



COMUNE DI TERNI

DIREZIONE SISTEMI INFORMATIVI

CENTROMULTIMEDIALE
PIAZZALE A. BOSCO 3/A
05100 TERNI

TELEFONO 0744.54.41514
FAX 0744.54.41.524

Relazione di programma:

Progetto: Realizzazione di una piattaforma UTM (Unified Threat Management) nelle more del Bando prodotto da Centro di Competenza sull'Open Source (CCOS) della Regione dell'Umbria - progetti FLOSS 2010

INTRODUZIONE

Il Comune di Terni da sempre gestisce in proprio i sistemi informativi dell'Ente: dapprima attraverso l'ausilio di sistemi centralizzati, dai sistemi a schede perforate fino ai sistemi mainframe enterprise; poi nel 1999 il Comune di Terni ha dato avvio ad una profonda rivoluzione informatica iniziata con la costruzione del Sito Web Istituzionale che aveva l'intenzione di avviare un colloquio con i cittadini e le imprese anche attraverso canali moderni e innovativi e l'implementazione di nuovi servizi interni basati su server dipartimentali su rete ethernet.

Questa fase è stata curata completamente dal personale interno del CED che si trasformava contemporaneamente in Servizi Informativi, le forze messe in campo sono state sempre estremamente esigue e si è lavorato sino ad oggi in situazione di emergenza continua.

La trasformazione profonda ha portato l'ente alla sostituzione dei mainframe con diversi server dipartimentali (ora circa 30), alle nuove esigenze di interazione tra le applicazioni e il mondo esterno, sono stati inoltre sostituiti i software applicativi verticali, in un'ottica di integrazione e cooperazione applicativa, al fine di snellire il lavoro del comune e, soprattutto, di rendere più veloce gli allora lenti procedimenti amministrativi; è stata creata una rete per il collegamento di tutti i personal computer dell'ente inclusi i principali siti istituzionali quali circoscrizioni e delegazioni. Questa trasformazione ha permesso inoltre al sistema informativo comunale di erogare molti nuovi servizi ed ha predisposto la macchina comunale verso la grande sfida dell'E-Government.

Oggi la rete comunale conta del collegamento in varie modalità a tutti gli uffici , più di 1000 Personal Computer.

La situazione di emergenza sempre in corso dal 1999 non ha consentito al personale dei S.I. comunali di approntare un vero e proprio programma di sviluppo ponderato che inquadrasse le soluzioni Open Source, in un ottica di valutazione funzionale confrontandole con le soluzioni di mercato per cui gli operatori interni possedevano un sufficiente know-how.

Nonostante queste difficoltà organizzative i Sistemi Informativi sono stati sempre attenti alla possibilità di sviluppo del Software e dei Sistemi O.S. contraddistinguendosi in operatività di diffusione dell'informazione (Seminari e Workshop) e sperimentazioni interne con i prodotti di Office Automation O.S., tuttora su ogni personal computer consegnato all'utente c'è una copia

aggiornata di Open Office lasciando, nei fatti, all'utente la possibilità di scegliere l'utilizzo di questo al posto della suite di Microsoft.

IL PROGETTO

Il sistema comunale oltre ai i sistemi in rete locale, consta di quattro principali accessi ad internet per la navigazione e per i servizi + 2 accessi dedicati alle VPN di interconnessioni con alcune periferie + 2 sistemi di DataWan riservati al collegamento di rete con le periferie, sistemi di pubblicazione web generici ed altri dedicati alle applicazioni verticali, intranet ed extranet, sistemi di gestione posta elettronica , servizi di interconnessione attraverso porte applicative e gateway istituzionali.

La complessità dell'infrastruttura induce alla costituzione di un sistema integrato di sicurezza, che consenta di diminuire sostanzialmente sia i rischi sia l'attuale mole di lavoro dedicata al controllo diversificato di tutti i sistemi di sicurezza.

Il progetto presentato al Bando 2009 del CCOS, ha due scopi fondamentali per l'Ente e per i Servizi Informativi Comunali, il primo è quello di dotarsi, come evidenziato in precedenza, di un sistema unificato di sicurezza e l'altro è essenzialmente didattico e finalizzato alla formazione interna.

Infatti non si acquista un prodotto già realizzato e funzionante, ma bensì si imposta il lavoro di realizzazione all'interno di una modalità di processo formativo che culmina con la realizzazione dell'oggetto, integrato precisamente, con l'infrastruttura tecnologica dell'Ente.

L'opportunità del Bando 2009, dà la possibilità al personale dei S.I., formati esclusivamente e verticalmente su prodotti commerciali, di cimentarsi con mondi e soluzioni tipiche dell'Open Source.

Il valore che può scaturire da questa esperienza è sicuramente quello di dotare di una nuova e approfondita consapevolezza al personale interno dei S.I. sui prodotti O.S. e sulle loro funzionalità, consapevolezza che poi, può sfociare, in un atteggiamento più cosciente nelle scelte future.

OGGETTO DA REALIZZARE

Per la realizzazione dell'UTM (Unified Threat Management) saranno utilizzati i seguenti sistemi e software:

- Sistema Operativo Linux CentOS
- VPN OpenVPN
- Firewall IPTables
- IDS / IPS Snort
- Proxy Squid
- Clamav antivirus
- Spamassassin service
- Mail Server Postfix
- Scanner e-mail Amavis

L'obiettivo è quello di integrare queste diverse tecnologie allo scopo di offrire un ottimo grado di protezione su più fronti.

Nello specifico l'utilizzo di postfix+amavis+clamav permette di avere un controllo completo su tutte le email in entrata sia per quanto riguarda lo spam (spamassassin è il miglior mail filter opensource in circolazione, che grazie alla sua rete neurale che si autoevolve riduce drasticamente il numero di falsi positivi) e insieme a clamav come antivirus offre un'ottima protezione anche

contro i malware. Fondamentale e' anche il ruolo di postfix, che impostato come front end rispetto al vero server di posta lo esonera dai carichi di lavoro di filtraggio più importanti.

L'integrazione Squid+clamav oltre a consentire di effettuare web filtering con delle policy statiche, ovvero di decidere quali sono i siti visitabili e quali no, anche con la possibilità di utilizzare DATABASE di categorizzazione esterni, permette di controllare la presenza di virus su ogni pagina web visitata da parte degli utenti della rete.

IPTABLES infine oltre a bloccare staticamente il traffico in base a dei filtri sui protocolli di rete, combinato con SNORT consente di gestire ed eliminare traffico malformato e di individuare e bloccare tentativi di intrusione dall'esterno.

MODALITA OPERATIVE

Dato il carattere particolare di progettazione e di esecuzione della realizzazione informatica, che vede la forte sinergia tra ditta esterna e personale interno, la realizzazione si svolgerà con tempistiche dilatate, che possano consentire al personale interno all'Ente di seguire compiutamente il progetto e nel contempo portare avanti correttamente gli altri impegni lavorativi; si prevede un arco temporale massimo di 6 mesi.

Scelta la ditta esterna con provate esperienze sia nel campo dell'oggetto sicurezza informatica e System Integration, il lavoro procederà suddiviso in sette macro fasi di lavoro che, quando possibile, saranno temporalmente sovrapposte:

- 1) Analisi del contesto e dei requisiti tecnici: questa attività, realizzata insieme alla ditta esterna, occuperà un arco temporale di 10 giorni complessivi e vedrà impegnato il personale sistemista per un totale di ore uomo effettivamente impegnate nella misura di 32 di personale interno e 8 di personale esterno.
- 2) Progettazione esecutiva: questa attività, realizzata insieme alla ditta esterna, occuperà un arco temporale di 20 giorni complessivi e vedrà impegnato il personale dirigenziale, sistemista e di sviluppo per un totale di ore uomo effettivamente impegnate nella misura di 8 di personale interno e 16 di personale esterno.
- 3) Acquisizione risorse hardware: questa attività sarà realizzata in autonomia dal personale interno ed occuperà un arco temporale di 30 giorni complessivi (dalla stesura del capitolato alla ricezione dell'hardware) e vedrà impegnato il personale dirigenziale, sistemista e amministrativo per un totale di ore uomo effettivamente impegnate nella misura di 8.
- 4) Implementazione del sistema: questa attività, realizzata insieme alla ditta esterna, occuperà un arco temporale di 30 giorni complessivi e vedrà impegnato il personale, sistemista e sviluppatore, per un totale di ore uomo effettivamente impegnate nella misura di 48 di personale interno e 64 di personale esterno.
- 5) Test funzionale e messa in produzione: questa attività, realizzata insieme alla ditta esterna, occuperà un arco temporale di 10 giorni complessivi e vedrà impegnato il personale, sistemista e sviluppatore, per un totale di ore uomo effettivamente impegnate nella misura di 16 di personale interno e 8 di personale esterno.

- 6) Formazione del personale: questa attività, realizzata insieme alla ditta esterna, occuperà un arco temporale di 30 giorni complessivi e vedrà impegnato il personale, sistemista e sviluppatore, per un totale di ore uomo effettivamente impegnate nella misura di 144 di personale interno e 48 di personale esterno. Alle 6 giornate di corsi parteciperanno sei operatori interni.
- 7) Ottimizzazione della soluzione: questa attività, realizzata insieme alla ditta esterna, occuperà un arco temporale di 60 giorni complessivi e vedrà impegnato il personale, sistemista e sviluppatore per un totale di ore uomo effettivamente impegnate nella misura di 16 di personale interno e 8 di personale esterno.

NOTE FINALI PER IL RIUSO

Durante tutto il periodo di esecuzione del progetto, saranno realizzati e collezionati tutti documenti necessari allo svolgimento dello stesso, con commenti operativi sulle risorse e sulla scelta di risoluzione delle problematiche incontrate nello sviluppo, al fine di includerli nella relazione finale descrittiva del progetto.

Il documento sopra descritto verrà incluso in un apposito DVD contenete tutti i software utilizzati e le varie routine in codice aperto e, in conformità al codice dell'amministrazione digitale, verrà reso disponibile per il riuso gratuito a tutte le Pubbliche Amministrazioni che dovessero richiederlo.

Ulteriormente verranno anche promosse attività di comunicazione istituzionale nei confronti di altre amministrazioni pubbliche e del mondo dell'impres e dell'associazionismo.

Terni 22 Ottobre 2009

Massimo Lesina
massimo.lesina@comune.terni.it
COMUNE DI TERNI
(CED) Direzione Sistema Informativo
Fax 07445441524 - Tel. 07445441514