Audizione Informale presso le Commissioni riunite I e IX della Camera dei Deputati

in merito al DL 105/2019

MEMORIA IBM ITALIA

IBM esprime apprezzamento per l'opportunità di confronto su un tema così fondamentale per lo sviluppo del Paese come quello del perimetro di sicurezza nazionale cibernetica.

Il nostro contributo all'audizione si articola sui seguenti punti:

1. Riflessioni introduttive sul tema della protezione dei dati e dei sistemi informatici e visione di IBM sulla Cybersecurity.
2. Alcune valutazioni specifiche in merito al DL 105/2019.
3. L'importanza della preparazione
4. Il Tema della collaborazione – Charter of Trust per la sicurezza nell'era digitale

Riflessioni introduttive sul tema della protezione dei dati e dei sistemi informatici e visione di IBM sulla Cybersecurity.

La Cybersecurity è un tema globale che viaggia con la geografia e i tempi della rete e quando si parla di protezione dobbiamo sempre aver presente questo aspetto.
Da 107 anni, IBM è una società di innovazione al servizio delle aziende e delle istituzioni di tutto il mondo. La strategia è quella di operare con l'ecosistema di riferimento e di perfezionare continuamente il portafoglio di offerta per trasferire al mercato un reale valore di business. Con un obiettivo: contribuire al processo di trasformazione digitale del sistema-Paese. Con 12 centri di ricerca globali, IBM detiene da 26 anni il record nel numero di brevetti. Oggi la proposizione di IBM si articola in precise aree strategiche: dai Big Data-Analytics all'Intelligenza Artificiale, dal Cloud alla Sicurezza, dalla Blockchain al Computer Quantistico. In Italia opera dal 1927.

Come IBM siamo tra le aziende leader sulla sicurezza, grazie alla nostra ricerca che tra l'altro nel 2018 ha prodotto 1400 brevetti relativi alla sicurezza informatica, ai diversi centri di ricerca dedicati ed al team IBM X-Force che è uno dei team specializzati più importanti al mondo.

Alcuni elementi sono particolarmente importanti da sottolineare per avere un quadro d'insieme sul tema della cyber:

- **Digitalizzazione pervasiva:** Tanto più l'ecosistema si digitalizza e si apre a nuove tecnologie (es: Industy 4.0 o Internet of things - IoT) quanto più i dati e le identità digitali diventeranno il tema centrale degli attacchi e della protezione.
- **Gap di competenze:** Stiamo lavorando tutti per mitigare questi rischi con risorse limitate. Gli esperti prevedono una carenza di 1.8 milioni di posizioni aperte in ambito sicurezza entro il 2022.
- **Costi e tempi per la soluzione dei problemi:** secondo i dati del "2019 Cost of Data Breach Study" (condotto da Ponemon Institute con la collaborazione di IBM) su 500 aziende nel mondo. il ciclo di vita medio di una violazione è di 279 giorni. Le aziende ne impiegano 206 per identificare una violazione dopo che è avvenuta, e altri 73 sono necessari per contenere i danni. Tuttavia, le aziende coinvolte nello studio che sono state in grado di rilevare e contenere una violazione in meno di 200 giorni hanno speso 1,2 milioni in meno rispetto al costo totale medio di una violazione non rilevata.
- **Complessità degli ambienti di sicurezza:** Tale tema è molto spesso il risultato di una consuetudine a rispondere a nuovi rischi aggiungendo nuovi strumenti di sicurezza all'ambiente esistente. A titolo di esempio, possiamo trovare aziende che utilizzano 85 modelli di strumenti informatici di 45 rivenditori diversi.
- **Modello di difesa in continua evoluzione:**
    - Un decennio fa, la sicurezza si concentrava principalmente sulla costruzione di difese perimetrali con firewall, antivirus, vulnerability scanner, IPS e così via, ma questo approccio frammentato ha lasciato varchi dove gli aggressori hanno potuto e continuano a penetrare in maniera inosservata.
    - IBM ha guidato il settore della cybersecurity costruendo un sistema di controlli incentrati sulla **Security Intelligence**. L'azienda ha suddiviso i controlli di sicurezza in aree tecnologiche: dal cloud, alla protezione dei dati, fino alla gestione e governance delle identità e degli accessi, ma soprattutto si è focalizzata sull'integrazione di questi controlli. Per questo motivo IBM ha rappresentato il framework della sicurezza come un **sistema immunitario** con utilizzo di tecnologie cognitive nella implementazione dei vari controlli e l'integrazione con funzionalità di orchestrazione.
    - Per rispondere con la necessaria **velocità** e **proattività** con cui i controlli devono essere implementati, dovremmo avere un nuovo approccio, quello di una **"sicurezza connessa"**. Parliamo di piattaforme in cloud che aiutano ad attuare strategie di difesa in maniera proattiva, migliorando l'integrazione e la collaborazione tra i vari soggetti coinvolti. IBM basa la Cybersecurity su un approccio proattivo e personalizzabile, utilizzando template predefiniti in funzione del contesto.

Valutazioni in merito al DL 105/2019

Come IBM condividiamo l'approccio proposto dal decreto che impone una **organizzazione di sicurezza** strutturata e meccanismi di controllo indipendenti nella **valutazione dei rischi** oltre che dei processi di **notifica degli incidenti** formali e mandatori. Il modello così definito consente una gestione centralizzata di eventuali crisi oltre che la condivisione degli eventi significativi.

In questo contesto è evidente che la presenza richiesta di Sistemi di Gestione della Sicurezza delle Informazioni formalizzati e, se possibile, certificati, costituisce un ulteriore elemento di garanzia nella definizione di un modello condiviso.

- Per questo ci sentiamo di raccomandare l'adozione di modelli comuni e certificabili da enti esterni accreditati, che si aggiungerebbero ai già previsti meccanismi di verifica del Centro di Valutazione e Certificazione Nazionale - CVCN.

Condividiamo l'importanza attribuita dal decreto alla individuazione di un perimetro nazionale di Cybersecurity. Il punto che ci sembra importante sottolineare è che, per effetto della digitalizzazione pervasiva dello scenario, tale perimetro diventerà sempre più fluido, interconnesso e complesso da difendere. Al suo interno dovranno, quindi, rientrare le componenti più rilevanti del sistema socioeconomico nazionale:

- A nostro giudizio, ad esempio, accanto alle infrastrutture critiche "in senso stretto", e cioè quelle essenziali per il mantenimento delle operazioni economiche e di governo del Paese (es. le infrastrutture di comunicazione, di produzione e distribuzione dell'energia, i sistemi idrici, di trasporto e logistica, i servizi di emergenza, i sistemi finanziari, i sistemi per la difesa e il presidio delle sedi istituzionali, etc.), andranno considerate anche tutte le aziende private che hanno un impatto diretto sulla vita quotidiana della società (come le aziende alimentari, le aziende farmaceutiche, etc.).
- Nella definizione del perimetro, occorrerà, inoltre, considerare la dipendenza intrinseca tra le filiere produttive e di servizio (ad esempio, le aziende alimentari non potranno produrre i loro beni senza energia, il grano non potrà essere coltivato senza acqua e non potrà essere trasportato senza una rete di trasporti funzionante etc.); a tale riguardo, ci sentiamo di indicare il lavoro svolto dal Department of Homeland Security (DHS) americano: https://www.dhs.gov/cisa/infrastructure-security-division.
- In prospettiva, vista la crescente interdipendenza tra strutture e filiere pubbliche e private, riteniamo che potrebbe essere opportuno considerare la possibilità di far convergere le diverse responsabilità di presidio (oggi articolate tra Presidenza del Consiglio dei Ministri e Ministero per lo Sviluppo Economico) in modo da permettere una maggiore coerenza di gestione tra ambienti diversi, oltre che facilitare azioni integrate di ispezione e vigilanza.

La definizione del perimetro nazionale di Cybersecurity, però, non potrà essere solo frutto di una azione dirigistica di coordinamento e controllo. A nostro giudizio essa dovrà essere supportata da un'azione di accompagnamento che dovrà favorire lo sviluppo di una nuova e più diffusa sensibilità verso i temi della Cybersecurity, inclusi la creazione di nuovi percorsi di formazione e di nuovi e più focalizzati profili professionali.

- A tal fine riteniamo potrebbe essere utile prevedere la creazione di un adeguato piano di comunicazione e di sensibilizzazione rivolto alle imprese e ai decisori pubblici.
- Inoltre, potrebbe essere utile creare un adeguato sistema di misure ed incentivi che facilitino l'approvvigionamento continuo di professionalità, competenze e soluzioni da parte di diversi attori di mercato, ed in particolare le piccole e medie imprese che potrebbero diventare, se non opportunamente supportate, uno degli anelli potenzialmente più deboli all'interno delle varie filiere del Paese.

In questo scenario, gli appalti pubblici dovranno tener conto della duplice necessità di garantire il massimo presidio da un punto di vista della sicurezza, ma anche di non appesantire troppo le procedure di affidamento, in quanto, vista la velocità di evoluzione della tecnologia, procedure troppo lunghe ed onerose potrebbero rivelarsi non compatibili con le esigenze di velocità ed efficacia di intervento.

- Per questo motivo ci sentiamo di suggerire l'adozione di formule di approvvigionamento che privilegino forniture e modelli certificati e allineati ai principali standard internazionali.

Riteniamo importante chiarire come dovrebbe essere espletata la funzione di verifica e certificazione da parte del Centro di Valutazione e Certificazione Nazionale (verifica ex-ante o ex-post).

- In generale ci sentiamo di raccomandare che le procedure relative vengano ispirate alla necessità di trovare il giusto equilibrio tra regolazione e velocità nell'adozione delle soluzioni di protezione.

Vi è poi un secondo aspetto che ci sentiamo di condividere in questa sede, ovvero quello che riguarda la tutela della proprietà intellettuale e industriale.

- Occorrerà, sotto questo punto di vista, fare in modo che, qualora il CVCN dovesse operare ex ante, i dettagli delle soluzioni tecniche utilizzate da un determinato fornitore non debbano essere condivise con una terza parte, questo anche per salvaguardare il livello complessivo della sicurezza della soluzione.

Relativamente alle procedure per le notifiche da parte dei soggetti ricadenti nel perimetro di sicurezza nazionale degli incidenti è fondamentale considerare le relazioni fra i diversi paesi in Europa e non solo.

Al di là dei commenti specifici al testo del decreto, si condividono alcune considerazioni aggiuntive che, a nostro giudizio, potrebbero essere poste alla base di future iniziative di supporto al progetto sul perimetro nazionale.

- Come espresso in precedenza, il concetto di perimetro evolverà e dipenderà sempre più dal modo con cui i singoli attori recepiranno ed interpreteranno linee guida e raccomandazioni afferenti, in senso lato, al tema digitale (come, ad esempio, le linee guida europee per l'AI). Per questi motivi auspichiamo che possano essere definiti opportuni modelli di accompagnamento e supporto all'adozione sistemica delle varie raccomandazioni, che garantiscano coerenza nei modelli interpretativi e nelle azioni da adottare in caso di incidenti.
- Il perimetro, inoltre, sarà sempre più condizionato dalla intersezione di varie tecnologie (AI, IOT, Blockchain, etc.) per cui l'azione di regolazione dovrà essere sempre impostata per individuare velcemente i nuovi scenari di esposizione e di possibile intervento legislativo (e, più in generale, regolatorio).
- Le competenze sono e saranno sempre più il settore chiave su cui investire. Come IBM riteniamo sarà importante accompagnare lo specifico provvedimento in discussione con una raccomandazione per la creazione di percorsi formativi specializzati.

L'importanza della preparazione

Altra raccomandazione è rivolta alla sensibilizzazione verso le aziende che possono svolgere un ruolo attivo, all'interno del perimetro di sicurezza nazionale.

Storicamente, i team per la sicurezza informatica si sono concentrati sull'individuazione e la protezione dagli incidenti di Cybersecurity. Nello scenario delle minacce odierne le organizzazioni riconoscono la necessità di concentrarsi sul miglioramento della loro risposta durante e dopo un attacco importante, pianificando tale risposta e, soprattutto, testandola.

Concentrarsi subito sulla risposta agli incidenti può quindi aiutare a ridurne i tempi e, inoltre, , queste misure hanno anche una correlazione diretta con i costi complessivi. Poter contare su un team e su piani di risposta agli incidenti sono due dei maggiori fattori di risparmio che emergono dallo studio. Le aziende che avevano messo in atto entrambe le misure hanno speso in media 1,23 milioni in meno rispetto alle aziende che non potevano contare su nessuna delle due (3,51 milioni contro 4,74 milioni).

Quando si tratta di rispondere a un attacco informatico, la velocità nel rilevare e bloccare potenziali attacchi, limitare la finestra di accesso al proprio ambiente informatico, arginare danni alla reputazione e riportare la tecnologia critica online è tutto.

Una delle principali sfide in cui incorrono le aziende quando si trovano in questa situazione è che i team di lavoro non riescono a superare il loro approccio per compartimenti stagni alla risoluzione del problema. E ciò è in antitesi con la rapidità. Infatti, per rispondere rapidamente agli incidenti informatici, non è solo deputato il team tecnico, dell'IT, ma è necessario un coordinamento di questo, rappresentato dal CIO, con tutti i vertici dell'azienda: responsabili delle linee di vendita, delle risorse umane, della comunicazione, della contabilità e del marketing. Oltre a definire un piano di risposta è dunque di fondamentale importanza testare come tutti questi gruppi diversi lavoreranno insieme rapidamente dopo un attacco, tenendo presente che le strutture organizzative tradizionali hanno processi decisionali troppo lenti per essere applicati durante un attacco informatico. Devono quindi predisporsi per adottare ciò che è noto, nel campo delle risposte di emergenza negli scenari di crisi, come "Incident Command System".

Il Tema della collaborazione e la Charter of Trust

Una forte collaborazione e condivisione delle informazioni tra governi, società e industria sono fondamentali per attenuare l'impatto delle minacce informatiche.

Per tale motivo è stata creata la **Charter of Trust** per un mondo digitale più sicuro.

La Carta, nata su iniziativa di Siemens, rappresenta un impegno su base volontaria di aziende che credono nell'innovazione e al tempo stesso riconoscono la necessità di accompagnare la trasformazione digitale con trasparenza, responsabilità e professionalità.

Tale Carta ha stabilito **10 principi** chiave per la *cybersecurity*, che IBM, Siemens, Airbus, Allianz, Daimler e altri stanno adottando per rafforzare la fiducia nella sicurezza dell'economia digitale.

In qualità di azienda tecnologica globale con profonde radici europee, IBM ha adottato questa Carta come parte di un più ampio impegno per la responsabilità nella gestione dei dati e nella promozione delle nuove tecnologie. L'auspicio è che la Carta nata in Europa, possa essere estesa a livello globale dal momento che la sicurezza informatica è un tema di interesse planetario.

Di seguito la traduzione dei 10 principi che ci sembra importante richiamare in questa sede come spunti di riflessione per la possibile evoluzione del perimetro nazionale.

1. Ownership della cybersecurity e dell'IT security

Ancorare la responsabilità della Cybersecurity ai massimi livelli governativi e aziendali designando ministeri e CISO specifici. Stabilire misure e obiettivi chiari e la giusta mentalità in tutte le organizzazioni sulla base del principio che la cybersecurity: "È compito di tutti".

2. Responsabilità in tutta la supply chain digitale

Le aziende, e se necessario i governi, devono stabilire regole basate sul rischio che assicurino un'adeguata protezione su tutti gli strati dell'IoT con requisiti chiaramente definiti e obbligatori. Garantire la riservatezza, l'autenticità, l'integrità e la disponibilità impostando standard di base, come ad esempio:

- Gestione delle identità e degli accessi: i dispositivi connessi devono disporre di identità e misure di salvaguardia sicure che consentano solo agli utenti e ai dispositivi autorizzati di utilizzarli.
- Crittografia: i dispositivi connessi devono garantire la riservatezza per l'archiviazione e la trasmissione dei dati, laddove appropriato.
- Protezione continua: le aziende devono offrire aggiornamenti e patch in un ciclo di vita ragionevole per i loro prodotti, sistemi e servizi tramite un meccanismo di aggiornamento sicuro.

3. Security by default

Adottare il più alto livello appropriato di sicurezza e protezione dei dati e assicurarsi che sia preconfigurato nella progettazione di prodotti, funzionalità, processi, tecnologie, operazioni, architetture e modelli di business.

4. Centralità dell'utente

Operare come partner affidabile per un ciclo di vita ragionevole, fornendo prodotti, sistemi e servizi nonché indicazioni basate sulle esigenze, gli impatti e i rischi della Cybersecurity del cliente.

5. Innovazione e co-creazione

Agevolare la collaborazione per una comprensione congiunta tra le aziende e i responsabili delle norme sulla sicurezza informatica e le regole al fine di innovare e adattare continuamente le misure di sicurezza informatica alle nuove minacce; guidare e incoraggiare, per esempio, contratti di partenariato pubblico-privato.

6. Istruzione

Includere corsi dedicati di Cybersecurity nei programmi scolastici (come corsi di laurea in università, istruzione professionale ecc.) al fine di guidare la trasformazione delle competenze e dei profili professionali necessari per il futuro.

7. Certificazione per infrastrutture e soluzioni critiche

Le aziende, e se necessario i governi, stabiliscano certificazioni indipendenti obbligatorie di terzi (basate su definizioni "a prova di futuro", in particolare in tutti quegli ambiti dove la vita delle persone può essere a rischio) per infrastrutture critiche e per soluzioni IoT critiche.

8. Trasparenza e risposte

Partecipare a una rete di sicurezza informatica industriale per condividere nuove conoscenze, informazioni sugli incidenti e altri; segnalare incidenti al di là della pratica odierna che si sta concentrando sull'infrastruttura critica.

9. Quadro normativo

Promuovere collaborazioni multilaterali nel campo della regolamentazione e della standardizzazione per stabilire condizioni di parità che soddisfino la portata globale del WTO; inclusione di regole per la sicurezza informatica negli accordi di libero scambio (Free Trade Agreements).

10. Iniziative comuni

Promuovere iniziative comuni, che comprendano tutti i principali stakeholders, al fine di attuare i principi di cui sopra nelle varie parti del mondo digitale senza ritardi indebiti.