WHITE PAPER

11 controlli di sicurezza per ridurre il rischio informatico

Strategie pratiche per potenziare le tue difese, migliorare la tua resilienza informatica e ridurre i rischi della tua organizzazione.

SOPHOS

Riepilogo

In tutte le organizzazioni è importante che la leadership capisca che ottimizzare i controlli di sicurezza non significa solo proteggere dati e sistemi, ma anche e soprattutto limitare i rischi che minacciano la reputazione del brand, la fiducia dei clienti e la continuità aziendale. Gli attacchi informatici come ransomware e Business Email Compromise (BEC) possono avere gravissime conseguenze operative e finanziarie. Secondo Cyber Defense Magazine, si prevede che il costo del cybercrimine a livello mondiale nel 2025 sarà pari a 1,2 trilioni di USD[1]. Anche quando vengono mitigati, gli attacchi possono causare gravi disagi, se i sistemi devono essere disattivati, reimpostati e ricostruiti. Alcune organizzazioni sono in grado di superare problemi di questa entità. Altre invece si troverebbero ad affrontare questioni esistenziali che non avrebbero mai immaginato.

1,2 trilioni di USD

Si prevede che il costo del cybercrimine a livello mondiale nel 2025 sarà pari a 1,2 trilioni di USD[1].

Il ruolo dei controlli di sicurezza nell'ottimizzazione delle difese informatiche

I controlli di sicurezza sono i meccanismi di regolazione che i team di sicurezza possono modificare per ridurre il rischio e proteggere l'organizzazione dalle minacce. Esistono vari tipi di controllo, ma hanno tutti lo stesso obiettivo: prevenire incidenti e violazioni o, se dovessero verificarsi, limitarne i danni. Alcuni sono maggiormente orientati alla prevenzione, mentre altri offrono livelli diversi di mitigazione negli ambiti di prevenzione, rilevamento e risposta alle minacce. Applicare la giusta combinazione di controlli di sicurezza efficaci in tutti gli ambiti dei sistemi è una parte fondamentale di una difesa che agisce in profondità.

Inoltre, l'applicazione di controlli di sicurezza efficaci è anche un elemento critico per la gestione del rischio attraverso le cyberassicurazioni. Quando definiscono premi assicurativi e limiti di copertura, le compagnie di assicurazioni tengono conto dei controlli implementati dall'azienda.

Di solito, la copertura include:

Responsabilità in prima persona, tra cui i danni diretti che la tua organizzazione subirebbe in caso di cyberattacco o violazione, come i costi causati dall'interruzione delle attività, dal recupero dei dati, da eventuali furti o le somme di riscatto per il ransomware.

Responsabilità verso terzi, che derivano da clienti, partner, enti normativi o altri soggetti, e che possono includere cause legali, richieste di risarcimento o sanzioni normative imposte da enti governativi e/o associazioni di categoria.

Perché tutto questo è importante

Implementare controlli efficaci non serve solo a proteggere le tue attività operative, ma può anche diminuire i premi assicurativi e migliorare gli esiti delle richieste di indennizzo.

Riduci il rischio informatico con questi 11 controlli di sicurezza

Investire in controlli di sicurezza efficaci aiuta a ridurre il rischio informatico e potenzialmente a migliorare la posizione assicurativa e le condizioni della polizza. Qui trovi undici controlli essenziali per potenziare le tue difese in diverse categorie di prevenzione e riduzione dell'impatto degli attacchi.

Se implementati correttamente, questi controlli di sicurezza possono migliorare il tuo profilo di cybersecurity e fare in modo che i tuoi sistemi siano pronti ad affrontare tanto le minacce attuali che quelle future.

1. Identità e gestione degli accessi
2. Protezione degli endpoint
3. Autenticazione multi fattore (Multi-Factor Authentication, MFA)
4. Vulnerability Management
5. Protezione delle e-mail
6. Gestione delle sessioni in base ai privilegi
7. Gestione delle risorse
8. Segmentazione e architettura
9. Extended detection and response (XDR)
10. Backup e continuità aziendale
11. Protezione della rete e controllo del traffico

1. Gestione delle identità e degli accessi

La Gestione delle identità e degli accessi (Identity and Access Management, IAM) fa in modo che solo le persone autorizzate possano accedere ai sistemi e ai dati. La Gestione degli accessi privilegiati (Privileged Access Management, PAM) impone ulteriori limiti di accesso alle risorse, concedendolo solo agli utenti che ne hanno assolutamente bisogno. Tutto ciò sembra semplice, ma può facilmente diventare un caos, specialmente per le imprese più grandi. Consigliamo a tutte le aziende di mantenere processi molto rigidi di onboarding/offboarding, applicare pratiche efficaci per la gestione sicura delle password e controllare regolarmente gli accessi.

Indipendentemente dalle dimensioni, tutte le organizzazioni devono definire regole molto chiare per la rimozione delle identità che non vengono più utilizzate; in caso contrario, gli autori degli attacchi saranno in grado di sfruttare gli account dimenticati per ottenere privilegi più elevati e spostarsi lateralmente all'interno del tuo ambiente, il tutto passando completamente inosservati.

2. Protezione degli endpoint

Tutti i dispositivi collegati al tuo ambiente rappresentano un potenziale bersaglio. Il lavoro ibrido ha aumentato l'esposizione ai rischi, e per questo motivo la protezione degli endpoint non è mai stata così importante. Molti attacchi iniziano con minacce semplici, che i cybercriminali possono reperire facilmente e che possono essere rilevate e neutralizzate da strumenti endpoint efficaci. Tuttavia, spesso gli endpoint non utilizzati o con sistemi non supportati diventano i punti deboli dei sistemi, offrendo potenzialmente un'opportunità di accesso iniziale per gli attacchi di remote ransomware. Assicurati di proteggere tutti i dispositivi.

3. Autenticazione multi fattore

L'autenticazione multi fattore (Multi-Factor Authentication, MFA) convalida l'identità di un utente con più fattori: di conoscenza (ad es. una password), di possesso (ad es. un token) o di inerenza (ad es. l'impronta digitale). Poiché la compromissione delle credenziali rimane una delle principali cause di attacco[2], l'MFA rappresenta un controllo fondamentale per le organizzazioni moderne. Prendi in considerazione forme più avanzate quali la geolocalizzazione e la corrispondenza numerica, per incrementare la resilienza contro le tattiche di elusione degli autori degli attacchi, pur mantenendo il giusto equilibrio tra esperienza utente e privacy.

Conclusioni

Gli account inattivi e i privilegi non utilizzati costituiscono punti di ingresso estremamente facili da sfruttare per gli autori degli attacchi. Una volta infiltratisi nei sistemi, possono infatti approfittarne per ottenere maggiori privilegi di accesso ed estendere la portata dell'attacco, passando completamente inosservati.

Il punto di ingresso più comune è spesso quello meno visibile. Non permettere ai cybercriminali di trasformare i tuoi endpoint obsoleti in una backdoor.

Applica l'MFA adattiva per intensificare i controlli in scenari ad alto rischio, senza rallentare inutilmente i processi.

4. Vulnerability Management

Con il termine Vulnerability management (Gestione delle vulnerabilità) si intende il processo continuo di identificazione, valutazione e correzione delle vulnerabilità di sicurezza nell'intero ambiente. Include pratiche comuni come l'applicazione di patch a software e sistemi, gli aggiornamenti delle configurazioni e il monitoraggio della presenza di vulnerabilità emerse di recente. Poter contare su validi dati di intelligence sulle minacce è fondamentale per tenersi un passo avanti rispetto ai rischi emergenti.

Comprendere dove sono situate tutte le risorse all'interno della tua rete è essenziale per svolgere un'analisi completa. Con un tale livello di visibilità, le organizzazioni potranno adottare un approccio basato sul rischio per l'assegnazione delle giuste priorità alle vulnerabilità e sapere quali risolvere prima, in base all'esposizione, alla probabilità che vengano sfruttate e all'impatto commerciale.

5. Protezione delle e-mail

Anche se non si tratta di una tecnologia recente, le e-mail rimangono uno dei principali punti di ingresso per gli autori degli attacchi, e il phishing in particolare rappresenta un vettore estremamente comune per il ransomware e il furto di credenziali. Anche gli attacchi Business Email Compromise (BEC) rientrano tra le più frequenti cause delle richieste di indennizzo per le cyberassicurazioni[3]. Una potente soluzione di protezione delle e-mail può impedire che i contenuti dannosi vengano recapitati nelle caselle di posta degli utenti, e questa caratteristica la rende una prima linea di difesa indispensabile. Con il continuo miglioramento dell'IA generativa, le tattiche di phishing diventano sempre più efficaci, migliorando la grammatica e la qualità dei messaggi; di conseguenza, i sistemi di protezione si devono evolvere in modo da ridurre il tasso di successo di questi attacchi, prima ancora che raggiungano gli utenti.

Ma la protezione non deve fermarsi al recapito dei messaggi. Anche gli URL e gli allegati che hanno un aspetto sicuro possono trasformarsi in elementi dannosi non appena il messaggio viene recapitato nella casella di posta del destinatario. Le soluzioni di protezione avanzata delle e-mail offrono ora opzioni di rilevamento e correzione post-recapito: analizzano nuovamente i contenuti, richiamano i messaggi e neutralizzano i link se il profilo di rischio cambia. Questi controlli aiutano a intercettare le minacce che sfuggono al rilevamento delle difese iniziali, riducendo la permanenza dei messaggi dannosi nelle caselle di posta degli utenti.

Conclusioni

Identifica le vulnerabilità nelle app e nei servizi cloud di terze parti, non solo nei tuoi sistemi principali.

Anche un solo clic può rappresentare un pericolo. Il modo migliore per bloccare il phishing è assicurarti che gli utenti non vedano mai l'esca, anche dopo il recapito di un messaggio.

SOPHOS

6. Gestione delle sessioni in base ai privilegi

Gli account degli amministratori sono quelli che offrono più potere agli autori degli attacchi, specialmente quelli con privilegi che includono l'accesso ai sistemi di identità, ai controlli delle configurazioni e agli strumenti di sicurezza. Se un cybercriminale ottiene accesso come amministratore, avrà la capacità di disattivare le difese e distribuire il ransomware su vasta scala.

Per ridurre il rischio, consigliamo alle organizzazioni di implementare un modello a più livelli per gli accessi con privilegi elevati, e di monitorare attivamente come vengono utilizzati questi account. La Gestione delle sessioni privilegiate (Privileged Session Management, PSM) offre capacità di supervisione attraverso la registrazione, l'inclusione nei log e in alcuni casi il controllo delle sessioni di amministrazione in tempo reale. Questo aiuta a rilevare le attività sospette, a prevenire gli utilizzi impropri e a rispettare la conformità.

7. Gestione delle risorse

È impossibile proteggere quello che non si sa di avere. Le organizzazioni devono avere inventari aggiornati delle risorse fisiche e di quelle relative ai dati. Durante un incidente, sapere dove vengono conservati i dati di natura sensibile è fondamentale per poter condurre indagini tempestive ed efficaci, nonché per compilare report accurati e isolare rapidamente le minacce. Un'adeguata gestione delle risorse aiuta a svolgere indagini più accurate, a semplificare l'assegnazione di responsabilità e a ridurre l'impatto di una violazione.

8. Segmentazione e architettura

Se un cybercriminale riesce ad accedere al tuo ambiente, di solito il suo prossimo passo saranno i movimenti laterali: cercherà di ottenere privilegi più elevati, accedere a sistemi sensibili o distribuire ransomware. Una robusta segmentazione della rete e un'architettura efficace possono complicare la vita agli autori degli attacchi. Poiché crea difficoltà e costringe i cybercriminali ad agire in maniera più aperta, la segmentazione aumenta le tue probabilità di individuarli nelle prime fasi della catena di attacco.

L'architettura dei tuoi sistemi deve essere strutturata basandosi sui principi di riservatezza, integrità, disponibilità e resilienza. Questo significa anche limitare l'accesso da sistema a sistema e da utente a sistema applicando un modello zero trust, nell'ambito del quale ogni transazione viene verificata in base all'identità dell'utente, al dispositivo e alle autorizzazioni.

Conclusioni

Sei in grado di vedere chi ha effettuato l'accesso al livello di amministrazione dei tuoi sistemi martedì scorso, e il motivo esatto di tale accesso? Se la risposta è no, è il momento di intensificare la supervisione.

Conservare record che non ti servono più può aumentare i costi delle assicurazioni e moltiplicare i danni alla reputazione in caso di violazione.

Usa la segmentazione della rete per isolare i sistemi critici dagli access point utilizzati di routine.

SOPHOS

9. Extended detection and response (XDR)

Gestire decine di strumenti diversi può frammentare l'elaborazione degli avvisi, rallentare l'assegnazione di priorità e occultare l'attività delle minacce. L'Extended Detection and Response (XDR) risolve questi problemi offrendo una visione unificata delle attività rilevate per endpoint, firewall, rete, e-mail, identità, backup e sistemi di protezione del cloud. Riduce gli avvisi non pertinenti e aiuta a prendere più rapidamente decisioni informate. Evita agli analisti la necessità di dover passare da uno strumento isolato a un altro per svolgere indagini e rispondere alle minacce.

Inoltre, i sistemi XDR più potenti utilizzano analisi avanzate, rilevamenti con priorità stabilite dall'IA, ricerca approfondita dei dati, nonché correlazione ed escalation automatica degli avvisi. Questa convergenza di funzionalità migliora la precisione dei rilevamenti, accelera le indagini e aiuta i team di sicurezza a concentrarsi sulle minacce più gravi, senza essere rallentati da difficoltà legate agli strumenti.

10. Backup e continuità aziendale

Quando un incidente informatico interferisce con le attività operative o corrompe i sistemi, poter contare su backup preparati correttamente e su un piano di continuità aziendale efficace può essere il fattore determinante tra un rapido ripristino dei sistemi e un tempo di inattività prolungato. Tuttavia, non tutti i backup offrono gli stessi vantaggi. Per essere efficaci, i backup vanno verificati e testati regolarmente; in più, devono dimostrare di poter offrire un corretto ripristino di sistemi e dati, rispettandone l'integrità.

Uno dei più comuni punti deboli è la configurazione. Molte organizzazioni scoprono troppo tardi che i loro backup ripristinano i sistemi solo in parte, o che non contengono dati fondamentali, trasformando una breve interruzione del servizio in diverse settimane di caos.

È altrettanto importante che i backup siano protetti tramite autenticazione fuori banda. Senza questo accorgimento, un cybercriminale con privilegi di accesso estesi potrebbe cercare di disattivare o eliminare i backup nell'ambito del proprio attacco.

Conclusioni

L'XDR trasforma i singoli avvisi isolati in un'azione decisiva, accelerando le indagini e migliorando gli esiti delle attività di risposta.

Se possibile, assicurati che i backup siano segmentati e vengano conservati off-line. Le tue attività di ripristino non devono mai essere basate su un unico canale.

11. Protezione della rete e controllo del traffico

La rete è molto di più di un livello di connessione: è un punto di controllo strategico dove è possibile ispezionare, filtrare e gestire il traffico del tuo intero ambiente. I firewall, i sistemi di prevenzione delle intrusioni (IPS), i filtri DNS e i secure web gateway sono la spina dorsale dell'implementazione su più livelli.

Tuttavia, non tutti i firewall hanno le stesse funzionalità. Le soluzioni obsolete, configurate male o non utilizzate correttamente rischiano di creare lacune di sicurezza che possono essere sfruttate dagli autori degli attacchi. Per mantenere un alto livello di resilienza, è fondamentale svolgere una valutazione regolare delle difese che includa l'applicazione di tutte le patch, l'aggiornamento dei sistemi di protezione e la verifica della loro adeguatezza nell'attuale panorama delle minacce.

Le tecnologie di controllo più recenti, come Zero Trust Network Access (ZTNA) offrono capacità più granulari e sensibili al contesto per l'implementazione degli accessi. Unite ai tradizionali sistemi di sicurezza, aiutano a ridurre la superficie di attacco, a impedire i movimenti laterali e a prevenire l'esfiltrazione in ambienti cloud e ibridi.

Conclusioni

Integra i dati di telemetria della rete nel tuo stack di rilevamento per migliorare la visibilità, accelerare le indagini e segnalare attività anomale, in particolar modo i movimenti laterali e il traffico di comando e controllo.

Da una visione olistica a un approccio olistico

La cybersecurity non significa solo implementare i giusti strumenti: implica la realizzazione di una strategia che coinvolge persone, processi e tecnologie. Se applicati con regolarità e precisione, questi 11 controlli possono ridurre notevolmente l'esposizione della tua organizzazione ai rischi.

Per una resilienza a lungo termine, occorre un programma di cybersecurity efficace che sia riproducibile, adattabile e fondato su definizioni nitide delle responsabilità. Le tecnologie sono uno strumento potente, ma per essere utilizzate correttamente richiedono personale dotato delle giuste competenze e processi ben strutturati.

Le minacce si trasformeranno, le tecnologie cambieranno e la tua azienda si evolverà. Per tenere il passo, occorre pensare in maniera olistica, adattandosi continuamente e promuovendo una cultura nella quale la sicurezza non sia solo una casella da spuntare, ma un elemento chiave per il successo dell'azienda.

[1] Cyber Defense Magazine: The True Cost of Cybercrime: Why Global Damages Could Reach $1.2-$1.5 Trillion by End of Year 2025
[2] Sophos Threat Report 2025
[3] Dark Reading, "Email-Based Attacks Top Cyber-Insurance Claims", 8 maggio 2025

È ora di valutare il tuo programma di cybersecurity.

Parla subito con un esperto Sophos.

Vendite per Italia
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it