]HackingTeam[

SPARKASSE

CASSA DI RISPARMIO
SPARKASSE

PROGETTO NETWORK ACCESS CONTROL

SOLUZIONE UAC

Juniper NETWORKS

MILANO

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate

INFORMAZIONI		
Data di Emissione		
Versione		
Tipologia Documento	Allegato Tecnico	
Numero di Protocollo		
Numero Pagine	9	
Numero Allegati		
Descrizione Allegati	1	
	2	
Redatto da	Roberto Banfi	
Approvato da		

INDICE

1 Obiettivo

Lo scopo del presente documento consiste nel descrivere le soluzioni proposte da Hackingteam per quanto riguarda l'implementazione di una infrastruttura per il controllo e il monitoraggio dell'accesso alla rete da parte degli PC di Sparkasse e di consulenti temporanei. In particolare, la soluzione NAC permette al cliente di utilizzare le funzionalità essenziali di sicurezza a livello network, oltre che a permettere il controllo rispetto alle regole di conformità della banca, ed eventualmente di rendere conforme il PC prima che acceda alla rete di produzione.
La soluzione NAC proposta permette l'accesso alla rete aziendale in piena sicurezza utilizzando un client installato sui PC. Grazie a questa funzionalità è possibile accedere alla rete in modalità sicura e profilata, garantendo il rispetto delle politiche di sicurezza imposte dalla Banca.

2 Ambiente di riferimento

Le soluzioni proposte hanno il grande vantaggio di non impattare particolarmente sull'infrastruttura informatica aziendale esistente. In particolare la soluzione UAC non necessita cambiamenti sostanziali alla rete preesistente del cliente infatti è sufficiente integrarla con l'ambiente attualmente in uso. Dato che l'infrastruttura implica una metodologia di controllo dei computer collegati alla rete, si rende necessaria una modifica della configurazione degli apparati di rete, per permettere eventualmente le fasi di rimedio.
Verrà installato un apparato che si occuperà di gestire gli eventi di accesso alla rete, verifica dei client ed altri apparati e attività di "remediation o enforce".
Nella seguente figura è riportato uno schema di rete semplificato dove viene mostrato il posizionamento degli apparati proposti nella nostra soluzione.

3 Analisi dei requisiti

Riportiamo di seguito gli obiettivi della soluzione presentata nel presente documento:

- l'infrastruttura per l'implementazione UAC si baserà sul protocollo 802.1X. Tutti gli apparati di rete dovranno supportare il protocollo 802.1X
- protezione della fase di accesso alla rete Sparkasse di tutti i PC; i computer verranno dotati di un client "Odissey Access Client" per effettuare l'accesso e la comunicazione tramite protocollo 802.1X
- riconoscimento dei Computer Sparkasse durante la fase di accesso alla rete, tramite una specificata chiave di registro (dove possibile effettuare la modifica);
- riconoscimento e profilazione dei sistemi appartenenti alla rete Sparkasse che non prenderanno parte alle fasi del NAC, ma verranno identificati in altra modalità (per esempio tramite il MAC Address nel caso di stampanti o similari);
- controllo lato client dello stato dell'antivirus (UP/DOWN) e livello di aggiornamento. Nel caso in cui il PC non sia conforme, dovrà essere possibile un intervallo di tempo in cui rendere adeguato il livello di sicurezza della postazione (intervallo di update)
- controllo lato client dello stato di aggiornamento di windows update. Nel caso in cui il PC non sia conforme, dovrà essere possibile impostare un intervallo di tempo in cui rendere adeguato il livello di sicurezza della postazione. (intervallo di update)
- segnalazione e/o monitoraggio dello stato dei sistemi windows, sia essi client che postazioni server. Il livello di monitoraggio è legato alle politiche di sicurezza della Banca.
- segnalazione/blocco di eventuali tentativi d'accesso fraudolenti.
- riconoscimento e spostamento automatico nell'area "ospiti" riservata ai consulenti occasionali, con accesso limitato/segregato.

4 Descrizione della soluzione

Di seguito riportiamo in dettaglio le soluzioni proposte.

4.1 Juniper Infranet Controller 4500

Questa soluzione concentra le funzionalità utili per garantire la sicurezza dell'infrastruttura informatica per quanto riguarda il livello di accesso alla rete. Questo sistema permette di "colloquiare" con gli apparati di rete e i client Odissey, tramite il protocollo 802.1X e gestire gli eventi di accesso network.

Il cuore della infrastruttura UAC è l'Infranet Controller che è un apparato hardenizzato, un sistema centralizzato di gestione che tramite l'agent UAC (Odissey Client) può ottenere informazioni come l'autenticazione dell'utente, lo stato di sicurezza dell'endpoint. In base a queste informazioni può produrre delle regole dinamiche da propagare verso i dispositivi di accesso (es: firewall). Inoltre permette il controllo del dispositivo prima che intervenga la fase di autenticazione dell'utente e anche durante la fase di login. L'infranet controller ha integrato un sistema Radius denominato Juniper Networks Steel-Belted Radius che supporta le transazioni 802.1X quando gli endpoint si collegano alla rete. L'Infranet Controller centralizza la fase di controllo prima dell'autenticazione, l'autenticazione stessa, il mappaggio dei ruoli e il controllo delle risorse della postazione. Questo dispositivo può gestire migliaia di connessioni simultanee e può essere configurato in alta affidabilità per garantire sempre il servizio. Il sistema inoltre ha la possibilità di permettere l'installazione remota del client UAC che può essere preconfigurato, tramite Odyssey Client Administrator e scaricato sulle postazioni. È possibile distribuire il client tramite altri sistemi di software distribution. Inoltre questo sistema permette di controllare i dispositivi "non gestibili", come stampanti di rete, sistemi di controllo dei flussi di cash, apparati VoIP , tramite l'autenticazione del media access control (MAC) via RADIUS, in combinazione con white e black list di MAC address.

4.2 Odyssey Access Client

Per implementare una infrastruttura di UAC è necessario installare sui PC un client che permetta la comunicazione iniziale in fase di "up" della scheda di rete, tramite il protocollo 802.1X.

- Protegge le risorse grazie a criteri a livello granulare basati su utente ed endpoint specifici;
- Connette la postazione dell'utente nella VLAN specifica, dopo un controllo effettuato.

Il client UAC permette di raccogliere le credenziali sia del dispositivo che dell'utente e controllare lo stato di sicurezza del computer. Inoltre, dopo aver comunicato tramite protocollo 802.1X con l'infranet controller, permette di interagire con il personal firewall di Windows per creare delle politiche dinamiche di "enforce", oppure includere le funzionalità della VPN IPsec presente, per instaurare dei canali sicuri verso altri sistemi IPSec o integrare tramite single sign-on (SSO) la fase di login al dominio Microsoft Active Directory.

L'agent UAC ha integrata la funzionalità di Host Checker, che permette di definire le politiche di controllo sull'endpoint che si sta connettendo alla rete, controllando lo stato di applicazioni come Antivirus, Antimalware, Personal Firewall. È possibile inoltre creare dei controlli personalizzati di elementi come chiavi di registro, controllare l'MD5 per verificare la validità di una applicazione.
Inoltre è possibile controllare lo stato di aggiornamento delle signature dell'antivirus e la definizione del livello di patch installate sul sistema.

5 Descrizione degli impatti

Per implementare l'infrastruttura UAC è necessario eseguire i seguenti passi:

- Configurazione switch 802.1X
- Configurazione delle VLAN Guest, VLAN Remediation, VLAN Enforce sugli tutti switch
- Configurazione UAC Agent da distribuire
- Definizione dei controlli da effettuare sugli endpoint.
- Definizione delle politiche di remediation
- Definizione delle politiche di enforce
- Profilazione di tutti i dispositivi non gestibili, come stampanti e similari, tramite la raccolta dei MAC address

Se un computer non appartenente alla Banca Sparkasse accede alla rete, viene automaticamente posizionato nella VLAN Guest. In questa porzione di rete avrà la possibilità di accedere solamente ad un'area di scambio, con protocolli ben definti.
Se un computer appartenente alla Banca Sparkasse accede alla rete e risulta non conforme alle politiche, per permettergli di esegure la fase di remediation è necessario posizionarlo nella VLAN Remediation, che opportunamente ruotata e filtrata dal firewall, permetta la fase di aggiornamento dell'antivirus e/o effettuare l'operazione di windows update.
Nel caso la fase di remediation non vada a buon fine, l'apparato che ha tentato l'accesso alla rete risulta non conforme alle politiche aziendali e di conseguenza viene posizionato nella VLAN di enforce.

6 La metodologia

Di seguito vengono elencate le macro attività del progetto UAC:

6.1 Laboratorio di simulazione

Il laboratorio servirà per simulare l'implementazione dell'infrastruttura UAC, in un ambiente limitato, ma coprirà tutti gli aspetti del progetto e verrà simulata una filiale tipo.

6.2 Rilascio su due ambienti pilota: filiale medio/piccola, filiale medio grande.

Una volta verificati con buon esito tutti i punti principali durante la fase di laboratorio, verrà effettuato un primo rilascio dell'infrastruttura su due filiali, una di medio piccola e l'altra medio grande. In questa fase verranno affrontate tutte le problematiche non emerse durante la fase di laboratorio. Durante questa fase sarà necessario distribuire i client UAC preconfigurati sui sistemi windows delle filiali pilota, catalogare i dispositivi non gestibili e configurare sull'IC l'autenticazione di questi sistemi tramite l'indirizzo MAC. In questa fase si consiglia di configurare le politiche di accesso in modalità monitor senza bloccare o impedire l'accesso alla rete.

6.3 Corso operativo

Il corso operativo, predisposto per 5 operatori e della durata di 3 gg full-time, sarà specifico per l'infrastruttura realizzata e focalizzato a rendere le persone autonome nella gestione del sistema a regime.

6.4 Presidio start-up

Dopo che le filiali pilota saranno operative, si consiglia un ns. presidio tecnico di un paio di giorni.

6.5 Presidio di Deployement - Monte Giornate

Dopo che verrà distribuita la configurazione, si consiglia di prevedere delle giornate aggiuntive di supporto con fatturazione a consuntivo mensile.

7 Considerazioni

L'infrastruttura UAC assicura la protezione uniforme per l'accesso alla rete e il rispetto della conformità delle politiche definite dalla Banca. Un ulteriore vantaggio della soluzione Juniper è la presenza in tutte le filiali di Firewall Juniper. In questa situazione è possibile sfruttare l'integrazione tra Infranet Controller e i firewall in modo tale da creare regole di controllo anche dinamiche, coprendo la sicurezza dal livello 2 al livello 7.

Un altro vantaggio dell'infrastruttura è quello di facilitare una possibile ampliamento della rete dal punto di vista dell'introduzione di access point WIFI. In questo caso, i controlli attualmente implementati verranno solamente "spostati" di un livello.