CONTRIBUTO IBM

Nell’ambito dell’Indagine conoscitiva sulla difesa cibernetica: nuovi profili e criticità

IV Commissione Difesa – Camera dei Deputati

6 Novembre 2024

Indice degli argomenti

1. IBM e la Cybersicurezza

Con più di 110 anni di storia, IBM è un'azienda *leader* globale nell'innovazione al servizio di imprese e istituzioni in tutto il mondo, che opera in oltre 175 Paesi impiegando più di 280.000 dipendenti. *Cloud* ibrido, intelligenza artificiale (tra cui fondamentale la nuova piattaforma di tipo generativo, IBM *watsonx*), cybersicurezza, sistemi *hardware*, soluzioni *software, quantum computing* e servizi di consulenza, rappresentano le aree in cui IBM è riconosciuta come brand dal forte impegno etico nei confronti del mercato e del contesto sociale in cui opera.

Grande, infatti, l'attenzione verso l'integrità e l'affidabilità, principi che guidano imprescindibilmente la nostra azione di mercato, oltre che l'impegno profuso anche per creare e rafforzare nuove competenze professionali. Particolare attenzione infatti, è dedicata alla declinazione delle materie STEM e alla diffusione della cultura digitale e della sicurezza cibernetica, come testimoniato dalla recente apertura della IBM Cyber Academy a Roma.

La ricerca e lo sviluppo, in cui IBM investe oltre cinque miliardi di dollari l'anno, sono motore dello sviluppo scientifico nel mondo. IBM Research, la divisione di ricerca e sviluppo con primati su scala mondiale per l'ampiezza della sua organizzazione e per l'attività brevettuale, si concentra sul principio "*What's Next in Computing*" per creare e integrare le tecnologie che possono contribuire a risolvere alcune delle grandi sfide del mondo (ad esempio, a titolo esemplificativo e non esaustivo, nel campo del clima, della sanità e dello sviluppo di capacità di crittografia *quantum-safe).*

IBM opera in Italia dal 1927 contribuendo allo sviluppo dell'innovazione e della sostenibilità in ogni settore economico. Tra i suoi clienti si possono annoverare i principali istituti bancari, le amministrazioni pubbliche e le aziende leader di ogni settore industriale[1].

IBM è presente nella gestione della cyber security di un gran numero di infrastrutture critiche e può vantare capacità operative in diversi settori come quello della Difesa,

[1] Per approfondire: http://www.ibm.com/annualreport e www.ibm.com

Bancario, dell'Energia, delle Telecomunicazioni, dei Trasporti, del Manifatturiero e Medicale, potendo contare su una grande capacità progettuale, sia diretta che applicata mediante un ecosistema di business partner radicati nel territorio.

L'approccio di IBM alle tecnologie innovative è ispirato a principi **di responsabilità, etica e trasparenza.** Siamo stati i primi a lanciare questi principi e a metterli in pratica al nostro interno come all'esterno. Nel febbraio 2020 IBM ha siglato la "Rome Call for AI Ethics" voluta dalla Pontificia Accademia per la Vita e sostenuta anche da Papa Francesco. A gennaio 2023 l'impegno è stato ribadito e ampliato con l'adesione all'iniziativa delle tre religioni abramitiche, unite nella promozione di una intelligenza artificiale etica, trasparente, responsabile, inclusiva, imparziale, affidabile e pienamente rispettosa del diritto alla privacy e, nel gennaio 2024, è stato esteso anche alle religioni asiatiche.

Siamo convinti che l'Italia meriti un ruolo di primaria importanza nello scenario internazionale. Un ruolo che si reggerà sempre più sulla capacità di creare un ecosistema basato su valori condivisi e di lavorare con tecnologia e capitale umano per innovare e modernizzare il Paese. Questo è l'impegno di IBM per l'Italia: fare la propria parte per costruire il Paese del futuro, rendendolo capace di scalare posizioni di rilievo nello scenario europeo e globale Con riferimento all'ambito della Cybersicurezza: fornire il proprio contributo con competenze e tecnologie, incluso l'apporto che può offrire l'intelligenza artificiale, facendo fronte comune al cyber rischio sostenendo la collaborazione pubblico-privato.

2. La difesa cibernetica secondo IBM: risposta ad una minaccia informatica mutevole

Il team di ricerca IBM X-Force[2] analizza le minacce e gli attacchi a cui sono soggetti i clienti IBM di tutto il mondo e pubblica periodicamente studi e ricerche, riconosciuti per la grande autorevolezza nella comunità informatica e non solo. Sulla base di questo, IBM adegua le proprie soluzioni secondo un processo di miglioramento continuo, per far sì che le organizzazioni possano prepararsi al meglio e rispondere in tempi sempre più rapidi in un contesto di minacce informatiche estremamente mutevoli nel tempo (*cyber threat landscape).*

[2] https://www.ibm.com/it-it/x-force/team

Secondo l'*IBM Security Threat Intelligence Index 2024* [3], nel corso degli ultimi 12 mesi, l'accesso alle reti, ai sistemi e ai dati delle vittime di un attacco cyber è avvenuto sfruttando account validi (30% degli accessi), catturati anche attraverso il phishing e con l'abuso di applicazioni e servizi esposti su Internet (29% degli accessi). Il volume degli attacchi che hanno utilizzato credenziali valide è cresciuto del 71% anno su anno confermando l'affermarsi del principio secondo il quale gli attaccanti fanno *log-in* piuttosto che *hack-in*, per poi compiere azioni malevole solo in un secondo momento.

Per rispondere a un tale panorama di minacce, IBM lavora senza soluzione di continuità su due fronti:

1. creazione di consapevolezza riguardo la minaccia informatica e diffusione della cultura della preparazione;
2. sviluppo di soluzioni tecnologiche e di servizi di supporto consulenziale per le aziende, in grado di sostenerle nel percorso di adeguamento e rafforzamento rispetto ad una minaccia cyber sempre più ampia e sofisticata.

Sul primo fronte IBM ha recentemente inaugurato a Roma la Cyber Academy[4], un luogo in cui, in sinergia con la strategia nazionale di cybersicurezza, è possibile accrescere il livello di consapevolezza delle organizzazioni verso la minaccia informatica e nel quale è possibile prepararsi al meglio per gestirla e minimizzare gli impatti della stessa, attraverso percorsi basati sulla simulazione e sull' approfondimento tecnico. In tale ambito, quello che si rileva maggiorante è la necessità della diffusione di una nuova cultura della cybersicurezza che deve permeare sempre di più tutti gli ambiti di una organizzazione piccola o grande che sia, pubblica o privata.

Sul secondo fronte, quello più tecnologico, IBM mette a disposizione soluzioni per il *Threat Management*, (volte a anticipare, prevenire e rispondere alle minacce), per la *Identity Security* (di utenti, app e dispositivi nel cloud e in locale), per la *Data Security e Compliance*, volta alla protezione dei dati e alla conformità delle operazioni.

Hybrid Cloud e Intelligenza Artificiale sono le principali tendenze che influenzano la postura tecnologica e di sicurezza delle organizzazioni.

Se, infatti, si assiste ad una tendenza sempre più forte alla migrazione verso architetture Cloud per flessibilità, scalabilità ed efficienza, rimane tuttavia la necessità di mantenere alta l'attenzione sulla gestione dei dati in relazione al loro livello di criticità. Secondo il recente Studio IBM *Cost of a Data Breach Report 2024*[5] (luglio 2024), infatti, il 40% delle

[3] https://www.ibm.com/it-it/reports/threat-intelligence
[4] https://it.newsroom.ibm.com/cyberacademy
[5] https://www.ibm.com/it-it/reports/data-breach

violazioni hanno coinvolto dati archiviati nel cloud, pubblico, privato o in più ambienti. Tali ambiti porteranno le aziende ad affrontare nuovi rischi e sfide in materia di sicurezza legati alla gestione di ambienti più complessi e frammentati, alla necessità di centralizzazione di enormi quantità di dati e ad una conseguente espansione della superficie di attacco. È imperativo quindi proteggere infrastrutture, applicazioni e dati ovunque questi siano, specie per dati sensibili o critici di un'organizzazione (cloud/on premise/hybrid).

E' importante riflettere sulle implicazioni della progressiva diffusione dell'AI, che in IBM usiamo sintetizzare con lo slogan AI for Security e Security for AI, intendendo che esiste un rapporto bidirezionale tra le due. L'AI sta trasformando il modo in cui lavoriamo e nell'ambito della cybersecurity offre un valido contributo all'azione di contrasto, sia nella fase di identificazione delle minacce che in fase di risposta, ma allo stesso tempo introduce ulteriori sfide circa ciò che dobbiamo proteggere.

- Lo studio Enterprise generative AI: State of the market (2023), a cura dell'IBM Institute of Business Value, mostra che il 64% degli intervistati hanno interesse e spinta nell'adozione dall'AI generativa, ma vedono i rischi cyber security delle soluzioni AI scelte come uno dei principali ostacoli al progresso dell'adozione.
  L'AI generativa apre innumerevoli nuovi fronti di minaccia ed attacco ai dati delle organizzazioni.
  Quello che a nostro avviso aiuta in questo caso è dotare le soluzioni di AI generativa di strumenti di controllo e di governance in grado di rilevare e mitigare eventuali distorsioni.

I nostri controlli di sicurezza incentrati sui dati e sulle identità e l'esperienza in materia di AI, hybrid cloud e quantum garantiscono ai clienti di rimanere al passo con l'innovazione e con la sfida di mantenerne una corretta governance.

A titolo esemplificativo, la soluzione di *Security Information Event Management (SIEM*) di IBM protegge dati e sistemi installati nei propri data center (*on-premise*) o nel *cloud*, oppure ancora di soluzioni ibride in cui parte dei dati o delle applicazioni sono nei propri data center e parte in *cloud*. Questa soluzione è dotata delle certificazioni internazionali *Common Criteria* che la rendono utilizzabile anche in contesti sensibili e fortemente regolamentati. È inoltre riconosciuta da 14 anni come "leader" dalla società di consulenza e ricerca tecnologica Gartner, per la completezza di visione e la capacità di esecuzione.

Anche l'applicazione dell'AI rappresenta uno strumento formidabile a supporto all'azione di contrasto. A titolo esemplificativo, un uso particolarmente promettente di Intelligenza Artificiale nelle soluzioni di Cyber Security è relativo agli strumenti di supporto al triage degli allarmi, anche con visualizzazioni grafiche delle minacce: tale soluzione aumenta l'accuratezza dell'analisi e diminuisce il tempo di risposta nell'analisi delle minacce e degli attacchi.

Più in generale, il Machine Learning è alla base di una grande classe di soluzioni software che, analizzando il comportamento degli utenti nell'accesso a dati, file e risorse di varia natura, è in grado di generare alert su comportamenti anomali nell'accesso ad applicazioni, database, sistemi e reti. Le soluzioni IBM di *Endpoint Detection and Response* identificano proprio in questo modo malware o software spia presenti sulle workstation o sui dispositivi mobili.

Anche la soluzione *IBM Verify Identity Protection*, sempre a titolo esemplificativo, sfrutta algoritmi di AI per rilevare e rispondere agli attacchi basati sulle identità. Effettua una mappatura continua di tutti i flussi di accesso su tutte le applicazioni sia SaaS che on-premise. Rileva e abilita la correzione di falle di sicurezza, come accessi "ombra", asset esposti, identità compromesse, app SaaS sconosciute, mancanza di autenticazione a più fattori. Verify Identity Protection combina funzionalità end-to-end di gestione del livello di sicurezza delle identità e rilevamento e risposta alle minacce alle identità, al fine di identificare e reagire velocemente a potenziali attacchi e/o scoperture.

Algoritmi di intelligenza artificiale sono alla base anche di analoghe funzionalità ITDR embedded nella soluzione *IBM Security Verify (SaaS)* che permettono un'analisi e correlazione continua degli eventi di autenticazione, così come una verifica continua delle credenziali al fine di identificare eventuali compromissioni.

Inoltre, il modulo di accesso adattivo utilizza tecniche di machine learning per calcolare un rischio in tempo reale rispetto a parametri legati al dispositivo utilizzato, alla sessione e al comportamento dell'utente. Tali dati vengono analizzati rispetto a deviazioni sui dati storici di *accesso* e a *pattern* noti come malevoli, al fine di attribuire un punteggio di rischio che può poi essere utilizzato per costruire policy di access *risk-based*.

Nell'ambito dello sviluppo di applicazioni di Intelligenza Artificiale, è di particolare importanza la protezione dei dati a supporto di tali sistemi. La piattaforma IBM *Guardium Data Security Center,* riconosciuta come leader di mercato tra le soluzioni di Data Security, permette di implementare una serie di misure di sicurezza sui dati utilizzati per addestrare i modelli di AI. Tra queste misure troviamo il monitoraggio degli accessi ai database, audit delle attività sui dati ai fini di compliance e security, generazione di

allarmi in caso di accesso rischiosi, gestione della postura di sicurezza dei dati, discovery/classificazione dei dati, discovery dei modelli di AI nascosti oppure analisi delle vulnerabilità all'interno di tali modelli.

La piattaforma IBM Guardium stessa presenta funzionalità di Machine Learning ed AI con lo scopo di aiutare gli analisti di sicurezza nell'individuare situazione ed azioni sospette (rispetto a dei comportamenti normalmente osservati) oppure per migliorare l'accuratezza nelle scansioni di discovery e classificazione dei dati.

2.1 Il nuovo fronte degli attacchi all'Intelligenza Artificiale

Lo studio *Enterprise generative AI: State of the market*[6] (2023), a cura dell'IBM Institute of Business Value, mostra che il 64% degli intervistati hanno interesse e spinta nell'adozione dalla Intelligenza Artificiale Generativa, ma vedono la cyber security delle soluzioni AI scelte come il principale ostacolo al progresso dell'adozione.

L'intelligenza artificiale generativa apre innumerevoli nuovi fronti di minaccia ed attacco ai dati delle organizzazioni.

In questo ambito tra gli attacchi sempre più comuni troviamo:

- *Prompt Injection*, per manipolare i modelli di AI e indurli ad eseguire azioni indesiderate, evadendo le barriere di protezione e le limitazioni imposte dagli sviluppatori.
- *Data Poisoning*, inserendo dati artificiosamente errati in fase di addestramento per modificare il comportamento del sistema e creare allucinazioni.
- *Model Evasion,* per aggirare il comportamento previsto dal modello creando e inserendo input che lo ingannino.
- *Model Extraction* per estrarre completamente il comportamento di un modello osservando le relazioni tra input e output.
- *Inversion Attacks* per estrarre informazioni sui dati utilizzati nella fase di addestramento.
- S*upply Chain Attacks* per generare modelli dannosi che nascondono comportamenti dannosi o prendono di mira le vulnerabilità nei sistemi connessi ai modelli di AI.

La nostra raccomandazione in questo caso, è dotare le soluzioni di AI generativa di strumenti di controllo e di *governance* in grado di rilevare e mitigare eventuali distorsioni.

[6] https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/enterprise-generative-ai

IBM è impegnata nel rendere disponibili soluzioni innovative per la governance della sicurezza dell'AI che aiutino a proteggere le organizzazioni che hanno integrato l'AI nella propria infrastruttura dalle vulnerabilità di sicurezza e dalle violazioni delle politiche di governance dei dati, in un momento in cui l'adozione dell'AI generativa e il rischio di "shadow AI", ossia la presenza di modelli non autorizzati, sono in aumento.

Nel 2023, IBM ha lanciato la sua piattaforma di AI generativa chiamata *watsonx* che si compone principalmente di 3 moduli, tra cui watsonx.governance che è pensato proprio per proteggere l'organizzazione anche da queste nuove forme di attacco oltre che per assicurare eticità e compliance normativa ai sistemi di AI adottati.

Più recentemente, nel mese di ottobre 2024, IBM ha annunciato IBM Guardium AI Security per gestire i rischi di sicurezza e i requisiti di data governance per i dati sensibili utilizzati dall'AI e per gli stessi modelli di AI. Aiuta a identificare le applicazioni dell'intelligenza artificiale, ad affrontare la conformità, a mitigare le vulnerabilità e a proteggere i dati sensibili nei modelli di AI attraverso una visione comune dei data asset. IBM Guardium AI Security si integra con IBM watsonx e altri provider SaaS di intelligenza artificiale generativa. Ad esempio, IBM Guardium AI Security aiuta a scoprire i modelli di "shadow AI" ed è in grado di condividerli con IBM watsonx.governance, in modo che non sfuggano alla governance complessiva.

2.2 Difesa dagli attacchi basati su AI

IBM è molto attenta a valutare e prevenire le implicazioni dell'utilizzo non etico dell'AI, come dimostra l'essere stata tra i primi firmatari della *Rome Call for AI ethics* già nel 2020 e l'essersi dotata già diversi anni fa di un *Ethic Board* a livello globale per il controllo su tutte le soluzioni e prodotti IBM rilasciati sul mercato.

È innegabile, tuttavia, che le organizzazioni criminali stiano iniziando a sfruttare le potenzialità dell'AI per creare attacchi sempre più sofisticati.

Ad esempio, mentre in passato personalizzare campagne di phishing mirate sul singolo individuo sulla base dei suoi interessi era un'attività condotta solo verso target di "alto livello" adesso, sfruttando l'AI, è possibile condurre queste attività anche per utenti standard, sicuramente meno formati a riconoscere attacchi di questo tipo.

Inoltre, assistiamo alla creazione di *deep fake*, che ricreano voci o addirittura video degli interlocutori portando a truffe significative e di non immediata riconoscibilità. Si tratta di evoluzioni raffinate che giocano sulla *buona fede* degli utenti.

Per questo motivo, a nostro avviso, è fondamentale mettere in pratica un approccio *zero-trust* che si basa sulla circoscrizione al minimo dei privilegi assegnati in termini di azioni che un utente è autorizzato a compiere. Adottando questo approccio ogni singola attività viene validata e monitorata nel perimetro identificato.
Per rendere questo approccio efficace, è necessario intervenire con soluzioni che siano in grado di applicare policy di accesso adattate, di volta in volta, al rischio rilevato nella singola transazione, garantendo così sicurezza senza impattare la produttività degli utenti.

Proprio in quest'ambito, IBM ha recentemente lanciato una soluzione in grado di identificare eventuali accessi eseguiti dagli utenti tentando di aggirare lo strato di sicurezza.

2.3 Attacchi alla crittografia: le sfide del Quantum computing

IBM, come altre aziende nel mondo, è impegnata da anni nella realizzazione di computer quantistici sempre più performanti. Questa tipologia di computer è in grado di risolvere in maniera estremamente rapida alcune classi specifiche di problemi finora irrisolvibili tra cui anche gli attuali algoritmi di crittografia dei dati che, sulla base della evoluzione esponenziale che sta interessando la computazione quantistica negli ultimi anni ci si aspetta possano essere invalidati nel giro di pochi anni.

Gli attacchi provenienti dai computer quantistici metteranno principalmente in crisi gli algoritmi crittografici a *chiave asimmetrica* basati sulla fattorizzazione di grandi numeri primi, le curve ellittiche e i logaritmi discreti. *L'algoritmo per rompere questi schemi crittografici usando un computer quantistico è già noto dal 1994*[7].

La crittografia a chiave asimmetrica è oggi utilizzata per meccanismi di autenticazione a sistemi informatici, firma digitale di documenti e protezione di dati storici archiviati. Questo significa che, quando sarà realizzato un computer quantistico abbastanza potente da esercitare l'algoritmo esistente e poter rompere questo tipo di crittografia, un agente malevolo potrà accedere liberamente a portali e sistemi protetti da autenticazione sicura, modificare il contenuto di documenti firmati digitalmente e leggere il contenuto di dati storici cifrati.

Nonostante il giorno in cui saranno disponibili computer quantistici abbastanza potenti per poter portare attacchi di questo tipo sia ancora abbastanza lontano, assistiamo già a fenomeni di raccolta dati massiva da parte di organizzazioni che attendono la

[7] https://arxiv.org/abs/quant-ph/9508027

disponibilità reale di computer quantistici che saranno in grado, tra qualche anno, di decriptare i dati ora raccolti (*harvest now, decrypt later*).

Per informazioni altamente sensibili o che non possano essere rese obsolete (ad esempio dati sanitari) è fondamentale, quindi, adeguare quanto prima i meccanismi di protezione dei dati, anche in questa ottica.

Il NIST – l'Agenzia governativa americana per gli standard e la sicurezza - dopo un processo di selezione durato circa otto anni, ha certificato nel 2023 alcuni *algoritmi post-quantum*, cioè resistenti anche alla capacità di decriptare che avranno i computer quantistici, ed IBM è fiera di aver contribuito sostanzialmente al loro sviluppo avendo proposto tre dei quattro algoritmi adottati. Il NIST ha, inoltre, pubblicato gli standard di applicazione di 3 dei quattro algoritmi di crittografia post quantistica sopra citati nell'agosto del 2024; questo significa che tali algoritmi sono oggi utilizzabili in sistemi di produzione. Questa competenza ci ha consentito di realizzare, già dal 2022, *sistemi hardware mainframe z16* che *implementano in hardware gli algoritmi selezionati*, permettendo a questi sistemi di ottenere il *massimo livello di certificazione Common Criteria* È inoltre possibile richiamare da IBM Cloud servizi di generazione di chiavi crittografiche post quantistiche in cloud.

Un recente studio dell'Institute for Business Value di IBM sul tema[8], realizzato intervistando 565 top manager di diversi settori industriali, in collaborazione con GSMA (Global System for Mobile Communications Association) e Oxford Economics, ha evidenziato che il tempo necessario per integrare la sicurezza quantistica nei sistemi informatici di grandi aziende e pubbliche amministrazioni richiederà *circa 12 anni*. Ciò significa che qualora si dovesse riuscire a costruire un computer quantistico abbastanza potente da rompere la crittografia asimmetrica in meno di 12 anni molte aziende e istituzioni sarebbero esposte ad attacchi.

Già dal 2022 il governo statunitense a seguito di un *executive order* del Presidente Biden[9] diretto alle agenzie governative, ha cominciato a fare l'inventario dei sistemi crittografici attualmente in uso e ha definire processi per sostituire tali algoritmi in tempi rapidi.

Riteniamo, quindi, sia fondamentale che le organizzazioni arrivino preparate per affrontare l'inadeguatezza degli attuali sistemi di protezione dei dati.

Le azioni, che ci sentiamo di raccomandare in base alla nostra esperienza internazionale in materia, per mettere in sicurezza i sistemi informatici sono le seguenti:

[8] https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/quantum-safe

[9] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/

- realizzare un inventario dei sistemi crittografici presenti all'interno di istituzioni e aziende di rilevanza sistemica;
- identificare i dati e le applicazioni che dovranno essere migrate alla crittografia post quantistica prima degli altri per motivi di rilevanza sistemica;
- definire procedure per poter cambiare gli schemi crittografici attualmente in uso. Processi che vengono definiti di *crypto agility*;
- prepararsi adottare soluzioni tecnologiche "Quantum safe", che consentono di implementare una governance crittografica efficace e mantenere agilmente la sicurezza nel tempo o di "confidential computing", come la crittografia omomorfica.

La *crittografia omomorfica* si distingue dagli altri metodi di crittografia in quanto consente di eseguire l'elaborazione direttamente sui dati crittografati, senza la necessità di decrittografarli e senza richiedere l'accesso a una chiave segreta per elaborarli. Una soluzione di crittografia omomorfica IBM è stata recentemente adottata da una delle più grandi banche italiane[10].

Nuove soluzioni estendono la visibilità e il controllo sulla crittografia usata all'interno dell'organizzazione, individuando vulnerabilità o obsolescenza negli algoritmi crittografici usati, anche in preparazione post-quantum. Recentemente IBM ha lanciato la soluzione in questo ambito Guardium Quantum Safe[11].

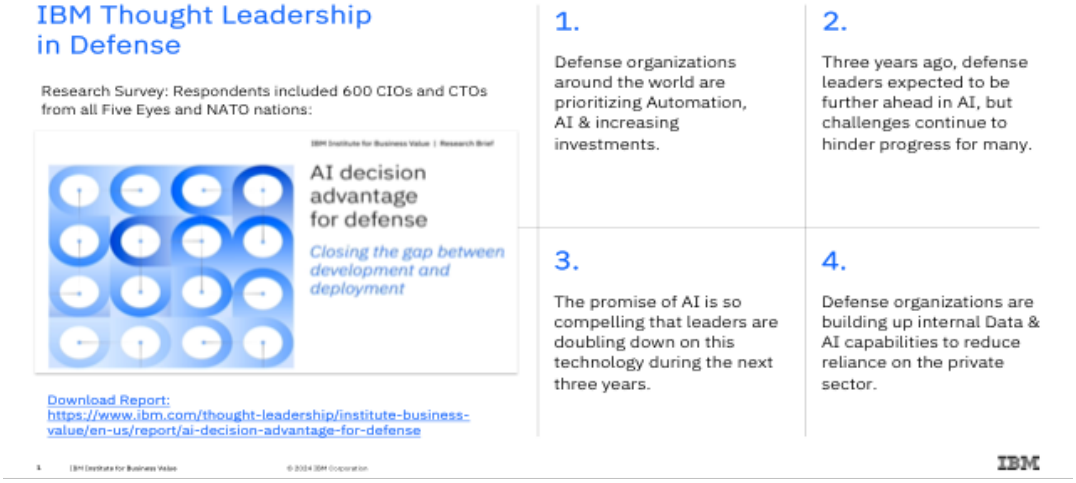
È importante sottolineare che le azioni sopra descritte porteranno nelle aziende una cultura della gestione centralizzata delle chiavi e degli schemi crittografici - che oggi spesso risulta mancante - e che garantirà un miglioramento nella gestione della sicurezza cibernetica anche indipendentemente dalla realizzazione di una minaccia quantistica.

Riteniamo infine essenziale che il legislatore inserisca previsioni e disposizioni in questo ambito nelle norme in discussione in Parlamento, attuali e future.

3. La Strategia e le esperienze IBM in ambito Difesa

[10] https://www.ibm.com/blog/intesa-sanpaolo-ibm-secure-digital-transactions-fhe/
[11] https://www.ibm.com/quantum/quantum-safe

Relativamente all'AI, IBM sta attualmente lavorando con organizzazioni governative in tutto il mondo, applicando tecnologie innovative come l'AI per aiutare a realizzare programmi di trasformazione per incrementare la resilienza e diventare "pronti per il futuro".
Questa attività prevede un percorso di trasformazione che abbraccia diverse aree della Pubblica Amministrazione, dai servizi al cittadino fino alla Difesa.
Per supportare il processo decisionale per l'adozione dell'AI nella Difesa, IBM attraverso l'Institute of Business Value (IBV) ha pubblicato lo scorso Maggio 2024 il report **AI Decision Advantage for Defense**[12].



In questa analisi sono stati intervistati 600 leader in ambito difesa in 32 nazioni e la maggior parte degli intervistati sostiene che, in un'epoca di sfide geopolitiche, è importante rivolgersi all'intelligenza artificiale come capacità strategica per aumentare la superiorità tattica, migliorare l'efficacia operativa e aumentare l'efficienza.
Da questa ricerca sono emerse **3 conclusioni:**

1. *Le organizzazioni della difesa danno priorità a* AI *e automazione*: ora più che mai stanno aumentando gli investimenti in questa tecnologia all'avanguardia e vedono il potenziale dell'AI per prendere decisioni ed ottenere vantaggi strategici. Il 35% dei leader della difesa indica che l'AI sarà estremamente importante nei prossimi anni.

2. *L'effettiva implementazione dell'AI è in ritardo rispetto alle aspettative*: tre anni fa, i leader della difesa si aspettavano di essere più avanti con l'implementazione dell'AI, ma la carenza di competenze, i problemi di governance dei dati e le sfide

[12] https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ai-decision-advantage-for-defense

etiche continuano a essere ostacoli. Nonostante le sfide, i leader stanno raddoppiando l'adozione dell'AI, in particolare le capacità di AI generativa.

3. *La collaborazione con il settore privato sta cambiando.* Le organizzazioni che operano nell'ambito della difesa stanno progressivamente sviluppando capacità interne di AI per ridurre la dipendenza dal settore privato, ma continuano a lavorare con questi ultimi in misura significativa durante le fasi iniziali.

3.1 L'esperienza IBM a supporto: l'AI per la Difesa

In un contesto sempre più sfidante nell'ambito della sicurezza informativa, abbiamo lavorato con il Dipartimento della Difesa di un Paese europeo, che riconosce la crescente minaccia rappresentata dai criminali informatici che cercano di sfruttare i progressi della tecnologia per scopi malevoli.
Per contrastare questa minaccia, abbiamo affiancato il Dipartimento della Difesa ad adattarsi e a rispondere con lo stesso livello di sofisticazione sfruttando l'AI generativa per la sicurezza informatica. In particolare:

- L'Utilizzo dei modelli (LLM) appositamente addestrati nelle attività di sicurezza, fornendo approfondimenti e risposte in pochi secondi, consente di ridurre il carico di lavoro manuale, consentendo agli esperti di liberare tempo prezioso.

- L'AI generativa può aiutarci a riqualificare e a migliorare i talenti esistenti, consentendo al personale meno esperto di svolgere compiti impegnativi con la guida di agenti virtuali. Questo permette anche al personale più competente di concentrarsi su altre responsabilità mission-critical.

- Tenere traccia di nuovi standard, leggi e regolamenti in materia di sicurezza informatica e privacy dei dati è un lavoro in continuo divenire. L'AI generativa può aiutare i CISO ad adeguare i documenti interni ai nuovi requisiti, a suggerire modifiche per conformarsi alle normative e persino a redigere rapporti sugli incidenti informatici.

Affrontare le preoccupazioni sulla sicurezza dell'AI generativa sarà fondamentale anche per costruire la fiducia dei cittadini. I cittadini hanno già espresso preoccupazione per la mancanza di controllo umano, la privacy, la sicurezza, l'etica, i pregiudizi e la discriminazione. Per rispondere a queste preoccupazioni, abbiamo proposto di istituire

un Centro di eccellenza (CoE) per l'AI generativa, responsabile di garantire un utilizzo sicuro, trasparente e affidabile dell'AI generativa nella pubblica amministrazione.

Per ottimizzare l'utilizzo delle risorse, anche in campo militare, e ridurre i tempi di inattività delle apparecchiature, IBM ha sviluppato una soluzione all'avanguardia che sfrutta l'IA e gli algoritmi di machine learning per prevedere i guasti alle apparecchiature e consigliare la manutenzione preventiva necessaria.

IBM Cognitive Equipment Advisor analizza i dati storici di manutenzione, i manuali tecnici e il feedback dei sensori in tempo reale, per identificare schemi e anomalie che facciano presagire ad un imminente guasto delle apparecchiature. Ciò consente ai responsabili militari di adottare misure proattive per risolvere i problemi prima che diventino gravi, riducendo così al minimo i tempi di inattività e il rischio di incidenti.

I vantaggi della soluzione di manutenzione, guidata dall'IA, sono numerosi. Con la manutenzione proattiva, è possibile ridurre al minimo il tempo dedicato alle riparazioni e massimizzare quello dedicato alle operazioni militari critiche. Affrontando tempestivamente i problemi, i è possibile evitare costose riparazioni e ridurre la necessità di ricorrere a costose parti di ricambio. Inoltre, questo tipo di soluzioni incrementano la sicurezza riducendo il rischio di incidenti e migliorano il livello di adeguatezza assicurando che le truppe abbiano gli strumenti necessari per svolgere efficacemente le loro missioni.

L'Esercito degli Stati Uniti ha già riscontrato notevoli vantaggi dall'implementazione del Cognitive Equipment Advisor. Ha ridotto i tempi di riparazione fino al 75%, i costi di riparazione fino al 50% e incrementato la disponibilità delle apparecchiature fino al 30%.

Altre organizzazioni della Difesa nei Paesi della NATO stanno già sperimentando questa soluzione e altre basate sull'IA generativa, che sono destinate a cambiare radicalmente la manutenzione predittiva nelle operazioni militari.

Con la NATO, infine, IBM ha siglato a Gennaio 2024 un accordo per contribuire al consolidamento della cybersecurity dell'alleanza, grazie a una migliore visibilità della sicurezza e gestione delle risorse su tutte le reti aziendali della NATO.

Questo servizio mira a fornire una vista unificata in materia di sicurezza. L'organizzazione interverrà con analisi dei dati, rilevamento di asset, integrazioni ed esperti di sicurezza per fornire una 'single source of truth' di informazioni su asset, configurazioni, vulnerabilità e patch in tutti gli ambienti della NATO. In questo modo, l'alleanza avrà una migliore visibilità dei rischi informatici e potrà gestire i potenziali problemi con maggiore facilità e velocità in tutta la sua rete.

Questo permetterà di agire due punti citati in precedenza, toccando sia gli aspetti di prevenzione delle minacce informatiche sia del monitoraggio degli asset gestiti negli ambienti NATO.

4. Conclusioni e raccomandazioni

La sfida della difesa Cybernetica è in continua evoluzione e muta rapidamente e progressivamente i profili di criticità.

I temi relativi all'adeguata preparazione e consapevolezza risultano quindi a nostro avviso centrali per alzare l'asticella della qualificazione in ambito digitale e di cybersicurezza e la competitività nel nostro Paese. A questo proposito, riteniamo essenziale lo sviluppo di iniziative congiunte pubblico-private per far sì che ci sia sempre maggiore accesso e possibilità di formazione in ottica inclusiva, ampliando così il bacino di reclutamento.

La IBM Cyber Academy, che rappresenta lo sforzo di IBM in questo senso, come luogo in cui Istituzioni, aziende pubbliche e private, ma anche studenti provenienti da scuole o università, possono aumentare la loro consapevolezza rispetto al tema della sicurezza digitale e agli strumenti a supporto, formarsi e formare le proprie organizzazioni contribuendo così allo sviluppo delle competenze necessarie a rendere il nostro paese un paese digitale e sicuro.

Rinnoviamo pertanto l'invito alla Commissione a visitare l' IBM Cyber Academy nel cuore di Roma, e a sperimentare le possibilità formative e di approfondimento in ambito.

Alla luce, inoltre, di quella che riteniamo essere la sfida più prossima e consistente che ci troviamo ad affrontare, e cioè quella legata all'affermarsi della computazione quantistica con i benefici, ma anche i rischi, che questa comporta soprattutto dal punto di vista della crittografia, di seguito alcune nostre raccomandazioni sulle quali riteniamo necessaria una azione di sistema sin da subito.

1. **Validare e certificare per l'uso in Italia i sistemi di crittografia resistenti agli attacchi quantistici** già certificati nell'agosto del 2024 dal National Institute of Standards and Technology (NIST) statunitense.

2. Effettuare **l'inventario dei sistemi di cifratura attualmente in uso** dalle istituzioni italiane di rilevanza sistemica entro il 2025 e prepararsi al cambio di algoritmi crittografici per alcuni sistemi critici tramite processi di sostituzione degli schemi crittografici (crypto-agility).

3. Richiedere come **requisito preferenziale**, e in alcuni casi obbligatorio, nei **processi di acquisto di tecnologia per la pubblica amministrazione e per le**

aziende di rilevanza sistemica la capacità dei sistemi hardware e software di **utilizzare algoritmi crittografici resistenti** ad attacchi quantistici.

Ringraziamo la Commissione per l'opportunità fornitaci e ribadiamo la nostra disponibilità per approfondimenti.

Contatti

Alessandra Santacroce

IBM Italia - Relazioni Istituzionali

Alessandra_santacroce@it.ibm.com