

Progetto NAC (Network Access Control)



MARCO FAGIOLO

Introduzione



- **Per sicurezza in ambito ICT si intende:**
 - Disponibilità dei servizi
 - Prevenire la perdita delle informazioni
 - Evitare il furto delle informazioni

Scenario (I)



- In merito alla sicurezza negli ultimi anni le Aziende hanno posto la loro attenzione ed i loro investimenti nelle seguenti due aree:
 - La **sicurezza perimetrale** per evitare il furto delle informazioni dall'esterno o per contrastare attacchi, sempre dall'esterno, aventi lo scopo di compromettere i servizi ICT erogati (es. firewall, IDS/IPS, appliance per la rilevazione di malware, spam, reverse proxy, etc...)

Scenario (II)



- La **sicurezza delle Server Farm** per prevenire la perdita di informazioni e per garantire l'affidabilità e la continuità del servizio; nel primo caso si fa uso di tecniche sempre più sofisticate e molteplici di salvataggio dei dati e la diversa dislocazione geografica degli stessi; nel secondo caso ci si avvale di elaboratori sempre più affidabili (power supply redundancy, disk mirroring, cluster configuration) e di soluzioni tecnico/organizzative mirate alla continuità del servizio come la virtualizzazione, la "Business Continuity" ed il "Disaster Recovery"

Sicurezza interna (I)



- Tutte le più recenti statistiche dimostrano che la maggior parte degli incidenti legati alla sicurezza hanno origine all'interno dell'azienda.
- Tali incidenti si possono dividere in due macro categorie:
 - **Dolosi** - quando gli attacchi effettuati hanno lo scopo di trafugare informazioni o provocare danni all'infrastruttura, ai servizi, alle applicazioni ad opera di personale interno o esterno per motivi economici, di vendetta, di rivalsa, dimostrativi, etc...

Sicurezza interna (II)



- **Colposi** – (i più diffusi) quando gli incidenti che comportano la perdita di informazioni aziendali o danni alle applicazioni e servizi sono provocati da azioni inconsapevoli.

Tali azioni sono frutto generalmente di disattenzione, di noncuranza, di non rispetto o non conoscenza delle direttive aziendali in materia di sicurezza.

Criticità della Sicurezza Interna



- Ma quali sono le criticità specifiche nell'implementare delle soluzioni per la sicurezza interna di un'azienda? Consideriamone due in particolare su cui abbiamo posto maggiore attenzione nel progetto:
 - **Impatto organizzativo.** Una soluzione efficace non può essere basata solo su strumenti tecnologici ma deve prevedere anche delle regole precise e chiare che guidino gli utenti a dei comportamenti corretti.
 - **Impatto sui servizi.** La ricerca del miglior livello di sicurezza interna, troppo spesso porta ad una “rigidità” nell'utilizzo dei servizi e delle applicazioni; questo va nella direzione opposta rispetto alle richieste degli utenti e del management che esigono sempre maggiore flessibilità e fruibilità delle risorse informatiche.

Cosa è stato già fatto



- Negli ultimi due anni nella nostra azienda sono state portate a termine varie attività e progetti mirate a migliorare la sicurezza interna, tra cui:
 - Il backup giornaliero e in automatico dei documenti presenti nelle postazioni di lavoro degli utenti
 - La realizzazione di soluzioni per la raccolta, l'analisi e la storicizzazione delle operazioni maggiormente critiche effettuate dagli utenti o dagli amministratori dei sistemi
 - La riorganizzazione fisica e logica della rete aziendale e l'introduzione di firewall interni con lo scopo di separare e gestire le interazioni tra le varie aree funzionali (dipendenti, ospiti, top management, server, apparati tecnologici, etc.).

L'obiettivo del progetto



- L'obiettivo di questo progetto è quello di introdurre delle nuove soluzioni tecnologiche e delle nuove regole organizzative per gestire in sicurezza anche l'ultimo componente fino ad oggi generalmente trascurato: l'**endpoint**.
- Con il termine “endpoint” viene generalmente indicato qualsiasi dispositivo informatico o telematico collegato ad una rete dati (ad esempio desktop/notebook, stampanti, palmari, telefoni, etc...)



NAC (Network Access Control)

NAC - Obiettivi



- Il NAC è una soluzione che deve permettere di controllare ed abilitare, in modo sicuro, l'accesso ad una rete informatica di un endpoint.
- Il NAC deve essere indipendente dal supporto fisico utilizzato per connettersi alla rete aziendale (wired o wireless)
- L'autenticazione deve poter avvenire o attraverso delle credenziali (user e password) o attraverso un certificato digitale.

NAC - Compiti



- Il NAC, nella sua forma più completa, deve essere composto da due componenti:
 - Un primo componente che verifica le credenziali dell'utente o del dispositivo ed autorizza l'accesso, secondo un profilo, alle risorse della rete, definite nello profilo stesso;
 - Un secondo componente che verifica il contenuto software del dispositivo per valutarne il grado di sicurezza e l'aderenza alle policy stabilite dall'azienda.

NAC – Il mercato



- Solo negli ultimi due anni il mercato ha cominciato a proporre delle soluzioni in questo settore, con strategie e prodotti spesso non ancora ben delineati che rendono difficile la selezione.
- Le due componenti necessarie del NAC (autenticazione e analisi software dell'endpoint) risultano difficilmente soddisfatte, con grado di eccellenza, da un unico prodotto. Infatti mentre la fase di autenticazione deve essere gestita dagli apparati di rete e quindi risultano vincenti i produttori di networking (Cisco, Juniper, etc..) nell'altra i produttori di software specializzato (Sophos, Symantec, McAfee) ottengono i migliori risultati.

NAC – La soluzione



- Pertanto l'unica maniera di ottenere una soluzione che soddisfacesse, in modo completo ed ottimale, i nostri requisiti è stata quella di scegliere di integrare le soluzioni di due produttori leader nelle rispettive aree: Cisco e Sophos.
- Il NAC di Cisco (“ACS”) è stato scelto per verificare le credenziali dell'utente che desidera connettersi alla rete o l'autenticità dei dispositivi che offrono i loro servizi sulla rete come stampanti, telefoni VoIP, apparati di rete.
- Il NAC di Sophos (“NAC Advanced”) si occuperà della verifica della compliance dell'endpoint.

NAC – I profili utente



- Dopo un'attenta analisi, abbiamo individuato le tipologie di utenti che potranno accedere alla rete aziendale (utenti interni, ospiti, personale tecnico, etc) e sulla base delle loro caratteristiche abbiamo creato dei profili a cui corrispondono delle particolari visibilità all'interno della rete.

NAC – Gestione Guest (I)



- La gestione dei Guest avviene come segue:
 - L'ospite entra in azienda e si reca alla reception per la registrazione;
 - La reception oltre alle normali operazioni di registrazione chiederà all'ospite se vorrà usufruire dell'accesso ad Internet;
 - In caso positivo compilerà un campo della scheda di registrazione che genererà automaticamente una mail al servizio di Help Desk interno;
 - Il personale tecnico provvederà a creare un account che verrà inserito nell'unità organizzativa dei guest; successivamente contatterà l'ospite per fornirgli le sue credenziali;

NAC – Gestione Guest (II)



- Analogamente quando l'ospite uscirà dall'azienda e la reception chiuderà la scheda di registrazione, verrà generata una seconda mail sempre diretta all'Help Desk;
- A seguito di questa mail il personale tecnico provvederà a disabilitare l'account creato
- L'account, come consuetudine, verrà disabilitato e non cancellato per mantenere i log delle attività
- Se gli ospiti sono dei tecnici di manutenzione verrà creata una VPN interna per permettergli di raggiungere esclusivamente i loro apparati

NAC – Il processo di autenticazione (I)



- Il processo di autenticazione avviene come segue:
 - Appena si collega un endpoint alla rete, viene inviata allo stesso una richiesta di credenziali ed una chiave di cifratura da utilizzare nei successivi scambi di informazioni.
 - Per gli endpoint aziendali sarà lo stesso sistema operativo Windows a fornire (in maniera trasparente all'utente) le credenziali (login e password di accesso alla LAN), mentre per gli altri endpoint comparirà una finestra con la richiesta di inserimento dei dati.
 - Una volta ricevute le credenziali, il server NAC le invierà al sistema di autenticazione del dominio Microsoft (Active Directory) per verificare che l'utente esista, sia attivo e la password sia corretta.

NAC – Il processo di autenticazione (II)



- Se le informazioni sono corrette il server NAC fornirà attraverso l'apparato di rete a cui è collegato l'endpoint tutti i parametri (corrispondenti al profilo) e permetterà l'accesso.
- In caso contrario provvederà a disabilitare la porta di accesso.

NAC – Compliance dell'endpoint (I)



- Non è sufficiente che l'utente si colleghi alla rete in modo autorizzato per garantire la sicurezza della stessa, è necessario che anche l'endpoint possieda determinate caratteristiche di sicurezza. Qui interviene il secondo componente del sistema per la compliance dell'endpoint;
- L'architettura di questo componente è la seguente:
 - Un modulo software (agent) installato sugli endpoint che verifica in tempo reale che la configurazione dello stesso sia aderente alle policy stabilite centralmente;
 - Una console di gestione che distribuisce l'agent sugli endpoint e verifica che sia attivo, distribuisce le policy di sicurezza definite centralmente, riceve gli allarmi di non compliance, genera report.

NAC – Compliance dell'endpoint (II)



- I controlli che lo strumento è in grado di effettuare sull'endpoint sono:
 - Verificare che sia presente, sia attivo e aggiornato un antivirus
 - Verificare che siano installate tutte le patch di sicurezza relativamente al Sistema Operativo utilizzato
 - Verificare che non siano installati e/o in esecuzione prodotti software non autorizzati o potenzialmente pericolosi (blacklist)
 - Verificare la presenza di eventuali file specifici
 - Verificare la presenza di specifiche chiavi nei registri
 - Verificare la presenza di specifici processi in esecuzione
 - Verificare lo stato di attivazione del personal firewall

NAC – Compliance dell'endpoint (III)



- Le azioni che possono essere attivate a seguito della non compliance di un endpoint sono:
 - Allarme - viene generato un avviso sulla console di gestione e, opzionalmente, inviata una mail o sms al personale tecnico;
 - Isolamento – oltre all'allarme sopra citato la console di gestione impone alla rete di isolare l'endpoint
- La verifica di compliance non viene effettuata solo nel momento dell'accesso in rete dell'endpoint ma l'agent locale effettua un controllo continuo sulla stessa.
- Analogamente, se l'agent locale si accorge che nell'endpoint isolato sono state corrette le non conformità, comunica di riammetterlo nella rete.

NAC – Compliance dell'endpoint (III)



- Attualmente nel database interno delle applicazioni controllabili sono presenti 1.600 prodotti software. Altri possono essere definiti dall'amministratore.
- I report a disposizione includono lo stato generale di conformità di ciascun utente e i dettagli sulla sessione, compreso lo stato di conformità di ciascuna applicazione installata sul computer. I report possono essere visualizzati in tempo reale o storicizzati.



Grazie

MARCO FAGIOLO