CONTRIBUTO IBM ITALIA

Nell'ambito del Ciclo di Audizioni sull'esame del disegno di legge "Disposizioni in materia di rafforzamento della Cybersicurezza Nazionale e di reati informatici" (AC 1717)
Commissioni riunite, I Commissione affari Costituzionali e II Commissione Giustizia, Camera dei Deputati

08 Aprile 2024

1. Presentazione di IBM

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. L'azienda – leader nelle soluzioni di Cloud Ibrido, Intelligenza artificiale e Quantum Computing, offre alle organizzazioni di ogni settore l'accesso alle tecnologie esponenziali e ai servizi di consulenza per la trasformazione digitale e la modernizzazione dei modelli di business. Cloud ibrido, intelligenza artificiale, sistemi hardware quali mainframe, power e storage, soluzioni software, cybersecurity e quantum computing: queste le aree in cui IBM è riconosciuta come leader a livello globale e come brand dal forte impegno etico nei confronti del mercato e del contesto sociale in cui opera. Grande, infatti, l'impegno profuso anche per creare e rafforzare nuove competenze professionali, con particolare attenzione alla declinazione delle materie STEM al femminile e alla diffusione di una cultura della sicurezza cybernetica, come testimoniato dalla recente apertura della IBM Cyber Academy a Roma.

IBM è impegnata ad aiutare le organizzazioni pubbliche e private a cogliere tutte le opportunità della trasformazione digitale in corso abilitata dalle tecnologie emergenti, come l'intelligenza artificiale, accelerando il loro percorso di innovazione. L'IBM watsonx è la piattaforma di AI generativa e dati dedicata alle imprese annunciata nel 2023. Basata sulle migliori tecnologie aperte disponibili e progettata secondo principi di trasparenza, responsabilità e governance, è pensata per casi d'uso aziendali mirati. Inoltre, permette di addestrare, perfezionare, distribuire e governare i dati e i modelli di AI per trarre vantaggio dal valore che generano.

La ricerca scientifica rappresenta il motore della crescita per IBM, i suoi clienti e i partner. IBM Research, la divisione di ricerca e sviluppo di IBM è la più grande organizzazione di ricerca industriale del mondo, con dodici laboratori in sei continenti. Il suo lavoro si concentra sul "What's Next in Computing" per creare e integrare le tecnologie grazie alle quali risolvere le grandi sfide del mondo, portando significativi progressi nella scienza del clima, nella scoperta dei materiali, nella sanità e altro ancora. Ciò ha assicurato a IBM numerosi primati nella classifica dei brevetti depositati negli Stati Uniti.

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.

Per approfondire:
www.ibm.com/anualreport
www.ibm.com

2. La strategia IBM sulla Cybersicurezza

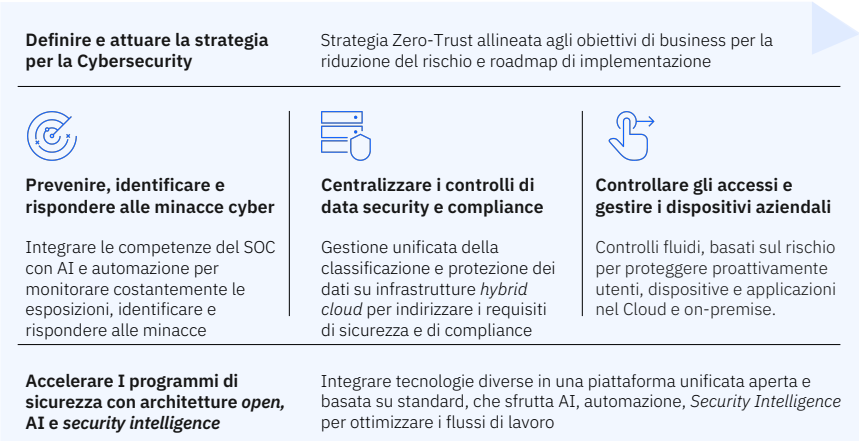
IBM ITALIA opera in Italia da quasi 100 anni mettendo a disposizione **soluzioni tecnologiche e servizi** che consentono alle aziende di affrontare le nuove sfide digitali e i rischi cyber legati alle infrastrutture ICT. Un impegno storico che si avvale anche del lavoro costante di IBM Research, che attraverso i suoi numerosi centri di eccellenza nel mondo e in Europa (con il laboratorio di Zurigo) è costantemente impegnata nella individuazione di soluzioni all'avanguardia per contrastare le minacce attuali e future, come ad esempio lo sviluppo di capacità di crittografia *quantum-safe.*
Per questo siamo grati e onorati di poter portare il nostro contributo su un tema delicato e trasversale quale quello della Sicurezza cibernetica, di primaria importanza per la resilienza e la competitività del Paese, soprattutto in questo momento storico.

Nel merito, la strategia di IBM per la Cybersecurity si articola **sulle seguenti aree fondamentali** (si veda figura successiva):

1. **Definizione e attuazione della strategia per la Cybersecurity**: strategia zero-trust allineata agli obiettivi di business per la riduzione del rischio e disegno della roadmap di implementazione.
2. **Gestione delle minacce cyber**: l'obiettivo è fornire le tecnologie più avanzate per il controllo delle esposizioni e dei rischi, per l'identificazione delle minacce, per la gestione degli allarmi e degli incidenti e l'eventuale ripristino dei sistemi e dei servizi; queste tecnologie possono quindi essere integrate in un framework unificato in cui i flussi di lavoro si svolgono in modo rapido ed efficiente.
3. **Protezione dei dati aziendali**: accompagnare le aziende in un percorso che va dalla conoscenza e dalla classificazione delle informazioni, all'implementazione delle misure di controllo e al monitoraggio delle attività di accesso, per indirizzare i requisiti di compliance, ma anche per individuare tempestivamente anomalie o fenomeni sospetti. Tutto ciò su un patrimonio informativo sempre più complesso e frammentato tra on-premise e molteplici Cloud, su repository tradizionali e una varietà di repository di ultima generazione, strutturati o non-strutturati, acceduti da una molteplicità di utenti, applicazioni e servizi di terze parti.
4. **Protezione delle identità digitali**: offrire gli strumenti che aiutano le aziende a ridisegnare i programmi per la gestione delle identità digitali, col duplice obiettivo di introdurre misure di controllo più efficaci e sicure e di applicare queste misure in modo consistente e coerente a dispetto della varietà di servizi e applicazioni, di tipologie utente, di dispositivi e canali di accesso.

IBM Security strategy

Proteggere infrastrutture *hybrid cloud* e informazioni *mission critical*



IBM Security 4

Per le organizzazioni la sicurezza è una materia trasversale che deve supportare lo sviluppo ed integrarsi nella strategia delle organizzazioni. Per questo motivo, per rendere sostenibile l'implementazione della sicurezza nelle aziende, anche a fronte della maggiore complessità e della scarsa disponibilità di risorse e competenze, è necessario uno sforzo di innovazione che interessi l'intera organizzazione e che, per IBM, si traduce in tre punti cardine: **integrazione, automazione e AI**.

1. **Integrazione**: l'uso di una molteplicità di strumenti e tecnologie può creare rallentamenti e inefficienze; la disponibilità di piattaforme flessibili e aperte, in grado di interoperare e collaborare efficacemente con altri strumenti di sicurezza, anche di terze parti, è fondamentale per la semplificazione dei processi operativi.
2. L'**automazione** è essenziale per migliorare l'operatività e ottimizzare i flussi lavoro: con l'automazione possiamo sollevare il personale dallo svolgimento delle attività scontate e ripetitive a favore di quelle a maggior valore, e garantire il rispetto delle procedure e dei tempi.
3. L'**AI** porta efficacia – ad esempio, tempestività, precisione e accuratezza nella identificazione delle minacce – ed efficienza, perché consente di estendere le attività che possono essere automatizzate, con conseguente accelerazione del ciclo di gestione degli allarmi e riduzione dei tempi di risposta e ripristino. **AI e Generative AI** sono preziose alleate per portare sempre maggiore accelerazione nelle Security Operations.

Riteniamo che solo le organizzazioni che sono in grado di dotarsi di una appropriata strategia di Cybersicurezza, che si basa su tecnologie, visione e competenze potranno cogliere appieno l'opportunità della trasformazione digitale in corso, soprattutto nel quadro in linea con la Strategia Nazionale promossa dall'Agenzia di Cybersicurezza Nazionale

3. Considerazioni generali sul disegno di legge "Disposizioni in materia di rafforzamento della Cybersicurezza Nazionale e di reati informatici" (AC 1717)

Considerata la centralità e la trasversalità del tema per il Paese nell'ottica della sua competitività e resilienza, plaudiamo l'impianto del disegno di legge che riteniamo rispetti ad oggi alcuni principi generali che illustriamo di seguito. Tali principi risultano, a nostro avviso, essenziali ed in quanto tali, ci auspichiamo siano costantemente tenuti presenti in questa fase e nelle successive dell'iter parlamentare del disegno di legge, fino alla sua fase attuativa.

- **Armonizzazione**:
    - garantire l'armonizzazione delle nuove norme con la legislazione nazionale vigente (ad esempio, garantire che non si sovrappongano i requisiti in materia di gestione del rischio o di segnalazione);
    - evitare regole che vanno oltre il framework NIS2.

- **Obblighi di segnalazione**:
    - Gli obblighi di segnalazione degli incidenti devono essere chiari, concentrarsi sugli incidenti che sono davvero significativi, concedere tempo sufficiente per fornire informazioni preziose e incentivare le entità a dare priorità alla risoluzione delle violazioni informatiche
    - Attenersi, con riferimento agli obblighi di informativa, alla scadenza di 24-72 ore stabilita in NIS2;
    - evitare la segnalazione obbligatoria di minacce o mancati incidenti;
    - evitare la sovrapposizione degli obblighi di comunicazione a livello nazionale;
    - chiarire il punto di ingresso per la segnalazione (come fatto con l'ACN) e favorire approcci che parlino di "punti di ingresso unici" (ossia la segnalazione ai sensi di leggi diverse va indirizzata sempre alla stessa istituzione) a livello nazionale o dell'UE;
    - chiarire gli obblighi di comunicazione tra i fornitori di TIC e i loro clienti:
        - *In particolare "Se un operatore di servizi essenziali si affida a un fornitore terzo di servizi digitali per la fornitura di un servizio essenziale per il mantenimento di attività sociali ed economiche critiche, tale operatore notifica qualsiasi impatto significativo sulla continuità dei servizi essenziali dovuto a un incidente che interessa il fornitore di servizi digital al quale si è affidato."*
- **Vulnerabilità**:
    - promuovere la divulgazione coordinata delle vulnerabilità (CVD) come politica riconosciuta a livello internazionale per la gestione delle vulnerabilità;
    - fare riferimento a standard internazionali come ISO/IEC 29147 e ISO/IEC 30111, nonché a best practice del settore, come la CERT Guide to CBVD pubblicata dal Software Engineering Institute della Carnegie Mellon University;
    - evitare approcci che obblighino i ricercatori di vulnerabilità a segnalare la vulnerabilità a un intermediario (ad esempio CSIRT) prima di informare il produttore;
    - Evitare qualsiasi segnalazione obbligatoria delle vulnerabilità, soprattutto prima del rilascio di una patch.
- **Misure di gestione del rischio**:

- astenersi da un linguaggio eccessivamente prescrittivo o da obblighi tecnologici (ad esempio, forzare la crittografia);
- tenere conto della natura dei soggetti che rientrano nell'ambito di applicazione (ad esempio, i soggetti che operano in infrastrutture digitali, i soggetti che operano in più Stati membri o in settori diversi, ad esempio i fornitori di servizi cloud). I sistemi di gestione del rischio dovrebbero essere accompagnati da criteri aperti e misurabili in modo da poter essere applicati a livello intersettoriale: ad esempio, le misure dovrebbero fare riferimento agli standard internazionali esistenti (ad esempio, ISO27001) anziché a requisiti vaghi come l'attuazione di "capacità all'avanguardia".

- **Vigilanza e applicazione delle norme**:
  - il regime sanzionatorio e di sorveglianza dovrebbe essere proporzionato e consentire ai prestatori di servizi di operare senza soluzione di continuità in diversi settori;
  - evitare pratiche di "naming and shaming" in caso di non conformità;
  - secondo la NIS 2.0 va incoraggiato un approccio incentivante includendo garanzie, riconoscendo i meccanismi esistenti e chiarendo le condizioni in cui tali poteri possono essere esercitati dalle autorità di controllo (anche in vista del coordinamento con altre autorità competenti);
  - va inoltre attribuito un ruolo più importante alla documentazione e ai meccanismi esistenti (come gli audit di terze parti) per consentire alle entità di dimostrare la conformità.
- **Certificazione**:
  - ribadire la natura volontaria dei sistemi di certificazione dell'UE;
  - evitare la certificazione obbligatoria nell'ambito dei sistemi nazionali.

3.1 Considerazioni specifiche relative al disegno di legge in merito agli articoli 1,2,3,6

La direzione in cui il disegno di legge indirizza le disposizioni in materia di Cyber Security risulta coerente con la rilevanza della materia, con le osservazioni della ricerca IBM relative agli impatti degli attacchi informatici e con il punto di vista di IBM sulla direzione dalla Intelligenza Artificiale.

La ricerca IBM, con il report “X-Force Threat Intelligence Index 2024” rilascia ogni anno una analisi che si basa su insight e osservazioni che derivano dal monitoraggio di oltre 150 miliardi di eventi legati alla cybersecurity che si verificano ogni giorno, in più di 130 paesi. Inoltre, i dati sono stati raccolti e analizzati da più fonti all'interno di IBM, inclusi IBM X-Force Threat Intelligence, Incident Response, X-Force Red, IBM Managed Security Services e i dati forniti da Red Hat Insights e Intezer, che hanno contribuito al report per il 2024.

Alcuni aspetti rilevanti osservati nel Report 2024 che ha analizzato il 2023:

- Quasi un attacco su tre osservato a livello mondiale ha preso di mira l'Europa (32%), un numero mai raggiunto prima d’ora in una singola area analizzata.
- Sempre nel 2023, l'Italia è il 5 paese più attaccato (8% degli attacchi)
- In tutta Europa, X-Force ha osservato un aumento del 66% degli attacchi causati dall'uso di account validi rispetto all'anno precedente.

- I principali punti deboli registrati sono le identità digitali e le e-mail, entrambi sfruttati nel 30% delle violazioni di account validi e phishing.
- I tre fattori che hanno impattato maggiormente le organizzazioni europee sono stati la raccolta di credenziali (28%), l'estorsione (24%) e la fuga di dati (16%).
- Quasi il 74% degli attacchi osservati ha riguardato infrastrutture critiche.

Questi valori sottolineano quanto un "ingresso facile" per gli aggressori è più complesso da rilevare e comporta una risposta costosa da parte delle aziende. Secondo X-Force, gli incidenti più gravi causati da criminali informatici che utilizzano account validi richiedono ai responsabili della sicurezza misure di risposta più complesse del 200% rispetto all'incidente medio, oltre alla necessità di distinguere tra attività di utenti legittimi e malintenzionati sulla rete.

Nel report rilasciato da IBM nel Novembre 2023, il "Cost of a Data Breach 2023" abbiamo evidenziato come, per una organizzazione italiana il costo medio di una esfiltrazione di dati per una azienda Italiana registrato è di 3,55 Milioni di euro ed abbiamo infatti rilevato che le violazioni causate da credenziali rubate o compromesse hanno richiesto circa 11 mesi per essere rilevate e recuperate: il ciclo di vita della risposta più lungo rispetto a qualsiasi altro vettore di infezione.

In un contesto così critico plaudiamo la scelta del disegno legge di prevedere l'identificazione di un Referente per la cybersicurezza prevista **nell'articolo 6** e della necessità di realizzare un piano ben definito e monitorato dalla Agenzia per la Cybersicurezza Nazionale può dare a tutte le organizzazioni che non si fossero già dotate di una struttura interna adibita alla prevenzione di minacce informatiche, di potersi strutturare per prevenire incidenti con impatti dannosi. Infatti, sempre nel report X-Force Threat Intelligence Index 2024 viene indicato come in quasi l'85% degli attacchi ai settori critici, la compromissione si sarebbe potuta limitare grazie all'applicazione di patch, all'autenticazione a più fattori oppure al principio del privilegio minimo. Ciò significa che quella che storicamente è stata descritta come "sicurezza di base" potrebbe essere più difficile da realizzare di quanto si pensi.

L'introduzione deli **articoli 1, 2 e 3** poi pone una attenzione molto alta anche alla tematica della gestione degli incidenti e della preparazione delle Organizzazioni sul perimetro nazionale per rispondere agli attacchi informatici e gestire le complessità tecniche, ma anche quelle comunicative e di segnalazione.

Su questo tema IBM investe sin dal 2016 supportando le organizzazioni per prepararsi a rispondere e soprattutto a gestire la comunicazione durante un attacco informatico. IBM ha infatti realizzato nel 2016 il primo Cyber Range commerciale a Boston ma ha poi dato seguito a questa iniziativa con il Cyber Tactical Operation Center in Europa tra il 2018 ed il 2020, il Cyber Range di Bangalore nel 2020 e nel 2024 con il Cyber Range di Washington DC e la Cyber Academy a Roma.

Proprio la Cyber Academy di Roma, inaugurata il 19 Marzo 2024, si pone come iniziativa centrale per supportare la direzione verso cui si muove questo decreto legge.

Nella Cyber Academy, infatti, per le Organizzazioni pubbliche e private sarà possibile lavorare sulla consapevolezza relativamente alle tematiche di sicurezza informatica andando a toccare tematiche quali:

- Preparazione del processo di risposta agli indicenti informatici

- Testing dei processi di gestione di incidenti e crisi informatiche
- Approfondimento di tematiche di consapevolezza
- Formazione su tecnologie

Il tutto sfruttando una struttura che permetterà di rilasciare attestati riconosciuti nel mondo del lavoro tramite la piattaforma gratuita "SkillsBuild", andando quindi a supportare la necessità di fornire le skills necessarie per poter affrontare questa trasformazione legata al mondo della sicurezza informatica.

3.2 Considerazioni specifiche relative al disegno di legge, in merito agli articoli 7, 9, e 10

Con riferimento all'art 10 in tema di criteri di cybersicurezza negli appalti, plaudiamo l'impianto dell'articolo evidenziando che nella fase attuativa del disegno di legge, in relazione alla individuazione dei criteri di cybersicurezza da tenere in considerazione in relazione alle attività di approvvigionamento di beni e servizi informatici impiegati in settori connessi alla tutela degli interessi nazionali strategici, sarà importante che tali criteri rimangano di natura squisitamente tecnica salvaguardando così i principi della collaborazione transatlantica e della apertura come strumenti di tutela della sicurezza e della resilienza nazionale.
Un punto di attenzione che riteniamo possa nella fase di attuazione inficiare il principio alla base della disposizione in oggetto, è rappresentato dalla indicazione di tali criteri come criteri "essenziali".
E' possibile infatti che questi criteri vengono recepiti pedissequamente dalle PA e inseriti nei Capitolati come requisiti minimi, con conseguenti possibili effetti restringenti. Quindi, a nostro avviso sarebbe opportuno che questi elementi venissero sin da subito descritti come delle linee di indirizzo e che si rimarcasse la facoltà delle stazioni appaltanti di indicare anche elementi diversi, unitamente alla possibilità degli o.e. di dimostrare il rispetto delle esigenze di tutela di cui sopra con misure equivalenti.

Con riferimento, infine, all' Art. 7 in tema di promozione e sviluppo di "ogni iniziativa, anche di partenariato pubblico-privato, per la valorizzazione dell'intelligenza artificiale come risorsa per il rafforzamento della sicurezza e della resilienza cibernetiche nazionali, anche al fine di favorire un uso etico e corretto dei sistemi basati su tale tecnologia" accogliamo con favore in particolare il disposto che riconosce all'Agenzia per la Cybersicurezza Nazionale (ACN) il ruolo di promotore dello sviluppo di iniziative, volte a valorizzare l'IA a supporto della sicurezza nazionale. Come IBM, ci siamo già fatti interpreti di questo spirito di collaborativo pubblico-privato aprendo recentemente la IBM Cyber Academy a Roma, sotto il patrocinio della ACN, che ha riconosciuto in tale iniziativa un valore importante a servizio dello sviluppo della cultura e della consapevolezza in ambito cibernetico nel Paese, supportato dalle tecnologie di ultima generazione come l'Ai generativa. Una Ai che per IBM deve rispettare essere etica, aperta, spiegabile, sicura e affidabile, come dimostrato dalla nuova piattaforma watsonx e dal modulo watsonx.gov che recepisce le ultime disposizioni in materia di Ai e non solo e assicura un sistema di controllo e difesa dalle allucinazioni che questa tecnologia, se non opportunamente governata, può generare.
In questa ottica, quindi, riteniamo importante il peso dato dall'art.9 al ruolo delle risorse umane e alla necessità di una collaborazione a livello di ecosistema affinché i profili qualificati si moltiplichino. Non pensiamo però che la soluzione sia limitare la concorrenzialità nel mercato delle figure più qualificate.

Per alzare l'asticella della qualificazione in ambito digitale e di cybersicurezza nel nostro paese, riteniamo essenziali iniziative congiunte pubblico-private per far si 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.

Riferimenti

Sara Marini
Relazioni Istituzionali - IBM Italia
sara.marini@it.ibm.com