La sicurezza informatica di una rete ospedaliera in un IRCCS: evoluzione architetturale, virtualizzazione e sistemi di gestione della rete

D. Cacciari[B], D. Zotti[B], E. Sossa[B], M. Bava[A,B]
[A]Dipartimento di Elettronica Elettrotecnica ed Informatica, Facoltà di Ingegneria, Università di Trieste
[B]Servizio Informativo, IRCCS "Burlo Garofolo", Trieste
mail: bava@burlo.trieste.it

INTRODUZIONE

L'IRCCS "Burlo Garofolo" è un ospedale ad alta specializzazione e di rilievo nazionale nel settore pediatrico ed in quello della tutela della maternità e della salute della donna. Proprio il connubio tra attività di ricerca e servizi di tipo sanitario offerti genera uno scenario complesso con particolare riguardo alla gestione della sicurezza informatica di sistemi, reti e basi di dati sia scientifiche che ospedaliere.
Da un'analisi approfondita che è sempre "in itinere" sia a causa del continuo processo di innovazione e avanzamento tecnologico, sia del continuo aumento delle minacce e dei rischi associati, è emerso come occorra ripensare l'infrastruttura della rete e dei servizi connessi implementando soluzioni architetturali con lo scopo di migliorare l'affidabilità e la robustezza dei sistemi e dei servizi pensati sia per l'utenza interna (ricercatori, universitari, clinici, amministrativi) sia di quella esterna (utenti e pubblico).
Da un punto di vista operativo questo processo sta comportando una revisione di tutta l'architettura della rete interna, portando la gestione "in house" con un maggiore controllo interno da parte dello staff ICT dell'Ospedale. Le problematiche di questa serie di interventi, oltre che tecniche, sono anche di livello organizzativo e impongono incontri con i vari attori protagonisti della variegata situazione relativa sia alle reti che alla sicurezza. Inoltre il continuo supporto che deve essere dato a servizi di teleassistenza su apparecchiature e sistemi, o a soluzioni per la ricerca sanitaria impongono di proteggere al meglio le risorse e le informazioni aziendali, soprattutto in accordo alle normative di riferimento.
In particolare vengono analizzate e proposte alcune soluzioni sia di tipo topologico/architetturale della rete, sia infrastrutturali (virtualizzazione e storage) sia di tipo gestionale/di monitoraggio per un miglior utilizzo e controllo delle risorse hardware e software disponibili. Vengono mostrate alcune soluzioni che sono state utilizzate e la messa in opera di alcuni servizi per facilitare le operazioni di gestione e monitoraggio delle risorse tecnologiche.
Pur evidenziando come alcune criticità sono state affrontate e risolte, restano aperte molte problematiche connesse tanto alle scelte fatte quanto alla necessità di dover corrispondere ai crescenti requisiti relativi alla sicurezza informatica.

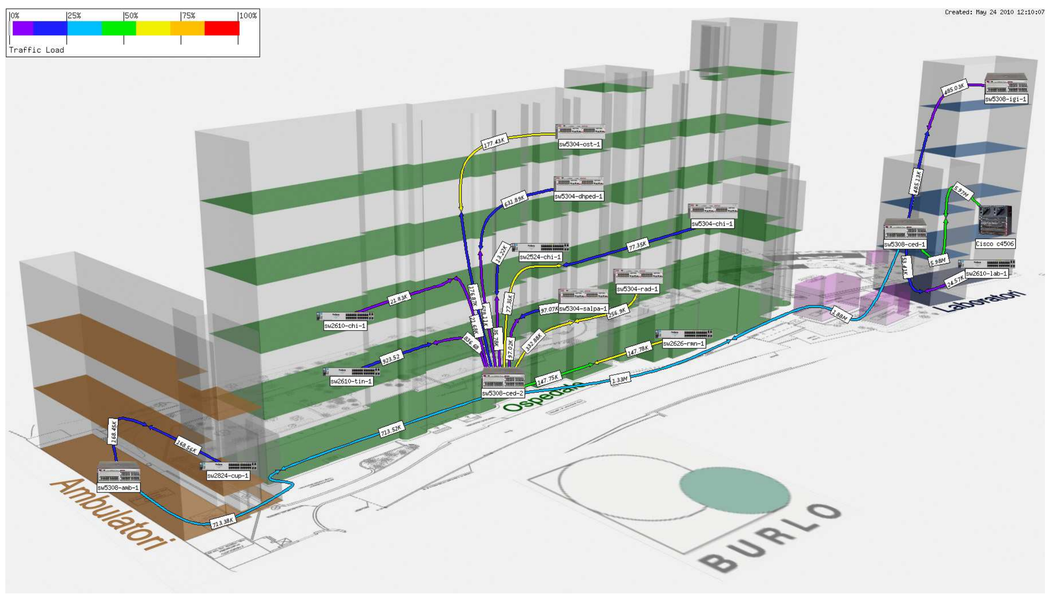

Fig 1. Sistema di monitoraggio "topografico" continuo utilizzando phpWeatherMap

RISULTATI E CONCLUSIONI

Tutti questi software sono stati integrati in una interfaccia utente con accesso solo per gli Amministratori di sistema e di rete. Questa singola interfaccia consente un'analisi più agevole all-in-one permettendo di individuare falle e problemi prima che questi vadano ad interferire sull'attività dell'utente, sia esso appartenente al personale dell'ospedale o un degente. In più, visualizzando ad un dettaglio così elevato le possibili cause dei vari problemi, si può fare in modo di rilevare facilmente guasti e problemi.
Per garantire un accesso sicuro alla rete, oltre all'attività di monitoraggio, è stato implementato il protocollo 802.1x (per quanto riguarda il wired) e il WPA AES MSCHAPv2 (per quanto riguarda il wireless) con un server freeradius completamente integrato con Active Directory.

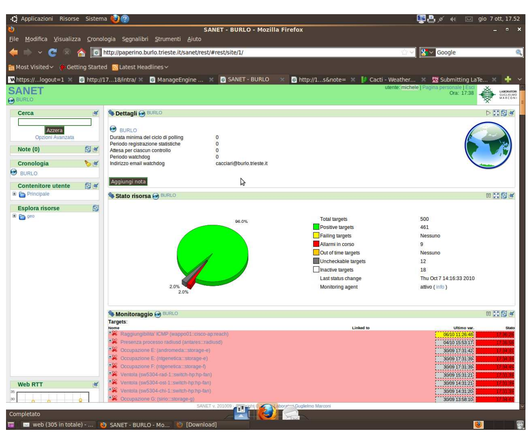

Fig 3 e 4. Oputils e Sanet

REFERENCES

[1] Bava M. et al.: Information security risk assessment in healthcare: the experience of an Italian pediatric hospital; Proceedings of the 1st International conference on computational Intelligence, communication systems and networks (CICSYN2009), Indore, India 23-25 July 2009; pp 321-326, IEEE Computer Society

MATERIALI E METODI

Innanzitutto è stata fatta un'analisi dettagliata del rischio per poter determinare le possibili falle e adottare le misure necessarie per prevenire le vulnerabilità [1]. Presso l'IRCCS "Burlo Garofolo" coesistono realtà diverse: il personale sanitario che gestisce in prima persona i dati personali e sensibili dei pazienti, i tecnici di laboratorio che devono garantire h24 le analisi necessarie e la relativa affidabilità, il personale amministrativo che accede a programmi e sistemi per il budget, il magazzino, la rendicontazione, i ricercatori che devono accedere a basi di dati e a strumenti di calcolo e analisi dei dati. A questi utenti "interni" si aggiungono e infine i lungodegenti che hanno tutto il diritto di avere l'accesso a internet, compresi alcuni servizi sulla intranet, senza però rischiare di compromettere le normali attività dell'ospedale.
L'analisi condotta ha fatto capire che la consapevolezza degli utenti e la sicurezza della rete sono i due aspetti principali per minimizzare i rischi.
La prima, considerata come aspetto "organizzativo", la si può ottenere sensibilizzando e formando costantemente gli utenti su come gestire al meglio gli strumenti informatici che sono loro affidati.
La seconda si ottiene essenzialmente in due fasi: riprogettando la rete, tenendo conto della tipologia delle singole zone migliorandone architettura ed affidabilità, e avviando una gestione intelligente della rete stessa, adottando sistemi di monitoraggio ed alert che permettano di migliorare la capacità di far fronte e risolvere problemi rilevati con l'evolversi delle situazioni.

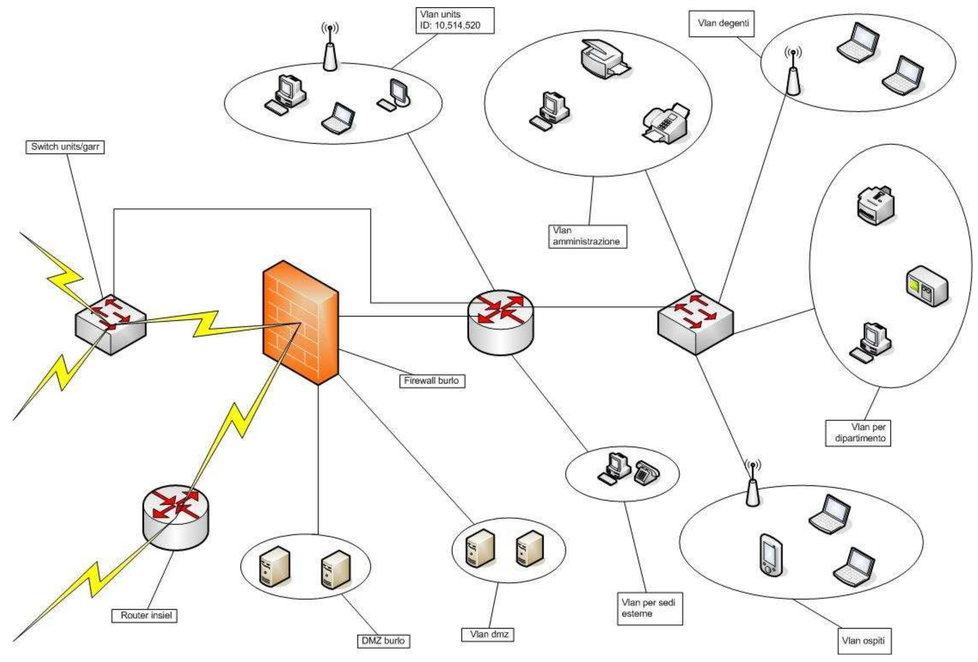

Fig 2. Nuova architettura della rete LAN del Burlo

2.1 Architettura della rete

Come mostrato in Fig. 2 si è deciso di attuare una suddivisione logica e "tipologica" della rete, creando VLAN basate sul tipo di attività svolta.
Per esempio una VLAN dedicata all'amministrazione, una per le sale operatorie; una per la terapia intensiva neonatale e una per la rianimazione, una per i laboratori, una per i lungodegenti, ecc..
Per creare queste VLAN è stata utilizzata una coppia di router CISCO4500 che funge da centro-stella.
A questa coppia di router è stata aggiunta una coppia di firewall SonicWall NSA5500 configurati in alta affidabilità che non solo gestisce l'accesso a internet dell'intero ospedale, ma anche una VLAN dedicata per i lungodegenti oncologici, esclusivamente utilizzando la rete wireless con dei CISCO air-ap1131 che devono avere l'accesso all'esterno senza alcuna visibilità della parte interna della rete.

2.2 Gestione della rete

Per la parte di gestione sono stati utilizzati singoli software opensource quali phpWeatherMap (Fig.1), Cacti (per monitorare lo stato dei singoli nodi di rete e OpUtils della Manage Engines (Fig.3).
Quest'ultimo permette di modificare la configurazione del singolo apparato, mediante il protocollo SNMP, per reagire ad un problema rilevato.
Il software SANET (Security Architecture NETwork) invece, é un NMS per esperti che integra in un solo applicativo le funzionalità di cacti e phpWetherMap (Fig.4).
Ha una WUI più user-friendly in quanto il singolo utente visualizza solo le risorse alla cui gestione è abilitato, raggruppando in un'unica pagina (Fig.4) le informazioni relative a stato, connettività e raggiungibilità dei nodi interessati. Segnalazioni di tipo visivo, sonoro, sms e mail permettono di avere un monitoraggio molto preciso e dettagliato delle risorse sotto osservazione quali interfacce di apparati, servizi sui server, occupazione dello storage, raggiungibilità ed operatività di servizi e sistemi.

2.3 Virtualizzazione

Allo stato attuale per la virtualizzazione di tutta una serie di servizi interni quali la intranet aziendale, alcuni DB relativi alla pratica clinica, i server dhcp, uno dei Domain Controller, il proxy viene utilizzato VMware ESXi su 2 SunFire X4450 equipaggiati con 2 Quad-Core Xeon X7350, 32Gb di Ram e 8 Dischi SAS da 73Gb 15krpm ciascuno. Entro l'anno è prevista l'implementazione di uno storage da 12 TB per il consolidamento dei rimanenti server (AV, Desktop management, vari File Server, server di genetica e delle immagini ecografiche).