Microsoft

6 passaggi per creare una strategia di sicurezza olistica

Queste informazioni sono destinate a te

se sei un Chief Information Security Officer o un responsabile della sicurezza IT che:

- Ha bisogno di una guida rapida e pratica a una strategia di sicurezza complessiva.
- Desidera rimanere al corrente sulle procedure più recenti relative alla sicurezza.

Tempo di lettura stimato: <9 minuti

Sommario

Affrontare la sfida

La protezione di dati e sistemi è una priorità assoluta per le aziende. Riuscire in questo intento diventa però ogni giorno più difficile per vari motivi: gli attacchi diventano sempre più sofisticati, i dipendenti usano una serie più ampia di dispositivi e applicazioni e i flussi di dati entrano ed escono dall'azienda in molti più modi. Con il passaggio in massa al lavoro da remoto, la sicurezza diventa ancora più fragile.

I leader devono trovare un equilibrio tra queste sfide e l'esigenza di collaborare, innovare ed espandere il business. È necessario un approccio alla sicurezza completo, che garantisca la protezione costante di tutti gli endpoint, rilevi tempestivamente le violazioni e risponda prima del verificarsi dei danni. Indipendentemente dalla validità delle difese in atto, le misure preventive non sono più sufficienti. È anche necessario adottare un approccio basato sulla "supposizione di una violazione" che includa misure di rilevamento e risposta.

I CISO (Chief Information Security Officer) di oggi necessitano di framework di sicurezza agili che consentano la trasformazione digitale e siano supportati da strategie olistiche integrate in tecnologie, processi e programmi di formazione. Anche se tutto ciò è disponibile per le soluzioni locali, la verità è che il passaggio al cloud migliora immediatamente le funzionalità di sicurezza in tutta l'azienda.

> **Questo e-Book illustra le sei procedure consigliate di CISO che hanno fatto della sicurezza la pietra angolare del successo aziendale. Le procedure si riferiscono a uno scenario locale, ma sono estremamente più facili da attuare in uno scenario cloud.**

1. Utilizzare prodotti per la sicurezza integrati per consentire una risposta rapida

75

Numero di prodotti per la sicurezza usati in media dalle aziende di grandi dimensioni.[1]

Le minacce non sono più attacchi simili a effrazioni, volti a compromettere i sistemi con l'obiettivo di conquistare una presenza persistente e a lungo termine. Gli hacker usano oggi un'ampia gamma di vettori, con tecniche e strumenti sempre più avanzati: furto di credenziali, installazione di malware che si autocancella per non essere rilevato, modifica di processi interni e reindirizzamento dei dati di rete, truffe di ingegneria sociale e persino attacchi contro i dispositivi domestici e mobili dei dipendenti.

Le aziende stanno adottando un numero sempre maggiore di strumenti di sicurezza per far fronte a tali minacce. Queste soluzioni, però, sono finalizzate a rispondere a problemi specifici e raramente interagiscono. Molte usano dashboard, console e log proprietari. Le difficoltà di integrazione rendono difficile avere una visione globale e assegnare rapidamente una priorità alle minacce. La sfida diventa ancora più grande quando si tratta di gestire risorse sia cloud sia locali. Di conseguenza, gli attacchi possono passare inosservati per oltre 140 giorni.[2]

[1] "Symantec introduce la nuova era della protezione avanzata dalle minacce", Businesswire, ottobre 2015.

[2] "Panorama delle minacce: i numeri", Mandiant, una società FireEye, 2016.

Prova questo

La capacità di rilevamento e risposta in tempi rapidi è sempre più importante. Sono quindi emerse queste procedure consigliate:

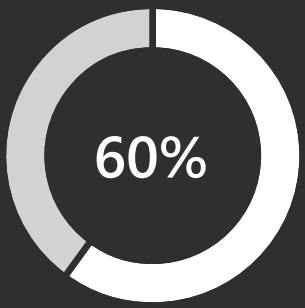
- Ottieni una visione olistica della sicurezza per l'intera rete, inclusi gli ambienti cloud e ibridi.
- Crea un ecosistema di prodotti e piattaforme per la sicurezza che si integrino tra loro e forniscano informazioni dettagliate.
- Collabora con fornitori di soluzioni tecnologiche che cooperano e condividono informazioni nel settore della sicurezza.

Principali spunti di riflessione

Per i team addetti alla sicurezza, la mancanza di integrazione tra i prodotti per la sicurezza costituisce un ostacolo alla loro capacità di individuare e contrastare le minacce in modo rapido e olistico.

Cerca prodotti progettati per integrarsi con altri.

2. Gestire l'accesso tramite l'identità, non gli endpoint



delle violazioni ha origine da un endpoint compromesso.[3]

Una violazione dei dati può comportare costi enormi. Stabilire controlli di sicurezza sufficienti per ottenere visibilità su minacce e attacchi è un modo per contrastare i costi elevati. Tuttavia, i team addetti alla sicurezza devono anche supportare la consumerizzazione dell'IT, ovvero il fenomeno in base al quale i dipendenti non lavorano più esclusivamente su dispositivi aziendali attentamente controllati, ma si aspettano di poter lavorare ovunque, su qualsiasi dispositivo o piattaforma, indipendentemente dal fatto che sia stato approvato dal reparto IT aziendale.

In una realtà di questo tipo, le strategie di sicurezza basate sull'identità collegano l'accesso non ai dispositivi, ma all'identità. I controlli si applicano in base al ruolo e alle esigenze, indipendentemente da come l'utente si connette. Concentrandosi sull'autenticazione e sulla gestione degli utenti al momento dell'accesso alle risorse aziendali, le aziende possono proteggere i propri dati indipendentemente da dove sono archiviati, dalla modalità di accesso o dagli utenti con cui vengono condivisi.

[3] "Le cinque principali minacce alla sicurezza per la tua azienda e come rispondere", Blog di Microsoft Secure, ottobre 2016.

Prova questo

L'abbandono di una strategia di sicurezza incentrata esclusivamente sugli endpoint assicura un approccio più solido. Questi strumenti possono essere utili:

- Soluzioni di **gestione delle identità e degli accessi** e soluzioni di **gestione delle applicazioni mobili con prevenzione della perdita dei dati**. Entrambe aiutano a ridurre il rischio proteggendo l'accesso alle applicazioni e ai dati nelle risorse aziendali e nel cloud. La gestione delle identità e degli accessi può eliminare la necessità di credenziali multiple, fornendo ai dipendenti una singola identità per l'accesso alle risorse cloud e locali. I sistemi di gestione delle identità e degli accessi basati sul cloud possono inoltre usare l'analisi e l'intelligence sulle minacce dei provider di tecnologia per rilevare meglio i tentativi di accesso anomali e rispondere automaticamente in modo appropriato.
- L'**autenticazione a più fattori** offre un ulteriore livello di protezione, richiedendo agli utenti di fornire un'informazione a loro nota (la password) e una in loro possesso (autenticazione secondaria tramite un dispositivo, l'impronta digitale o il riconoscimento facciale). Tra le altre tattiche efficaci vi è l'accesso basato su criteri di rischio utente, dispositivo, applicazione e persino posizione. Queste funzionalità permettono di autorizzare o bloccare automaticamente un utente in tempo reale oppure richiedere l'autenticazione a più fattori, a seconda dei criteri impostati, permettendo così alle aziende di aumentare la protezione all'ingresso.

Principali spunti di riflessione

Una strategia di sicurezza basata sull'identità sposta l'attenzione dal monitoraggio degli endpoint (dispositivi) alla gestione degli utenti che accedono ai dati aziendali.

Una protezione degli endpoint più solida fornisce informazioni post-violazione sulle tecniche dell'avversario.

3. Adottare un modello Zero Trust per eliminare le minacce

17.000
avvisi di malware

In media, le aziende di grandi dimensioni devono esaminare questo volume di avvisi ogni settimana.[4]

Gli hacker sanno che in ogni azienda esistono più punti di ingresso. Usano tentativi di phishing, attacchi con malware e spyware, exploit tramite browser e software, accesso mediante dispositivi smarriti e rubati, tecniche di ingegneria sociale e altre tattiche per violare la sicurezza. È necessario prestare un'attenzione costante per mantenere la visibilità sulle minacce già note e individuare le vulnerabilità emergenti.

Alcuni strumenti possono aiutare a mantenere la sicurezza sempre attiva, ma è preferibile adottare un approccio più ampio. Gli strumenti tradizionali mirano alla prevenzione, ma questo non è più sufficiente. Le aziende devono presupporre che una violazione sia già avvenuta o che avverrà a breve, secondo un modello noto come Zero Trust. Devono quindi trovare metodi efficaci per ridurre significativamente il tempo necessario per rilevarla e risolverla.

[4] "Il costo del contenimento del malware", Ponemon Institute, gennaio 2015.

Prova questo

Approfondisci le tue competenze in sicurezza avanzata. Anticipare le minacce può significare guardare indietro e imparare da incidenti passati e dalle attività e dai passi intrapresi dagli hacker.

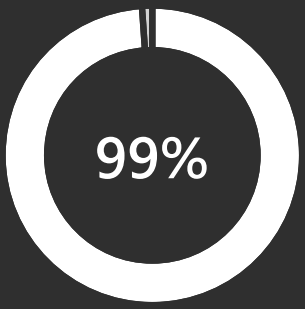
- Molte applicazioni di sicurezza utilizzano funzionalità integrate di analisi e apprendimento automatico per analizzare il modo in cui un hacker ha ottenuto l'accesso. Le soluzioni di analisi e sicurezza più avanzate usano queste informazioni intervenendo automaticamente per prevenire e risolvere violazioni simili, contribuendo così a ridurre significativamente i tempi di mitigazione.
- Queste soluzioni si basano su intelligence e segnali estremamente vasti e, se combinate con l'esperienza e le conoscenze di professionisti, possono diventare strumenti molto potenti contro minacce messe in atto sempre più velocemente.

Principali spunti di riflessione

Le applicazioni native per il cloud supportano un modello Zero Trust più facilmente delle applicazioni legacy.

Per poter supportare l'accesso condizionale basato sull'identità, le applicazioni legacy devono essere modernizzate.

4. Passare al cloud in tutta sicurezza



dei problemi di sicurezza cloud sarà da imputare al cliente fino al 2025.[5]

Ogni azienda si trova in una fase diversa del percorso verso il cloud. Requisiti di adeguamento, normative locali e altre sfide legate alla migrazione fanno sì che non tutte le aziende siano pronte a trasferire i workload critici nel cloud. Le strategie di cloud ibrido sono un modo in cui le aziende possono fare ingresso nel cloud, mantenendo alcuni workload in locale e trasferendone altri.

I modelli di servizi cloud influiscono sul modo in cui service provider e clienti condividono le responsabilità. Insorgono così problematiche per i CISO, i quali devono risolvere le criticità legate alla cessione di alcuni dei controlli delle soluzioni locali a favore della maggiore sicurezza che i fornitori di servizi cloud possono offrire.

Come regola generale, la sicurezza cloud è una responsabilità condivisa. I provider di soluzioni cloud devono offrire sicurezza e crittografia all'avanguardia, ma i clienti devono assicurarsi che i servizi acquistati siano effettivamente sicuri ed estendere i criteri di sicurezza necessari alle nuove risorse cloud.

[5] "Il cloud è sicuro?", Gartner, ottobre 2019.

Prova questo

Poni le domande giuste. Scegliere un provider di soluzioni cloud non significa semplicemente scegliere un servizio, ma anche decidere a chi affidare i propri dati. Ecco alcune domande fondamentali sulla sicurezza e sul controllo degli accessi che dovresti porre:

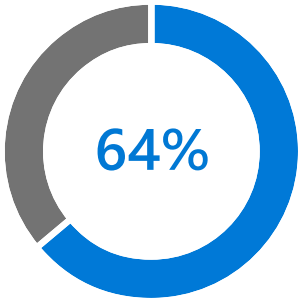
- I nostri dati sono protetti da sicurezza avanzata e tecnologia all'avanguardia?
- La privacy è incorporata in modo predefinito e consente il controllo dei dati nel cloud aziendale?
- Che tipo di investimenti avete effettuato in processi di adeguamento solidi e innovativi per aiutare la nostra azienda a soddisfare le esigenze di adeguamento?
- Dove verranno archiviati i nostri dati, chi potrà accedervi e perché?
- Vengono condotte revisioni annuali da terze parti per garantire il rispetto degli standard di sicurezza e adeguamento?
- Verranno rifiutate eventuali richieste di divulgazione di dati personali dei clienti non legalmente vincolanti?
- Aderite agli standard di adeguamento e normativi di diversi paesi e sedi? In caso affermativo, di quali standard si tratta?

Principali spunti di riflessione

Nella scelta del service provider di soluzioni cloud, assicurati che aderisca a standard internazionali.

Cerca fornitori che pubblicano informazioni dettagliate su come gestiscono i servizi e i dati.

5. Prestare attenzione allo shadow IT



dei dipendenti ha creato almeno un account (registrandosi a un sito Web o un'app correlata al lavoro) senza coinvolgere il reparto IT.[6]

Quando un dipendente crea un account basato sul cloud senza l'autorizzazione o la consapevolezza della propria azienda, si parla di shadow IT. Gli account sembrano innocui: ad esempio, uno strumento per correggere la grammatica scritta. In realtà questi account creano vulnerabilità anche nelle configurazioni di sicurezza più rigide.

Gli utenti spesso accettano le condizioni senza leggerle e senza comprendere del tutto a cosa concedono l'accesso. Le soluzioni tradizionali per la sicurezza di rete non sono progettate per proteggere i dati presenti nelle app SaaS e non possono offrire all'IT visibilità sull'uso del cloud da parte dei dipendenti.

In definitiva, non si tratta di sopprimere le motivazioni alla base dello shadow IT. Consentire a singoli e team di usare le applicazioni cloud più adatte alle loro esigenze lavorative significa incentivare la produttività e l'innovazione. Ottenere la visibilità, il controllo e la capacità di protezione dalle minacce legate alle app SaaS shadow è il primo passaggio per gestire il rischio e favorire la trasformazione digitale già in atto nell'azienda.

[6] "Una nuova ricerca rivela i rischi dello shadow IT", 1password, febbraio 2020.

Prova questo

Ottieni le informazioni necessarie. Le soluzioni CASB (Cloud Access Security Broker) offrono alle aziende un quadro dettagliato di come i dipendenti usano il cloud:

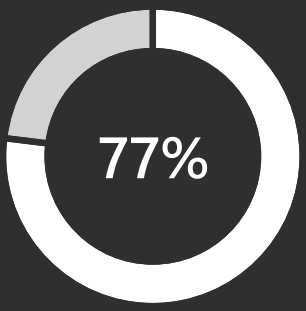
- Quali app cloud usano i dipendenti?
- Quali rischi comportano queste app per l'azienda?
- Come viene eseguito l'accesso a queste applicazioni?
- Quali tipi di dati vengono inviati a queste applicazioni e quindi condivisi?
- Che tipo di traffico di upload/download si verifica?
- Ci sono anomalie nel comportamento degli utenti, come comunicazione impossibile, tentativi di accesso non riusciti o indirizzi IP sospetti?

Principali spunti di riflessione

Le soluzioni CASB possono offrirti un quadro dettagliato di come i dipendenti usano il cloud.

Con una visibilità migliore, puoi impostare criteri con cui monitorare e determinare come i dipendenti usano queste app.

6. Semplificare protezione e produttività



dei CISO si sente posto davanti a due scelte inconciliabili: lasciare lavorare il personale liberamente e mantenere l'azienda protetta.[7]

La condivisione dei dati da parte di dipendenti, partner e clienti porta sempre più spesso a perderne il controllo. La condivisione favorisce la produttività e l'innovazione, ma può avere conseguenze importanti nel caso in cui dati altamente sensibili cadessero nelle mani sbagliate. I responsabili della sicurezza devono gestire e proteggere i dati archiviati in più sedi e condivisi oltre i confini internazionali nel rispetto delle normative.

I dipendenti sono disposti a tollerare i disagi solo fino a quando non trovano il modo di aggirare i requisiti di sicurezza. La classificazione e la crittografia sono i modi migliori per garantire la sicurezza dei dati consentendo nel contempo un uso produttivo e la condivisione delle informazioni. Per evitare errori umani, è possibile automatizzare la classificazione dei dati. Esistono strumenti in grado di capire il contesto dei dati, ad esempio i numeri di carta di credito in un file, o il livello di riservatezza dei dati in base alla loro provenienza. Dopo aver etichettato i dati sensibili, è possibile applicarvi automaticamente contrassegni visivi, come intestazioni, piè di pagina e filigrane, nonché proteggerli con crittografia, autenticazione e diritti di utilizzo.

[7] "La sicurezza IT ostacola la produttività e l'innovazione, secondo un sondaggio", ComputerWeekly.com, ottobre 2017.

Prova questo

Prendi confidenza con i dettagli. I team addetti alla sicurezza devono essere in grado di monitorare l'attività sui file condivisi con un elevato livello di riservatezza o un importante impatto sul business, revocandone l'accesso, quando necessario.

- Questa protezione persistente rimane associata ai dati proteggendoli in ogni momento, indipendentemente da dove vengono archiviati o con chi vengono condivisi.
- Un sistema di gestione degli accessi e delle identità alleggerisce l'onere del monitoraggio dei file altamente riservati.

Principali spunti di riflessione

La sicurezza a livello di dati è una responsabilità di tutti.

Bisogna classificare ed etichettare i dati al momento della creazione e i team addetti alla sicurezza devono poter monitorare le attività sui file e intervenire rapidamente.

Microsoft

Conclusioni

Considerando le molte sfaccettature delle minacce informatiche, non è più sufficiente risolvere solo alcune delle sfide della sicurezza. Ogni azienda ha esigenze di sicurezza uniche, ma tutte si trovano ad affrontare le stesse sfide e a condividere le stesse responsabilità di protezione di dati, persone e sistemi, favorendo l'innovazione e la crescita. Sono necessari framework di sicurezza flessibili che promuovano e sostengano la trasformazione digitale, supportati da strategie di sicurezza olistiche integrate in tecnologie, processi e programmi di formazione.

Se non hai preso in considerazione il passaggio al cloud, è il momento giusto per esplorare le maggiori funzionalità di sicurezza che offre. Microsoft 365 offre una soluzione completa e intelligente, adatta ad aziende di ogni dimensione, che supporta la trasformazione digitale con funzionalità di sicurezza e adeguamento integrate a ogni livello.

Scopri di più in questa serie di webinar completa e gratuita.

Guarda la serie >