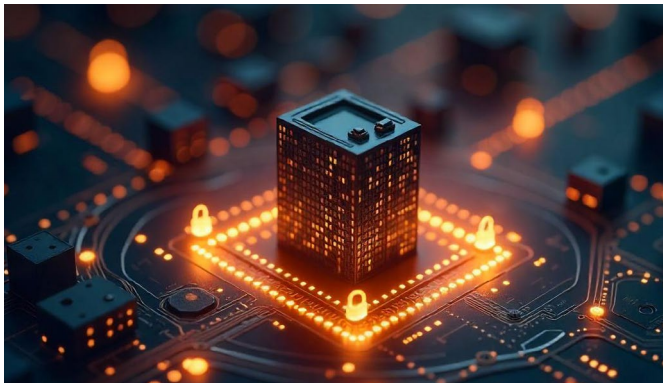
Il controllo degli accessi è un processo di sicurezza dei dati che consente alle organizzazioni di gestire chi è autorizzato ad accedere ai dati e alle risorse aziendali, utilizzando policy che verificano che gli utenti siano chi dichiarano di essere e garantiscono che vengano concessi agli utenti livelli di accesso al controllo appropriati.

La direttiva sottolinea l'importanza di valutare e garantire la sicurezza delle catene di fornitura

Per implementare pratiche di gestione delle risorse per identificare e proteggere sistemi informativi e risorse critiche si potrà:

- Sviluppare regolamenti interni per l'accesso logico e fisico.
- Vietare l'accesso ai servizi internet in specifiche aree e regioni.
- Implementare una soluzione PAM (Privileged Access Management).
- Implementare una soluzione WAF (Web Application Firewall solution).
- Attivare una soluzione DLP (Prevenzione della Perdita dei Dati) per monitorare gli accessi, i comportamenti e proteggere gli asset.
- Implementare misure di anonimizzazione dei dati, come DDM (Dynamic Data Masking), politiche di conservazione dei dati e misure del diritto all'oblio.
- Implementare l'autenticazione MFA (Multi-Factor Authentication) per l'accesso remoto, l'accesso ai sistemi e alle applicazioni.

Con l'avvicinarsi della scadenza del 2025, le aziende devono agire rapidamente per adattarsi al nuovo panorama normativo di NIS2 e DORA, analizzando i requisiti e assegnando valutazioni di Security Posture per comprendere le mitigazioni attualmente in atto e quelle da implementare. L'era della resilienza operativa digitale è alle porte e chi non si prepara rischia di rimanere indietro.



Studio sanitario di piccole dimensioni: la sicurezza a prova di budget in cinque passaggi

A cura di Riccardo Ferraretto

L'Italia è un paese noto per la forte presenza di PMI, caratteristica che si riflette anche nel settore sanitario. Basti pensare che nel 2024 risultano registrate oltre 50 mila strutture sanitarie, contando grandi ospedali, poliambulatori, studi associati e studi mono professionali (fonte annuario statistico – infodent – U.A.P.). Di queste una significativa percentuale è assimilabile a strutture di piccole dimensioni, ovvero con un ridotto numero di addetti tra medici e assistenti. Prendiamo ad esempio un poliambulatorio con 8 addetti tra cui 4 medici, 2 assistenti, 1 segreteria e 1 amministrativo (esempi analoghi li potremmo identificare con studi associati, studi dentistici e studi mono professionali).

Per la tipologia di attività, ci si trova a dover gestire una grande mole di dati sensibili, tra cui stato di salute del paziente e referti. Inoltre, c'è da tener conto che spesso la struttura opera regolarmente con l'ausilio di dispositivi di diagnostica, tra cui ECG, Holter, Radiologici, Ecografi, Elettromiografi, Diagnostica per Immagini ed elettromedicali in generale, producendo esami clinici che, in base alla specifica tipologia e ambito, per legge vanno conservati per almeno 10 anni (articolo 4 del decreto ministeriale del 14 febbraio 1997).

In questo contesto le esigenze di sicurezza informatica, vista appunto la sensibilità dei dati trattati e gli obblighi di legge, sono assimilabili a quelle di una grande struttura. Tuttavia, proprio per le dimensioni contenute della struttura stessa, ci si trova a dover fare i conti con un budget risicato e con una scarsa consapevolezza da parte dei titolari ed incaricati delle singole strutture. Tornando al nostro esempio del piccolo poliambulatorio, spesso si trova un sistema informatico non strutturato, composto di pochi elaboratori, e gestito da figure tecniche diverse, per via dell'integrazione con i dispositivi di diagnostica presenti. In generale, manca un referente unico per la struttura e la manutenzione dei sistemi viene affidata a personale interno non abbastanza competente, o ancora peggio a personale esterno ogni volta diverso. Questo scenario crea un terreno fertile per i cyber criminali che, approfittando della situazione, hanno possibilità di colpire facilmente creando non pochi disagi alla struttura e ai suoi pazienti.

Occorre quindi agire su due fronti: aumentare la consapevolezza in merito alla necessità di dotarsi di misure di sicurezza minime, anche e soprattutto per le piccole strutture, e adottare le misure corrette.

Sul primo punto la tematica è già stata ampiamente trattata dal legislatore e più volte ripresa dalle varie associazioni di categoria, inclusa Assintel. Occorre continuare e persistere su questa strada.

Vogliamo invece concentrarci sul secondo punto, identificando cinque passaggi chiave che permettano di arrivare ad un sufficiente livello di sicurezza, contenendo al massimo il budget. Una dovuta premessa va fatta tenendo in considerazione che il ragionamento è idoneo per strutture con un numero limitato di endpoint, e che possono accettare alcuni compromessi relativamente alle tempistiche di ripristino in caso di guasto o incidente di sicurezza. Ulteriore premessa: vogliamo concentrarci su un approccio prevalentemente tecnico, che possa comunque essere preparatorio per la redazione delle documentazioni previste per legge (ad esempio Privacy e GDPR, NIS2, autorizzazione sanitaria).

Primo passaggio: audit completo e referente

È indispensabile che vi sia un unico referente competente in materia di sicurezza e che preferibilmente conosca seppur a livello generale tutti gli applicativi e i dispositivi utilizzati all'interno della struttura. Identificare un ruolo del genere, interno o esterno che sia, avrà una rilevante incidenza sul budget. D'altro canto, sarà quello che, alla fine, ci permetterà di avere un risparmio in merito alle tecnologie utilizzate, evitando inutili dispendi di energia e andando a sopperire, almeno parzialmente, alla frammentazione delle singole assistenze derivante dai dispositivi elettromedicali presenti. Dovrà quindi redigere una lista completa dei sistemi presenti, inclusi, appunto, i dispositivi elettromedicali. Per ciascun dispositivo andrà presa nota del fornitore e/o dell'assistenza tecnica specialistica di ogni singolo dispositivo. Se il dispositivo prevede il collegamento di un elaboratore dedicato va verificata la presenza di un software di gestione che possa essere integrato. Vanno infine interrogate preventivamente le assistenze dei singoli dispositivi, prendendo nota di eventuali incompatibilità con tecnologie di sicurezza informatica in particolare antivirus, EDR/MDR e zero trust.

Secondo passaggio: infrastruttura identificazione delle basi dati

Sempre con riferimento al nostro piccolo poliambulatorio di esempio, i costi dell'implementazione di una infrastruttura client/server, on premise o cloud che sia, potrebbero essere difficili da sostenere. Tutto ruota intorno ai dispositivi elettromedicali che, oltre al costo di acquisto iniziale, richiedono un elaboratore di appoggio on premise dove risiede la base dati degli esami svolti dal dispositivo. La quasi totalità dei dispositivi elettromedicali in commercio (ad esempio gli ecografi o i radiologici per l'odontoiatria) funziona così a causa di limiti tecnologici o di efficienza, costringendo la struttura a dotarsi di una infrastruttura di rete che possa essere di supporto alle tecnologie di sicurezza necessarie, ad esempio per mettere in piedi un sistema di backup automatico. In questo contesto potrebbe non essere necessario eseguire un backup di tutti gli endpoint, e concentrarsi esclusivamente sul backup delle singole basi dati dei singoli applicativi, o dei singoli elaboratori di appoggio. Questo punto è fondamentale per il contenimento dei costi, tuttavia, la struttura va adeguatamente informata che, in caso di problematiche inerenti alla parte informatica, il piano di disaster recovery da attuare in caso di incidente prevederà tempi più lunghi rispetto ad un piano che preveda l'adozione un backup completo dei singoli sistemi.

Terzo passaggio: software gestionale e controllo accessi

Cruciale è la presenza di un software gestionale che possa essere integrabile con i dispositivi medicali. Alcuni software in commercio prevedono l'integrazione nativa con diversi dispositivi medicali, e possono prevedere un controllo accessi direttamente "a bordo" del gestionale stesso. In questo scenario i singoli elaboratori diventerebbero dei "terminali" che non possono accedere direttamente ai dati dello studio, senza prima fare login, appunto, sul software di gestione. Questo potrebbe essere sfruttato a nostro vantaggio al fine del contenimento dei costi, perché si potrebbe evitare di installare un controllo accessi sul sistema operativo evitando tutti i costi che ne conseguono (es. Active Directory). Questo punto è molto delicato e contestato, ed è attuabile a condizione che non vi siano altri dati accessibili prima del login sul gestionale. Ad esempio, inibendo a livello sistemistico la possibilità di salvare qualsiasi tipo di dato sul singolo elaboratore o la possibilità di accedere direttamente al database del dispositivo medicale.

Quarto passaggio: adozione delle tecnologie di sicurezza

Avendo già risparmiato su backup e controllo accessi, occorre prevedere l'adozione di tecnologie di sicurezza sufficienti a garantire la riservatezza dei dati presenti all'interno della struttura. In questo scenario, antivirus e firewall sono dei requisiti minimi, dai quali non si può prescindere. Va inoltre tenuto conto che le strutture sanitarie sono tra le più attaccate a livello informatico pertanto è preferibile, budget permettendo, l'adozione di un EDR e di un sistema di controllo applicazioni zero trust. Quest'ultimo in particolare permette di ottenere un livello di sicurezza nettamente superiore con un budget relativamente limitato.

Quinto passaggio: assistenza e verifiche periodiche

Il rapporto con il referente indicato al passaggio primo dovrà continuare nel tempo, coordinando le richieste di assistenza tecnica della struttura anche per le assistenze specialistiche dei dispositivi medicali. Vanno incluse verifiche periodiche della funzionalità dei backup con opportuni test di ripristino e monitorati gli aggiornamenti di sistema necessari.

Conclusioni

Da comprovata esperienza questo approccio può consentire alle strutture sanitarie di piccole dimensioni di svolgere il loro lavoro in sicurezza, tutelando i dati dei propri pazienti e soprattutto rendendo resiliente l'operatività della struttura. Il tutto ottimizzando il budget, accettando qualche compromesso.

Può essere anche utilizzato in strutture di nuova costituzione, che in una fase iniziale devono, per ovvi motivi, contenere al massimo le spese, per poi andarsi a strutturare via via, nel tempo, al crescere del volume d'affari, senza rinunciare ai requisiti minimi che consentano di avere un sufficiente livello di sicurezza.

"Le strutture sanitarie sono tra le più attaccate a livello informatico pertanto è preferibile, budget permettendo, l'adozione di un EDR e di un sistema di controllo applicazioni Zero Trust".

Le PMI italiane e la direttiva NIS2: una sfida da trasformare in opportunità

A cura di Antonio Assandri

Negli ultimi anni il panorama della sicurezza informatica è cambiato radicalmente. Anche l'Unione Europea ha manifestato una crescente consapevolezza di questo cambiamento e della minaccia, sempre più concreta, rappresentata dalla criminalità informatica.

Gli organi comunitari hanno, pertanto, deciso di agire con determinazione, attraverso l'introduzione di normative più severe ed omogenee a livello comunitario.

La NIS2 - Direttiva UE 2022/2555 - rappresenta un passaggio fondamentale per migliorare la resilienza delle reti e dei sistemi informativi, grazie a standard più elevati per la cyber security ed al coinvolgimento di una gamma più ampia di settori rispetto alla sua versione precedente, del 2016.

Le Direttive NIS: un passo avanti nella sicurezza digitale

La Direttiva NIS (Network and Information Security) originale, adottata nel 2016, è stata la prima normativa a livello europeo a trattare in modo organico la questione della sicurezza delle reti e dei sistemi informativi.

L'obiettivo della NIS2 è andare oltre, migliorando la capacità degli Stati membri di prevenire, affrontare e rispondere agli incidenti informatici. Per farlo, la direttiva introduce standard comuni per la sicurezza delle reti e dei sistemi informativi, ponendo enfasi su settori cruciali come l'energia, i trasporti, la finanza, la sanità, ma anche i servizi digitali ed il settore manifatturiero.

Perché anche le PMI devono adeguarsi alla NIS2

Perché una piccola o media impresa italiana dovrebbe preoccuparsi di adeguarsi alla NIS2, anche se non opera in settori considerati "strategici"?

Partiamo da uno degli aspetti più discusso della NIS2, quello di obblighi, responsabilità e sanzioni.

A differenza della Direttiva NIS, che lasciava margini più ampi di discrezionalità ai singoli stati membri su come implementare le misure di sicurezza, la NIS2 prevede standard minimi più stringenti. Inoltre, imprenditori e dirigenti aziendali sono ora soggetti a maggiore responsabilità e potrebbero essere direttamente sanzionati in caso di mancata conformità.

Le aziende che non rispettano i requisiti minimi di sicurezza, o che non segnalano gli incidenti entro i tempi previsti, rischiano multe che possono raggiungere il 2% del fatturato annuo globale, o fino a 10 milioni di euro, a seconda di quale delle due cifre risulti più alta.

Ci sono, però, varie altre risposte, molto più interessanti, concrete e convincenti, derivanti, anche, da quanto sopra.

La prima è, forse, la più scontata: la digitalizzazione ha reso tutte le imprese, grandi o piccole, potenziali bersagli per attacchi informatici.

Se fino a qualche anno fa la sicurezza informatica sembrava un tema relegato alle grandi aziende, o alle sole infrastrutture critiche, oggi anche per le PMI diventa cruciale affrontare il tema della cyber security.

Ad esempio, come evidenziato dal Cyber Report 2023 di Assintel Confcommercio, (https://www.assintel.it/wp-content/uploads/2024/04/Assintel-Cyber-Report-2023.pdf) sono proprio le PMI ad essere sempre più oggetto di attacchi ransomware da parte della criminalità informatica.

Forse meno immediata, ma decisamente più significativa, è la considerazione che, nel mondo moderno, è quasi impossibile per le aziende non fare parte di catene di approvvigionamento più ampie e collaborare con altre imprese o enti pubblici. Ciò le espone al fenomeno del cosiddetto "supply chain attack", un attacco informatico che prende di mira un'azienda attraverso le sue reti di collaborazione e fornitura. Negli ultimi anni, casi del genere si sono moltiplicati, mostrando come una piccola impresa possa essere il punto di accesso per violare reti più complesse.

Per questo motivo, la NIS2 prevede, specificatamente, il concetto di monitoraggio delle terze parti.

Proprio in virtù dei rischi legati al "supply chain attack" ed agli obblighi in merito al monitoraggio delle terze parti, si arriva all'importanza della NIS2 anche per le PMI: saranno, inevitabilmente, i loro clienti a chiedere di adeguarsi alle regole previste dalla direttiva, anche nel caso non fossero direttamente interessate od obbligate a farlo.

L'impatto della NIS2 sulle PMI italiane

Le PMI italiane si troveranno, pertanto, di fronte a nuove sfide che partono dalla necessità di adeguarsi a requisiti di sicurezza più stringenti.

Sfide che comporteranno, per forza di cose, anche investimenti economici e di tempo.

Gli obblighi imposti dalla NIS2 non riguardano, infatti, solo la sicurezza tecnica, ma anche la governance aziendale. Le imprese devono dotarsi di un piano di gestione degli incidenti, formare il personale e predisporre procedure per la segnalazione tempestiva degli attacchi. Inoltre, le autorità nazionali di ciascun Paese membro saranno tenute a monitorare più da vicino l'attuazione delle misure di sicurezza, aumentando la pressione sulle imprese che operano in settori considerati critici. Imprese che, come detto poso sopra, rivolgeranno analoga pressione sulla loro supply chain.

Per adeguarsi alla NIS2, le PMI devono, poi, prevedere una serie di misure pratiche. Tra queste, la formazione del personale rappresenta uno degli elementi più importanti. Molti attacchi informatici avvengono a causa di errori umani, spesso derivanti da una scarsa consapevolezza delle minacce. Formare dipendenti e collaboratori su come riconoscere phishing, malware, o altre tecniche di attacco, è fondamentale per ridurre il rischio.

Un altro passo importante è la creazione di un piano di risposta agli incidenti. Non tutte le aziende possono permettersi un reparto IT dedicato, ma ciò non significa che debbano essere impreparate. Avere un piano di emergenza che stabilisca chi contattare, quali misure adottare e come comunicare con i clienti in caso di un attacco può fare la differenza tra una rapida ripresa e un danno duraturo alla reputazione aziendale.

Infine, investire in strumenti di sicurezza tecnologici è essenziale. Firewall, crittografia dei dati, monitoraggio di dispositivi e reti, adozione di strumenti di autenticazione a più fattori, backup regolari e piani di business continuity sono solo alcune delle misure che anche le PMI possono adottare per proteggersi.

NIS2: da sfida ad opportunità

Come abbiamo visto la direttiva NIS2 rappresenta una sfida per molte PMI italiane.

Allo stesso tempo offre una grande opportunità, per crescere in termini di sicurezza e resilienza. Adeguarsi alle normative europee non deve, quindi, essere visto solo come un obbligo, ma come un passo necessario per proteggere la propria attività in un contesto sempre più digitalizzato ed interconnesso.

Adottare misure preventive e prepararsi adeguatamente può non solo evitare gravi perdite economiche ma, anche, migliorare la fiducia dei clienti ed aumentare la competitività a livello internazionale. Con il supporto di incentivi nazionali ed europei, molte imprese potrebbero trovare nel rispetto della NIS2 l'occasione per rafforzare la propria posizione nel mercato.

CYBER
Think Tank
ASSINTEL

Cyber Think Tank Assintel

Cyber per tutti

Istruzioni semplici per questioni complesse!

Video pillole

Podcast

Infografiche

Fumetti

Check list

Per info scrivi a: segreteria@assintel.it

La trappola della perfezione nella cybersicurezza: il meglio è nemico del bene

A cura di Paolo Cannistraro

Negli ultimi anni, la cybersicurezza è diventata una priorità assoluta per aziende, governi e cittadini. Ogni giorno, nuove minacce informatiche mettono a rischio i nostri dati e i nostri sistemi. In questo contesto, cresce la pressione per trovare soluzioni sempre più sofisticate, puntando a livelli di protezione sempre più alti a volte quasi inaccessibili. Tuttavia, c'è un problema insidioso che si nasconde in questa corsa alla perfezione dove il meglio può essere nemico del bene. Un concetto antico che risuona con forza anche nel mondo digitale, dove puntare a soluzioni perfette può rivelarsi un errore strategico.

Quando si parla di cybersicurezza, l'idea di creare un sistema "perfetto" è seducente. Il problema, però, è che questo livello di protezione è molto spesso irraggiungibile e si scontra con le necessità di business. Le minacce sono in costante evoluzione e, mentre i vari team di esperti si affrettano per sanare le vulnerabilità dei nostri sistemi, i criminali informatici sviluppano nuovi strumenti e strategie per violarlo.

Nella costante corsa per inseguire la perfezione, si rischia di perdere di vista l'obiettivo principale: ridurre il più possibile le vulnerabilità nel minor tempo possibile.

In contrapposizione alla perfezione, c'è l'approccio pragmatico del "bene". In ambito tecnologico, il "bene" non significa accontentarsi di soluzioni mediocri, ma piuttosto implementare misure di sicurezza sufficientemente efficaci nel breve termine. Si tratta di azioni tempestive che proteggono da rischi immediati, senza dover aspettare di aver creato un ecosistema perfetto. .

Ad esempio, l'installazione di patch di sicurezza e l'aggiornamento regolare dei software sono misure preventive che, pur non garantendo la protezione assoluta, riducono significativamente le probabilità di attacco. Anche se queste misure non risolvono ogni problema, rappresentano un baluardo efficace contro molte minacce note.

Cercare di raggiungere la perfezione nella cybersicurezza non è solo difficile, ma anche costoso. Ogni passo verso una maggiore sicurezza richiede risorse, tempo e competenze specifiche. In molte aziende, soprattutto quelle di piccole o medie dimensioni, i budget dedicati alla sicurezza informatica sono limitati, e ogni euro speso nella rincorsa alla perfezione potrebbe togliere risorse ad altre aree critiche.

Non solo: più complesso è un sistema, più è difficile da gestire. Questo aumenta il rischio di errori umani, un fattore cruciale nella cybersicurezza. Gli operatori potrebbero commettere sbagli durante la configurazione o la gestione di sistemi troppo sofisticati, aprendo inavvertitamente nuove falle di sicurezza. In molti casi, soluzioni semplici e ben collaudate si rivelano più sicure perché sono facili da implementare, controllare e mantenere.

Un possibile approccio più realistico e sostenibile potrebbe essere quello della sicurezza adattiva. Questo modello riconosce che non esiste una soluzione perfetta e definitiva, ma che è possibile lavorare su sistemi che si evolvono e si adattano alle nuove minacce. In pratica, si implementano misure di sicurezza sufficientemente efficaci tenendo in considerazione la criticità delle risorse impattate dalle vulnerabilità e alcuni indicatori macro di esposizione al rischio, come ad esempio se la risor-

sa sia esposta oppure no, aggiornando il sistema man mano che nuove vulnerabilità emergono.

Un esempio potrebbe essere quello di utilizzare l'intelligenza artificiale per rilevare le minacce informatiche. Le tecnologie di machine learning non offrono una protezione perfetta, ma sono in grado di identificare comportamenti anomali e segnalare potenziali attacchi prima che diventino dannosi. Questo approccio dinamico non cerca la perfezione, ma punta a una sicurezza in continuo miglioramento, che evolve insieme alle minacce.

Nelle aziende, adottare una strategia basata sulla gestione del rischio è il cuore di una cybersicurezza efficace e vincente.

Questo processo consente di identificare e prioritizzare le minacce in base alla loro gravità e alla probabilità che si verifichino. Invece di puntare alla protezione totale (spesso irrealistica), la gestione del rischio permette di concentrare le risorse sulle aree più critiche.

Questo approccio responsabilizza le divisioni aziendali coinvolte, rendendole parte attiva nel processo decisionale su quali rischi affrontare e con quali modalità, favorendo una maggiore consapevolezza e collaborazione all'interno dell'organizzazione.

Un altro buon esempio è la difesa a più livelli (defense-in-depth), una strategia che combina diverse misure di sicurezza. Questo metodo non si basa su una singola linea di difesa, ma su una serie di barriere, ognuna delle quali mitiga una parte delle minacce. Se una misura fallisce, altre possono comunque entrare in azione. Questo sistema è meno vulnerabile agli errori e offre un equilibrio tra protezione, costo e complessità.

In conclusione è doveroso citare che oltre agli aspetti tecnici analizzati, una delle variabili più importanti nella cybersicurezza rimane la cultura aziendale. Le organizzazioni che spingono verso la perfezione possono creare un clima di insicurezza decisionale, dove i dipendenti evitano di agire per paura di sbagliare. Al contrario, aziende che promuovono il pragmatismo e la rapidità di azione riescono a rispondere più efficacemente alle minacce.

Promuovere una cultura della cybersicurezza significa educare i dipendenti sull'importanza di azioni preventive, come il corretto utilizzo delle password o il riconoscimento di e-mail phishing. Politiche di sicurezza che siano realistiche e facili da rispettare sono altrettanto fondamentali. Se le procedure sono troppo complesse, i dipendenti potrebbero aggirarle, esponendo l'azienda a rischi evitabili.

Nel panorama odierno della cybersicurezza tentare di rincorrere la perfezione rischia di rallentare i processi e ritardare decisioni cruciali a vantaggio delle vulnerabilità, con il rischio di aumentare la probabilità di un incidente.

Al contrario, un approccio pragmatico, che accetta l'impossibilità della perfezione e si concentra su soluzioni efficaci e realistiche, offre una protezione solida e flessibile. Le minacce digitali sono in costante evoluzione, e solo un sistema adattivo e basato sulla gestione del rischio può tenere il passo.

In definitiva, la vera sicurezza non sta nella perfezione, ma nella capacità di reagire prontamente e di migliorare continuamente.

Riconoscere che il bene è spesso la soluzione migliore ci permette di costruire un ambiente digitale più sicuro, senza rimanere intrappolati nell'illusione di una sicurezza assoluta dove Il meglio è nemico del bene.

Disclaimer

Gentile lettore,

Ti informiamo che il contenuto pubblicato su questo magazine è fornito a scopo puramente informativo e di intrattenimento. Tutte le opinioni, idee e punti di vista espressi negli articoli sono esclusivamente quelli degli autori e non riflettono necessariamente l'opinione di Assintel o dei suoi redattori.

Tutte le informazioni fornite sono basate sulle conoscenze e le fonti disponibili al momento della pubblicazione. Tuttavia, non possiamo garantire l'accuratezza, l'integralità o l'aggiornamento delle informazioni fornite. Pertanto, l'utilizzo delle informazioni presenti su questo magazine avviene a proprio rischio e discrezione.

Si prega di tenere presente che il contenuto potrebbe evolvere nel tempo e potrebbe non essere più aggiornato o rilevante al momento della lettura. Pertanto, consigliamo di verificare sempre l'attualità delle informazioni fornite e di consultare professionisti qualificati per eventuali questioni specifiche o decisioni importanti.

Inoltre, il Cyber Think Tank di Assintel declina ogni responsabilità per eventuali errori, omissioni o danni derivanti dall'uso delle informazioni contenute nel presente magazine. Non siamo responsabili per qualsiasi rivendicazione, perdita o danno di qualsiasi tipo che possa sorgere direttamente o indirettamente dall'utilizzo delle informazioni qui presentate.

Ti invitiamo a fare affidamento su più fonti di informazione per ottenere una visione più completa e a considerare che i punti di vista espressi possono variare in base all'esperienza e alle opinioni personali degli autori.

Infine, vorremmo sottolineare che il magazine non fornisce consulenza legale, finanziaria, medica o professionale di alcun genere. Si consiglia di consultare sempre un professionista qualificato per risolvere eventuali questioni specifiche che riguardano la tua situazione personale.

Cordialmente

La redazione

CYBER
Think Tank
ASSINTEL

Riferimenti

- Osservatorio Cyber CRIF
- https://www.tinextacyber.com/analisi-darkweb-2024/
- Può l'intelligenza artificiale generativa diventare un'arma nelle mani di attaccanti?
- FraudGPT: The Villain Avatar of ChatGPT
- WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks
- Same targets, new playbooks: East Asia threat actors employ unique methods
- China tests US voter fault lines and ramps AI content to boost its geopolitical interests
- You can poison AI datasets for just $60, a new study shows
- L'intelligenza artificiale è immune da attacchi hacker?
- PwC, 2022 Global Digital Trust Insights: https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights/organisational-complexity.html
- IBM System Science Institute Relative Cost of Fixing Defects: Defects found in testing were 15 times more costly than if they were found during the design phase and 2 times more than if found during implementation. https://www.researchgate.net/publication/255965523_Integrating_Software_Assurance_into_the_Software_Development_Life_Cycle_SDLC
- IBM - Cost of a Data Breach Report 2021
- (ISC)² Cybersecurity Workforce Study
- NIST Cybersecurity Framework (NIST CSF)= https://www.nist.gov/cyberframework
- ISO/IEC 27001= https://www.27000.org/
- NIS2 Directive https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022L2555
- Matrici RACI https://it.wikipedia.org/wiki/Matrice_di_assegnazione_responsabilit%C3%A0
- KPMG International. (2023). Cybersecurity in ESG. Disponibile: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2023/04/big-shifts-small-steps.pdf
- Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J., & Zema, T. (2021). Cybersecurity and Sustainable Development. Procedia Computer Science, 00, 000– 000.
- https://doi.org/10.1016/j.procs.2021.01.001
- Alqudhaibi, A., Deshpande, S., Jagtap, S., & Salonitis, K. (2023). Towards a sustainable future: developing a cybersecurity framework for manufacturing. Technological Sustainability, 2(4), 372–387.

CYBER MAGAZINE

CYBER
Think Tank
ASSINTEL

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

Contattaci:

segreteria@assintel.it
www.assintel.it