POR CAMPANIA FESR 2014-2020

ASSE 2 "ICT E AGENDA DIGITALE"

OBIETTIVO SPECIFICO 2.2 "DIGITALIZZAZIONE DEI PROCESSI AMMINISTRATIVI E DIFFUSIONE DI SERVIZI DIGITALI PIENAMENTE INTEROPERABILI"

AZIONE 2.2.1 "SOLUZIONI TECNOLOGICHE PER LA DIGITALIZZAZIONE E L'INNOVAZIONE DEI PROCESSI INTERNI DEI VARI AMBITI DELLA PUBBLICA AMMINISTRAZIONE NEL QUADRO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ"

SOGGETTO PROPONENTE	**AO "Sant'Anna e San Sebastiano" di Caserta**
CODICE FISCALE	**02201130610**
REFERENTE PROGETTO	**Giovanni Sferragatta**

TITOLO DEL PROGETTO
Potenziamento Sistemi di Cybersecurity

DESCRIZIONE DELLE ATTIVITÀ ESEGUITE, CON EVIDENZA DEGLI ELEMENTI DI COERENZA CON LA DGR N. 354 DEL 19/06/2023 E CON L'AZIONE 2.2.1 DEL POR CAMPANIA FESR 2014-2020

Realizzazione di un'architettura basata su SD-WAN che offre sicurezza di nuova generazione e funzionalità di rete, per migliorare l'efficienza della WAN e LAN senza compromettere la sicurezza.

Potenziamento dell'infrastruttura informatica dell'AO di Caserta, basandosi sulle misure minime di sicurezza dettate dall'Agid ed aderendo così alle raccomandazioni del perimento nazionale di sicurezza e delle principali raccomandazioni internazionali (NIST). Tale modus operandi ha consentito di proteggere dal punto di vista network tutti gli endpoint, aumentando drasticamente il livello globale di protezione della rete stessa.

E' stato realizzato il primo step di modifica architetturale dei Layer 3, ad oggi configurati sull'infrastruttura di switching, ee è stato effettuato un aggiornamento tecnologico, effettuando la segmentazione della rete, utilizzando i Firewall individuati come Default Gateway di tutto il contesto IT.

La segmentazione della rete ha consentito di separare i segmenti logici e fisici di rete attraverso funzionalità di firewall. Questo approccio ha previsto di assegnare ai firewall le funzioni di routing con i conseguenti vantaggi:

- di avere completa visibilità delle caratteristiche dei flussi di traffico di rete e dei contenuti, creando un riferimento statistico utilizzabile da sistemi analisi statistica e comportamentale;
- di identificare e contenere gli attacchi ed i movimenti laterali
- di implementare politiche di routing e segmentazione estremamente granulari, basate su applicazioni/utenti/contenuti in aggiunta a quelle basate semplicemente sugli indirizzamenti IP, come avviene per i router.
- di rendere la rete agile poiché è possibile modificare politiche di routing e sicurezza in tempo reale da una consolle centralizzata (SDN-like).
- di aderire a quanto raccomandato dalla normativa NIS2 alla quale sono soggette le organizzazioni sanitarie.
- di ridurre il rischio di errori di configurazione e semplificazione operativa mediante la centralizzazione e l'automazione dell'attuazione delle policy del configuration management.

Sulla sede del'AORN "Sant'Anna e San Sebastiano" è stato installato un doppio apparato NGFW configurati in alta affidabilità.

Questa soluzione ha consentito all'Azienda Ospedaliera di predisporre l'infrastruttura tecnologica atta ad accogliere i collegamenti previsti nel progetto "Sanità Connessa".

Elenco delle attività eseguite:

- La progettazione di High Low Level Design dell'intera soluzione;
- La redazione della documentazione di site preparation;
- La definizione della strategia di migrazione, procedure di rollback e schemi di collaudo;
- La migrazione legacy dei firewall presso la sede sui FortiGate scelti per tale sede;
- La definizione delle zone sdwan e delle strategie di steering del traffico sull'HUB (application, business critical, ottimizzazione delle connettività disponibili);
- L' istallazione, configurazione e tuning del FortiManager, soluzione di management centralizzata;
- La definizione degli oggetti e le relative normalizzazioni, template di Provisioning e Policy Package per la configurazione automatizzata della sede;
- L'attività di analisi per identificazione e tuning delle policy di sicurezza attuabili attraverso Security Profile da definire nel contesto del Presidio Ospedaliero;
- Lo studio e la migrazione della sede in SDWAN.

RISULTATI OTTENUTI

L'obiettivo raggiunto è stato il miglioramento del livello di sicurezza generale dell'AO attraverso funzionalità avanzate di protezione.

La segmentazione dei contesti di rete attraverso firewall ha permesso di realizzare un'architettura Zero Trust Network Access (ZTNA) mediante l'implementazione di politiche di routing e sicurezza sulla base delle informazioni ricavate dai sistemi ZTNA al momento dell'accesso delle utenze. l'Ospedale di Caserta si è dotato di un'infrastruttura di Firewalling di FrontEnd dimensionata opportunamente per adempiere alle esigenze di gestione del traffico e sessioni degli utenti da e verso il contesto WAN.

Il dispositivi installati hanno consentito all'Ospedale di Caserta di attivare oltre alle funzioni basiche di Firewalling anche tutte le funzionalità di:

- Application Control
- WebFiltering
- SSL inspection
- Antivirus
- Antimalware

La soluzione Secure SD-WAN realizzata offre sicurezza di nuova generazione e funzionalità di rete che hanno migliorato l'efficienza della WAN senza compromettere la sicurezza, garantendo un elevato throughput VPN e il miglior rapporto prezzo/prestazioni, migliorando così le prestazioni ed i servizi offerti.