Panoramica

Vantaggi

- **Centralizzare e unificare il controllo sicuro degli accessi** in base al ruolo aziendale per fornire una policy di accesso alla rete coerente per gli utenti finali, sia che essi si connettano attraverso una rete cablata, wireless o VPN.
- **Migliorare la visibilità e identificare i dispositivi in modo più accurato** grazie alla gestione dei profili dei dispositivi e al servizio di feed dei profili dei dispositivi di Cisco® Identity Services Engine (ISE), i quali, insieme, riducono il numero di endpoint sconosciuti.
- **Semplificare l'esperienza degli utenti guest** per agevolare l'onboarding e l'amministrazione degli utenti guest attraverso portali di accesso per dispositivi mobili e desktop completamente personalizzabili, creati in pochi minuti con procedure dinamiche che consentono di gestire facilmente l'esperienza guest.

Cisco Identity Services Engine

Oggi i confini della rete aziendale non sono più quelli tradizionali. La rete si estende ovunque si trovino i dipendenti e i dati. I dipendenti vogliono poter accedere alle risorse di lavoro da dispositivi diversi e attraverso reti non aziendali. La mobilità e Internet of Everything (IoE) stanno cambiando il nostro modo di vivere e lavorare. Le aziende devono supportare un numero sempre maggiore di nuovi dispositivi di rete, mentre una miriade di minacce esistenti e i casi famosi di violazioni dei dati dimostrano chiaramente che è importante proteggere l'accesso a questa rete aziendale estesa.

Poiché la rete moderna si espande, anche la complessità dell'amministrazione delle risorse, la gestione di soluzioni di sicurezza non integrate e il controllo dei rischi crescono di pari passo. Se a tutto questo si aggiunge la connettività ubiqua di IoE con le risorse di IT già limitate, il potenziale impatto dell'incapacità di individuare e risolvere le minacce alla sicurezza assume dimensioni decisamente notevoli.

È necessario un approccio diverso sia per la gestione che per la sicurezza della rete aziendale moderna. La soluzione è Cisco® Identity Services Engine (ISE).

Ridurre l'esposizione e i rischi

Per prevenire le minacce è fondamentale innanzitutto avere visibilità e controllo. La visibilità completa sugli utenti e sui dispositivi che accedono alla rete e il controllo dinamico sono parte integrante della prevenzione, in quanto fanno sì che soltanto le persone giuste che usano i dispositivi giusti possano accedere ai servizi aziendali.

La soluzione ISE 2.0 semplifica ulteriormente il controllo degli accessi sicuro e coerente sulle reti multivendor cablate e wireless e le connessioni VPN remote. Grazie alle funzionalità intelligenti dei profili e di supporto dei sensori, Cisco ISE può arrivare in profondità nella rete per fornire una visibilità superiore su chi e cosa accede alle risorse. Mediante la condivisione di dati di contesto vitali con le integrazioni delle soluzioni dei partner dell'ecosistema e l'implementazione di policy Cisco TrustSec per la segmentazione definita dal software, Cisco ISE trasforma la rete da un semplice veicolo per i dati a un elemento che applica la sicurezza e riduce i tempi necessari a rilevare le minacce della rete e a risolverle.

- **Accelerare il supporto per BYOD e mobilità** con una procedura di configurazione semplice, l'onboarding e la gestione self-service dei dispositivi, la gestione dei certificati dei dispositivi interni e il software integrato di Enterprise Mobility Management (EMM) fornito dai partner per l'onboarding dei dispositivi on premises e off premises.
- **Creare una policy di segmentazione definita dal software per contenere le minacce della rete** utilizzando la tecnologia Cisco TrustSec® per implementare il controllo degli accessi basato su ruoli a livello di routing e switching. Segmentare dinamicamente l'accesso senza la complessità di più VLAN o la necessità di riprogettare la rete.
- **Condividere i dati contestuali completi con la rete e le soluzioni di sicurezza** dei partner per migliorarne l'efficacia globale e ridurre i tempi necessari a rilevare le minacce della rete e a risolverle.
- **Contenere automaticamente le minacce** mediante l'integrazione con Cisco Firepower Management Center in quanto ISE può contenere gli endpoint infettati per la risoluzione, l'osservazione o la rimozione.

Gli aggiornamenti e i miglioramenti di ISE 2.0 comprendono:

- Integrazione con Cisco Mobility Services Engine (MSE) per fornire i dati di posizione con cui creare e applicare l'accesso specifico in base alla posizione in modo che, ad esempio, il personale medico possa accedere alle cartelle dei pazienti solo dal pronto soccorso.
- Miglioramento della nostra architettura aperta per alcuni partner dell'ecosistema ISE, in modo che i clienti possano utilizzare le proprie soluzioni di sicurezza esistenti insieme a ISE per individuare le minacce nella rete e riuscire a contenerle e risolverle rapidamente.
- Supporto per dispositivi di accesso alla rete (Network Access Device) ed endpoint IPv6 di terze parti per estendere la portata di ISE per la conformità degli endpoint su una gamma di reti più ampia.
- Gestione semplificata delle policy, compresa la semplificazione dell'amministrazione dei dispositivi di autenticazione, autorizzazione e accounting (AAA) con funzionalità di accesso TACACS+ e RADIUS, per rendere molto più facile l'implementazione della policy di controllo sicuro degli accessi per le reti cablate.
- Cisco AnyConnect 4.2 comprende il nuovo modulo Network Visibility (NVM) che fornisce un livello di dettagli sui flussi di traffico delle applicazioni in precedenza non disponibile negli endpoint off-premise.

Inoltre, ISE utilizza la tecnologia Cisco Platform Exchange Grid (pxGrid) per condividere dati contestuali con le soluzioni integrate dell'ecosistema dei partner. Questa tecnologia accelera la capacità di identificare, ridurre e risolvere le minacce alla sicurezza nella rete estesa. In generale, il controllo sicuro degli accessi è centralizzato e semplificato così da fornire alle aziende, con la massima sicurezza, i servizi fondamentali di cui hanno bisogno, migliorare la sicurezza dell'infrastruttura, applicare la conformità e semplificare le operazioni dei servizi.

Attraverso le integrazioni con le soluzioni leader di Security Information and Event Management (SIEM) e Threat Defense (TD), la profonda visibilità sulla rete e le funzionalità di controllo sicuro degli accessi, ISE assume un ruolo fondamentale nelle soluzioni Cisco Cyber Threat Defense, Network-as-a-Sensor e Network-as-an-Enforcer. Infine, ISE fornisce la visibilità, il contesto e il controllo dinamico di cui le aziende hanno bisogno per implementare efficacemente una soluzione di sicurezza in grado di controllare tutte le fasi dell'attacco, gestendo l'accesso alla rete prima di un attacco; fornendo visibilità e contenimento delle minacce durante l'attacco e riducendo i tempi necessari a rilevare le minacce e risolverle dopo un attacco.

Altre risorse

Per ulteriori informazioni su Cisco ISE, visitare http://www.cisco.com/go/ise o contattare il rappresentante locale.

C45-654884-13 10/15