CONTRIBUTO IBM ITALIA

Nell'ambito dell'esame dell'Atto del Governo n. 164, recante recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione (cd. NIS2)

Commissioni riunite I Commissione Affari Costituzionali e IX Commissione Trasporti, Camera dei Deputati

19 Luglio 2024

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* e *quantum computing* 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'impegno profuso anche per creare e rafforzare nuove competenze professionali, con particolare attenzione 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 scientifica, rappresenta il motore della crescita nella strategia aziendale: 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, nella sanità e lo 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].
Nella Cybersicurezza la strategia IBM si articola sulle seguenti aree:

1. Definizione e attuazione della strategia "*zero-trust", che* mira ad essere allineata agli obiettivi di business dei clienti ai fini della riduzione dei rischi cyber.
2. Gestione delle minacce cyber attraverso tecnologie avanzate, che (i) garantiscano il controllo dei rischi, l'identificazione delle minacce e la gestione degli incidenti, e (ii) si integrino

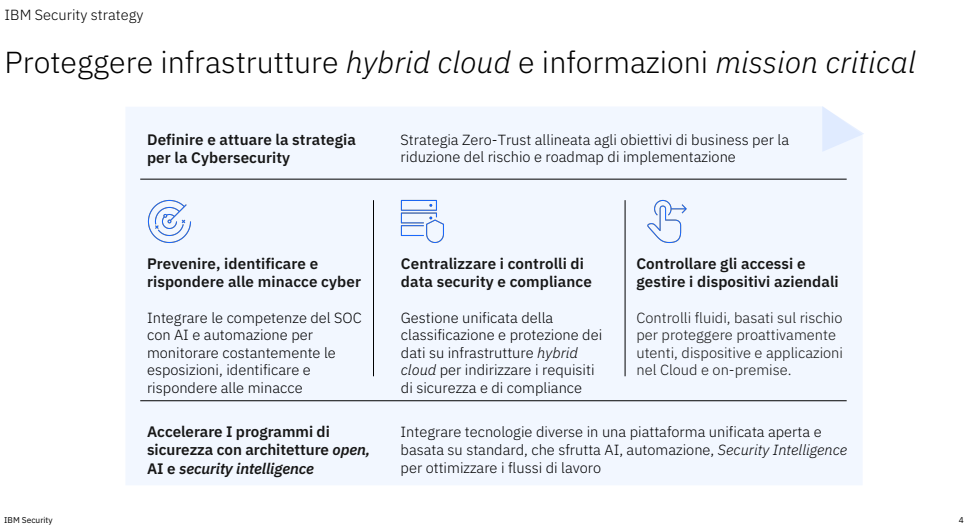
[1] Per approfondire:

http://www.ibm.com/annualreport

www.ibm.com

all'interno dell'organizzazione dei clienti nel rispetto della rapidità ed efficienza dei flussi di lavoro presenti.

3. Protezione dei dati aziendali 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.
4. Protezione delle identità digitali con strumenti che aiutano a ridisegnare i programmi per la gestione delle stesse, sia per introdurre misure di controllo più efficaci e sicure sia per applicare le stesse coerentemente all'organizzazione di riferimento.



Per rendere sostenibile l'implementazione della sicurezza nelle organizzazioni attraverso la strategia sopra indicata, anche a fronte della maggiore complessità e della scarsa disponibilità di risorse e competenze, IBM ritiene che siano tre i punti cardine:

1. L'**integrazione**, attraverso piattaforme flessibili e aperte, che essendo in grado di interoperare e collaborare efficacemente con altri strumenti di sicurezza, anche di terze parti, possono contribuire semplificare ed efficientare i processi operativi.
2. L'**Automazione**, che risulta spesso essenziale per migliorare l'operatività e ottimizzare i flussi lavoro.
3. L'**Intelligenza Artificiale**, anche di tipo generativo, che può contribuire ad aumentare l'efficacia (es. maggior tempestività e accuratezza nella identificazione delle minacce) e l'efficienza, perché consente di estendere le attività che possono essere automatizzate, con conseguente accelerazione del ciclo di gestione dei rischi.

2. Considerazioni sulla NIS2 e sull'atto del Governo n.164

La direttiva NIS2 rafforza il quadro per la collaborazione in materia di cibersicurezza, aumenta ulteriormente la consapevolezza informatica, migliora le capacità di condivisione delle informazioni sulle minacce e sviluppa competenze in tutta l'UE. La sua implementazione arriva in un momento cruciale caratterizzato da un aumento senza precedenti degli attacchi informatici a livello globale, mentre l'Europa in particolare è stata identificata come la regione più colpita, come risulta dallo Studio IBM X-Force Threat Intelligence Index 2024.

Considerata la centralità e la trasversalità del tema per il Paese nell'ottica della sua competitività e resilienza, plaudiamo l'impianto del progetto di legge italiana che recepisce la direttiva NIS2. Sulla base della nostra esperienza al servizio dei clienti a livello globale nei settori critici, vorremmo condividere alcune raccomandazioni che auspichiamo vengano tenute in considerazioni in questa fase e nelle successive dell'iter parlamentare, fino alla sua fase attuativa.

- **Armonizzazione e coerenza dell'impianto normativo**

  Il tema della coerenza dell'impianto normativo riveste particolare importanza sia in termini di efficienza complessiva sia in termini di ottimizzazione dell' impiego delle risorse da parte delle organizzazioni. L'armonizzazione del quadro di riferimento rappresenta un requisito fondamentale per supportare le organizzazioni nel processo di adeguamento alla norma.
  Su questo aspetto, facendo eco alle Associazioni di categoria già intervenute nelle audizioni dei giorni scorsi, riteniamo che sia fondamentale la collaborazione tra le Autorità competenti e le aziende private nella fase attuativa e plaudiamo le iniziative già lanciate da ACN, che auspichiamo continuino nei prossimi mesi.

- **Condivisione delle informazioni all'esterno**

  Articolo 15 (3-7), Art 25 (11): È importante garantire che qualsiasi informazione condivisa esternamente dal CSIRT non includa informazioni su incidenti o vulnerabilità notificati dai soggetti interessati, senza il loro previo consenso. Analogamente, l'Autorità Nazionale competente non può rendere pubbliche le informazioni sugli incidenti senza il previo consenso del soggetto segnalante. La legge dovrebbe fornire un quadro affidabile per la cooperazione tra i soggetti, i CSIRT e l'Autorità Nazionale competente, in cui le informazioni siano condivise in modo controllato.
  Riteniamo infatti che le disposizioni proposte renderebbero le entità interessate più riluttanti a condividere ulteriori dettagli su vulnerabilità e incidenti, eventualità che contraddirebbe gli obiettivi della norma. Pertanto, si si raccomanda di **inserire una clausola aggiuntiva al testo per garantire che i CSIRT e le ACN possano condividere informazioni sugli incidenti con terzi, compresi i destinatari dei servizi, o rendere pubbliche tali informazioni, solo previo consenso del soggetto segnalante**.

- **Governance**

  Articolo 23: il testo proposto fa riferimento ai compiti e alle responsabilità degli organi amministrativi e di gestione. Normalmente gli organismi dei soggetti essenziali e importanti dispongono già di team dedicati alla sicurezza informatica in possesso delle qualifiche specialistiche necessarie. Suggeriamo quindi di prevedere che i compiti e responsabilità in oggetto vengano assegnati in capo a tali referenti che seguendo quotidianamente le operazioni in materia.

- **Misure di gestione del rischio**

  Le entità incluse nel perimetro dovrebbero essere in grado di soddisfare i propri obblighi di gestione del rischio facendo riferimento agli standard globali comunemente accettati per la sicurezza informatica, lo sviluppo sicuro dei prodotti e l'integrità della catena di approvvigionamento. Standard globali ampiamente adottati come SDDF, NIST SP 800-53, ISO 27001 e ISO 20243 forniscono già una guida significativa e una solida base per politiche e pratiche di sicurezza informatica efficaci.

  Articolo 24: accogliamo con favore l'approccio basato sul rischio adottato nel progetto di legge.

  Art 24(2): sulla crittografia – raccomandiamo di incoraggiare le organizzazioni a pianificare la transizione alla Post Quantum Cryptography come parte integrante della loro strategia di crittografia.

- **Obblighi di comunicazione**

  Articolo 25: Accogliamo con favore il fatto che sia previsto un unico punto di ingresso per le notifiche rappresentato dal CSIRT Italia. Infatti, richiedere molteplici segnalazioni destinate a differenti autorità di regolamentazione rischia di trasformare l'obbligo di segnalazione degli incidenti in un esercizio burocratico di dubbia efficacia. Questo imporrebbe di fatto alle organizzazioni vittime di attacchi a perimetro di destinare le limitate risorse specializzate di cui dispongono per rispondere a obblighi normativi sovrapposti, piuttosto che concentrarsi sulla mitigazione degli incidenti e sul ripristino delle attività delle infrastrutture critiche.

  Accogliamo inoltre con favore la clausola di responsabilità che implica che l'entità segnalante non dovrebbe essere soggetta a una maggiore responsabilità a seguito della notifica. Un riferimento sicuro in materia incoraggerà le entità a farsi avanti tempestivamente per condividere le informazioni. Fornire forti protezioni di riservatezza e responsabilità per i soggetti segnalanti promuoverà la condivisione delle informazioni e un clima di partnership con CSIRT Italia.

  L'articolo 25 (9-10) dovrebbe a nostro avviso fornire indicazioni più precise sulla condivisione delle informazioni relative agli incidenti con i destinatari dei servizi. Le entità devono notificare ai destinatari del servizio gli eventi imprevisti significativi che avranno per loro un impatto. Esistono già molteplici segnalazioni legate alla sicurezza informatica che le organizzazioni già affrontano quotidianamente; pertanto, non ravvisiamo alcun vantaggio nel gravare i destinatari del servizio con ulteriori informazioni su minacce e incidenti, se non per loro significative e con un impatto rilevante. Tale obbligo di segnalazione dovrebbe, quindi, essere limitato ai casi in cui sono effettivamente interessati e solo quando devono intraprendere azioni specifiche per attenuare gli effetti di tali incidenti.

  Articolo 25 (12): accogliamo con favore lo sforzo di semplificare le regole di comunicazione. A riguardo raccomandiamo di avere un unico punto di ingresso per la NIS2 e la CRA per garantire l'armonizzazione operativa e la coerenza legislativa.

  Al fine di sviluppare una condivisione coerente e fruibile delle informazioni sulle minacce, le definizioni e le soglie di segnalazione dovrebbero essere stabilite a livello dell'UE. In tale ambito dovrebbero essere considerati i seguenti fattori:

- *Danno materiale e gravità*. La segnalazione dovrebbe essere richiesta per gli incidenti che hanno un impatto significativo sui servizi critici e che possono causare danni materiali alle attività commerciali materiali, alla sicurezza nazionale, alla stabilità economica o alla salute e alla sicurezza pubblica. A titolo esemplificativo, alcuni elementi da considerare potrebbero essere:
  - numero di individui;
  - dati o sistemi coinvolti;
  - durata di un'interruzione o di un'esposizione;
  - novità della tipologia di attacco per un determinato attore della minaccia;
  - disponibilità di sistemi di back-up.
- *Intento doloso*. Andrebbe presa in considerazione la possibilità di utilizzare la discriminante dell'intento doloso per concentrare le risorse sulle minacce reali alla sicurezza.
- *Casi isolati*. Gli incidenti non sistemici e isolati che non sono causati da attività dolose dovrebbero essere esclusi dall'obbligo di notifica, a meno che non comportino un'interruzione significativa dei servizi critici o un grave impatto sulla salute umana o un pregiudizio economico e sociale significativo.

- **Reporting nel contesto B2B**

  La norma dovrebbe ripartire più chiaramente le **responsabilità di segnalazione nel contesto B2B**, soprattutto perché alcuni soggetti contemplati dalla legge possono essere contemporaneamente sia fruitori che fornitori di servizi per le infrastrutture critiche. Il progetto di legge proposto non tiene conto, nella formulazione attuale, dei diversi ruoli e responsabilità di tali entità, il che potrebbe portare a obblighi di comunicazione ambigui e/o duplicati. In particolare, se un'organizzazione a perimetro agisce come fornitore di terze parti di servizi di un cliente dell'entità che è vittima di un incidente informatico segnalabile, dovrebbe essere chiaro che è il cliente di tale 'entità che è tenuto a segnalare, e non il fornitore di servizi di terze parti.

  Solo l'entità che è stata colpita dall'incidente informatico può valutare l'impatto e la gravità di tale incidente. In base all'attuale proposta, un fornitore di terze parti, come potrebbe essere ad esempio un fornitore di servizi cloud o qualsiasi altro fornitore di infrastrutture digitali ritenute essenziali, potrebbe dover segnalare all'autorità di regolamentazione un incidente che ha un impatto sul suo cliente senza disporre delle informazioni necessarie o di una panoramica degli utenti finali interessati.
  Raccomandiamo pertanto di includere nella proposta di legge nazionale di recepimento della NIS2 un chiarimento simile a quello di cui all'articolo 16, paragrafo 5, della direttiva NIS originaria del 2016:
  "[w]here an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator."

- **Certificazioni e specifiche tecniche**

  In merito al punto sulla determinazione di ACN di certificazioni e specifiche tecniche adatte all'adempimento degli obblighi previsti dal decreto ci preme sottolineare come tale misura possa determinare un grande impatto sulle organizzazioni se non adeguatamente disegnata. IBM mette a disposizione le proprie competenze per facilitare l'Autorità in questo compito. Tuttavia, sembra opportuno evidenziare come ad oggi le procedure per certificare prodotti secondo i sistemi di certificazione di cui all'articolo 49 del regolamento (UE) 2019/881 richiedano tempi lunghi e costi gravosi alle aziende produttrici. Il rischio che ravvisiamo è che

l'Autorità abbia a disposizione una scarsa selezione di prodotti, servizi e processi TIC da imporre ai soggetti NIS2. Sarebbe, pertanto, a nostro avviso utile prevedere un periodo di regime transitorio sufficiente a consentire alle imprese di ottenere le certificazioni necessarie o nel quale possa essere considerato adeguato il mero avvio delle procedure di certificazione.

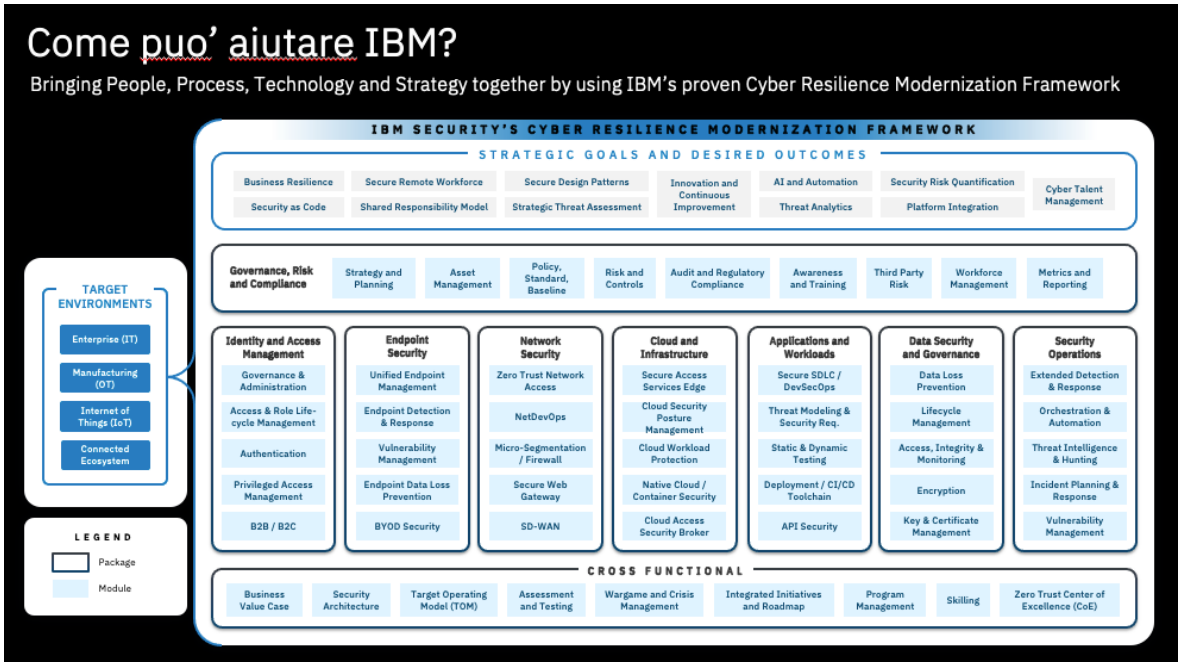
- **Vigilanza e applicazione**

  Il regime sanzionatorio e di sorveglianza dovrebbe essere proporzionato e consentire ai prestatori di servizi di operare senza soluzione di continuità in diversi settori.
  Sconsigliamo pratiche di "naming and shaming"; infatti, rilasciare pubblicamente informazioni sugli incidenti o condividere tali informazioni con gli utenti senza il consenso di un'entità crea seri rischi per la sicurezza informatica. Ciò detto, tali politiche mettono a dura prova la fiducia tra entità e CSIRT/Autorità Nazionali competenti e compromettono gli sforzi per promuovere un ecosistema di condivisione delle informazioni trasparente e proattivo.

  La legge dovrebbe infine, incoraggiare un approccio incentivante includendo garanzie, riconoscendo i meccanismi esistenti e chiarendo le condizioni in cui tali poteri possono essere esercitati dalle autorità di vigilanza (anche in vista del coordinamento con altre autorità competenti).

3. Come l'esperienza IBM può supportare l'implementazione della NIS2

Sulla base di quanto sopra esaminato, riteniamo più in generale che lo Schema proponga un set di politiche e procedure di sicurezza strutturato ed aggiornato, sebbene perfettibile.
IBM da sempre propone sistemi di sicurezza delle informazioni strutturati e standardizzati in tutti gli Stati in cui opera. Così come richiesto dalla Direttiva, IBM gestisce infatti le norme di sicurezza attraverso un insieme di politiche e procedure che vengono applicate a livello mondiale, proponendo attraverso i propri consulenti di cybersecurity sistemi di gestione della sicurezza basati sui principali standard (NIS CSF, ISO 27001, ISF, CIS, ISA 62443, PCI/DSS,...) come da framework a seguire:



IBM supporta quindi lo Schema che propone una gestione degli incidenti strutturata e organizzata, in grado di notificare all'autorità competente (ACN) ogni evento rilevante.
Nell'attuale contesto, sempre più sollecitato da attacchi cyber più sofisticati e pericolosi, anche in virtù delle risorse a disposizione degli attaccanti, deve essere sempre presente all'interno delle organizzazioni un piano di gestione della crisi e della continuità operativa in modo da ridurre al minimo gli impatti non solo sull'organizzazione stessa, ma anche e soprattutto sul contesto socio-economico nel quale essa opera.
In quest'ottica IBM sta già da tempo supportando diverse organizzazioni nella preparazione alla gestione della crisi e dell'emergenza derivante da attacchi cyber, con processi, strumenti organizzativi e tecnologie.

La maggior parte degli incidenti di sicurezza che occorrono alle organizzazioni risulta causata da vulnerabilità presenti sulla catena di approvvigionamento. In questo senso, l'attenzione rivolta all'interno dello schema a questo tema, per quanto da un lato contribuisca ad ampliare sensibilmente lo scope della normativa, dall'altro è da considerare assolutamente positiva per la sicurezza ed il benessere dell'intero contesto economico-sociale. A questo proposito il tema dell'analisi dei rischi delle terze parti è sempre stato centrale nella strategia IBM, con particolare attenzione alla gestione del relativo processo di sicurezza e alla definizione dei requisiti di sicurezza dei fornitori e delle forniture. Le metodologie adottate, gli strumenti a supporto e l'esperienza in ambito risk management sono infatti messi a disposizione per costruire sistemi sempre più automatizzati e volti a integrare tutte le informazioni utili per un'adeguata analisi e gestione dei rischi.

Lo schema richiede un approccio operativo volto a prevenire gli attacchi attraverso una struttura di governance delle vulnerabilità nonché attraverso l'applicazione del principio di *Security by Design*, elemento questo che sposa appieno l'approccio IBM al tema.

Un ulteriore elemento di valutazione positiva dello schema, che rispecchia la visione e l'azione di IBM, è la promozione di un'attività di monitoraggio del *sistema di gestione* utilizzato, che aiuti le organizzazioni a migliorare continuamente la propria postura di sicurezza e a tenere sotto controllo i possibili rischi socio-economici derivanti.

L'aumento della *consapevolezza dei rischi cyber e la formazione* degli operatori di security costituisce un tema essenziale per la protezione delle organizzazioni. IBM si impegna da anni a supportare i programmi di *awareness*, di training on the job sui temi di sicurezza e nelle attività di cyber range. A questo proposito ha recentemente inaugurato a Roma una sede dedicata alle attività di formazione e di simulazione di attacchi cyber, che ha ricevuto anche il patrocinio di ACN, per le sinergie con gli obiettivi della strategia nazionale di Cybersicurezza, esempio di una virtuosa esperienza di collaborazione pubblico-privato.

Altro tema toccato dallo schema è quello della *cifratura dei dati*. Si tratta di un aspetto molto importante su cui IBM ha investito significativamente negli ultimi anni sia in termini di tecnologie che di formazione del personale, con particolare attenzione al tema della Crittografia *Quantum Safe*. A questo proposito sarebbe opportuno inserire in modo esplicito un riferimento a questo rischio all'interno dello schema che risulterà sempre più concreto mano a mano che la computazione quantistica si andrà affermando. Sarebbe altresì utile inserire un richiamo sulle attività di preparazione che ciascuna organizzazione dovrebbe intraprendere per essere pronta in un prossimo futuro a fronteggiare tale rischio.

Il richiamo all'Identity Access Management (IAM) risulta significativo rappresentando uno dei pilastri della sicurezza e sul quale IBM è impegnata sia dal punto di vista tecnologico che consulenziale, supportando da diversi anni i propri clienti pubblici e privati su questa tematica.

Infine, l'indicazione di alcuni sistemi di protezione specifici come la *Multifactor Authentication* (MFA) o sistemi di *alerting* indicati all'interno dello schema costituiscono senza dubbio uno spunto da tenere in considerazione, ma sarebbe opportuno ancora una volta che fosse la gestione del rischio a guidare le soluzioni da utilizzare di volta in volta.

4. Conclusioni

Ringraziamo i Presidenti e le Commissioni per averci consentito di portare le nostre considerazioni, su un tema tanto rilevante quanto trasversale. Nell'auspicio che questo canale di dialogo possa rimanere aperto, anche in altre forme nel tempo, ribadiamo la nostra completa disponibilità a mettere la nostra esperienza a servizio della resilienza, della sicurezza e della competitività del nostro Paese.

Riferimenti

Alessandra Santacroce
Relazioni Istituzionali - IBM Italia
Alessandra_santacroce@it.ibm.com