IBM Italy News Room

IBM aiuta le imprese ad adottare un approccio Zero Trust alla sicurezza

IBM Cloud Pak for Security aggiunge funzionalità Zero Trust; nuove blueprint e maggiore integrazione con un'ampia rete di partner per semplificare l'adozione di Zero Trust

CAMBRIDGE, Massachusetts, 05 maggio 2021 – IBM (NYSE: IBM) Security introduce una nuova versione Software as a Service (SaaS) di IBM Cloud Pak for Security progettata per semplificare il modo in cui le aziende adottano l'architettura Zero Trust nelle proprie organizzazioni. La società annuncia inoltre la partnership con il leader nel mercato del network & cloud security, Zscaler, e nuove blueprint per casi d'uso comuni di Zero Trust.

Per i professionisti della sicurezza, Zero Trust è il framework che li aiuta ad aggiornare nell'insieme i programmi di sicurezza e ad adattarli ai nuovi rischi che emergono dalle mutate condizioni di business. Un recente studio ESG ha rilevato che il 45% delle aziende che avevano già adottato strategie Zero Trust ha effettuato una transizione molto più agile verso il lavoro da remoto, rispetto all'8% delle imprese ancora poco mature[1].

"Con una forza lavoro mobile e dati presenti ovunque, Internet è diventata la nostra rete principale", **ha affermato Mauricio Guerra, CISO di The Dow Chemical Company, che interverrà al prossimo IBM Think Summit dell'11 maggio.** "L'adozione dell'architettura Zero Trust ci permette di aggiungere nuove funzionalità e rafforzare la sicurezza. La collaborazione con IBM Security e Zscaler ci aiuterà a fornire agli utenti remoti un accesso sicuro alle applicazioni, ovunque queste si trovino".

Le nuove blueprint di IBM Security offrono un framework di riferimento per definire un programma di sicurezza applicando i principi di base Zero Trust: accesso con privilegi minimi; mai fidarsi, verificare sempre; supporre sempre la violazione. Queste blueprint offrono alle aziende una roadmap rigorosa sulle capacità di sicurezza necessarie, assieme a linee guida su come integrarle all'interno di una architettura Zero Trust. Le capacità e le linee guida sono state definite sulla base di progetti reali con clienti che sono stati supportati nel loro percorso e nei loro investimenti su Zero Trust, con un approccio pragmatico volto ad allineare al meglio gli obiettivi di sicurezza e di business.

Le blueprint Zero Trust di IBM Security aiutano le aziende su questi aspetti:

- **Preservare la privacy dei clienti**: le capacità e le integrazioni della blueprint privacy uniscono le capacità di sicurezza e conformità necessarie alle aziende nella protezione dell'integrità dei dati dei clienti e nella gestione delle normative sulla privacy. Utilizzando questo modello, le aziende possono rafforzare gli accessi limitati e condizionati a tutti i dati, riducendo l'esposizione in caso di compromissione. Questa connessione aiuterà a generare informazioni sull'utilizzo dei dati e sui rischi di privacy, applicando politiche che assicurino che i dati vengano utilizzati solo per gli scopi prefissati. Questo approccio aiuta le aziende a rilevare e a rispondere in modo efficiente alle problematiche di rischio e di conformità grazie a processi di remediation automatizzati, che utilizzano più strumenti, inclusa l'ultima versione di IBM Cloud Pak for Security che comprende un più ampio set di funzionalità di data security della soluzione IBM Security Guardium.

- **Proteggere la forza lavoro ibrida e remota** : con hybrid workforce blueprint le aziende possono disporre di forza lavoro in grado di connettersi in modo totalmente sicuro a qualsiasi applicazione su qualsiasi rete,

da qualsiasi luogo e utilizzando qualsiasi dispositivo. In questo ambito, IBM annuncia la partnership con Zscaler per aiutare le aziende a collegare gli utenti alle applicazioni in modo trasparente e sicuro. IBM Security Services unisce alla tecnologia Zscaler l'esperienza di IBM per aiutare le imprese ad adottare un approccio SASE (Secure Access Service Edge) end-to-end. Inoltre, l'integrazione di Zscaler Private Access™ e Zscaler Internet Access™ con le principali tecnologie di IBM Security, come IBM Security Verify, getterà le fondamenta di un'architettura Zero Trust.

- **Ridurre il rischio di minacce interne**: con insider threat blueprint, le aziende possono gestire proattivamente le minacce interne da ogni vettore, rafforzando la resilienza e limitando le interruzioni di business. Le capacità delineate in questo blueprint sono progettate per rilevare le anomalie nel comportamento degli utenti, rinforzare in modo adattivo le politiche di sicurezza con l'automazione e isolare i dati più preziosi. Le rilevazioni di nuove minacce mobile da parte di IBM Security MaaS360 con Watson hanno migliorato le funzionalità di analytics sul comportamento degli utenti fornite da IBM Cloud Pak for Security.

- **Proteggere il cloud ibrido:** l'hybrid cloud blueprint aiuta le aziende a rinnovare il loro programma di sicurezza per avere maggiori visibilità e controllo su dati e attività sensibili durante la migrazione verso il cloud. Le capacità incluse in questo progetto sono progettate per consentire continuità di compliance, reportistica e risposta, monitorando le configurazioni errate nel cloud e garantendo l'applicazione coerente delle policy di sicurezza su tutti i carichi di lavoro in cloud. Secondo questa blueprint, le aziende potranno scegliere di avvalersi di IBM Security Services for Cloud, in quanto offrono un approccio aperto e automatizzato per aiutare a semplificare la sicurezza del cloud ibrido. Questa soluzione unisce l'esperienza nella security del cloud di tutti i diversi fornitori con un set integrato di soluzioni tecnologiche cloud proprietarie e di terze parti.

IBM Security ritiene sia necessario un approccio open per affrontare le complesse e frammentate sfide di sicurezza di oggi secondo una strategia Zero Trust. Per aiutare a semplificare e connettere la sicurezza all'interno di tutto l'ecosistema di fornitori, IBM sta collaborando con i maggiori provider tecnologici. La partnership con Zscaler è una componente fondamentale dell'approccio Zero Trust per assistere le aziende nella semplificazione del lavoro da remoto e nella modernizzazione della sicurezza della rete.

"Il lavoro da remoto unito all'adozione del cloud e di funzionalità SaaS da parte delle aziende ha reso il perimetro di sicurezza esistente obsoleto e le difese tradizionali inefficaci", **ha affermato Jay Chaudhry, CEO e fondatore di Zscaler**. "L'unico modo di rendere sicuro il business di oggi, sempre più digitale, è l'adozione di un modello di sicurezza Zero Trust dove la validazione dell'identità dell'utente è combinata con le policy dell'azienda per consentire un accesso diretto alle applicazioni e alle risorse autorizzate. La nostra alleanza con IBM Security, parte dell'ecosistema Zscaler Zero Trust, aiuta le aziende e i dipendenti a svolgere il lavoro da remoto proteggendo al contempo i dati aziendali".

IBM sta anche collaborando con il proprio ecosistema di partner per aiutarli ad adottare strategie Zero Trust con i propri clienti. Ad esempio, Tech Data offrirà l'accesso alle blueprint di IBM Security Zero Trust come parte della sua Cyber Range, consentendo ai business partner e agli utenti di testare e sperimentare come queste soluzioni, unendosi, consentono un approccio Zero Trust per i principali casi d'uso.

Cloud Pak for Security amplia i modelli di delivery

Un approccio aperto Zero Trust richiede una piattaforma di sicurezza fondata sugli stessi principi di apertura e collaborazione. IBM Cloud Pak for Security combina funzionalità leader nella gestione delle minacce e nella

sicurezza dei dati in un'unica soluzione modulare e di facile utilizzo. Grazie alle nuove funzionalità di IBM Cloud Pak for Security-as-a-Service, le aziende possono scegliere tra un modello di delivery proprietario oppure *hosted* a seconda dell'ambiente IT e delle esigenze. Inoltre, questa soluzione fornisce accesso a una dashboard unificata per gli strumenti di gestione delle minacce, con la possibilità di adeguarne facilmente l'uso grazie a un approccio di pagamento basato sull'utilizzo.

"I nostri clienti devono proteggere i loro ambienti aziendali, in continua e rapida evoluzione, senza causare ritardi o attriti nelle loro operazioni quotidiane", **ha dichiarato Mary O'Brien, IBM Security General Manager.** "Non è raro avere utenti, dati e applicazioni che operano in ambienti diversi: l'importante è che si connettano tra di loro, in modo rapido, trasparente e in sicurezza. Un approccio Zero Trust offre il modo migliore di affrontare la complessità della sicurezza che oggi le aziende devono fronteggiare".

Per saperne di più su Cloud Pak for Security as a Service: https://www.ibm.com/products/cloud-pak-for-security

Per saperne di più sulle soluzioni IBM Security Zero Trust: https://www.ibm.com/security/zero-trust

Partecipa all'IBM Think 2021 per ascoltare gli interventi di Mary O'Brien, IBM Security General Manager; Mauricio Guerra, Dow Chemical CISO; e Jay Chaudhry, CEO di Zscaler. Registrati qui: ibm.com/think.

IBM Security
IBM Security offre uno dei portafogli più avanzati e integrati di prodotti e servizi di sicurezza aziendale. Il portafoglio, supportato dalla ricerca IBM Security X-Force di fama mondiale, consente alle organizzazioni di gestire efficacemente i rischi e difendersi dalle minacce emergenti. IBM gestisce una delle più ampie organizzazioni di ricerca, sviluppo e delivery di soluzioni di sicurezza al mondo, monitora oltre 150 miliardi di eventi di sicurezza al giorno in più di 130 Paesi e ha ottenuto più di 10.000 brevetti di sicurezza in tutto il mondo. Per ulteriori informazioni: www.ibm.com/security; @IBMSecurity su Twitter, oppure visita IBM Security Intelligence blog.

[1] ESG Research Report, *The State of Zero-trust Security Strategies*, aprile 2021

Per ulteriori informazioni: Claudia Ruffini - IBM Security Communications Leader - cla@it.ibm.com - +39 335 6325093
