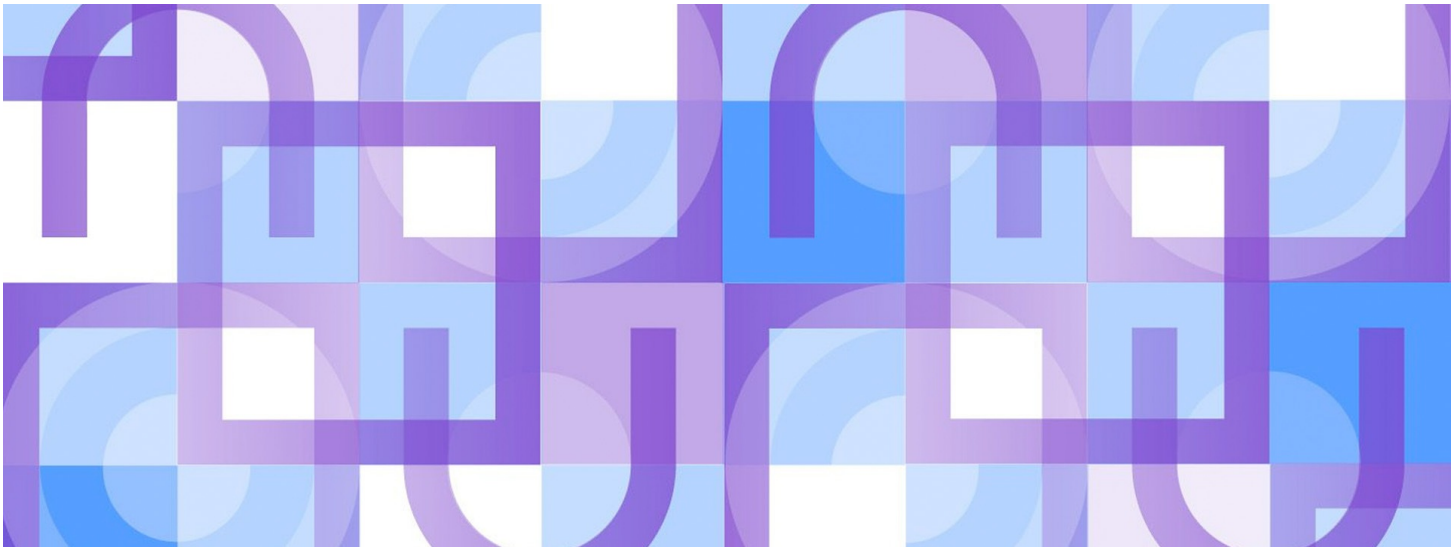
IBM Italy News Room

Preparare i governi agli shock futuri: un piano d’azione per sviluppare la cyber resilience in un mondo di incertezza

L'IBM Institute for Business Value (IBV) e l'IBM Center for The Business of Government, in collaborazione con la National Academy of Public Administration e il Centro Studi Americani, propongono misure concrete per aiutare i governi ad affrontare gli shock informatici attuali e futuri.



ROMA, ITALIA – 20 aprile 2023 – IBM (NYSE: IBM) ha annunciato oggi al **Centro Studi Americani** i risultati delle roundtable organizzate a livello mondiale dall’**IBM Institute for Business Value (IBV)** e dall’**IBM Center for The Business of Government** in collaborazione con la **National Academy of Public Administration e il Centro Studi Americani** per discutere di cyber resilience e leadership governativa. Il report, dal titolo Preparing governments for future shocks, è il frutto delle tavole rotonde tenutesi a Washington e a Roma in cui si sono svolti dibattiti approfonditi su questi temi che oggi sono centrali nell’agenda dei leader di governo e Istituzioni. I risultati evidenziati dal report potrebbero aiutare gli Stati Uniti, l'Italia e i governi di tutto il mondo a sviluppare e attuare strategie di cybersecurity che promuovano la resilienza attraverso partnership pubblico-private.

Negli scorsi anni i governi hanno avuto modo e tempo per imparare a gestire situazioni di grande crisi, come quella causata dalla pandemia, e le relative conseguenze. Hanno sicuramente imparato a non affidarsi a decisioni basate sui cambiamenti di scenario dell’ultimo minuto e oggi sono in grado di guardare più consapevolmente al futuro, immaginando quali potrebbero essere i prossimi “shock”, per anticiparli ed essere pronti ad affrontarli. Nello scenario attuale è sempre più probabile che eventi con conseguenze impattanti e negative, gli “shock” appunto, si verifichino sempre più spesso. Possono manifestarsi più o meno velocemente, a livello regionale o globale, variando per portata e natura, ma sicuramente richiedendo strategie proattive pensate da ora.

I governi per essere resilienti e poter perseguire i propri obiettivi anche nell'incertezza potrebbero trarre significativi vantaggi dallo sviluppo di *insight*. Per farsi trovare pronti, sarà necessario dare priorità alla leadership e agli investimenti, oltre a definire e orchestrare strategie, con capacità fondamentali per essere meglio preparati alle sfide che potranno prensentarsi in futuro nei più diversi ambiti.

Le tavole rotonde tenutesi a Washington DC e a Roma si sono concentrate sulla resilienza cyber, uno dei temi più caldi nell'attuale situazione mondiale. Ogni anno, il volume degli attacchi informatici e il loro impatto raggiungono livelli crescenti. Nella seconda metà del 2022, il numero di attacchi informatici rivolti ai governi è aumentato del 95% a livello mondiale, rispetto allo stesso periodo del 2021. Attacchi di alto profilo, come quello di Solar Winds, hanno dimostrato quanto la sicurezza informatica sia strettamente legata alla continuità del business e alla resilienza operativa.

I governi hanno un ruolo fondamentale nel favorire la collaborazione tra i principali stakeholder per identificare i rischi informatici, accrescere la capacità di risposta e di rimanere resilienti di fronte a questi rischi. Le istituizioni oggi hanno anche un importante ruolo di leadership per guidare il cambiamento verso un futuro più resiliente nel contesto degli obiettivi dei loro programmi di goveno.

Dallo studio emergono alcuni passi fondamentali per supportare i governi a livello globale a sviluppare e attuare strategie di cyber security che promuovano la resilienza attraverso una partnership tra pubblico e privato. I principali sono:

- **Aumentare i talenti specializzati in cyber security**

Per affrontare il divario crescente tra domanda e offerta di professionisti di cyber security, i partecipanti alle roundtable hanno indicato, in cima alla lista delle priorità da perseguire, l'importanza di aumentare i talenti competenti in sicurezza informatica. Come sottolineato da diversi partecipanti, la carenza di competenze informatiche riguarda un'ampia gamma di discipline, tra cui l'analisi, la progettazione e lo sviluppo di software, la threat intelligence, il penetration testing, l'auditing e la consulenza, la digital forensics e la crittografia.

- **Migliorare la collaborazione per rispondere più rapidamente agli attacchi**

Nonostante i recenti progressi nel migliorare il coordinamento tra pubblico e privato, l'aumento della cooperazione tra i criminali cyber continua a essere una minaccia costante. Infatti, gli attaccanti cyber legati a governi ostili e associazioni criminali, stanno sviluppando infrastrutture e servizi da utilizzare per scopi fraudolenti. Inoltre, stanno anche adottando rapidamente nuove tecnologie per penetrare nelle reti e vanificare

gli sforzi per contenere le minacce, che spesso dipendono dal coordinamento tra entità con standard, obiettivi e priorità diverse.

Il coordinamento e la collaborazione sono temi chiave del documento ***National Cybersecurity Strategy*** pubblicato dalla Casa Bianca nel marzo 2023. Questa strategia pone l'accento sui partenariati tra la società civile e l'industria e promuove la collaborazione con gli alleati per rafforzare le norme di comportamento responsabile degli Stati, per responsabilizzare i Paesi colpevoli di comportamenti irresponsabili e distruggere le reti criminali che si celano dietro gli attacchi informatici.

- **Allineare le priorità di cybersecurity tra settore pubblico e privato**

I partecipanti hanno evidenziato numerose idee per la cooperazione tra industria e governo al fine di migliorare la sicurezza informatica su vasta scala, identificando le sfide comuni e condividendo le migliori pratiche. In questo senso, si dovrebbe promuovere l'assunzione di professionisti cyber provenienti da diversi contesti. È inoltre imporante concentrarsi maggiormente sull'innovazione in sicurezza, vedendola come un vantaggio competitivo, e sostenere approcci *zero-trust,* basati sul presupposto che la sicurezza informatica sia sempre a rischio di minacce, interne ed esterne.

Inoltre, è importante investire sulla consapevolezza delle problematiche informatiche all'interno delle istituzioni e della pubblica amministrazione. È quindi necessario migliorare gli standard, le metriche e i dati relativi alla cyber security per rafforzare la comprensione delle minacce e promuovere gli investimenti pubblici e privati volti a contrastarle e contenerle.

- **Studiare modi per sostenere le istituzioni democratiche contro gli attaccanti cyber**

Gli attacchi cyber sono progettati per influenzare il sostegno e il coinvolgimento dei cittadini nei processi elettorali, legislativi o normativi, cercando di manipolare l'opinione pubblica o di minare le norme di comportamento democratico. Sebbene l'obiettivo primario di queste campagne, palesi od occulte, sia quello di seminare confusione sociale nel breve termine, i partecipanti hanno riconosciuto che, a lungo termine, questi sforzi potrebbero riuscire a influenzare stabilmente l'opinione pubblica. A causa delle complessità rappresentate da queste sfide informatiche soprattutto rispetto alle forme di governo più rappresentative, i partecipanti non concordavano univocamente sui modi più efficaci per difendersi da questa crescente minaccia e hanno chiesto di approfondire la ricerca sulle misure in grado di contrastare le minacce informatiche alla democrazia.

- **Formare leader resilienti ai rischi cyber, in grado di affrontare il futuro**

La dipendenza globale dall'open technology rappresenta tutto quello che fa progredire le comunità, in particolare la connettività sociale, le comunicazioni e la collaborazione. Questi fattori sono determinanti per il **benessere nazionale e internazionale**, e allo stesso tempo, la sua dipendenza dalle tecnologie lo rende

bersaglio privilegiato dei criminali informatici. Le attuali misure di sicurezza funzionano in parte, ma in troppi casi sono insufficienti.

L'IBM Institute for Business Value (IBV) fornisce insight di business scrupolosi e basati sulla tecnologia, combinando le competenze di esperti di settore e accademici di spicco con ricerche globali e dati sui diversi ambiti. Per oltre 20 anni, i rapporti di *thought leadership* dell'IBV hanno fornito raccomandazioni utili per affrontare le sfide e le opportunità più urgenti.

Creato nel 1998, l'IBM Center for The Business of Government collega la ricerca alla pratica, applicando la ricerca alle soluzioni che le pubbliche amministrazioni possono prendere per risolvere i problemi del mondo reale. Il Centro stimola la ricerca e facilita la discussione di nuovi approcci per migliorare l'efficacia del governo a livello federale, statale, locale e internazionale.

Informazioni su IBM

IBM è un'azienda leader a livello mondiale nel settore del cloud ibrido, dell'AI e dei servizi alle imprese e opera con le imprese di oltre 175 Paesi aiutandole a capitalizzare sugli insight dei loro dati, a semplificare i processi aziendali, a ridurre i costi e a ottenere un vantaggio competitivo nei loro settori d'industria. Quasi 3.800 enti governativi e aziende in aree infrastrutturali critiche come quelle dei servizi finanziari, delle telecomunicazioni e sanità si basano sulla piattaforma cloud ibrida di IBM e su Red Hat OpenShift per realizzare la loro trasformazione digitale in modo rapido, efficiente e sicuro. Le innovazioni di IBM nell'ambito dell'AI, del quantum computing, delle soluzioni cloud specifiche per settore d'industria e nei servizi sono offerte con opzioni open e flessibili. Tutto questo è supportato dal ben noto impegno di IBM per la trasparenza, la responsabilità, l'inclusività e il servizio. Per maggiori informazioni, visitate il sito www.ibm.com.

Per maggiori informazioni:
Claudia Ruffini, *IBM Communications Leader, Italia*
email: cla@it.ibm.com.
tel. : +39 335 6325093
