DIGITAL TRANSFORMATION: SECURITY

1. Descrizione progetto

Le attuali tecnologie digitali stanno trasformando il business ICT, con un numero crescente di aziende che sta adottando dispositivi Internet-of-things (IoT) e trasferendo la quasi totalità dei propri dati in ambienti cloud.
Tali tecnologie stanno di fatto spingendo le aziende a rivalutare i precedenti modelli di business, al fine di introdurne di nuovi per sfruttare al meglio la disponibilità dei dati raccolti e favorire la crescita aziendale.
La cosiddetta "Digital Transformation" riunisce al suo interno sia grandi opportunità che sfide probanti, a cui le aziende moderne devono poter fornire risposta in maniera efficace e, soprattutto, in tempi brevi.
La proposta progettuale di Key Data affronta la "Digital Transformation" nella sua declinazione in ambito "Security", ponendo dunque l'attenzione su quella che viene ritenuta la sfida più significativa e più ricca di insidie, in virtù dell'importanza che il dato, e la tutela di questo, sta assumendo nel mondo odierno.
La percezione di quanto sia fondamentale l'aspetto "Sicurezza" trova una perfetta sintesi nel risultato di un recente sondaggio condotto da Fortinet, secondo il quale a livello globale circa l'85% dei Responsabili Sicurezza IT aziendali ritiene che la trasformazione digitale porti con sé enormi rischi alla sicurezza, troppo grandi da fronteggiare con gli attuali strumenti e policy in essere (rif. Fortinet 2018 Security Implications of Digital Transformation Report).
Nello specifico, più aumentano le applicazioni, i dati ed i processi digitalizzati, maggiori sono le opportunità di intrusione per gli hacker specializzati ed altri malintenzionati.
La presenza di ulteriori potenziali punti di accesso, rende ancor più difficile per i professionisti della sicurezza IT rilevare tutte le vulnerabilità e tenere traccia di tutte le minacce.
Inoltre stanno aumentando esponenzialmente i cosiddetti "attacchi laterali", ovvero quelle tecniche di hacking che consentono di acquisire i privilegi di tutti gli utenti che sono connessi ad una macchina compromessa e, man mano, permettono di utilizzare quei privilegi per muoversi lateralmente nella rete locale alla quale la macchina stessa è connessa, applicando il medesimo attacco: ciò significa che una rete è sicura tanto quanto il suo punto più debole.
Ovviamente anche il potenziale danno causato da una intrusione nei sistemi informatici è maggiore rispetto al passato: oggi un attacco hacker potrebbe avere effetti devastanti sull'intera rete energetica di una città, oppure su strumenti ospedalieri connessi in rete, così come mettere fuori uso i nuovi veicoli che dispongono di apparati digitali sempre connessi.
Per valutare attentamente l'impatto che la trasformazione digitale può avere sulla sicurezza, Key Data ha attuato una serie di analisi sulla propria infrastruttura, con un focus specifico sugli aspetti riportati di seguito.

Sicurezza integrata: è opportuno utilizzare applicazioni e dispositivi che abbiano una protezione "nativa", ovvero progettati con sistemi di sicurezza al proprio interno tali da garantirne il funzionamento solo in presenza di policy di sicurezza avanzate, già impostate come opzione predefinita.

Formazione del personale: i ritardi nell'aggiornamento delle competenze relative alle tecnologie digitali e alla sicurezza informatica possono esporre l'azienda a minacce sempre più sofisticate, tra cui quelle basate sul fattore umano, che sfruttano un "abbassamento delle difese" alla ricezione di messaggi fraudolenti ma verosimili, poiché riguardanti le attività ricorrenti dell'azienda (mail phishing, anche via PEC, su fatturazioni, conti bancari, ricezione merci, ecc.).

Esecuzione di test periodici: condurre Penetration Test a cadenza periodica è fondamentale per scovare potenziali vulnerabilità ed introdurre tempestivamente misure di sicurezza preventive.

Automazione delle pratiche di sicurezza informatica: grazie all'impiego di applicativi evoluti, che si avvalgono dell'Intelligenza Artificiale, si possono introdurre automatismi nei processi di sicurezza, per consentire di monitorare costantemente il flusso di dati e arginare le minacce limitando comportamenti potenzialmente fraudolenti (es. autenticazione da una sede non consueta, fuori dagli orari lavorativi, mediante un dispositivo mai utilizzato prima, ecc.).

Condivisione delle informazioni sulle minacce: qualora venissero scoperte informazioni su una potenziale minaccia, è fondamentale la tempestiva condivisione all'interno dell'organizzazione, affinché tutti possano prendere provvedimenti per ridurre al minimo i rischi.

Proattività: è il fattore comune che caratterizza le azioni sopra individuate, poiché solo partendo da un approccio proattivo le aziende possono di volta in volta adeguare le proprie strategie di sicurezza e contrastare per tempo le minacce in continua evoluzione.

All'inizio del 2018 è stata rivelata l'esistenza di pericolose falle nell'architettura di numerosi microprocessori (CPU) di diversi produttori, sfruttabili mediante attacchi di tipo side-channel denominati "Meltdown" e "Spectre".
Vari test hanno dimostrato come gli attacchi consentivano di sfruttare debolezze nella tecnica di ottimizzazione delle prestazioni detta "esecuzione speculativa" (speculative execution), utilizzandola per aggirare le misure di sicurezza implementate nell' hardware dei processori di nuova generazione ed accedere ad aree di memoria protette, con conseguente potenziale divulgazione di informazioni sensibili.
Ad agosto 2019 sono state individuate nuove vulnerabilità dei processori progettati da Intel, che permetterebbero agli hacker di accedere a password, token, conversazioni private, file crittografati e altri dati sensibili degli utenti.
Durante il Def Con di Las Vegas, Bitdefender, una delle società leader nella cybersecurity globale, ha rivelato la presenza di una vulnerabilità che interessa i processori di
Intel progettati negli ultimi 8 anni.

La vulnerabilità principale, rilevata nei processori Intel prodotti negli ultimi 8 anni, è chiamata SwapGs e permetterebbe ai pirati informatici di aprire un varco verso un attacco laterale, consentendo così all'aggressore di accedere a tutte le informazioni contenute nel Kernel, ovvero il nucleo fondamentale del sistema operativo.
Essendo il processore CPU l'elemento che sovraintende tutte le attività del computer, se vulnerabile può compromettere l'intera macchina.
Al pari delle vulnerabilità Spectre e Meltdown, anche SwapGs sfrutta il particolare processo chiamato "esecuzione speculativa", la cui funzione principale è cercare di velocizzare la CPU istruendola a prevedere le istruzioni successive: tutte le informazioni non utilizzate dall'esecuzione speculativa lasciano pericolose tracce nella cache, che gli aggressori utilizzano per infiltrarsi nella memoria del nucleo del sistema operativo, basata su privilegi.
A differenza degli attacchi operati su Spectre e Meltdown, sporadicamente arginati nel corso dei mesi scorsi con patch di sicurezza risolutive, le azioni malevole verso SwapGs non hanno alcun tipo di risoluzione, rappresentando di fatto la più grave e vasta tra le vulnerabilità finora note sui processori CPU.
In considerazione dei molteplici fattori di rischio analizzati, Key Data ha ritenuto necessario operare degli interventi di securizzazione mirati, attuati in maniera sistemica ed integrata con lo scopo di ottenere un'infrastruttura in Alta Affidabilità (High Availability – HA), in cui siano pressoché eliminati i "punti critici".
Per ottenere ciò è fondamentale che i dispositivi che compongo l'infrastruttura (server, storage, router, firewall, load balancer, reverse proxy, oltre che i relativi apparati di monitoraggio) siano tutti ridondati sia a livello di network che a livello applicativo, garantendo così il massimo dell'affidabilità.

2. Finalità

Il progetto "DIGITAL TRANSFORMATION: SECURITY" di Key Data ha avuto finalità di operare una securizzazione mirata, sistemica ed integrata per ottenere un'infrastruttura in Alta Affidabilità.

3. Risultati

Di seguito i risultati conseguiti da Key Data grazie al progetto "DIGITAL TRANSFORMATION: SECURITY", cofinanziato dall'Unione Europea:

- Introduzione di due server configurati in coppia ridondata in "Alta Affidabilità", per garantire "fault-tolerance" (tolleranza e resilienza ai guasti), continuità nei servizi erogati e integrità dei dati memorizzati all'interno dell'infrastruttura.

- Aggiornamento dell'infrastruttura con introduzione nuova CPU equipaggiata con chip TPM 2.0 che consente l'elaborazione di dati cifrati nativamente. L'architettura TPM (Trusted Platform Module) prevede per ogni chip la presenza di una coppia di chiavi crittografiche uniche, che lo rendono univocamente identificabile, e di un motore per la crittografia asimmetrica per la criptazione dei dati.

- Implementazione di un Firewall virtuale per la segmentazione della rete, mediante l'introduzione della soluzione SonicWall Network Security Virtual (NSV) 50 Virtual Appliance. Tale soluzione, specifica per gli ambienti virtualizzati, offre protezione dalle vulnerabilità zero-day, blocca gli accessi non autorizzati alle risorse di dati protette, blocca azioni dannose e intrusive come la diffusione di malware, l'esecuzione di comandi del sistema operativo, l'esplorazione del file system ed introduce innovativi sistemi di sicurezza che si avvalgono di logiche basate sul "machine learning".

- Implementazione di una Storage Area Network virtuale, realizzata tramite virtualizzatore VmWare Standard Edition e gestita mediante applicativo VSAN. La sostituzione della precedente SAN fisica con una SAN virtuale scongiura i rischi derivanti dalle possibili rotture e/o indisponibilità delle unità fisiche di archiviazione.

- Conseguimento di un vantaggio competitivo nel proprio mercato di riferimento, in virtù di un'offerta a catalogo rivista e aggiornata per garantire alla clientela prodotti e servizi avanzati in conformità ai requisiti GDPR su integrità, riservatezza e disponibilità del dato.

4. Sostegno Finanziario Ricevuto

Con Determinazione n. G06133 del 22 maggio 2020, pubblicata sul BURL n. 67 del 26 maggio 2020, il Direttore della Direzione Regionale per lo Sviluppo Economico e le Attività Produttive, ha ammesso a sovvenzione, per un importo pari a € 12.500,00, il progetto "DIGITAL TRANSFORMATION: SECURITY" (Domanda prot.A0322-2019-29859), finanziato a valere sulle risorse di cui all' Avviso Pubblico "Contributi per il sostegno dei processi di digitalizzazione delle imprese del Lazio – DIGITAL IMPRESA LAZIO" approvato con Determinazione n. G08196 del 17 giugno 2019 nell'ambito del POR FESR LAZIO 2014 – 2020.