



In conformità alle nuove norme l'Università di Pisa adotta una soluzione d'avanguardia per la riduzione dei costi e la protezione delle proprie reti

Cisco Network Admission Control garantisce nuove e potenti funzioni di sicurezza che si integrano con i componenti di sicurezza preesistenti per creare una Self-Defending Network

DESCRIZIONE AZIENDA

Nome cliente

Università di Pisa

Settore

Istruzione

Luogo

Italia

Numero di utenti della rete

Oltre 10.000

Obiettivi

- Soddisfare le nuove norme obbligatorie in materia di sicurezza (c.d. "Decreto Pisanu", decreto legge 27 luglio 2005 n.144 convertito con la legge 31 luglio 2005 n.155 "Nuove norme per il contrasto del terrorismo internazionale e della criminalità")
- Migliorare la protezione della rete universitaria
- Rendere la rete una piattaforma di sviluppo futuro

Soluzione

- Cisco Network Admission Control consente di automatizzare il riconoscimento, l'autenticazione, l'autorizzazione e il ripristino di tutti i metodi di accesso, compresi quelli LAN, WAN, wireless e da remoto
- Basato sulla visione Self-Defending Network di Cisco, fornisce alle organizzazioni un'architettura che consente di ottimizzare e valorizzare gli investimenti tecnologici pre-esistenti invece di sostituirli

Risultati

- Prima implementazione del genere in Italia che stabilisce un nuovo standard nella gestione della sicurezza per grandi reti universitarie utilizzando risorse IT limitate
- Strategia dai costi contenuti che consente l'adeguamento alla normativa legale e la riduzione dei rischi contro la contrazione e diffusione di infezioni da worm e virus
- Riduzione del downtime e delle possibili interruzioni delle attività di insegnamento, studio e ricerca al fine di garantire un servizio di qualità agli utenti e un migliore utilizzo delle risorse IT a disposizione
- Possibilità di espansione per supportare la creazione già programmata di una nuova rete wireless cittadina

Il Contesto

Nelle università un numero sempre crescente di attività di ricerca, di funzioni essenziali di istruzione e di comunicazioni hanno attualmente luogo attraverso la rete universitaria. Tuttavia, con migliaia di utenti, terminali e applicazioni costantemente in uso, sta diventando sempre più difficile proteggere le reti universitarie. Inoltre, i tempi di propagazione si stanno riducendo così come i tempi di risposta a un attacco prima che questo causi danni su vasta scala.

In un sondaggio condotto da Gartner¹ e The Chronicle of Higher Education quasi tutti gli intervistati hanno dichiarato di aver avuto esperienze di attacchi di virus e worm nell'ultimo anno; il 73% ha anche affermato che il problema è in aumento. Gli attacchi, inoltre, stanno diventando sempre più pericolosi. Il 53% ha riferito che gli attacchi hanno tentato di paralizzare le reti universitarie mentre il 41% ha confermato che gli hacker sono riusciti a penetrare nei loro sistemi.

La Sfida

In Italia, l'Università di Pisa conosce bene questi problemi. La sua rete rappresenta una piattaforma collaborativa per l'istruzione e la ricerca che connette e include 55.000 studenti e circa 4.500 dipendenti distribuiti su 11 facoltà, 55 dipartimenti e 130 diversi siti. Grazie a più di 9.000 km di cavi in fibra ottica, tutta l'infrastruttura (di cui l'università è l'unica proprietaria) gioca un ruolo molto importante anche per la città. Gestita da Serra, il ramo dell'università che si occupa delle telecomunicazioni, essa dà origine a reti private virtuali che servono comunità omogenee di utenti disperse geograficamente sul territorio.

¹ Best Practices for Justifying and Allocating Higher Education Security Resources, 14 Febbraio 2006, Gartner

Grazie a questo modello innovativo, la rete viene condivisa fra processi o comunità con un diverso livello di criticità: da quelle ad alto grado di riservatezza (come quelle connesse all'area sanitaria o cittadina), ad altre che richiedono un'alta affidabilità (telesorveglianza, telecontrollo), a quelle istituzionali cioè connesse alle attività di ricerca e didattica; ambienti, questi ultimi, notoriamente aperti e basati su scambio e reciprocità. Nonostante la condivisione infrastrutturale la rete deve essere in grado di garantire ad ogni comunità o ad ogni processo le caratteristiche di sicurezza richieste dalle specificità intrinseche.

Recentemente, per l'Università di Pisa la sicurezza è divenuta ancora più importante. La crescita delle attività criminali e terroristiche a livello mondiale ha determinato l'introduzione in Italia di nuove leggi atte a proteggere le reti e le informazioni. In seguito all'approvazione del cosiddetto 'decreto Pisanu' (decreto legge 27 luglio 2005 n.144 convertito con la legge 31 luglio 2005 n.155 'Nuove norme per il contrasto del terrorismo internazionale e della criminalità'), oggi è obbligatorio per i provider sapere esattamente e documentare chi utilizza la rete, quando e per quale motivo. Ciò implica la registrazione obbligatoria degli indirizzi IP, dell'ora, delle date e dei comportamenti degli utenti. Tali informazioni devono essere conservate per un periodo di cinque anni (v. <http://www.parlamento.it/parlam/leggi/05155l.htm>).

“Considerato un numero di utenti così elevato ed eterogeneo, volevamo ridurre i rischi adottando un approccio più olistico ai problemi della sicurezza. Non potevamo fare tutto questo usando sistemi proprietari e software open source. Sarebbe stato troppo costoso gestire la manutenzione di questi modelli e troppo difficile variarne le dimensioni; inoltre, non sarebbe stato possibile attuare politiche gestite centralmente in rete”.

—Stefano Suin, Dirigente dell'Area Servizi rete di Ateneo - SERRA



Stefano Suin, Dirigente dell'Area Servizi Rete, spiega: “Considerato un numero di utenti così elevato ed eterogeneo, volevamo ridurre i rischi adottando un approccio più olistico ai problemi della sicurezza. Non potevamo fare tutto questo usando sistemi proprietari e software open source. Sarebbe stato troppo costoso gestire la manutenzione di questi modelli e troppo difficile variarne le dimensioni; inoltre, non sarebbe stato possibile attuare politiche gestite centralmente in rete”.

Soluzione Di Rete

Come per molti altri centri universitari pubblici, cercare di raggiungere l'eccellenza accademica diminuendo i costi è un obiettivo costante per l'Università di Pisa. Per questo motivo, era fondamentale trovare una soluzione che assicurasse elevata disponibilità e, allo stesso tempo, costi contenuti. "Per noi era essenziale rimanere entro limiti di spesa competitivi". Stefano Suin aggiunge: "Dovevamo proteggere i nostri investimenti ICT e quindi la nuova soluzione avrebbe dovuto completare piuttosto che sostituire le soluzioni per la sicurezza e la gestione della rete preesistenti".

Dopo avere accuratamente esaminato le varie proposte del mercato e un attento studio delle possibilità offerte dal software open-source, l'università ha scelto la soluzione Cisco® Network Admission Control (NAC), uno dei capisaldi della strategia Self-Defending Network di Cisco, e il suo approccio alla sicurezza basato sull'intelligenza distribuita. Alla base di questo approccio vi è la possibilità di consentire alle organizzazioni di identificare, prevenire e rispondere alle possibili minacce tramite un'architettura di sicurezza comune che risulti:

- **Integrata:** ogni elemento della rete agisce da punto di difesa.
- **Collaborativa:** sinergia di varie reti e componenti di sicurezza per creare nuovi sistemi di protezione.
- **Adattativa:** metodi comportamentali innovativi in grado di riconoscere e adattarsi automaticamente ai nuovi tipi di minaccia nel momento in cui insorgono.

Cisco NAC Appliance è una potente soluzione per la sicurezza. Permette agli amministratori di rete di autenticare, autorizzare, riconoscere e ripristinare gli utenti e le loro macchine collegate via cavo, wireless e da remoto, prima che accedano alla rete. La soluzione Cisco NAC Appliance riconosce se i dispositivi in rete come portatili, telefoni IP o console giochi sono conformi alle politiche di sicurezza e corregge eventuali vulnerabilità prima di consentirne l'accesso in rete. L'aspetto più importante consiste nel fatto che questa soluzione può sfruttare sia un'infrastruttura Cisco, sia integrarsi con componenti eterogenei preesistenti di altri produttori.

Diversamente dai prodotti open source, l'Università è stata in grado di utilizzare una soluzione "pronta all'uso" per ottenere una maggiore possibilità di dimensionamento affiancata da un team tecnico di specialisti qualificati per l'assistenza in fase di progetto e di realizzazione. Un gruppo di specialisti della sicurezza e di sistemisti Cisco ha infatti aiutato a sviluppare una soluzione che rispondesse alle esigenze specifiche della rete universitaria pisana. È seguita poi un'implementazione graduale, che si è conclusa con una verifica positiva e un estensivo periodo di prova di sei mesi che ha coinvolto 1.500 utenti al fine di mettere a punto le configurazioni software. La soluzione è attualmente in fase di attuazione e riguarda un centinaio di siti e più di 3.000 utenti.

“Per noi era essenziale rimanere entro limiti di spesa competitivi. Dovevamo proteggere i nostri investimenti IT e quindi la nuova soluzione avrebbe dovuto completare piuttosto che sostituire le soluzioni per la sicurezza e la gestione della rete preesistenti”.

—Stefano Suin, Dirigente dell'Area Servizi rete di Ateneo - SERRA

Grazie a una visione unica e capillare della rete e a un set di funzioni di sicurezza dinamiche, l'università adesso può:

- Riconoscere gli utenti, i loro dispositivi e il loro ruolo nella rete nella fase di autenticazione, prima che eventuale codice maligno possa causare danni o propagarsi in rete.
- Migliorare la visibilità sugli endpoint e automatizzare le procedure di riconoscimento per garantire che i dispositivi gestiti, non gestiti, ospiti e sconosciuti soddisfino le politiche di sicurezza differenziate in funzione della classe di utenti a cui appartengono. Ciò può includere software antivirus o anti-spyware specifici, aggiornamenti del sistema operativo o patch.
- Assegnare diritti diversi a differenti tipi di utenti, di dispositivi o di sistemi operativi. Ciò è utile per esempio, per soddisfare le diverse esigenze di docenti, amministratori, studenti e visitatori.
- Far rispettare le politiche di sicurezza bloccando, isolando e riconfigurando in maniera automatica i dispositivi non conformi.

“La soluzione Cisco NAC Appliance è estremamente efficace. Ci garantisce una perfetta integrazione dei nostri sistemi e dispositivi di sicurezza ed è molto semplice da implementare. Inoltre, essendo parte della Self-Defending Network Cisco, rappresenta una piattaforma logica per poter sviluppare in futuro servizi di sicurezza più avanzati senza dover affrontare costosi aggiornamenti tecnologici o potenziamenti”.

—Stefano Suin, Dirigente dell'Area Servizi rete di Ateneo - SERRA

Risultati

Traendo vantaggio dalla propria reputazione di leader nel campo della tecnologia, l'Università di Pisa ha sviluppato un modello in grado di dimostrare che una vastissima rete universitaria può essere protetta e gestita in modo efficace utilizzando risorse IT limitate.

Ciò è stato possibile grazie al fatto che il sistema NAC (Cisco Network Admission Control) ha permesso di ottenere la conformità normativa riducendo al contempo la complessità, i rischi e i costi relativi alla protezione di reti di queste dimensioni. Un esempio è rappresentato dal fatto che il sistema automatico di riparazione e aggiornamento dei dispositivi ha sostituito la necessità della presenza di un tecnico sul posto per eseguire interventi localizzati. Dovendo dedicare meno tempo alle attività amministrative, il team IT adesso è libero di concentrarsi sulle attività che possono realmente aggiungere valore all'università e beneficio agli utenti.

Ridurre la capacità di virus e worm di penetrare nella rete universitaria significa contribuire alla riduzione del downtime e delle interruzioni nelle attività di insegnamento, studio e ricerca. Inoltre, il sistema NAC di Cisco ha fornito un modello di gestione e un piano di intervento per affrontare i picchi di domanda dei servizi di rete. Grazie alle migliorate funzioni di sicurezza, in caso di traffico eccessivo, l'università può ora ridefinire le priorità degli utenti in modo da ottimizzare le risorse disponibili e mantenere la qualità del servizio per le applicazioni critiche o gli utenti privilegiati.

Sviluppi Futuri

Il passaggio al sistema NAC di Cisco ha significato anche la costruzione di una solida piattaforma di sviluppo futuro. L'università sta progettando di utilizzare il suo investimento ampliando la soluzione per gestire una nuova rete wireless cittadina. Ciò aiuterà a fornire il servizio a un numero ancora maggiore di utenti mediante la creazione di 150 punti di accesso wireless, pur lasciando inalterate -anzi, mutuandole- le caratteristiche di sicurezza e gestione della rete.

Stefano Suin conclude: "La soluzione Cisco NAC Appliance è estremamente efficace e garantisce un alto grado di robustezza permettendo configurazioni di ridondanza estremamente affidabili. Ci garantisce una perfetta integrazione dei nostri sistemi e dispositivi di sicurezza ed è molto semplice da implementare. Inoltre, essendo parte della Self-Defending Network di Cisco, rappresenta una piattaforma logica per poter sviluppare in futuro servizi di sicurezza più avanzati senza dover affrontare costosi aggiornamenti tecnologici o potenziamenti".

Caratteristiche Tecniche

Cisco Network Admission Control aiuta le aziende a ridurre i rischi, evitando che gli host vulnerabili ottengano e conservino il normale accesso alla rete. Il sistema Cisco NAC consente di garantire che tutti gli host siano aggiornati, ad esempio con gli antivirus, i software di sicurezza e le patch dei sistemi operativi più recenti, prima di poter accedere alla rete. È possibile isolare gli host vulnerabili e non conformi e consentire loro solo un accesso limitato alla rete fino a quando non rispondano ai criteri di sicurezza e conformità stabiliti dalle policy, evitando così che diventino sorgente o bersaglio di infezioni da worm e virus. La soluzione NAC di Cisco è utile alle organizzazioni di qualsiasi dimensione che intendono limitare l'accesso al loro ambiente solo a sistemi autorizzati e conformi, o che richiedono la verifica e il monitoraggio dell'accesso di tutti gli endpoint all'interno della rete. La soluzione riguarda tutti i metodi di accesso alla rete utilizzati dagli host, compresi gli accessi WLAN (reti di aree locali wireless) e quelli da remoto.

Per Ulteriori Informazioni

The Cisco Self-Defending Network

<http://www.cisco.com/go/sdn>

Cisco Network Admission Control

<http://www.cisco.com/go/cca>

Eleno Prodotti

- Cisco NAC Appliance



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0704R)