

Toyota Financial Services, una rete aziendale più sicura con il controllo degli accessi Cisco NAC



Azienda:

Toyota Financial Services

Settore:

Finanziamenti, leasing, noleggio.

La sfida:

Adottare una soluzione di protezione proattiva per la propria infrastruttura che operi in maniera estesa e pervasiva all'interno della Rete.

Configurare la soluzione in modo che garantisca gli standard richiesti dalle policy di Sicurezza per gli asset aziendali ed esterni.

Ottimizzare i processi e ridurre i rischi legati alle vulnerabilità.

Obiettivi raggiunti:

Avere protetto il proprio ambiente di business aperto e distribuito (utenti mobili, utenti connessi da accessi remoti, partner con contratti di outsourcing, ospiti e personale temporaneo) grazie a un efficace sistema di controllo degli accessi.

Consentire l'accesso al proprio network interno proteggendolo dai rischi di accessi non autorizzati e assicurando l'operatività in ogni momento e da qualsiasi accesso remoto.

Avere migliorato la produttività dei dipendenti, la protezione delle informazioni confidenziali e ridotto i costi del ciclo vitale della soluzione.

Avere quantificato un ROI certo e veloce sulla base delle minacce che l'azienda intende affrontare con la soluzione NAC.

Toyota è il secondo costruttore mondiale di automobili: produce ogni anno oltre 9 milioni di veicoli e possiede 67 stabilimenti in tutto il mondo. La corporation è presente sul territorio italiano con più di 233 punti vendita e 227 centri di assistenza. "Financial Services" è la divisione finanziaria del gruppo.

Per aziende come la Toyota non è più sufficiente affidare la propria sicurezza informatica alla sola difesa perimetrale, è necessaria invece l'adozione di soluzioni integrate che operino in maniera estesa e pervasiva all'interno della Rete.

Per questo motivo l'azienda ha richiesto la progettazione di una soluzione innovativa che consenta l'applicazione delle policy di sicurezza a tutti i dispositivi finali collegati (gestiti o meno dal dipartimento IT), indipendentemente dalla loro modalità di accesso, dall'appartenenza, dalla tipologia dei dispositivi, dalla configurazione applicativa e dai modelli di remediation. In pratica una protezione proattiva che migliori la resilienza della Rete e permetta di proteggere l'infrastruttura di rete dell'azienda in maniera profonda ed estesa.

L'ambiente di business dell'azienda è aperto e distribuito. Molti utenti mobili portano i loro laptop e i loro dispositivi cellulari dentro e fuori dagli uffici, li connettono sia all'interno sia all'esterno della rete aziendale e con utenti connessi da accessi remoti in luoghi pubblici,

con partner con contratti di outsourcing che fanno uso del network interno e con ospiti e personale temporaneo che utilizzano Internet. Una simile struttura aziendale richiede un'infrastruttura solida e sicura che garantisca per tutti gli asset gli standard richiesti dalle policy di Sicurezza.

Per la migliore risoluzione di queste problematiche è stata scelta la tecnologia **Cisco NAC** (Network Admission Control). Cisco NAC è una soluzione che permette di delegare al network la verifica e il controllo della conformità alle policy di sicurezza per tutte le periferiche in accesso alla rete. L'accesso è consentito ai dispositivi conformi e affidabili (inclusi PC, server, telefoni IP e stampanti), mentre può essere negato alle periferiche non conformi, che in tal caso vengono reindirizzate verso un'area di quarantena e remediation.

Cisco NAC permette di definire e adottare policy di sicurezza complete e granulari, trasformabili in regole processabili e applicabili in maniera affidabile, sistematica, automatica e pervasiva nella Rete, garantendo una sicurezza proattiva estesa a tutta l'azienda. Questo si realizza per mezzo di un'architettura scalabile, con una componente centralizzata per la definizione delle policy, una componente di verifica e controllo distribuita a livello di rete e con la possibilità di un'integrazione allargata con altri prodotti e tecnologie per la sicurezza.

Per la prevenzione degli accessi non autorizzati, la gestione di parte del network, completamente separata dalla LAN di produzione, è stata assegnata a consulenti esterni. In questo modo si è garantito l'accesso a Internet senza esporre il network interno a rischi.

Il NAC controlla le connessioni da sede remota, il che è di grande utilità quando è necessario permettere la connessione di un partner in applicazioni extranet.





Sono situazioni delicate quelle in cui è impossibile determinare chi si stia collegando alla rete dalla sede del partner, ma la possibilità di controllare l'accesso prima, durante e dopo l'autenticazione di un utente garantisce l'efficace mantenimento della sicurezza e della protezione delle informazioni riservate dell'azienda.

La soluzione Cisco NAC è stata implementata adottando la tecnologia Cisco Clean Access (CCA). Nel caso specifico della Toyota, la tecnologia è composta da due tipi di apparati: il Clean Access Manager (CAM) e il Clean Access Server (CAS), entrambi proposti in modalità ridondante.

Clean Access Manager fornisce un'interfaccia Web per la creazione di policy di sicurezza e la gestione degli utenti online e può funzionare anche come proxy di autenticazione per i server. Gli amministratori possono usare Clean Access Manager per stabilire ruoli-utenti, controlli della conformità e richieste di remediation. Clean Access Manager comunica e gestisce con Clean Access Server, che è il componente di attuazione della soluzione NAC.

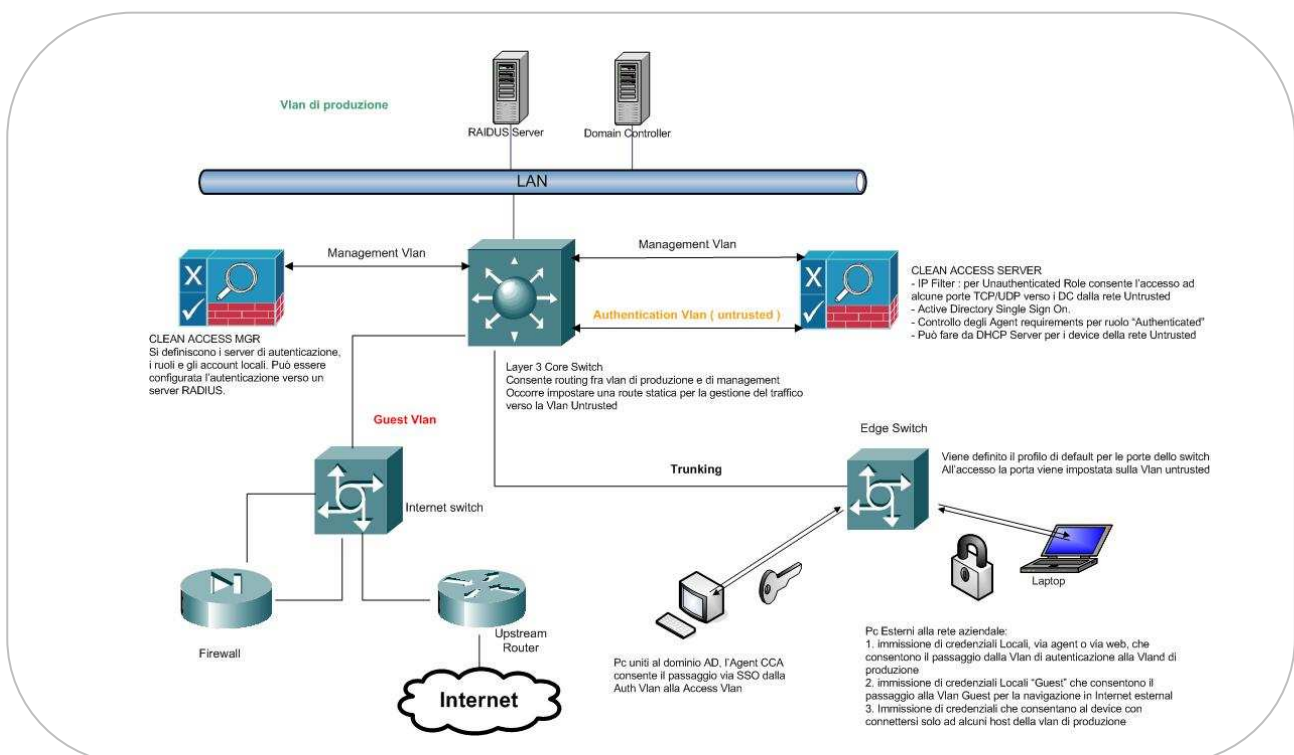
Clean Access Server fornisce un'interfaccia Web per la creazione di policy di sicurezza e

la gestione degli utenti online. Per Toyota è stato installato in modalità Out-of-Band Real-IP Gateway, in Layer 2 restricted e implementato centralmente nella sede HQ.

Grazie a un ambiente informatico stabile, efficiente e sicuro la Toyota ha migliorato la produttività dei dipendenti, protegge le informazioni confidenziali, ha ridotto i costi totali del ciclo di vita della soluzione e può affrontare con successo le sfide dei mercati.

Il Ritorno dell'Investimento (ROI) è certo, veloce e quantificabile sulla base delle minacce che l'azienda intende affrontare con la soluzione NAC.

Una strategia di sicurezza esauriente e di provata efficacia assicura inoltre importanti vantaggi, tra cui l'ottimizzazione dei processi, il taglio dei costi e la riduzione degli incidenti con budget e risorse limitati. La protezione delle risorse (aziendali e non) con un asset management efficace e che consenta la standardizzazione, la riduzione dei costi del ciclo di vita della soluzione e dei costi operativi, riduce i rischi legati alle vulnerabilità, assicurando la migliore protezione a tutte le periferiche in rete.





Headquarter: L.go G. Falcone, 4 – 00045 Genzano di Roma

Tel. +39 069391360 - info@aminformatica.it

<http://www.aminformatica.it>