Protezione delle reti aziendali e sicurezza degli accessi

Indice

Management Summary

Il presente documento ha lo scopo di evidenziare le principali esigenze in ambito di protezione delle reti aziendali identificando delle contromisure e fornendo al contempo degli hightlights sulla strategia di mitigazione le problematiche utilizzando soluzioni Cisco Meraki: *secure access to the corporate networks*.

Si discuterà pertanto di accesso alla rete aziendale nei contesti di rete cablata (rete fisica) e wireless (rete Wi-Fi) per le categorie di utenza "corporate", "consultant" e "guest" e si evidenzieranno i principali problemi e i possibili scenari risolutivi per l'accesso alle risorse (es. accesso ai server ed ai servizi interni, navigazione Internet, etc.).

Tipologie di utenza

Si riepilogano brevemente le esigenze d'accesso relative alle macro categorie di utenza:

Utenza corporate: ovvero l'utenza interna che tipicamente deve avere accesso alla rete aziendale per usufruire delle applicazioni e dei servizi aziendali. Questa tipologia di utenza deve essere governata mediante l'enforcement di politiche aziendali che derivino da considerazioni tecniche ed organizzative, in termini di utilizzo degli strumenti informatici, delle applicazioni, della connettività internet e deve inoltre essere soggetta alla verifica della compliance ovvero, deve essere inibita alla connessione alla rete di dispositivi non autorizzati (es. access point, switch da tavolo, dischi rimovibili, chiavette internet, etc.).

Utenza consultant: ovvero i collaboratori aziendali. Sono utenze trasversali alle funzioni aziendali che svolgono attività di vario genere sui sistemi, sulle applicazioni, sui dati aziendali e per cui devono poter connettersi alla rete, spesso utilizzano loro PC, dei quali non si ha il controllo. Sono un costo d'investimento per l'azienda e quindi devono poter lavorare con la massima efficienza e produttività ma al contempo creano un rischio di sicurezza (accesso incontrollato). Questa tipologia di utenza deve essere assoggettata a delle politiche di sicurezza minime che consentano di proteggere la rete aziendale e le altre categorie d'utenza da un traffico Internet sconsiderato/incontrollato o dalla presenza di software malevolo ospitato sui PC (es. virus).

Utenza guest: ovvero gli ospiti che tipicamente richiedono un accesso alla rete necessario alla fruizione della navigazione Internet. L'accesso, anche in questo caso, benché semplificato rispetto alle altre categorie d'utenza, andrebbe comunque assoggettato a delle misure minime di sicurezza e regolamentato in conformità alle normative vigenti.

Prescindendo dalle categorie d'utenza, l'azienda deve cercare di applicare delle misure di controllo minime che la tutelino, sia sul fronte della tutela del segreto industriale (protezione dei dati), sia sul fronte della continuità del business. Le misure minime introdotte dovrebbero essere il meno intrusive possibile per evitare che un controllo più tight degeneri in una complessità di gestione e di fruizione del servizio stesso che impatterebbe ovviamente sull'operatività utente e conseguentemente sulla relativa produttività.

Tipologia di accesso

Si riepilogheranno brevemente le due principali modalità di accesso alle reti aziendali:

Accesso wired: ovvero l'accesso alla rete cablata effettuato direttamente tramite cavo ethernet. E' un accesso trasversale alla tipologia di utenza che tipicamente viene maggiormente utilizzato dalla categoria "corporate". Comunemente, in una realtà strutturata, questa tipologia di accesso

costringe il dipartimento IT a configurare delle porte d'accesso sugli switch di rete andandole ad attestare su particolari reti logiche (VLAN). Questo processo comune di segmentazione serve ad imputare dei traffici dati tipicamente diversi e a confinare il traffico di broadcast al fine di evitare che "applicazioni" che risiedono sullo stesso segmento di rete impattino l'una sull'altra. Il caso tipico è la segregazione del traffico VOIP su una VLAN dedicata dal traffico dati effettuato da altri applicativi o servizi presenti nell'ecosistema aziendali quali ad esempio i terminali a radiofrequenza, le stampanti, i server, le reti di management, etc.

Accesso wireless: ovvero l'accesso al network Wi-Fi effettuato tramite l'etere e implementato mediante dispositivi access point. E' anch'essa una tipologia di accesso trasversale alla tipologia di utenza "corporate", "consultant" e "guest". Comunemente, in una realtà strutturata, questa tipologia di accesso è segmentata in una o più sotto reti (SSID) inputate su una o più VLAN, tipicamente dedicate al confinamento ed alla distinzione del traffico "interno" e "ospite".

Prescindendo dalla categoria d'accesso, è davvero importante che un dispositivo connesso alla rete aziendale sia riconosciuto prima che gli sia consentito l'accesso alla stessa ed alle relative risorse. Anche se l'accesso avvenisse in modalità self service, auspicabile per massimizzare l'efficacia della soluzione, questo dovrebbe avvenire solo dopo un'accurata verifica da parte dell'IT aziendale del dispositivo stesso, così da scongiurare qualsiasi tipo di rischio (es. presenza dell'antivirus, adeguato livello di patching del dispositivo, etc.). E' inoltre indispensabile che l'accesso sia controllato e che il dispositivo sia controllabile, senza impattare l'operatività dell'utilizzatore (es. senza un ritiro del dispositivo per verifiche).

L'ecosistema aziendale dal punto di vista delle infrastrutture

In un azienda che opera sul mercato globale e che pone la dislocazione delle proprie sedi sulla medesima scala, il problema dell'accesso sicuro alle reti aziendali assume un grado di complessità maggiore. Tipicamente, per via dei costi, è davvero raro avere un presidio IT adeguato su tutte le sedi aziendali e questo fenomeno rende tipicamente difficile se non impossibile aggredire il problema della sicurezza dell'accesso alla rete aziendale. Inoltre, anche in realtà periferiche, per esempio dislocate in altri continenti, è molto difficile dal punto organizzativo e tecnico implementare soluzioni globali che aggrediscano il problema con semplicità ed ad un costo contenuto. Le soluzioni adottate in questi contesti aziendali sono tipicamente poco uniformi ed abbracciano solo in parte il problema.

Le principali criticità

Di seguito viene riportata un elenco delle principali criticità relative all'accesso alle reti aziendali. Sebbene l'accesso ai server ed ai servizi centrali avvenga solo se si è in possesso di credenziali di autenticazione e sebbene ogni postazione PC aziendale sia dotata di software antivirus:

1. Non è tipicamente possibile individuare e/o prevenire la connessione di un dispositivo alla rete aziendale.
2. Non è tipicamente possibile bloccare un dispositivo connesso alla rete che stia effettuando grandi quantità di traffico dati all'interno della rete aziendale (a meno dell'adozione di strumenti dedicati);
3. Non è tipicamente possibile evitare che un PC infetto da virus (es. di un consulente o ospite) una volta connesso alla rete, possa infettare anche i computer aziendali;
4. E' estremamente difficile identificare un tentativo di violazione dei server aziendali se proveniente dall'interno della rete;
5. …

La risposta ai più comuni problemi appena accennati viene fornita da soluzioni puntuali e molto spesso poco integrate che comportano un implicito aumento della complessità di gestione delle reti

che spesso richiedono competenze specialistiche di alto profilo ed un conseguente aumento dei costi mantenimento e gestione.

Scenari di mitigazione

Nei seguenti paragrafi saranno presentate brevemente tre soluzioni di NAC (network access control) che possano indirizzare la risoluzione delle problematiche di accesso alla rete aziendale. In particolare saranno presentate le soluzioni Cisco ISE, ForeScout CounterACT, Cisco Meraki.

Le prime due soluzione affrontano nello specifico la problematica di NAC, sono totalmente on-premise e si integrano più o meno bene nell'ecosistema aziendale che va adattato per ospitarle.

La terza soluzione, Cisco Meraki, una soluzione completamente cloud, affronta la problematica NAC dal punto dello stack di networking proponendo una soluzione tecnologica di ultima generazione per ottenere la stessa user experience a partire dall'accesso LAN, al Wireless, fino ad arrivare all'MDM (mobile device management) ed all'interconnessioni delle sedi periferiche (MPLS over Internet).

Soluzione Cisco ISE

Cisco ISE è una soluzione miratamente dedicata al mercato Cisco Large Enterprise che ha dei requisiti architetturali molto stringenti e propedeutici al supporto delle funzionalità offerte dalla soluzioni, requisiti che spesso vincolano ad un aggiornamento parziale o totale dell'architettura LAN e/o Wireless. Dato il modello di operatività, il deployment è tipicamente centralizzato. Per la gestione dei device Corporate è indispensabile l'utilizzo di certificati digitali distribuiti da una infrastruttura PKI Enterprise.

Cisco ISE è una piattaforma di tipo identity-based, sensibile al contesto che riunisce informazioni in tempo reale provenienti dalla rete, dagli utenti e dai dispositivi; ISE utilizza quindi queste informazioni per prendere decisioni proattive sulla governance applicando policy centralizzate all'intera infrastruttura di rete.

Caratteristiche principali del prodotto:

- Applicazione coerente di policy basate sul contesto, all'interno delle reti cablate e wireless;
- Visibilità sull'intero sistema, che consente di monitorare gli utenti e i dispositivi presenti nella rete cablata, wireless o VPN;
- Servizi integrati AAA (Authentication, Authorization, Accounting), profiling, controllo dello stato e gestione degli ospiti;
- Identificazione accurata dei dispositivi utilizzando probe implementati da ISE, informazioni raccolte da dispositivi di rete integrati e scansione attiva degli endpoint;
- Conformità dei dispositivi mobili basata su policy, e provisioning delle applicazioni utilizzando soluzioni per la gestione multi-dispositivo integrata;
- Onboarding BYOD semplificato attraverso la registrazione self-service.

Il licensing viene effettuato sul numero massimo di endpoint, cioè dispositivi capaci di accedere alla rete: pertanto nel conteggio occorre contemplare tutti i PC (aziendali e guest), i dispositivi mobili e i device passivi (stampanti, telecamere, etc.).

Soluzione ForeScout CounterACT

Forescout CounterACT è una soluzione molto flessibile, che offre diverse metodologie di autenticazione e di gestione delle politiche di access control. Si adatta ad architetture di rete eterogenee, garantendo interoperabilità con diversi vendor di Network & Security. In relazione al modello di operatività, il deployment può essere centralizzato oppure distribuito. Consente la classificazione automatica e la gestione dei device Corporate mediante integrazione WMI con tutti i dispositivi connessi all'Active Directory. La soluzione consente il deployment delle diverse funzionalità anche a step, consentendo una rapida attivazione delle policy di Device Classification, Compliance e Guest Management.

ForeScout CounterACT è una piattaforma di security control che consente di vedere monitorare e controllare tutti i dispositivi presenti in rete, tutti i sistemi operativi, tutte le applicazioni e gli utenti. E' semplice da installare in quanto non richiede software, agenti, upgrade hardware o riconfigurazioni.

La soluzione proposta aiuta a gestire le tematiche NAC in modo semplice ed automatizzato:

- Forescout lavora con la maggior parte dell'infrastruttura di rete esistente, switch, router, firewall, endpoints, patch management systems, directories, ticketing systems; non richiede, come requisito, il cambio o l'upgrade dell'infrastruttura;
- Forescout non richiede l'installazione di software; se un dispositivo tenta l'accesso in rete, il sistema lo identifica, lo profila, lo esamina e ne controlla l'accesso anche senza l'installazione di agent, rendendo compatibili con la soluzione tutte le tipologie di Endpoints, managed oppure unmanaged, conosciuti oppure ignoti, autorizzati o meno;
- Forescout si installa Out-of-band, senza introdurre latenza o point-of-failure; tipicamente è attivato dietro uno o più flussi di traffico in mirror dagli switch di Core oppure Distribution, sui flussi di traffico interessanti client-server,
- Forescout fornisce uno spettro completo di possibilità di Enforcement della Policy, dall'approccio Alerting, al Remediate fino all'approccio aggressivo, con possibilità di blocco o disabilitazione delle porte LAN di accesso.

Di seguito riassumiamo gli ambiti in cui è in grado di operare la soluzione Forescout:

- Classificazione dei dispositivi connessi alla rete;
- Gestione degli utenti aziendali;
- Gestione dei consulenti;
- Gestione degli utenti guest;
- Gestione Malware e Warm – protezione Zero Day;
- Network Asset Management;
- Gestione PCI Compliance;
- Gestione utenti remote.

Il licensing viene effettuato sul numero massimo di endpoint, cioè dispositivi capaci di accedere alla rete: pertanto nel conteggio occorre contemplare tutti i PC (aziendali e guest), i dispositivi mobili e i device passivi (stampanti, telecamere, etc.).

Soluzione Cisco Meraki

Cisco Meraki, a differenza delle soluzioni presentate in precedenza, è una soluzione completa di cloud networking che integra nativamente una soluzione di Network Access Control. La funzionalità di NAC è implementata su tutte le tipologie di prodotto a partire dagli access point wireless, agli switch di rete ed agli apparati di security. Tramite l'adozione della soluzione Meraki su tutti i livelli di rete d'accesso, mediante un paradigma cloud, è possibile gestire da una semplicissima interfaccia web denominata dashboard tutta la rete aziendale anche se distribuita globalmente.

Le principali caratteristiche della soluzione, in ambito NAC, sono le seguenti:

- Accesso uniforme sia alla rete LAN che Wireless tramite splash page;
- BYOD semplificato attraverso la registrazione self-service;
- Gestione completa dei dispositivi fissi e mobili tramite componente MDM;
- Definizione di politiche di accesso in base alla categoria di utente o dispositivo;
- Bandwidth shaping in base alla categoria di utenza e/o dispositivo;
- Integrazione nativa con Active Directory / RADIUS 802.1X;
- Verifica della compliance mediante la rilevazione della presenza di un antivirus installato a bordo del dispositivo connesso;
- La soluzione non prevede la fornitura di controller locali poiché completamente ridondati e demandati al Cloud;
- L'aggiornamento automatico degli apparati non richiede costosi progetti di upgrade;
- Il costante rilascio di nuove funzionalità garantisce la durabilità dell'investimento;
- Semplicità e uniformità di gestione;
- Garanzia a vita su tutti i prodotti.

Il licensing viene effettuato a livello di dispositivo (es. access point, switch, security appliance), il numero di utenze è illimitato.

Impatti sull'utenza corporate

L'implementazione di una qualsiasi soluzione di network access control, come quelle presentate in precedenza, ha un impatto più o meno forte sull'utenza. Per esemplificare il problema basta pensare che, alla base della funzionalità di NAC, vi è un meccanismo di autenticazione: un utente deve autenticarsi alla rete aziendale per essere riconosciuto e correlato ad una particolare categoria d'utenza, corporate, consultant o guest.

Il meccanismo di autenticazione può essere particolarmente intrusivo come ad esempio l'autenticazione mediante presentazione di una splash page di richiesta credenziali. Vi sono tuttavia altri tipi di integrazione oltre la splash page, soprattutto in domini Microsoft, che permettono un autenticazione diretta del dispositivo / utente secondo un modello di single sign-on. La funzionalità di single sign-on, tuttavia, è tipicamente disponibile solo per postazioni di lavoro dotate di sistema operativo Microsoft e connesse al dominio aziendale.

La minimizzazione dell'impatto sull'utenza dovuto all'implementazione di una soluzione di network access control avviene mediante un efficace e preventiva identificazione delle utenze interne che prevede soprattutto l'identificazione dei dispositivi/asset aziendali che si collegano alla rete. Mediante un censimento preventivo dei dispositivi o più comunemente durante una fase di dry run, è possibile applicare meccanismi di whitelisting che inibiscano il meccanismo di autenticazione rendendo meno invasiva la tecnica di autenticazione e minimizzando eventuali "disservizi" durante

il periodo di transizione (sia essa basata su splash page, su integrazione active directory o mediante altri protocolli di autenticazione come ad esempio il radius).

Impatti sull'utenza consultant e guest

L'implementazione di una soluzione di network access control serve specificatamente ad impedire un accesso incontrollato alla rete aziendale e pertanto, per le categorie di utenza "esterna" saranno forzati meccanismi di autenticazione previsti nativamente dalla soluzione (eventualmente allargando le possibilità anche introducendo meccanismi di self provisioning delle credenziali).

In ogni caso, una volta implementato il meccanismo di autenticazione dell'utente esterno (es. tramite splash page di autenticazione e richiesta delle credenziali), sarà possibile forzare principalmente le seguenti verifiche/componenti:

1. Raccogliere le generalità (minime) dell'utente es. nome e cognome;
2. Associare alle credenziali garantite dal sistema il dispositivo d'accesso così da creare un link automatico tra utilizzatore e dispositivo;
3. La verifica della presenza di un software antivirus sul dispositivo utilizzato;
4. Forzare o meno l'installazione di un componente software MDM compatibile con i sistemi operativi più comuni (es. Microsoft, OS X, iOS, Android, etc.) e con i dispositivi più comuni per la rilevazione puntuale delle caratteristiche del dispositivo e del software installato sullo stesso.

Ovviamente il set di attività che sarà possibile condurre sull'utenza sono molto specifiche della soluzione adottata e di conseguenza esulano da questa trattazione.

Tabella riassuntiva delle soluzioni esaminate

Obiettivo	**Cisco ISE**	**ForeScout**	**Cisco Meraki**
Complessità di gestione	Alta	Alta	Bassa
Costo del progetto	Alto	Medio/Alto	Medio
Limite di utilizzo	Per utente	Per utente	Illimitato
Vantaggi collaterali al progetto	Bassi	Bassi	Alti
Costo di mantenimento della soluzione	20% c.acq.	20% c.acq.	20% c.acq.
Collocazione della soluzione	On-Top	On-Top	Sostituzione
Costo di mantenimento switching	Paritetico	Paritetico	Minimale, solo L3
Gestione utenti corporate	Radius	Active Directory	Active Directory
Gestione utenti consultant	Splash Page	Splash Page	Splash Page
Gestione utenti guest	Splash Page	Splash Page	Splash Page
Gestione utenze wired e wireless	Uniforme	Uniforme	Uniforme
Mobile Device Management	Non presente	Non presente	Integrato
Check della compliance antivirus	Presente	Presente	Presente
Check compliance software	Parziale	Parziale	Parziale
Assets inventory (hardware / software)	Non presente	Parziale	Integrato
Gestione politiche per device	Presente	Presente	Presente
Gestione politiche per utente	Presente	Presente	Presente
Bandwidth shaping per categoria	Non presente	Non presente	Presente
Garanzia della soluzione	Limitata	Limitata	A vita
Continuous improvement	Non presente	Non presente	Presente
Modello di gestione	On-Premise	On-Premise	Cloud

Costi housing datacenter	Da prevedere	Da prevedere	Non presenti
Soluzione aperta o proprietaria	Proprietaria	Proprietaria	Proprietaria
Innovatività della soluzione	Bassa	Bassa	Alta
Tempistiche di implementazione	Lunghe	Medio Basse	Medio Basse

Conclusioni

Le soluzioni prese in esame sono state tutte censite da GARTNER, le soluzioni Cisco ISE e ForeScout, in particolare, si attestano come leader di mercato, la soluzione Cisco Meraki è un challenger / visionario (in realtà è sempre una soluzione Cisco). In linea di massima i costi di implementazione delle tre soluzioni si equivalgono benché la soluzione Cisco ISE sia tipicamente decisamente più costosa delle altre due presentate. In termini di complessità ci sono dei forti limiti sulle prime due soluzioni che sostanzialmente si pongono on-top all'attuale infrastruttura non migliorandone sostanzialmente le caratteristiche se non in termini di soluzione puntuale. La soluzione Meraki, a differenza, si pone come parte integrante dell'infrastruttura aziendale uniformando il layer d'accesso e garantendo al contempo uniformità, semplicità di gestione, un basso costo di mantenimento e non meno importante, un continuo aggiornamento evolutivo.