Criterio di sicurezza di rete: White paper sulle procedure ottimali

Sommario

Introduzione

Senza un criterio di protezione, la disponibilità della rete potrebbe essere compromessa. La policy inizia con la valutazione del rischio per la rete e la creazione di un team per rispondere. La continuazione della policy richiede l'implementazione di una procedura di gestione delle modifiche alla sicurezza e il monitoraggio della rete per rilevare eventuali violazioni della sicurezza. Infine, il processo di revisione modifica la politica esistente e si adatta agli insegnamenti tratti.

Il documento si divide in tre aree: preparazione, prevenzione e risposta. Esaminiamo in dettaglio ognuno di questi passaggi.

Preparazione

Prima di implementare un criterio di protezione, è necessario eseguire le operazioni seguenti:

- Creare istruzioni di criteri di utilizzo.
- Eseguire un'analisi dei rischi.
- Stabilire una struttura del team di sicurezza.

Crea istruzioni di criteri di utilizzo

Èconsigliabile creare istruzioni dei criteri di utilizzo che definiscano i ruoli e le responsabilità degli utenti in relazione alla sicurezza. È possibile iniziare con una politica generale che copra tutti i

sistemi e i dati di rete all'interno dell'azienda. Questo documento dovrebbe fornire alla comunità di utenti generici una comprensione della politica di sicurezza, del suo scopo, delle linee guida per migliorare le loro pratiche di sicurezza e delle definizioni delle loro responsabilità di sicurezza. Se l'azienda ha identificato azioni specifiche che potrebbero sfociare in azioni punitive o disciplinari contro un dipendente, tali azioni e il modo per evitarle devono essere chiaramente illustrati in questo documento.

La fase successiva consiste nel creare una dichiarazione sull'utilizzo accettabile da parte del partner, che fornisca ai partner una comprensione delle informazioni a loro disposizione, la prevista eliminazione di tali informazioni, nonché la condotta dei dipendenti dell'azienda. È necessario spiegare chiaramente tutti gli atti specifici identificati come attacchi alla sicurezza e le azioni punitive che verranno intraprese nel caso in cui venga rilevato un attacco alla sicurezza.

Creare infine un'istruzione di utilizzo accettabile da parte dell'amministratore per illustrare le procedure di amministrazione degli account utente, applicazione dei criteri e revisione dei privilegi. Se la tua azienda ha politiche specifiche relative alle password degli utenti o alla successiva gestione dei dati, presenta chiaramente anche queste politiche. Confrontare la policy con le istruzioni sull'utilizzo accettabile dal partner e con quelle sull'utilizzo accettabile dall'utente per garantire l'uniformità. Assicurarsi che i requisiti dell'amministratore elencati nella politica sull'utilizzo accettabile siano rispecchiati nei piani di formazione e nelle valutazioni delle prestazioni.

Esecuzione di un'analisi dei rischi

Un'analisi dei rischi deve identificare i rischi per la rete, le risorse di rete e i dati. Ciò non significa che si debba identificare ogni possibile punto di ingresso alla rete, né ogni possibile mezzo di attacco. Lo scopo di un'analisi dei rischi è quello di identificare parti della rete, assegnare un livello di minaccia a ciascuna parte e applicare un livello di sicurezza appropriato. In questo modo è possibile mantenere un equilibrio funzionale tra sicurezza e accesso alla rete richiesto.

Assegnare a ciascuna risorsa di rete uno dei tre livelli di rischio seguenti:

- Sistemi **a basso rischio** o dati che, se compromessi (dati visualizzati da personale non autorizzato, dati danneggiati o persi) non possono interrompere l'attività o causare ripercussioni legali o finanziarie. Il sistema o i dati di destinazione possono essere facilmente ripristinati e non consentono l'ulteriore accesso ad altri sistemi.
- **Rischio medio** I sistemi o i dati che, se compromessi (dati visualizzati da personale non autorizzato, dati danneggiati o persi) causano un'interruzione moderata delle attività aziendali, piccole conseguenze legali o finanziarie o forniscono ulteriore accesso ad altri sistemi. Il sistema o i dati di destinazione richiedono un moderato sforzo di ripristino oppure il processo di ripristino comporta l'interruzione del sistema.
- Sistemi **ad alto rischio** o dati che, se compromessi (dati visualizzati da personale non autorizzato, dati danneggiati o persi) causano un'interruzione estrema del business, causano gravi conseguenze legali o finanziarie o minacciano la salute e la sicurezza di una persona. Il sistema o i dati di destinazione richiedono un notevole sforzo per il ripristino, altrimenti il processo di ripristino comporta l'interruzione delle attività aziendali o di altri sistemi.

Assegnare un livello di rischio a: dispositivi di rete principali, dispositivi di rete di distribuzione, dispositivi di accesso alla rete, dispositivi di monitoraggio della rete (monitor SNMP e sonde RMON), dispositivi di sicurezza della rete (RADIUS e TACACS), sistemi di posta elettronica, file server di rete, server di stampa di rete, server applicazioni di rete (DNS e DHCP), server applicazioni dati (Oracle o altre applicazioni autonome), computer desktop e altri dispositivi (server

di stampa autonomi e fax di rete).

Le apparecchiature di rete, quali switch, router, server DNS e server DHCP, possono consentire un ulteriore accesso alla rete e sono pertanto dispositivi a rischio medio o alto. È inoltre possibile che il danneggiamento di queste apparecchiature causi il collasso della rete stessa. Un tale fallimento può essere estremamente dannoso per l'azienda.

Una volta assegnato un livello di rischio, è necessario identificare i tipi di utenti del sistema. I cinque tipi di utenti più comuni sono:

- **Amministratori** Utenti interni responsabili delle risorse di rete.
- Utenti interni **privilegiati** che necessitano di un maggiore accesso.
- **Utenti** Utenti interni con accesso generico.
- **Partner** Utenti esterni con la necessità di accedere ad alcune risorse.
- **Altri** utenti o clienti esterni.

L'individuazione del livello di rischio e del tipo di accesso richiesto per ciascun sistema di rete costituisce la base della seguente matrice di sicurezza. La matrice di protezione fornisce un riferimento rapido per ogni sistema e un punto di partenza per ulteriori misure di protezione, ad esempio la creazione di una strategia appropriata per limitare l'accesso alle risorse di rete.

Sistema	Descrizione	Livello di rischio	Tipi di utenti
Switch ATM	Dispositivo di rete principale	Alta	Amministratori per la configurazione dei dispositivi (solo personale di supporto); Tutti gli altri per l'utilizzo come trasporto
Router di rete	Dispositivo rete di distribuzione	Alta	Amministratori per la configurazione dei dispositivi (solo personale di supporto); Tutti gli altri per l'utilizzo come trasporto
Interruttori armadio	Accedere a un dispositivo di rete	Media	Amministratori per la configurazione dei dispositivi (solo personale di supporto); Tutti gli altri per l'utilizzo come trasporto
Server ISDN o di connessione remota	Accedere a un dispositivo di rete	Media	Amministratori per la configurazione dei dispositivi (solo personale di supporto); Accesso speciale per partner e utenti privilegiati
Firewall	Acced	Alt	Amministratori per la configurazione

	ere a un dispositivo di rete	a	dei dispositivi (solo personale di supporto); Tutti gli altri per l'utilizzo come trasporto
Server DNS e DHCP	Applicazioni di rete	Media	Amministratori per la configurazione; Utenti generici e privilegiati
Server di posta elettronica esterno	Applicazione di rete	Bassa	Amministratori per la configurazione; Tutti gli altri per il trasporto della posta tra Internet e il server di posta interno
Server di posta elettronica interno	Applicazione di rete	Media	Amministratori per la configurazione; Tutti gli altri utenti interni
database Oracle	Applicazione di rete	Medio Alto	amministratori per l'amministrazione del sistema; Utenti privilegiati per gli aggiornamenti dei dati; utenti generali per l'accesso ai dati; Tutti gli altri per l'accesso parziale ai dati

Definizione della struttura di un team per la sicurezza

Creare un team di sicurezza interfunzionale guidato da un Security Manager con partecipanti di ciascuna area operativa della società. I rappresentanti della squadra devono essere a conoscenza della politica di sicurezza e degli aspetti tecnici della progettazione e dell'attuazione della sicurezza. Spesso ciò richiede una formazione aggiuntiva per i membri del team. Il team addetto alla sicurezza ha tre aree di responsabilità: sviluppo, prassi e risposta delle politiche.

Lo sviluppo delle politiche è incentrato sulla definizione e la revisione delle politiche di sicurezza per l'azienda. Riesaminare almeno annualmente sia l'analisi dei rischi che la politica di sicurezza.

L'esercitazione è la fase durante la quale il team preposto alla sicurezza esegue l'analisi dei rischi, l'approvazione delle richieste di modifica della sicurezza, esamina gli avvisi di sicurezza di entrambi i fornitori e della mailing list CERT e trasforma i requisiti dei criteri di sicurezza in implementazioni tecniche specifiche.

L'ultima area di responsabilità è la risposta. Mentre il monitoraggio della rete spesso identifica una violazione della sicurezza, sono i membri del team di sicurezza che si occupano effettivamente della risoluzione dei problemi e della correzione di tale violazione. Ciascun membro del team preposto alla sicurezza deve conoscere nei dettagli le funzionalità di sicurezza fornite dall'apparecchiatura nella propria area operativa.

Sebbene siano state definite le responsabilità del team nel suo complesso, è necessario definire i ruoli e le responsabilità individuali dei membri del team di sicurezza nel criterio di sicurezza.

Prevenzione

La prevenzione può essere suddivisa in due parti: approvare le modifiche alla protezione e monitorare la protezione della rete.

Approvazione delle modifiche alla protezione

Le modifiche alla sicurezza sono definite come modifiche alle apparecchiature di rete che hanno un possibile impatto sulla sicurezza complessiva della rete. I criteri di protezione devono identificare requisiti di configurazione specifici in termini non tecnici. In altre parole, invece di definire un requisito come "Nessuna connessione FTP a origini esterne sarà consentita attraverso il firewall", definire il requisito come "Le connessioni esterne non devono essere in grado di recuperare file dalla rete interna". È necessario definire un insieme univoco di requisiti per l'organizzazione.

Il team addetto alla sicurezza deve esaminare l'elenco dei requisiti del linguaggio comune per identificare problemi specifici di configurazione o progettazione della rete che soddisfano i requisiti. Dopo che il team ha creato le modifiche di configurazione della rete necessarie per implementare il criterio di sicurezza, è possibile applicarle a qualsiasi modifica di configurazione futura. Anche se il team per la sicurezza può esaminare tutte le modifiche, questo processo consente solo di esaminare le modifiche che presentano rischi sufficienti per richiedere un trattamento speciale.

Èconsigliabile che il team di sicurezza esamini i seguenti tipi di modifiche:

- Qualsiasi modifica apportata alla configurazione del firewall.
- Qualsiasi modifica agli elenchi di controllo di accesso (ACL).
- Qualsiasi modifica apportata alla configurazione di SNMP (Simple Network Management Protocol).
- Qualsiasi modifica o aggiornamento nel software che differisce dall'elenco dei livelli di revisione approvati.

Si consiglia inoltre di attenersi alle seguenti linee guida:

- Modificare le password in dispositivi di rete su base regolare.
- Limitare l'accesso ai dispositivi di rete a un elenco approvato di personale.
- Verificare che gli attuali livelli di revisione del software delle apparecchiature di rete e degli ambienti server siano conformi ai requisiti di configurazione della sicurezza.

Oltre a queste linee guida per l'approvazione, chiedere a un rappresentante del team di sicurezza di far parte del consiglio di approvazione della gestione delle modifiche, al fine di monitorare tutte le modifiche che il consiglio revisiona. Il rappresentante del team di sicurezza può rifiutare qualsiasi modifica considerata una modifica di sicurezza fino a quando non viene approvata dal team di sicurezza.

Monitoraggio della sicurezza della rete

Il monitoraggio della sicurezza è simile al monitoraggio della rete, con la differenza che è incentrato sul rilevamento delle modifiche nella rete che indicano una violazione della sicurezza. Il punto di partenza per il monitoraggio della sicurezza è stabilire cosa sia una violazione. In Conduct a Risk Analysis, abbiamo identificato il livello di monitoraggio richiesto in base alla minaccia per il sistema. In Approvazione delle modifiche alla sicurezza, sono state identificate

minacce specifiche per la rete. Esaminando entrambi i parametri, svilupperemo un'immagine chiara di ciò che è necessario monitorare e con quale frequenza.

Nella matrice di analisi dei rischi, il firewall viene considerato un dispositivo di rete ad alto rischio, pertanto è necessario monitorarlo in tempo reale. Dalla sezione Approvazione delle modifiche alla protezione è possibile verificare se sono necessarie modifiche al firewall. Ciò significa che l'agente di polling SNMP deve monitorare aspetti quali i tentativi di accesso non riusciti, il traffico insolito, le modifiche al firewall, l'accesso concesso al firewall e le connessioni impostate attraverso il firewall.

In base a questo esempio, creare un criterio di monitoraggio per ogni area identificata nell'analisi dei rischi. Si consiglia di monitorare le apparecchiature a basso rischio ogni settimana, quelle a medio rischio ogni giorno e quelle ad alto rischio ogni ora. Se è necessario un rilevamento più rapido, eseguire il monitoraggio in un intervallo di tempo più breve.

Infine, i criteri di protezione devono indicare come notificare al team di protezione le violazioni di protezione. Spesso il software di monitoraggio della rete è il primo a rilevare la violazione. Dovrebbe attivare una notifica al centro operativo, che a sua volta dovrebbe informare la squadra di sicurezza, utilizzando un cercapersone, se necessario.

Risposta

La risposta può essere suddivisa in tre parti: violazioni della sicurezza, ripristino e revisione.

Violazioni della sicurezza

Quando viene rilevata una violazione, la capacità di proteggere le apparecchiature di rete, determinare l'estensione dell'intrusione e ripristinare le normali operazioni dipende da decisioni rapide. Avendo queste decisioni prese in anticipo, rispondere a un'intrusione è molto più gestibile.

La prima azione successiva al rilevamento di un'intrusione è la notifica al team di sicurezza. Senza una procedura in atto, ci sarà un notevole ritardo nell'indurre le persone giuste ad applicare la risposta corretta. Definire una procedura nel criterio di sicurezza disponibile 24 ore al giorno, 7 giorni alla settimana.

Èquindi necessario definire il livello di autorità assegnato al team di sicurezza per apportare modifiche e l'ordine in cui le modifiche devono essere apportate. Le possibili azioni correttive sono:

- Implementare modifiche per impedire l'ulteriore accesso alla violazione.
- Isolamento dei sistemi violati.
- Contattare il vettore o l'ISP nel tentativo di rintracciare l'attacco.
- Utilizzare dispositivi di registrazione per raccogliere prove.
- Disconnessione dei sistemi violati o dell'origine della violazione.
- Contattare la polizia o altre agenzie governative.
- Arrestare i sistemi violati.
- Ripristino dei sistemi in base a un elenco di priorità.
- Notifica al personale direttivo interno e legale.

Accertati di aver apportato in dettaglio le modifiche che possono essere eseguite senza l'approvazione della direzione nei criteri di sicurezza.

Esistono infine due motivi per cui è necessario raccogliere e mantenere le informazioni durante un attacco alla sicurezza: determinare in che misura i sistemi sono stati compromessi da un attacco alla sicurezza e perseguire le violazioni esterne. Il tipo di informazioni e le modalità di raccolta variano a seconda degli obiettivi.

Per determinare l'entità della violazione, eseguire le operazioni seguenti:

- Registrare l'evento ottenendo le tracce di sniffer della rete, copie dei file di registro, account utente attivi e connessioni di rete.
- Per limitare ulteriormente i rischi, disattivare gli account, scollegare le apparecchiature di rete dalla rete e disconnettersi da Internet.
- Eseguire il backup del sistema compromesso per un'analisi dettagliata dei danni e del metodo di attacco.
- Cercate altri segni di compromesso. Spesso, quando un sistema è compromesso, sono coinvolti altri sistemi o account.
- Mantenere ed esaminare i file di registro dei dispositivi di sicurezza e i file di registro di monitoraggio della rete, in quanto spesso forniscono indicazioni sul metodo di attacco.

Se sei interessato ad intraprendere un'azione legale, chiedi all'ufficio legale di controllare le procedure per raccogliere prove e il coinvolgimento delle autorità. Tale riesame accresce l'efficacia delle prove nei procedimenti giudiziari. Se la violazione è di natura interna, contatta l'Ufficio Risorse Umane.

Ripristino

Il ripristino delle normali operazioni di rete è l'obiettivo finale di qualsiasi risposta alle violazioni della sicurezza. Definire nel criterio di sicurezza le modalità di esecuzione, protezione e disponibilità dei normali backup. Poiché ogni sistema dispone di risorse e procedure specifiche per il backup, il criterio di protezione dovrebbe fungere da metacriterio, specificando per ogni sistema le condizioni di protezione che richiedono il ripristino dal backup. Se è necessaria l'approvazione prima di eseguire il ripristino, includere anche la procedura per ottenere l'approvazione.

Revisione

Il processo di revisione è l'ultimo sforzo per creare e mantenere una politica di sicurezza. È necessario esaminare tre aspetti: politica, postura e pratica.

La politica di sicurezza dovrebbe essere un documento vivo che si adatti a un ambiente in continua evoluzione. L'analisi dei criteri esistenti in base alle procedure ottimali note consente di mantenere aggiornata la rete. Consultare inoltre il sito Web CERT per suggerimenti, procedure, miglioramenti della sicurezza e avvisi utili da integrare nei criteri di sicurezza.

Èinoltre necessario esaminare la postura della rete rispetto alla postura di sicurezza desiderata. Un'azienda esterna specializzata in sicurezza può tentare di penetrare nella rete e testare non solo la postura della rete, ma anche la risposta di sicurezza dell'organizzazione. Per le reti ad alta disponibilità, si consiglia di eseguire questo test ogni anno.

Infine, per esercitazione si intende un'esercitazione o un test del personale di supporto per assicurarsi che abbia una chiara comprensione delle operazioni da eseguire durante una violazione della sicurezza. Spesso questa esercitazione non viene annunciata dalla direzione e viene eseguita in combinazione con il test della postura di rete. Tale riesame individua lacune nelle procedure e nella formazione del personale in modo da poter intraprendere azioni correttive.

Informazioni correlate

- Altri white paper sulle procedure ottimali
- Supporto tecnico – Cisco Systems