Comunicati stampa

IBM: la sicurezza nel cloud è una sfida primaria per tutte le organizzazioni

Nuovi dati indicano i principali rischi di sicurezza che le aziende devono affrontare

Cambridge, MA - 10 giugno 2020: IBM Security ha diffuso un nuovo studio sulle principali sfide e minacce da affrontare per preservare la sicurezza del cloud. Lo studio evidenzia come la facilità e la velocità con cui gli strumenti cloud possono essere implementati rendano ancora più difficile il controllo da parte dei team di sicurezza su come vengono utilizzati. Attraverso la ricerca e l'analisi di alcune case study, IBM ha rilevato che i principali fattori di rischio per la sicurezza delle imprese rimangono la governance, le vulnerabilità e gli errori di configurazione, aspetti che dovrebbero essere di particolare attenzione quando gli ambienti IT sono cloud-based. Le analisi relative agli incidenti di sicurezza verificatisi nell'ultimo anno, inoltre, ha messo in evidenza la tendenza dei criminali informatici a mirare sempre di più gli attacchi verso ambienti cloud, personalizzando malware, ransomware e altre minacce.

L'accelerazione nell'adozione del cloud in quanto, ad esempio, soddisfa le esigenze sempre più diffuse di lavoro da remoto, rende necessario comprendere ogni minaccia alla sicurezza per poter sviluppare strategie efficaci a contrastarne i rischi. Il cloud abilita funzionalità tecnologiche e di business primarie, pertanto l'adozione e la gestione delle risorse possono anche implicare delle complessità. Secondo IDC, più di un terzo delle aziende ha acquistato oltre 30 tipi di servizi cloud da 16 diversi fornitori solo nel 2019[1]. Un'architettura così dispersiva può rendere non chiara la ownership della sicurezza nel cloud, far emergere "punti ciechi" nelle policy e determinare vulnerabilità e configurazioni errate dovute allo Shadow IT.

Per comprendere più chiaramente lo stato dell'arte della sicurezza in un momento in cui le aziende hanno una maggiore predisposizione verso gli ambienti ibridi e multi-cloud, IBM Institute for Business Value (IBV) e IBM X-Force Incident Response and Intelligence Services (IRIS) hanno esaminato le sfide e le principali minacce alla sicurezza degli ambienti cloud. Queste le evidenze principali:

Ownership complessa: il 66% degli intervistati[2] ha dichiarato di affidarsi ai provider dei propri servizi cloud per la gestione e implementazione degli standard di sicurezza di base; tuttavia, la percezione dell'ownership della security da parte degli intervistati varia notevolmente tra piattaforme e applicazioni cloud specifiche2.

Applicazioni cloud come punto di ingresso: per compromettere gli ambienti cloud, il modo più semplice per i criminali informatici è inserirsi nelle applicazioni cloud-based, che rappresentano il 45% degli incidenti rilevati nei casi analizzati da IBM X-Force IRIS. In questi casi, i cybercriminali hanno approfittato degli errori di configurazione e delle vulnerabilità intrinseche alle applicazioni, spesso passate inosservate poiché installate dai dipendenti in totale autonomia, al di fuori dei canali ufficiali.

Amplificare gli attacchi: l'obiettivo principale degli attacchi cloud è stato il furto di dati [3], seguito da operazioni di cryptomining e ransomware [4], effettuate utilizzando risorse cloud per amplificarne l'effetto.

"Il cloud ha un potenziale enorme per l'efficienza e l'innovazione del business, ma può anche creare un "wild west" fatto di ambienti ampi e distribuiti che le organizzazioni devono saper gestire e proteggere", ha affermato Abhijit Chakravorty, Cloud Security Competency Leader, IBM Security Services. " *Se implementato nel modo giusto, il cloud può rendere la sicurezza scalabile e più flessibile, ma per compiere questo passo è necessario che le organizzazioni abbandonino convinzioni obsolete e si orientino verso nuovi approcci alla sicurezza progettati specificamente per questa nuova frontiera della tecnologia, sfruttando l'automazione laddove possibile. Questo percorso deve però avere alla base un quadro chiaro degli obblighi normativi e di conformità, oltre che delle particolari sfide alla sicurezza derivanti sia dalle caratteristiche tecniche che dalle policy e dalle minacce esterne rivolte al cloud.***"**

Chi è responsabile della sicurezza del cloud?
Secondo un'indagine dell'IBM Institute for Business Value, le organizzazioni intervistate che si sono affidate ai propri cloud provider per la gestione della cloud security sono state le principali responsabili dei data breach subiti, al netto dei problemi di configurazione, normalmente di responsabilità dei singoli utenti. Tale violazione dei dati ammonta a più dell'85% di tutti i data breach registrati nel 2019 dalle aziende intervistate4.

Inoltre, le organizzazioni intervistate hanno una percezione molto diversa in materia di responsabilità della sicurezza in funzione della varietà di piattaforme e applicazioni. Ad esempio, la maggior parte degli intervistati (73%) ritiene che i provider di servizi di public cloud siano i principali responsabili della sicurezza nel caso di soluzioni *Software-as-a-Service* (SaaS), mentre solo il 42% ritiene che questi siano i principali responsabili della sicurezza nel caso di offerte *Instrastructure-as-a-Service* (IaaS) 3.

Nonostante questo modello di responsabilità condivisa sia indispensabile nell'era ibrida e multi-cloud, lo stesso può anche portare a una variabilità di policy di sicurezza e a una mancanza di visibilità attraverso i diversi ambienti cloud. Le organizzazioni in grado di semplificare le operazioni cloud e security possono aiutare a ridurre questo rischio, attraverso policy definite in modo chiaro e applicabili a tutto l'ambiente IT.

Principali minacce nel cloud: furto di dati, cryptomining e ransomware
Gli esperti IRIS di X-Force Incident Response hanno analizzato in modo approfondito gli attacchi indirizzati agli ambienti cloud affrontati nel corso dell'ultimo anno[5]. Di seguito le principali evidenze:

Cybercriminali: il fattore economico è alla base della maggioranza delle violazioni del cloud rilevate degli esperti di IBM X-Force, sebbene le organizzazioni finanziate da enti governativi rappresentino un fattore persistente di rischio.

Le app in cloud: il punto di accesso più comune per indirizzare gli attacchi sono state le applicazioni cloud, forzate attraverso azioni volte a sfruttare le vulnerabilità e le configurazioni errate. Le vulnerabilità sono spesso rimaste inosservate a causa dello "Shadow IT", ovvero l'utilizzo da parte dei dipendenti di app cloud vulnerabili non approvate dall'organizzazione. La gestione delle vulnerabilità dei servizi cloud può rivelarsi complessa, in quanto fino al 2020 tali vulnerabilità non erano disciplinate dal sistema CVE, **Common Vulnerabilities and Exposures** (CVE).

Ransomware in cloud sono in crescita : nei casi di incident response affrontati da IBM, gli attacchi ransomware sono stati distribuiti 3 volte più di qualsiasi altro tipo di malware negli ambienti cloud, seguiti da cryptominer e malware botnet.

Il furto di dati è un classico : al di fuori della distribuzione di malware, il furto di dati ha costituito il tipo di attacco più comune negli ambienti cloud violati nell'ultimo anno. Il tipo di dati sottratti alle organizzazioni, come osservato da IBM, varia dalle informazioni di identificazione personale (PII) ai client di posta.

Effetti esponenziali: i criminali informatici hanno utilizzato risorse cloud per amplificare l'effetto di attacchi come cryptomining e DDoS. Il cloud è stato inoltre sfruttato per ospitare infrastrutture e operazioni malevole, associate ad azioni volte a impedirne il rilevamento.

"*I trend emersi durante l'analisi dei casi di incident response evidenzia una possibile e continua espansione ed evoluzioni dei casi di malware in ambito cloud contestualmente ad una sempre maggiore adozione di soluzioni cloud*", ha affermato Charles DeBeck, IBM X-Force IRIS. *"Il nostro team ha osservato come gli sviluppatori di malware abbiano già iniziato a crearne di nuovi in grado di disabilitare le soluzioni di cloud security più diffuse e a progettare malware che sfruttano la scalabilità e la flessibilità offerte dal cloud*".

Elevati livelli di CloudSec migliorano la capacità e la velocità di risposta in caso di attacchi

Le organizzazioni che sono in grado di orientarsi verso un modello di governance più maturo e semplificato saranno in grado di rendere più agile la propria infrastruttura di security e di migliorare le capacità di fronteggiare gli attacchi.

Lo studio di IBM Institute for Business Value rivela che le organizzazioni evolute che abbiano già ampiamente adottato soluzioni cloud e security sono in grado di identificare e contenere i data breach più rapidamente rispetto a quelle ancora all'inizio del percorso di migrazione verso il cloud. Quanto ai tempi di risposta, le organizzazioni con un maggior grado di maturità sono due volte più veloci nelle fasi di identificazione e contenimento delle violazioni rispetto alle organizzazioni meno mature: per le prime, il ciclo di vita medio delle minacce si attesta attorno ai 125 giorni contro 250 giorni per le organizzazioni impreparate.

Oggi il cloud è essenziale per le tutte le organizzazioni. Per questo, IBM Security ha delineato una serie di direzioni utili a migliorare la sicurezza in ambienti ibridi multi-cloud:

Stabilire governance e cultura collaborativa: adottare una strategia unificata che combini operazioni cloud e security, coinvolgendo tutti gli attori, dai developer ai dipartimenti di IT Operation e Security. Tale strategia richiede anche che siano delineate politiche e responsabilità chiare per la gestione e il controllo delle risorse cloud esistenti e per l'acquisizione di nuove.

Assumere una visione basata sul rischio : valutare i tipi di workload e di dati per i quali è previsto il passaggio a un ambiente cloud e definire policy di sicurezza appropriate. Il primo passo è mettere a punto una valutazione basata sul rischio di visibilità completa dell'ambiente cloud, per poi creare un processo mirato volto all'adozione graduale del cloud.

Adottare un sistema di strong access management: sfruttare le politiche di access management e gli strumenti per l'accesso alle risorse cloud, inclusa l'autenticazione a più fattori, per prevenire l'infiltrazione attraverso credenziali rubate. È quindi necessario limitare gli account autorizzati e impostare tutti i gruppi di utenti con il minimo dei requisiti necessari per ridurre il rischio di compromissione dell'account (modello "zero-trust").

Disporre degli strumenti giusti: assicurarsi che gli strumenti per il monitoraggio della sicurezza, la visibilità e la security response siano efficaci su tutte le risorse cloud e on-premise. A questo proposito, è consigliabile considerare il passaggio a tecnologie e standard open che consentono una maggiore interoperabilità.

Automatizzare i processi di sicurezza : per migliorare le capacità di rilevamento e risposta agli eventi, è consigliabile implementare un sistema di sicurezza automatizzato efficace, anziché fare affidamento sull'approccio manuale.

Fare ricorso a simulazioni proattive: simulare vari scenari di attacco può aiutare a identificare falle nella sicurezza e ad affrontare potenziali problemi di natura legale che possono sorgere in caso di indagini sugli attacchi.

Il Report completo X-Force IRIS Cloud Security Landscape è visualizzabile a questo link.

---

[1] IDC CloudPulse Summary Q119

[2] IBM Institute for Value Survey of 930 senior business and IT professionals

[3] IBM X-Force IRIS: "Cloud Security Landscape Report"

[4] IBM X-Force Threat Intelligence Index, 2020

[5] IBM X-Force IRIS “Cloud Landscape Report,” based on client incident response cases taking place between June 2018 and March 2020

Per ulteriori informazioni: Claudia Ruffini, Cross Communications, IBM Italy cla@it.ibm.com, +393356325093