Whitepaper

Proteggere il cloud e gli endpoint

WITH secure | blade informatica

Introduzione

Il cloud ha portato molti vantaggi evolutivi alle organizzazioni. La flessibilità di distribuire rapidamente i servizi, senza bisogno di investimenti di capitale in infrastrutture o di lunghe implementazioni, ha incrementato l'agilità e ha dato alle organizzazioni meno dotate di risorse la possibilità di affrontare concorrenti più grandi e con maggiori disponibilità finanziarie.

Eppure il cloud ha anche un lato oscuro. Man mano che le organizzazioni hanno aperto sistemi e processi al mondo della rete, sono diventate molto più vulnerabili ai malintenzionati. La complessità dei sistemi della maggior parte delle organizzazioni e i potenziali punti di accesso sono cresciuti in modo esponenziale, così come la diffusione degli attacchi. Inoltre, solo un'esigua minoranza dispone delle risorse necessarie per proteggersi efficacemente dalle minacce che sono ormai parte integrante dell'utilizzo del cloud.

Chiedere l'aiuto necessario per ottenere i giusti risultati

Nonostante la complessità di un'efficace sicurezza del cloud, la soluzione non è quella di abbandonare l'uso di questa tecnologia. Le aziende devono invece pensare in modo diverso a come ridurre al minimo i rischi. Il costo reale della proprietà del cloud deve includere il costo per affrontare le sfide di sicurezza che presenta, un fatto che può essere difficile da determinare finché non si verifica una violazione. Le organizzazioni devono concentrarsi sui risultati e, in molti casi, il modo più conveniente per ridurre i rischi di sicurezza del cloud a un livello accettabile è quello di collaborare con fornitori specializzati che abbiano l'esperienza, le competenze e le risorse per comprendere le priorità di sicurezza specifiche e garantire la presenza di difese adeguate.

WithSecure™ collabora con una serie di partner specializzati per aiutare a colmare le lacune nella sicurezza del cloud delle organizzazioni. I nostri partner esperti forniscono, distribuiscono, configurano e, nel caso dei nostri Managed Security Service Provider, gestiscono completamente la sicurezza del cloud dei clienti, con l'aiuto delle nostre tecnologie modulari di sicurezza del cloud.

Non puoi proteggere ciò che non vedi

Il primo grande problema da affrontare se si vogliono ridurre al minimo i livelli di rischio per la sicurezza del cloud è la mancanza di visibilità. Il cloud ha reso semplice per chiunque accedere a risorse di calcolo, storage e applicazioni come e quando ne ha bisogno, ma questa flessibilità ha reso più difficile per le organizzazioni tracciare con precisione quali risorse cloud vengono utilizzate, come e dove.

I reparti IT hanno da tempo affrontato la sfida del "bring your own device" (BYOD), ma questa sta rapidamente venendo eclissata dal "bring your own cloud" (BYOC). Anche prima di considerare le applicazioni SaaS, può essere molto difficile capire quali risorse cloud sono distribuite in un'organizzazione. I team possono avviare istanze cloud contenenti dati e sistemi sensibili con una semplice carta di credito. Alcune di queste istanze, anche se non tutte, possono essere difficili da vedere e da tracciare e ciò può causare complicazioni di ogni tipo in termini di dipendenza tra BYOC noti, cloud approvati dall'azienda e BYOC invisibili e non autorizzati.

La sfida della visibilità è particolarmente significativa negli ambienti di sviluppo, dove le istanze cloud vengono facilmente avviate, i dati di produzione distribuiti e i collegamenti ai sistemi interni creati, il tutto con una supervisione, una documentazione o pratiche di sicurezza minime.

Oltre alla sfida della scarsa visibilità, l'adozione massiccia e non strutturata del cloud significa anche che i singoli cloud di proprietà di team, reparti o persino di singoli dipendenti spesso non hanno una configurazione coerente.

Il passaggio della gestione della sicurezza al cloud può contribuire notevolmente1 a migliorare la visibilità, ma potrebbero essere necessari altri strumenti. Ad esempio, un cloud access security broker (CASB) è un mezzo per monitorare chi accede a quali servizi cloud e dove. Gartner definisce i CASB come "punti di applicazione dei criteri di sicurezza on-premise o basati sul cloud, collocati tra i consumatori di servizi cloud e i fornitori di servizi cloud per combinare e interporre i criteri di sicurezza aziendali durante l'accesso alle risorse basate sul cloud".

Tuttavia, i CASB possono essere complessi da configurare e gestire, in quanto coprono una moltitudine di criteri tra cui l'autenticazione, il single sign-on, l'autorizzazione, la mappatura delle credenziali, la profilazione dei dispositivi, la crittografia, la tokenizzazione, la registrazione, gli avvisi, il rilevamento/la prevenzione del malware e altro ancora. I CASB richiedono inoltre l'accesso agli endpoint per installare gli agenti. Di conseguenza, molte organizzazioni che non hanno le competenze interne per implementare i CASB preferiscono lavorare con specialisti di terze parti.

1. https://www.withsecure.com/en/expertise/resources/the-benefits-of-moving-security-management-to-the-cloud

Garantire una protezione completa per gli endpoint

La compromissione di una workstation, di un dispositivo mobile o di un server è il primo passo più comune in qualsiasi attacco serio, quindi è essenziale difendersi dalle minacce provenienti dagli endpoint. Il crescente utilizzo del cloud ha ampliato in modo massiccio la superficie di attacco, soprattutto in considerazione del fatto che molte organizzazioni devono consentire a dipendenti, partner, clienti e altri di accedere ai sistemi cloud tramite endpoint che l'organizzazione non possiede o controlla fisicamente.

Esistono diversi strumenti e tecnologie per mitigare i rischi posti dagli endpoint gestiti e non gestiti. La combinazione di difese più appropriata per la tua organizzazione dipende dalle circostanze specifiche, dalle priorità, dai livelli di tolleranza al rischio e dai risultati di sicurezza desiderati. Anche in questo caso, un fornitore specializzato sarà in grado di valutare efficacemente le tue esigenze, spiegare le opzioni e fornire raccomandazioni adeguate.

Per bloccare automaticamente la maggior parte delle minacce, è necessario implementare una piattaforma di protezione degli endpoint (EPP). L'EPP è una sorta di soluzione antivirus avanzata che blocca sia le minacce conosciute sia tutto ciò che mostra segni di comportamento sospetto, bloccando persino i ransomware prima che causino danni.

Tuttavia, gli EPP non catturano tutto, quindi per una protezione degli endpoint più efficace è necessario prendere in considerazione anche una forma di rilevamento e risposta degli endpoint (EDR) o di Managed Detection and Response (MDR), in grado di individuare e avvisare rapidamente gli amministratori di qualsiasi comportamento sospetto o indicazione di Advanced Persistent Threats (APT) sugli endpoint.

L'EDR si sta inoltre trasformando sempre più in Extended Detection and Response (XDR), soluzioni completamente basate sul cloud e aggiornate con le ultime informazioni sulle caratteristiche delle minacce, ad esempio tramite l'integrazione con il quadro delle minacce MITRE, costantemente aggiornato.

In effetti, l'intero settore della protezione degli endpoint è in rapida evoluzione, quindi ha senso collaborare con fornitori specializzati in grado di garantire una protezione a prova di futuro. Ad esempio, è probabile che le soluzioni future prevedano una migliore integrazione con i registri del pannello di controllo del cloud e funzionalità avanzate per rilevare il furto di credenziali da un endpoint.

Rimanere al sicuro senza soffocare la collaborazione nel cloud

L'uso di piattaforme di collaborazione nel cloud, come Microsoft 365, ha registrato un enorme cambiamento durante la pandemia di Covid e in futuro tali piattaforme diventeranno sempre più importanti. Dopo due anni in cui il lavoro da remoto è diventato "business as usual", molte organizzazioni accettano ora i notevoli vantaggi in termini di costi, produttività e soddisfazione del personale che si possono ottenere consentendo a un maggior numero di dipendenti di lavorare da remoto, in parte o per tutto il tempo.

Tuttavia, come possono testimoniare i "red teamer" di WithSecure™ (esperti di sicurezza che tentano di infiltrarsi nei sistemi per conto di un'organizzazione al fine di svelare eventuali punti deboli), le piattaforme di collaborazione e di comunicazione in tempo reale sono spesso gli obiettivi più fruttuosi quando si tratta di aggirare le difese di un'organizzazione.

Ad esempio, la posta elettronica è ancora il principale vettore di attacco. Oltre la metà (51%2) delle piccole e medie imprese ha subito un attacco negli ultimi due anni. Ciò è dovuto al fatto che molti aggressori cercano ora una preda facile, indipendentemente dalle dimensioni o dal settore dell'azienda. Gli attacchi via email automatizzati di massa sono poco costosi da realizzare e hanno un elevato ritorno sull'investimento per i criminali.

Formare il personale a una maggiore consapevolezza degli attacchi di phishing, in modo che sappia cosa cercare e sia meno propenso a cliccare su email sospette, è una parte della soluzione, ma sappiamo tutti che non è infallibile. L'uso crescente di piattaforme di collaborazione durante la pandemia ha portato a una crescita simultanea degli attacchi che utilizzano con successo il phishing per infiltrarsi nei sistemi. Questa tecnica è stata utilizzata nel 36% di tutte le violazioni, in aumento rispetto al 25% del 2019. Inoltre, circa il 46% delle minacce informatiche viene consegnato via email e gli stessi link email sospetti e file malevoli vengono frequentemente condivisi attraverso le piattaforme di collaborazione.

Tuttavia, la risposta non è rendere più difficile l'accesso ai dati tramite le piattaforme di collaborazione, anche se questo potrebbe essere il modo più semplice per garantire la sicurezza. Al contrario, si deve trovare un equilibrio che consenta di essere protetti dagli attacchi senza soffocare i notevoli vantaggi che la collaborazione a distanza comporta. Ciò significa assicurarsi di avere la capacità di impedire che le persone compiano azioni non autorizzate, come la condivisione di dati riservati in luoghi in cui non dovrebbero, e la visibilità per rintracciare attività insolite prima che si verifichino danni gravi.

Essendo la piattaforma più estesa e più utilizzata, la protezione di Microsoft365 è quella su cui abbiamo inizialmente concentrato lo sviluppo di queste capacità con la nostra WithSecure™ Elements Collaboration Protection. Stiamo inoltre potenziando la nostra soluzione di protezione delle email per proteggere Sharepoint, OneDrive e Teams, in modo da offrire una protezione completa della piattaforma, oltre a incorporare funzionalità per rilevare se un account utente è stato compromesso.

2. https://www.ibm.com/security/digital-assets/ cost-data-breach-report/#/

Conclusioni

WithSecure™ ritiene che una maggiore collaborazione e apertura sia una buona cosa, così come la possibilità di prendere decisioni individuali. I tempi in cui si bloccavano i sistemi a scapito dell'agilità dei dipendenti e dell'organizzazione sono finiti. Oggi dovresti parlare con il tuo fornitore di cyber security per capire come aiutarti a sviluppare un approccio alla sicurezza basato sui risultati e su un approccio positivo e decentralizzato alla protezione del cloud.

I nostri partner conoscono a fondo i vari strumenti e le tecnologie che offriamo e sono nella posizione migliore per consigliarti le soluzioni più adatte alla tua organizzazione. Inoltre, poiché le nostre soluzioni sono completamente modulari e basate sul cloud, possono personalizzare le tue soluzioni di sicurezza per soddisfare le esigenze specifiche dell'azienda.

3. https://withsecure.com/en/expertise/resources/the-future-of-corporate-cyber-security-is-all-in-one

Chi siamo

WithSecure™ è il partner di riferimento per la cyber security. Provider di servizi IT, MSSP e aziende, insieme alle più importanti istituzioni finanziarie, imprese manifatturiere e migliaia di fornitori dei più avanzati sistemi di comunicazione e tecnologie nel mondo si affidano a noi per conseguire una sicurezza informatica basata sui risultati, che protegge e consente le loro operazioni. La nostra protezione guidata dall'IA protegge gli endpoint e la collaborazione nel cloud e il nostro sistema di intelligent detection and response è alimentato da esperti che identificano i rischi aziendali tramite threat hunting proattivo e affrontando gli attacchi in tempo reale. I nostri consulenti collaborano con imprese e tech challenger per costruire la resilienza attraverso una consulenza sulla sicurezza basata su prove concrete. Con oltre 30 anni di esperienza nella costruzione di tecnologie che soddisfano gli obiettivi aziendali, abbiamo costruito il nostro portfolio per crescere insieme ai nostri partner attraverso modelli commerciali flessibili.

WithSecure™ fa parte di F-Secure Corporation, fondata nel 1988, ed è quotata sul listino NASDAQ OMX Helsinki Ltd.

WITH secure