Le 7 verità nascoste della sicurezza nel cloud

WITH secure

Sommario

Introduzione

Per quasi due decenni il cloud computing ha proposto, e realizzato, un sogno utopico. Le organizzazioni a corto di risorse possono fronteggiare concorrenti più grandi, meglio equipaggiati e con risorse economiche maggiori e questi colossi, a loro volta, godono della libertà e della flessibilità offerte dal cloud.

Il sogno è diventato una realtà che viviamo ogni giorno, ma è arrivato il momento di prendere atto di alcune amare verità circa gli effetti del cloud sulla sicurezza delle organizzazioni, esaminando prima di tutto la differenza tra i principi sottostanti e ciò che c'era prima.

Naturalmente, il cloud può assumere diverse forme, dalle offerte Infrastructure-as-a-Service (IaaS) e Platform-as-a-Service (PaaS) su cui tutti facciamo affidamento, ma di cui la maggior parte degli utenti finali è del tutto ignara, agli strumenti Software-as-a-Service (SaaS) come Microsoft 365 e Salesforce che molte persone usano ogni giorno.

Ciò che accomuna tutte queste tipologie di cloud è il concetto di responsabilità condivisa per la sicurezza: i clienti sono responsabili per tutto ciò che i cloud provider escludono dai propri controlli di sicurezza integrati.

Sono pochissime le organizzazioni che dispongono delle risorse per proteggersi dalle minacce che ormai sono parte integrante dell'utilizzo del cloud e c'è ben poco che si possa fare facilmente per cambiare la situazione. Il costo reale del possesso (o del noleggio) del cloud include la risposta alle sfide di sicurezza che ne derivano, che è spesso difficile da determinare finché non si verifica una violazione.

Qui presentiamo sette verità nascoste sulla sicurezza nel cloud per il 2022 e mostriamo come le organizzazioni stiano rimodellando le proprie regole per cogliere i vantaggi di un approccio cloud e assicurare che il cloud sia di aiuto, e non di intralcio, al raggiungimento dei loro obiettivi.

I vantaggi del cloud dovrebbero essere superiori ai rischi[1]. L'unico modo per andare avanti è adottare un approccio orientato al risultato.

> **“Mi vengono in mente non più di una o due organizzazioni a cui realisticamente potrei pensare di rivolgermi per rilevare gli attacchi nello spazio cloud. Gran parte delle capacità più rilevanti che abbiamo visto utilizzare dalle organizzazioni sono interamente sviluppate in-house. Questo è positivo se sei una banca con capitale di classe 1, ma non lo è affatto se fai parte del restante 99,5%.”**

Nick Jones,
Principal Security Consultant, WithSecure™

1. https://www.withsecure.com/en/expertise/resources/cloud-security-striking-the-balance

Verità nascosta 1

Non puoi proteggere ciò che non vedi

W / T H
secure

Verità nascosta 1

Non puoi proteggere ciò che non vedi

Ishan Singh-Levett
Director, Product Management

Non si può proteggere ciò che non si vede e la visibilità nel cloud è una variante di una grande sfida con cui i reparti IT sono alle prese: lo shadow IT. Il Bring Your Own Device (BYOD) è stato affiancato, se non soppiantato, dal BYOC (Bring Your Own Cloud).

Uno dei punti di forza del cloud è che chiunque può acquistare risorse di elaborazione, storage e applicazioni con il minimo sforzo in quantità facilmente assimilabili. Questa flessibilità complica anche il compito dei reparti IT e dei team di sicurezza, e quindi dell'intera organizzazione, di monitorare quali risorse cloud vengono utilizzate e dove.

È molto difficile capire quali risorse cloud sono distribuite in un'organizzazione, anche al netto delle applicazioni SaaS. I team possono avviare istanze cloud contenenti dati sensibili e sistemi semplicemente con una carta di credito. Alcune di queste istanze, anche se non tutte, possono essere difficili da vedere e monitorare e questo può causare vari problemi di dipendenze tra il BYOC noto, il cloud approvato dall'azienda e il BYOC invisibile e non autorizzato. Gli equivalenti on-premise sono più facili da rilevare mediante agent e scansioni.

La visibilità è una sfida significativa negli ambienti di sviluppo, in cui si possono avviare facilmente istanze cloud, distribuire dati di produzione al loro interno e creare link nei sistemi interni, il tutto con supervisione, documentazione o procedure di sicurezza ridotte al minimo. Naturalmente, a parte i problemi di sicurezza e di privacy, è anche molto probabile che le organizzazioni stiano pagando molto più del dovuto per i loro servizi cloud.

Affrontare la verità

A parte la sfida della scarsa visibilità, l'adozione massiccia e non strutturata del cloud comporta anche che i cloud di proprietà dei team, dei reparti o anche di singoli dipendenti spesso manchino di coerenza nella configurazione. Questo si inserisce nelle nostre verità numero due e cinque: configurazione coerente e sicura e protezione per i gap.

Un Cloud Access Security Broker (CASB) è un modo per tenere traccia di chi accede ai singoli servizi cloud e quando. Le organizzazioni usano CASB come proxy di intercettazione, come ulteriore livello di insight. Più avanti vedremo quanto questo possa essere importante. Il CASB, comunque, è una sorta di coltellino svizzero e le soluzioni single-cloud come Cloud Protection for Salesforce di WithSecure™ possono offrire la protezione necessaria con una minore complessità. Il CASB richiede anche l’accesso agli endpoint per installare agent, più o meno come accade per EDR (Endpoint Detection and Response) e MDR (Managed Detection and Response).

Verità nascosta 2

Gli errori di configurazione del cloud sono ovunque

WITH secure

Verità nascosta 2

Gli errori di configurazione del cloud sono ovunque

Nick Jones
Principal Security Consultant

La combinazione tra flessibilità e accesso pubblico implica che una configurazione sicura per il cloud sia tanto indispensabile quanto difficile da realizzare. Agli attaccanti non servono competenze o strumenti sofisticati se una configurazione errata lascia l'organizzazione aperta agli attacchi.

I cloud provider hanno semplificato i processi di protezione di un ambiente, tanto da farne un pilastro fondamentale dei prodotti che vendono. Definire una configurazione perfetta per un singolo account per un singolo carico di lavoro è assolutamente fattibile per qualsiasi reparto IT. I grandi cloud provider, forti di anni di esperienza, offrono tutti una documentazione e una strumentazione eccellenti per identificare i problemi di base.

Le difficoltà nascono quando occorre implementare la sicurezza su larga scala per più account, centinaia di carichi di lavoro e diversi cloud provider. Si tratta di un problema comune dato che oggi le organizzazioni si affidano generalmente a tre-cinque provider[2].

Esistono strumenti e servizi utili per iniziare a proteggere più ambienti, ma anch'essi devono essere configurati in funzione del profilo di sicurezza desiderato, adattati ai carichi di lavoro in costante evoluzione ed essere fruibili dalle persone incaricate di rilevare le violazioni. Questo si scontra con un problema che WithSecure™ conosce bene, dal punto di vista sia della consulenza che dei servizi gestiti: è raro che le organizzazioni non abbiano la visione su questi temi, ma spesso sono a corto di risorse per concretizzarla[3].

Detto questo, molti team riescono a farlo, applicando policy di sicurezza standard su un piccolo numero di provider o dedicando molto tempo ad affrontare la complessità che deriva dalla flessibilità[4]. In ogni caso, la gestione delle configurazioni cloud su larga scala è un compito tutt'altro che semplice e richiede una stretta collaborazione tra i team tecnici e di sicurezza che creano e gestiscono i carichi di lavoro.

2. https://www.cio.com/article/228677/it-governance-critical-as-cloud-adoption-soars-to-96-percent-in-2018.html

3. https://www.withsecure.com/en/expertise/campaigns/detect-to-respond

4. https://www.withsecure.com/en/expertise/resources/webinar-replay-cisos-step-up-on-cloud-and-cyber-priorities-for-2022

Alcune organizzazioni, pensiamo ad esempio agli istituti finanziari globali di alto livello, possono contare su risorse e competenze sufficienti per costruire enormi funzionalità in-house. Si tratta però di una minima parte delle organizzazioni che utilizzano il cloud.

Parte del problema è il numero di utenti del cloud: anche se i cloud provider sono abili a fornire strumenti e assistenza, come abbiamo detto prima, è impossibile raggiungere i singoli clienti con indicazioni sulla sicurezza, se non in senso molto generale. Se si aggiunge la complessità che deriva dalla presenza di più cloud e più configurazioni, si capisce bene da dove nasce il problema.

La licenza creativa che i cloud provider lasciano agli utenti è notevole e fa anche parte del fascino del cloud, ma questo rappresenta una sfida per chi si occupa di sicurezza.
Non esiste un unico strumento di diagnostica in grado di correggere tutte le lacune di sicurezza in un ambiente.

A complicare ulteriormente la situazione c'è il problema che una configurazione che è errata in un ambiente può essere assolutamente corretta in un altro, rendendo difficile individuare gli errori di configurazione mediante strumenti automatizzati. La risposta è adottare un approccio più umano al problema: è meglio avere poche persone competenti e adattabili piuttosto che un vasto assortimento di strumenti di diagnostica poco flessibili.

Affrontare la verità

Se la soluzione a questo problema suona familiare, forse è perché da molto tempo le società di consulenza specializzate e i fornitori di soluzioni di incident response e MDR correggono problemi come questo per l'IT on-premise.

La sicurezza nel cloud pone delle difficoltà specifiche, ma è utile ricordare che molte tecniche esistenti sono spesso facilmente adattabili, se non già adatte, per affrontare queste sfide.

I consigli di terze parti come i consulenti per la sicurezza nel cloud di WithSecure™ e i servizi MDR con funzioni di gestione del profilo di sicurezza nel cloud come WithSecure™ Countercept sono utili per colmare il divario tra le norme di sicurezza di un cloud provider e quelle della maggior parte delle organizzazioni utenti finali.

Verità nascosta 3

Il cloud ha cambiato le regole del gioco per tutti

W / T H
secure

Verità nascosta 3

Il cloud ha cambiato le regole del gioco per tutti

Jennifer Howarth
Product Manager - Cloud

Gli attacchi basati sull'identità crescono man mano che aumenta il numero di organizzazioni che adottano il cloud e le applicazioni fornite come servizio, comunemente chiamate XaaS. Perché? La superficie di attacco è fondamentalmente diversa da quella a cui ci hanno abituati i tradizionali ambienti IT on-premise, in cui gli endpoint[5] sono il bersaglio più ovvio per gli attaccanti e il punto migliore in cui concentrare le difese.

A parte IaaS, in cui il cloud viene utilizzato sostanzialmente come data center off-site per ospitare le VM, i carichi di lavoro cloud non espongono un sistema operativo agli attacchi. Concetti come exploit ed esecuzione di codice di attacco non sono più rilevanti, né lo sono le misure difensive perfezionate nel corso degli anni per contrastarli. Infatti, gli attaccanti raggiungono i propri scopi chiamando le API cloud con credenziali legittime. Da un punto di vista difensivo, di per sé non c'è nulla di intrinsecamente malevolo in una chiamata API, ma una sequenza di chiamate diversa rispetto alle normali operazioni di un utente, o insolita nel contesto di un particolare carico di lavoro, desta sospetti. È qui che entra in gioco l'analisi del comportamento degli utenti e delle entità (UEBA).

UEBA crea un quadro di ciò che avviene normalmente in un particolare carico di lavoro e in un determinato ambiente, se possibile in relazione a un'identità utente. La comprensione di ciò che è normale e di ciò che anomalo è stata una potente arma di rilevamento nel mondo on-premise, ma nel cloud è la base vera e propria di una strategia di monitoraggio efficace. È importante sottolineare che il rilevamento basato sull'identità fornito da UEBA non riguarda solo gli esseri umani. Gli utenti finali sono un ottimo punto di partenza per il monitoraggio degli ambienti SaaS, ma nel contesto dei servizi cloud di base, le identità system-to-system sono altrettanto importanti. In recenti incidenti affrontati dall'Incident Response Team di WithSecure™ è emerso che gli attaccanti erano più interessati alle credenziali macchina che agli account degli utenti finali.

5. https://www.withsecure.com/en/expertise/resources/detecting-attacks-in-the-cloud

Il cloud porta nuove tecnologie e nuovi modi di lavorare a cui i difensori hanno dovuto adattarsi per comprenderli e difendersi[6]. Alcuni attacchi avvengono al livello di gestione del cloud e non hanno bisogno di interagire con le infrastrutture tradizionali on-premise o strutture simili. Per questo è fondamentale che le organizzazioni costruiscano capacità di rilevamento e risposta appositamente per il cloud. L'Incident Response Team di WithSecure™ si trova sempre più a gestire indagini che riguardano solo il cloud e prevediamo un incremento di questa tendenza in futuro.

Affrontare la verità

La sicurezza nel cloud attualmente è una sfida. La threat intelligence è scarsa o inesistente, i dati possono essere difficili da trovare, il volume e la scala conosciuti degli attacchi sono ancora bassi e le organizzazioni che sono state colpite più duramente spesso sono riluttanti a parlare. Ma ci sono molti motivi per essere ottimisti.

Il rilevamento delle minacce si sta adeguando. La corretta preparazione strategica e l'adattamento delle funzionalità esistenti nelle piattaforme cloud aiutano anche i professionisti DFIR (Digital Forensics and Incident Response) a svolgere il proprio lavoro negli incidenti basati sul cloud.

Un altro raggio di luce è MITRE[8], che si sta adoperando per inserire più threat intelligence nel proprio framework degli attacchi. Ma resta vero che, almeno nel breve periodo, i fornitori e professionisti di cyber security operano in modalità di sperimentazione e ricerca.

Scopri di più su come l'Incident Response Team di WithSecure™ svolge il suo lavoro nel cloud: la corretta preparazione strategica e l'adattamento delle funzionalità esistenti nelle piattaforme cloud[9].

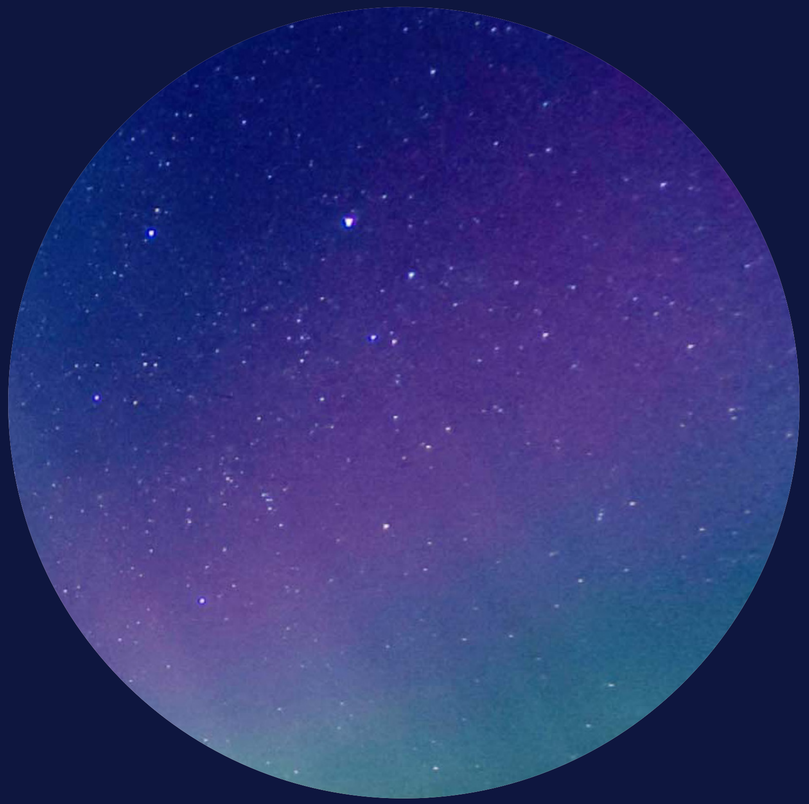
6. https://www.withsecure.com/en/expertise/resources/how-the-cloud-has-changed-response

8. https://attackevals.mitre-engenuity.org/enterprise/participants/f-secure/?adversary=carbanak_fin7

9. https://www.withsecure.com/en/expertise/resources/how-the-cloud-has-changed-response

Verità nascosta 4

Gli endpoint vanno comunque difesi



W / T H
secure

Verità nascosta 4

Gli endpoint vanno comunque difesi

Harri Ruusinen
Director, Global Sales Engineering

Anche se si implementa l'analisi UEBA, gli endpoint diventano punti di ingresso nel cloud. La superficie di attacco è cresciuta.

Nonostante l'adozione di massa dei servizi cloud, resta comunque necessario difendere i computer e gli altri dispositivi usati per accedere a questi servizi. L'EDR continua a essere utile in uno scenario di sicurezza nel cloud. Ma questo è solo un punto di partenza, l'impatto dell'EDR non finisce qui.

I servizi cloud prevedono generalmente diversi livelli di sicurezza. Ad esempio l'autenticazione a più fattori (MFA) impedisce agli attaccanti di accedere ai sistemi tramite credenziali sottratte. Se il dispositivo che utilizza il servizio viene compromesso da remoto o viene rubato fisicamente, la sessione potrebbe essere ancora attiva e l'attaccante potrebbe bypassare quel controllo di sicurezza aggiuntivo. L'assenza di MFA o crittografia sugli endpoint è un problema: se un attaccante dispone delle chiavi giuste per ottenere l'accesso, la responsabilità ricade sull'organizzazione dell'utente finale, non sul cloud provider. L'EDR, quindi, rimane essenziale per i dispositivi utilizzati per accedere al servizio cloud di qualsiasi organizzazione.

Affrontare la verità

La buona notizia è che molte organizzazioni hanno già predisposto gli strumenti necessari per curare questa ferita. Le soluzioni di protezione degli endpoint ed EDR sono più importanti che mai, visto il loro ruolo nel migliorare la cyber resilienza complessiva di un'azienda.

EDR permette a un team di sicurezza di identificare modelli di comportamento palesemente malevoli e anomali e di tenere un registro di tutte le azioni eseguite sugli endpoint, ma deve adattarsi per svolgere la sua funzione anche nella sicurezza cloud. Questo è un fatto che osserviamo in tutta WithSecure™ perché monitorare tutti gli ambienti contemporaneamente è una sfida sempre più importante.

Un aspetto da migliorare è la capacità di EDR di rilevare la sottrazione delle credenziali cloud da un endpoint, in modo da attivare un allarme al primo punto di ingresso e correlarlo alle anomalie UEBA cloud per evidenziare quando un attaccante ha compromesso un endpoint per arrivare al cloud.

Stiamo anche valutando il modo in cui la soluzione EDR di WithSecure™ segnala lo stato della sicurezza, compreso l'uso di funzionalità di sicurezza hardware, per ostacolare il più possibile la compromissione e la diffusione degli attacchi negli endpoint dei clienti.

La tecnologia EDR non è diventata inutile, anzi è ancora essenziale per proteggere gli endpoint e quindi tenere gli attaccanti fuori dal cloud.

WithSecure™ prevede un aumento delle sinergie tra EPP/EDR e la sicurezza nel cloud in futuro, che consentirà ai clienti e partner di rimanere resilienti man mano che adottano nuovi modi di lavorare.

Per altre informazioni sulle caratteristiche ottimali di un sistema EDR cloud-ready, leggi la nostra guida sulle 10 cose da tenere a mente prima di acquistare una soluzione EDR[10].

10. https://www.withsecure.com/en/expertise/resources/10-things-to-consider-before-buying-an-edr-solution

Verità nascosta 5

Una difesa disgregata è una difesa debole

W / T H
secure

Verità nascosta 5

Una difesa disgregata è una difesa debole

Domenico Gargano
Director, Technical Operations

Essere presenti nel cloud è già incredibilmente difficile: ogni organizzazione avrà come minimo una piccola presenza con un endpoint fisico per quanto riguarda l'IT. La suddivisione dei servizi e delle applicazioni tra ambienti on-premise e cloud allarga la superficie di attacco che può essere presa di mira. E se i cloud sono più di uno, il problema non fa che moltiplicarsi.

Identificare e colmare queste lacune di sicurezza è di importanza vitale, ovviamente, ed è anche più che probabile che la tua organizzazione, intenzionalmente o meno, si sia già attivata per affrontare questa sfida.

L'approccio "shift left" che implica lo spostamento della responsabilità della sicurezza verso gli sviluppatori[11], così come la recente tendenza che vede i chief information security officer (CISO) uscire dal confine del reparto IT per diventare leader cross-business, riflettono una maggiore attenzione verso il "raccordo" tra le applicazioni e i servizi cloud.

In sostanza, perché esiste questo problema? Per lo stesso motivo per cui i fornitori di software e sistemi operativi (e tutti noi) hanno avuto la stessa difficoltà con l'IT tradizionale on-premise quando il desktop computing è diventato la forza dominante nell'IT aziendale. I cloud provider dispongono di risorse di sicurezza enormi e sono in grado di fornire strumenti e conoscenze eccezionali ai clienti. Ma il servizio si ferma lì. Non hanno un modo economico per raggiungere i singoli clienti e offrire loro una sicurezza su misura senza aumentare il costo del cloud computing a un livello proibitivo.

A livello di infrastruttura e applicazioni, i cloud provider operano su una scala enorme e hanno l'esigenza di gestire le aspettative degli utenti. La strada da percorrere è fatta di una serie di impressionanti strumenti e configuratori di sicurezza, ma questi rappresentano solo una tessera del puzzle per quanto riguarda la protezione di un'organizzazione basata sul cloud.

11. https://www.withsecure.com/en/expertise/resources/tech-not-culture-is-key-to-devsecops

Difese frastagliate, team frastagliati?

I consulenti di WithSecure™ hanno notato che un numero significativo di organizzazioni gestisce centri operativi di sicurezza (SOC) separati per le proprie strutture cloud. Questa prassi ha riscosso un successo disomogeneo e spesso sembra andare a braccetto con un secondo fenomeno: la costante difficoltà di reclutare e trattenere gli esperti della sicurezza cloud. Ma questa non è certo una novità; si parla da decenni dello skills gap che caratterizza il settore IT.

La soluzione a questa particolare carenza, però, è piuttosto diversa: i team cloud ricorrono a funzionalità di sicurezza personalizzate, a volte scavalcando l'organizzazione di sicurezza. In alcuni casi, i consulenti per la sicurezza nel cloud di WithSecure™ finiscono per interfacciarsi sempre di più con il settore tecnico delle aziende, che di solito conosce meglio la sicurezza cloud dell'azienda rispetto al team della sicurezza IT. La tipica organizzazione di sicurezza è più frammentata rispetto al passato.

In mancanza di origini dati appropriate, si ottiene una visione incompleta delle attività all'interno dell'ambiente e questo rende molto più difficile identificare le anomalie significative o mettere in correlazione le varie parti dell'ambiente. Una situazione molto favorevole per gli attaccanti.

Essere in grado di correlare i punti di dati nell'infrastruttura on-premise e in quella nel cloud o nei cloud è molto importante per costruire un quadro completo di ciò che un attaccante potrebbe fare e, di conseguenza, per avere le migliori opportunità di rilevare e rispondere alla minaccia.

L'indagine di WithSecure™ sulle attività del gruppo hacker NOBELIUM ha evidenziato la sua capacità di penetrare attraverso un vettore on-premise per poi spostarsi nel cloud, mantenendo la persistenza e raccogliendo le informazioni di volta in volta necessarie.

I ricercatori di Microsoft hanno pubblicato ulteriori dettagli, mettendo in luce le strategie adottate da NOBELIUM per sottrarre credenziali che in seguito sono servite per accedere ai server ADFS (Active Directory Federation Services) dell'organizzazione target. Da lì, l'attaccante può accedere e persistere nel cloud.[12]

WithSecure™ ha replicato questa strategia in esercizi di "Red Teaming", scoprendo che, anche se i difensori rimuovono gli impianti on-premise, il Red Team riesce a mantenere una presenza negli ambienti cloud del cliente fino alla fine di un engagement.

Sygnia ha rilevato come, una volta acquisiti i diritti di amministratore ADFS, NOBELIUM comprometta il certificato SAML (Security Assertion Markup Language) della vittima[13].

Questo attacco "golden SAML" di fatto garantisce un accesso senza controllo ai servizi che fanno affidamento sui token emessi tramite SAML, permettendo la persistenza nei servizi cloud e XaaS.

CISA ha descritto[14] più in dettaglio le tecniche, tattiche e procedure (TTP) di NOBELIUM in un avviso.

In assenza di una correlazione tra i log di autenticazione ADFS e i log delle attività nel cloud, per le vittime è stato impossibile individuare gli utenti che erano riusciti ad accedere agli ambienti cloud senza doversi autenticare sul server ADFS dei sistemi on-premise che avrebbe concesso l'accesso.

12. https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/

13. https://www.sygnia.co/golden-saml-advisory

14. https://www.cisa.gov/uscert/ncas/alerts/aa21-008a

Proteggere la pipeline di build

Qui torniamo al problema del silo che abbiamo menzionato nel punto sugli errori di configurazione. I team di progettazione e sicurezza dell'infrastruttura non sempre comprendono il contesto delle attività registrate nei log e sarà necessaria anche l'esperienza dei team che si occupano del supporto delle pipeline e di altri strumenti di sviluppo. Gli errori di configurazione dovuti a team DevOps decentrati[15] sono stati il motivo principale delle violazioni cloud esaminate dall'Incident Response Team di WithSecure™ negli ultimi due anni.

Alcune cose diventano imperative e sono dettagliate nell'articolo citato nella nota a piè di pagina sopra: in primo luogo, sfruttare i vantaggi di DevOps e DevSecOps per integrare la responsabilità della sicurezza nel ciclo di sviluppo fin dalle prime fasi. Affinché vi sia armonia tra i team di sviluppo e di sicurezza, è necessario che le funzioni di business inizino a pagare per la propria sicurezza. In secondo luogo, è essenziale che ci siano solide linee di comunicazione tra i team di sicurezza e cloud engineering.

Anche qui, il nostro Incident Response Team nota che i CISO procedono operando in modo indipendente dal reparto IT e dalle security operations distribuite nelle singole unità di business. Questa non è una situazione per silos indipendenti e scarsamente connessi, ma per team decentrati e altamente connessi.

L'ultimo aspetto è che il decentramento non deve determinare attitudini al rischio molto diverse nell'organizzazione e questo richiede un nuovo livello intermedio in grado di fare da tramite tra le varie unità.

Punti deboli imprevisti

Gli incarichi di consulenza e risposta agli incidenti portati a termine da WithSecure™ hanno rivelato che, al di là di banali errori di configurazione, è raro che i punti deboli siano gli asset cloud esposti a Internet. Quelli che invece si rivelano spesso problematici sono i servizi, le applicazioni e gli strumenti che le organizzazioni usano per definire i cloud. Questi "gioielli della corona" sono rappresentati spesso da provider di identità, repository di codice sorgente, codice di infrastruttura e strumenti per l'implementazione dei servizi in produzione.

Gli strumenti di integrazione continua/delivery continua (CI/CD) come Jenkins hanno ed esercitano un potere e un privilegio enorme in un ambiente cloud: se un attaccante ottiene l'accesso, la battaglia è già persa.

Affrontare la verità

In questo contesto, è essenziale che si verifichi un cambiamento culturale, che in molte organizzazioni è già in atto e richiede solo piccole correzioni per indirizzarlo verso un profilo di sicurezza nel cloud più solido.

Demandare la responsabilità e la spesa per la sicurezza alle funzioni di business, sotto la responsabilità generale di un CISO indipendente dal team IT, può aiutare le organizzazioni a costruire una presenza nel cloud sicura.

15. https://www.withsecure.com/en/expertise/resources/security-team-of-the-future

Verità nascosta 6

Nessuno sa chi è responsabile dei dati nel cloud

W / T H
secure

Verità nascosta 6

Nessuno sa chi è responsabile dei dati nel cloud

Dmitriy Viktorov
Head of Product and
Technology, Cloud Solutions

La nota espressione "i dati sono il nuovo petrolio" indica che si tratta di un asset di enorme valore per qualsiasi organizzazione. Prima di spostare i dati nel cloud, quindi, bisogna riflettere attentamente per assicurarsi di mantenere un controllo e una visibilità adeguati e gli aspetti da considerare sono molti.

Quando si acquistano servizi cloud, la responsabilità della sicurezza dei dati viene trasferita in parte al cloud provider e questa è una prospettiva allettante. Bisogna però ricordare che la responsabilità in merito ai controlli basilari per la sicurezza dei dati resta sempre in capo al proprietario. Si tratta del cosiddetto Modello di Responsabilità Condivisa.

È di nuovo un problema di visibilità, in questo caso di visibilità sui dati. Devi sapere quali tipi di dati hai, come sono classificati, da dove provengono, chi può accedervi o dove sono diretti.

Se i dati provengono da fonti esterne e non attendibili (come l'email), devi bloccare i contenuti dannosi e non consentiti prima che raggiungano gli utenti interni o esterni.

In caso di requisiti di conformità, devi anche monitorare l'accesso ai dati sensibili e disporre di un audit trail, se è previsto da un requisito di conformità, e poi sapere chi può accedervi.

Uno dei rischi su cui devi riflettere è costituito dagli insider malintenzionati e dall'accesso non autorizzato ai dati. I servizi cloud SaaS possono diventare molto complessi, aprendo la strada a errori di configurazione o controlli di accesso inadeguati, come descritto nella Verità nascosta 2. Gli errori di configurazione, a loro volta, possono portare a violazioni dei dati.

Un altro rischio è il fatto che ai dati possano accedere altre applicazioni e altri servizi connessi al cloud SaaS tramite API. Se sono configurate in modo errato o concedono autorizzazioni eccessive rispetto a quanto necessario, anche queste potrebbero essere l'origine di una violazione. Anche se sono configurate correttamente, è importante ricordare che le API stesse potrebbero essere compromesse, come dimostrato da recenti attacchi alla supply chain.

Affrontare la verità

Man mano che aumenta il loro utilizzo, i servizi cloud SaaS come Salesforce, Microsoft 365, Google Workspace e così via diventano bersagli allettanti per gli attaccanti. Riteniamo che l'obiettivo finale degli attacchi futuri non sarà sempre la sottrazione di dati preziosi archiviati nel cloud. Gli attaccanti cercheranno di sfruttare i servizi cloud come "trampolini" per entrare nelle reti delle organizzazioni e attaccare altri sistemi interni ed esterni. Abbiamo già assistito ad alcuni attacchi di phishing e ransomware condotti attraverso i servizi cloud. Al variare del panorama delle minacce, WithSecure™ continuerà a migliorare le sue soluzioni e ad ampliare le capacità di rilevamento e risposta sui dispositivi endpoint e sulle piattaforme cloud IaaS, PaaS e SaaS.

Una delle soluzioni esistenti di WithSecure™, Cloud Protection for Salesforce[16], fornisce protezione in tempo reale da virus, trojan e ransomware e l'analisi di tutti i contenuti condivisi tramite il cloud Salesforce. L'esclusiva soluzione di WithSecure™ integra i controlli di sicurezza della piattaforma cloud di Salesforce e colma una lacuna nelle responsabilità di sicurezza condivise per quanto riguarda i dati dei clienti archiviati nel cloud. Grazie a questa soluzione, i clienti che utilizzano Sales Cloud, Service Cloud o Experience Cloud di Salesforce sono in grado di prevenire o fermare gli attacchi condotti tramite file malevoli o URL di phishing[17]. La soluzione offre inoltre visibilità completa e analisi dei contenuti a cui accedono gli utenti interni o esterni.

WithSecure™ Cloud Protection for Salesforce sfrutta una piattaforma di analisi delle minacce e reputazione dei contenuti basata sul cloud che prende il nome di WithSecure™ Security Cloud. Essenzialmente, Security Cloud si basa su più livelli di tecnologie all'avanguardia e su un repository in costante evoluzione di dati di cyber intelligence e sulle minacce raccolti in tempo reale da decine di milioni di sensori di sicurezza in tutto il mondo. Rappresenta il fulcro dei nostri pluripremiati prodotti per la protezione degli endpoint e di altre soluzioni di protezione per la collaborazione nel cloud, come WithSecure™ Elements Collaboration Protection.

16. https://www.withsecure.com/en/expertise/resources/salesforce-data-security

17. https://withsecure.com/en/expertise/campaigns/disrupting-the-kill-chain-with-withsecure-cloud-protection-for-salesforce

Verità nascosta 7

Le piattaforme di collaborazione diventeranno sempre più importanti

W / T H
secure

Verità nascosta 7

Le piattaforme di collaborazione diventeranno sempre più importanti

Juha Högmander
Director, Technical Offering

Pochi di noi ormai lavorano dalle sedi aziendali ed è molto probabile che la situazione rimanga tale anche in futuro. Per molte persone il lavoro da remoto è stato la "nuova normalità" per due anni e ci sono buone probabilità che per alcuni diventi una soluzione definitiva.

In queste condizioni, la collaborazione è diventata imprescindibile e ovviamente questo significa che la protezione è altrettanto importante. Occorrono metodi digitali per condividere materiali, tenere workshop e riunioni dal vivo e fare presentazioni. In altre parole, serve un modo per comunicare e collaborare. Negli esercizi di "Red Teaming" di WithSecure™ è emerso quanto le piattaforme di collaborazione e comunicazione in tempo reale fossero una miniera d'oro nei tentativi di infiltrazione nell'ambiente del cliente.

Una parte cruciale di questo discorso è che l'email è ancora il vettore di attacco principale. Circa la metà (il 51%[18]) delle piccole e medie imprese ha subito un attacco negli ultimi due anni e questo indica un cambio di mentalità dei cyber criminali. Molti di loro ora cercano una preda facile, indipendentemente dalle dimensioni dell'azienda o dal settore in cui opera, perché gli attacchi via email di massa automatizzati sono economici e assicurano un ottimo ritorno sull'investimento ai criminali.

Formare il personale in modo che abbia maggiore consapevolezza in merito agli attacchi di phishing e sappia a cosa deve prestare attenzione e su quali email sospette non deve cliccare è parte della soluzione, ma sappiamo bene che non è un sistema infallibile. Il phishing ha sfruttato la quarantena per aumentare di frequenza: oggi è presente nel 36% delle violazioni, contro il 25% del 2020[19]. I link nei messaggi email sono il principale vettore di malware nelle violazioni e circa il 46%[20] del malware viene consegnato tramite email.

18. Ponemon. IBM. 2020. Cost of a Data Breach Report. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

19. Verizon. 2021. Data Breach Investigations Report 2021. https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf

20. Verizon. 2020. Data Breach Investigations Report 2020 https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf

Non è pensabile impedire alle persone di accedere ai dati, anche se sarebbe il modo più semplice per garantire la sicurezza. Ciò che invece dobbiamo fare è impedire agli utenti di eseguire azioni non autorizzate, come condividere informazioni riservate in luoghi dove non è consentito, nonché disporre della visibilità necessaria per tenere traccia delle attività insolite.

Affrontare la verità

Microsoft 365 include molte di queste funzionalità ed è sicuramente la piattaforma più diffusa. Per questo motivo WithSecure™ ha dato priorità allo sviluppo della sua soluzione WithSecure™ Elements Collaboration Protection[21], ma sono previsti ulteriori sviluppi e WithSecure™ Cloud Protection for Salesforce offre già protezione della collaborazione agli utenti in quell'ambiente.

Abbiamo lavorato per migliorare la nostra soluzione di protezione email per proteggere Sharepoint e Teams, in modo da coprire la piattaforma completa. Abbiamo anche incorporato il rilevamento degli account compromessi, una funzione importante per proteggere l'intero servizio.

Pensando al mondo e alla sua attuale situazione, le nostre soluzioni di sicurezza non intendono opporsi in alcun modo alla tendenza verso l'apertura. La trasformazione nelle società tecnologiche, che si è allargata all'economia in generale, tende a consentire alle persone di prendere decisioni individualmente.

21. https://www.youtube.com/watch?v=rvzXvtXoyF8&t=1s

Conclusione

Gli strumenti e le procedure più recenti arrivano solo fino a un certo punto, per i cloud provider, per i fornitori di soluzioni di sicurezza e per i clienti. Il cambiamento culturale è nettamente più efficace e un approccio corretto alla sicurezza basato sul risultato può incrementare di mille volte la potenza di strumenti e tecniche di buon livello.

Investire nella creazione di un approccio forte e distribuito alla protezione del cloud, così come si protegge l'organizzazione stessa, ridurrà il costo nascosto che il cloud potrebbe rappresentare.

Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

WITH secure