



SICUREZZA SOLUZIONE FIRMATA CYBEROAM PER L'ORGANIZZAZIONE SANITARIA

Croce Rossa sopra il network

Gestire le identità ed eliminare le minacce per lavorare in tutta sicurezza anche in modalità mobile, perché è proprio sul campo che i suoi addetti operano e devono poter esprimere la propria attività al massimo dell'efficacia. È l'esigenza che ha spinto la Croce Rossa Italiana (Cri) a rivoluzionare i suoi



la Croce Rossa si è rivolta a **Horus Informatica**, distributore specializzato nella sicurezza e nel networking, che ha adottato le soluzioni di Unified threat management (Utm, gestione unificata delle minacce) sviluppate da Cyberoam: «Possiamo identificare i consulenti che si collegano

sistemi di filtro e monitoraggio delle comunicazioni fra le sedi, i consulenti e le diverse realtà del volontariato nazionale: la Cri in Italia ha una rete di oltre 150 mila volontari, 2.300 dipendenti e circa 2.500 fra addetti civili a tempo indeterminato e militari in servizio continuativo, oltre a un network di collaboratori che devono mantenersi in contatto frequente con le sedi dell'associazione. Il principale nodo da affrontare è stata la sicurezza di chi si connette in modalità mobile su rete wi-fi, che rischiava di diventare veicolo di diffusione di virus e malware. Per mettere in sicurezza la navigazione internet e gli scambi di posta elettronica,

in remoto ai sistemi centrali grazie a una procedura di autenticazione dei client basata sul web che profila in modo univoco i portatili con cui si connettono, spesso differenti da quelli utilizzati per il lavoro in sede», spiega Giulio De Matteis, responsabile dei sistemi informativi alla Croce Rossa. In particolare, questa soluzione è «in grado di gestire anche l'utenza slegata dal contesto Ip», sottolinea De Matteis, ovvero la gestione degli utenti che si collegano da remoto è svincolata dal tipo di configurazione della rete, l'utente è identificato in quanto tale e non più a seconda di «da dove o con che cosa si connette». Quella di Cyberoam è l'unica soluzione Utm disponibile oggi sul mercato in grado di garantire un approccio cosiddetto «granulare» alla sicurezza dei network, perché le policy di gestione sono definite caso per caso a seconda del singolo utente e del suo device che accede ai server centrali. «La gestione user-based degli accessi e le funzionalità di intrusion prevention e antivirus sono senza dubbio i tratti più significativi della soluzione Cyberoam», conclude De Matteis, «perché ci hanno consentito di offrire alle comunicazioni mobili un livello di sicurezza e di flessibilità superiore a quello delle precedenti installazioni, che erano centrate soltanto sulla numerazione degli indirizzi Ip. E tutto questo con investimenti complessivi inferiori a quelli effettuati in precedenza».

media (badge o chiave), sono stati installati 38 cilindri digitali per gli appartamenti e 62 lettori remoti per garantire la protezione degli accessi comuni. Un software gestisce le autorizzazioni necessarie agli accessi e i residenti possono aprire tutte le porte usando un solo media, con la possibilità di memorizzare direttamente su questo l'autorizzazione d'accesso, la cui durata può essere impostata individualmente per ogni singola serratura. Oltre a questo, si ha la possibilità di abilitare accessi temporanei, per fasce orarie, organizzare gli utilizzatori per gruppi, aggiungere e togliere abilitazioni in tempo reale e garantire la possibilità di scaricare la memoria eventi.

Alessandra Merlini Colucci

Patrizia Licata