Boxxapps S.r.l.

La piattaforma "X-INFRASTRUTTURA", permette di rappresentare dinamicamente il patrimonio ITC di un'organizzazione, monitorarlo e gestirlo nella sua totalità, non solo tecnica, ma anche amministrativa.

Oggi la concezione generale dei rischi legati ai sistemi informativi è spesso limitata alla messa in sicurezza degli asset tecnologici contro attacchi provenienti dal mondo esterno ma le cause di blocco o di failure di sistemi critici per lo svolgimento dei processi di un'organizzazione sono spesso da individuare nel sistema di scelte e di gestione dell'IT inserendo di fatto il concetto di amministrazione IT, dalla formazione dell'utente finale ad un governo fatto di scelte strategiche e funzionali dell'innovazione IT che possono essere prese solo con una consapevolezza globale del proprio sistema.

Il team ha conseguito la versatilità operativa del sistema, intesa come la possibilità di interfacciarsi con tutti i sistemi operativi presenti sul mercato e le potenziali infinite configurazioni dei vari sistemi da amministrare.

Il sistema rappresenta le informazioni sia alla data attuale, sia ad un determinato momento storico pregresso e offre per esempio l'evidenza della crescita o decrescita del sistema stesso.

Inoltre il gruppo di lavoro si è concentrato sulla creazione di un forte interfacciamento sinergico tra più dati, non più considerati solo nella loro singolarità, bensì nella loro completezza e interazione per ottenere un significato completamente nuovo dell'informazione.
In particolare, il team tecnico ha dato rilevanza alla raccolta dei dati in modalità automatica da tutti i sistemi presenti nel perimetro di analisi ed ha creato uno strumento informatico, caratterizzato da differenti ed appositi algoritmi afferenti:

1. ad una gestione centralizzata degli orari della programmazione della scansione pianificata full, atta a permettere una razionalizzazione dell'utilizzo delle risorse di connessione sia del datacenter sia della banda del cliente;
2. ad un Fast Scan: ovvero all'individuazione in "tempo reale" di nuovi dispositivi connessi alla rete con la possibilità di creare di fatto un sistema di allerting innovativo per la fascia di mercato;
3. ad una Stealth mode: una gestione intelligente della funzione portscan atta a permettere la ricerca di porte aperte senza che i comuni sistemi di rilevazione firewall la rilevino e la blocchino;
4. all'inoltro dei dati criptati;
5. alla scansione delle vulnerabilità degli asset con definizione dell'intervallo di scansione per singolo asset e con la possibilità di gestire processi paralleli limitati o illimitati al fine di non saturare la LAN o sovraccaricare l'asset;
6. alla rilevazione degli utenti e delle policy applicate agli asset;

7. al governo delle policy di sistema dalla piattaforma X-INFRASTRUTTURA, con la possibilità di creare di fatto un innovativo sistema centralizzato di amministrazione e controllo delle policy distribuite su più sistemi;

8. a scansioni contemporanee su più reti;

9. a Vulnerability Assesstment (VA) automatiche, integrate con sistemi esistenti, ma in grado di interpretare i risultati in modo integrato e sinergico con tutte le ulteriori informazioni in possesso della piattaforma;

10. a mappature e a segnalazioni IT con la possibilità di gestione di un primo e secondo livello di assistenza personalizzabile direttamente dall'utente finale pur non essendo presente in Azienda.

Nel dettaglio il modulo "Mirror Active Directory" permette di avere una immagine completa e anche pregressa del dominio windows dell'ente.
Il modulo "GPResult" effettua una scansione su tutti i computer Windows della rete per elencare le policy di dominio che fossero state applicate.
L'API Rest per modulo "Mirror Active Directory" e l'API Rest per modulo "GPResult" ricevono i dati dei moduli eseguiti nell'ente remoto.
Lo staff tecnico ha sviluppato il modulo Active Directory ed il modulo GPResult in C#.
Il servizio Windows xGPTemplate preleva le policy configurate nel server di Dominio poi attraverso le API Rest del modulo GPTemplate il servizio presente nell'ente destinatario riceve le policy configurate nella propria piattaforma in modalità crittografata.
Il Modulo "Gestione Group Policy da Remoto" verifica se ci siano policy da applicare nel Server di Dominio ed applicarle.
Un algoritmo tiene conto dei risultati dell'esecuzione delle VA, al fine di poter definire delle priorità, a seconda della severità legata al danno che può infliggere vulnerabilità al sistema.

Il progetto è in continua fase di miglioramento e conta dalla sua data di avviamento, oltre 15.000 ore uomo di sviluppo, per un importo approssimativo di 600.000 € di investimento.