Avira Success Story

A caccia di virus nelle terre del Sorbara

Case study del nostro cliente
Unione del Sorbara (Provincia di Modena)

ACHAB
Distribuiamo software e serenità

AVIRA
distribution partner

I Comuni dell'Unione del Sorbara (MO) hanno optato per una soluzione antivirus centralizzata per ottimizzare le risorse e massimizzare la protezione delle proprie reti di computer.

Aitec s.r.l. è un'azienda di Modena che dal 1996 opera nel settore dell'informatica. La sua attività spazia dalla fornitura di sistemi completi di PC e server alla sicurezza; inoltre Aitec opera come Internet Provider e fornisce servizi di consulenza, Web e mail server.

I clienti di Aitec sono per lo più aziende – circa all'80% – ma la struttura fornisce anche soluzioni e assistenza alle pubbliche amministrazioni di decine di Comuni, a cui offre servizi all inclusive.

L'esperienza maturata negli anni permette ad Aitec di studiare e presentare soluzioni complete per la gestione delle reti locali aziendali, offrendo il supporto tecnologico per mettere in comunicazione più sedi distaccate tramite soluzioni di tipo WAN realizzate con un'attenzione completa alla sicurezza. In questo campo Aitec è in grado di presentare soluzioni chiavi in mano che partono dalla progettazione della rete e arrivano sino all'assistenza alle attrezzature hardware, passando per tutti i punti intermedi, dai cablaggi LAN alla configurazione dei server fino alla formazione sull'utilizzo dei programmi di office automation.

Il problema: un antivirus avido di risorse e di personale

L'Unione dei Comuni del Sorbara della provincia di Modena, si è rivolta ad Aitec affinché fornisse un'alternativa in grado di ovviare alle difficoltà presentate dal software antivirus usato fino a quel momento . Marco Galli, responsabile tecnico-commerciale di Aitec, spiega: "La soluzione scelta fino a quel momento dai Comuni del Sorbara presentava diversi problemi oggettivi. Innanzitutto rendeva estremamente poco pratica l'amministrazione dei sistemi e, in particolare, l'individuazione e la rimozione dei virus: ogni PC disponeva di un proprio antivirus e ogni macchina, pur facendo parte della rete in fibra ottica che collega tutti e quattro i Comuni, era gestita individualmente". Come è facile immaginare, questo comportava un notevole dispendio di tempo ed energie per gli amministratori di sistema, che dovevano prima comunicare telefonicamente con gli utenti delle postazioni infette e poi recarsi sul posto ogni volta che il software indicava la presenza di un malware, intervenendo manualmente.

"Inoltre" – prosegue Galli - "vi era il problema della formazione del personale: un software indipendente su ogni computer, e che richiedeva l'intervento manuale nel caso in cui individuasse un virus, obbligava i dipendenti comunali ad

Sono quattro i Comuni della provincia di Modena riunitisi per dare vita all'Unione del Sorbara: Nonantola, Bomporto, Ravarino e Bastiglia. Vi sono dunque quattro sedi dislocate sul territorio, ciascuna dotata di una propria LAN e di un proprio server. In ognuna vi è poi un differente numero di client utilizzati dai dipendenti del Comune: a Nonantola sono 90, a Bomporto 60, a Ravarino 35 e a Bastiglia 25. Oltre a possedere ciascuno una propria rete locale, i quattro Comuni utilizzano un'infrastruttura a fibre ottiche per consentire le comunicazioni tra le varie sedi tramite VPN. All'interno di questa rete trovano posto complessivamente 10 file server. L'amministrazione di tutte le risorse è affidata al Centro Elaborazione Dati dell'Unione del Sorbara, che ha sede a Nonantola. Il lavoro del CED, quale parte del Sistema Informatico Associato, spazia dalle funzioni di assistenza tecnica e operativa ai Comuni dell'Unione alla fornitura di consulenza in materia informatica e comprende sia lo sviluppo di servizi per i cittadini che l'acquisto di materiale hardware e software e l'acquisizione di servizi professionali.

avere a che fare in prima persona con aspetti tecnici che in realtà non dovrebbero essere tenuti a conoscere per portare a termine il proprio normale lavoro. Così poteva capitare che un impiegato venisse colto alla sprovvista dagli allarmi dell'antivirus e non sapesse che cosa fare o, magari non avvisasse per tempo il responsabile dei sistemi. In questi casi un automatismo che sfrutti i sistemi di autoriparazione e quarantena è preferibile".

La soluzione adottata fino a quel momento dall'Unione del Sorbara era poi molto esigente dal punto di vista delle risorse hardware: occorreva un'alternativa che evitasse di dover cambiare i PC (210, contando tutti e quattro i Comuni) solo per soddisfare le richieste dell'antivirus.

Ad Aitec è stata quindi richiesta una soluzione che permettesse di amministrare in modo centralizzato le macchine presenti nelle quattro reti dei Comuni, che intervenisse in automatico sulle macchine infette e che non richiedesse risorse eccessive. Aitec ha scelto Avira AntiVir Network Bundle.

La soluzione: Avira AntiVir Network Bundle

Per scegliere un software in grado di sostituire il precedente sistema, che non forniva più garanzie sufficienti, Aitec ha dovuto tenere conto di alcune esigenze chiave: doveva trattarsi di una soluzione che lavorasse bene e senza intoppi in una struttura di rete multi-dominio, che non mostrasse problemi per via dell'interconnessione LAN/VPN e che si

potesse installare senza creare problemi a una realtà "delicata" quale può essere una pubblica amministrazione, che non può permettersi blocchi del sistema e che deve consentire ai propri dipendenti di continuare a lavorare senza farsi distrarre da questioni tecniche.

AntiVir Network Bundle è una soluzione integrata che comprende tre prodotti – il client Avira AntiVir Professional, Avira AntiVir Server e Avira Security Management Console (SMC)– i quali agiscono simultaneamente per assicurare la protezione delle macchine.

Ognuna delle quattro LAN dei Comuni dispone ora di una macchina su cui è installato Avira AntiVir Server che, oltre a fornire una protezione integrata multipiattaforma da virus, malware e rootkit, permette di reagire rapidamente ai nuovi pericoli grazie al centro di ricerca interno sul malware e si occupa di distribuire gli aggiornamenti nell'ambiente di rete.

Marco Galli, responsabile tecnico-commerciale di Aitec

Su ogni PC delle varie reti locali è poi presente il client AntiVir Professional, che si occupa di proteggere il computer in maniera discreta e silenziosa intervenendo automaticamente quando individua del malware, ponendolo in quarantena. In tal modo l'utente non viene disturbato né allarmato dall'attività dell'antivirus.

Infine esiste un'unica postazione, che è comune all'intera Unione del Sorbara, dove è installata la Avira Security Management Console: un solo server principale, da cui l'amministratore del sistema può tenere sotto controllo le attività dei software di sicurezza presenti sui quattro server e sui 210 PC delle amministrazioni comunali.

Grazie all'attività di logging e creazione dei report, Avira SMC permette al responsabile CED di rendersi conto in tempo reale della situazione delle reti che amministra. "La Console fornisce dei report con il numero di infezioni scovate su ogni determinata macchina, permettendo così di individuare i PC più a rischio o potenzialmente utilizzati in maniera poco ortodossa" spiega Fabio Baccolini responsabile del Ced. "Inoltre i report della SMC indicano quale sia il tipo di malware più diffuso, permettendo di preparare azioni mirate per proteggersi. Una volta terminata l'installazione dei software e condotto a termine il tuning iniziale, il sistema fornito da Avira si è dimostrato stabile e ha permesso di ottimizzare i tempi migliorando il lavoro".

I risultati si vedono

Prima dell'installazione della soluzione Avira, le attività relative alla sicurezza richiedevano circa 20 ore di lavoro al mese, così ripartite: il 45% del tempo era impiegato per individuare e rimuovere i virus, il 35% era dedicato all'analisi delle segnalazioni e il 20% serviva a compiere i sopralluoghi presso gli utenti. La mancanza di un sistema di monitoraggio remoto rendeva poi impossibile svolgere questa parte del lavoro, che si era così costretti a sacrificare.

Dopo l'installazione di Avira SMC il tempo necessario per rispondere alle esigenze di sicurezza è sceso a sole 10 ore al mese e l'impiego del tempo è drasticamente migliorato: ora solo il 5% viene impiegato per l'analisi delle segnalazioni e lo stesso quantitativo di tempo è utilizzato per i sopralluoghi, che quasi non sono più necessari grazie alla soluzione di monitoraggio centralizzato. L'individuazione e la rimozione dei virus ora richiedono soltanto il 20% del tempo e quanto resta – ossia il 70% - è dedicato al monitoraggio stesso, che permette di capire e prevenire i problemi.

Ora non è più necessario mantenere frequenti contatti telefonici con gli utenti per essere informati e venire a capo dei problemi causati dai virus: "Il sistema si è dimostrato robusto e stabile anche nell'ambiente di rete "misto" in cui s'è trovato a operare", conclude Galli. "Avira ha permesso di ridurre i tempi di analisi e risoluzione dei problemi, fornendo inoltre agli amministratori informazioni preventive sullo stato di salute delle macchine. Il monitoraggio remoto permette adesso di tenere sotto controllo la situazione. Prima dell'installazione di Avira si perdeva tempo due volte: una prima volta al telefono e poi recandosi fisicamente presso il PC da sistemare. Grazie al monitoraggio remoto non è più così, e si può lavorare in anticipo per risolvere il problema".

Come contattare Achab:

Achab S.r.l. – Piazza Luigi di Savoia, 2 – 20124 Milano
Tel: 02 54108204 – Fax: 02 5461894
www.achab.it
Informazioni commerciali: sales@achab.it
Informazioni tecniche: supporto@achab.it

AVIRA

Avira GmbH
Kaplaneiweg 1
88069 Tettnang
Germania

Telefono: +49 7542-500 0
Fax: +49 7542-500 3000
www.avira.com

live free.™