HADRIAN

CASO DI STUDIO

Gestione degli asset digitali e dei rischi nel settore dell'aviazione

Introduzione

Una multinazionale leader nel settore tecnologico che propone soluzioni software per il settore turistico e dei viaggi a livello mondiale attraverso le sue divisioni Global Distribution System (GDS) e Information Technology (IT).
Il gruppo, la cui sede centrale si trova in Spagna, la più grande base di dipendenti in Francia e il reparto tecnico in Germania, si rivolge alle aziende di tutto il mondo.
Il reparto GDS propone ai fornitori di servizi turistici soluzioni in tempo reale in tutte le aree geografiche e in tutti i fusi orari, mentre il settore IT si concentra sui software per le prenotazioni, la gestione dell'inventario e il controllo delle partenze.
L'azienda offre servizi a una vasta gamma di clienti, tra cui compagnie aeree, hotel, tour operator, assicurazioni e società di autonoleggio.

PAESI IN CUI OPERA	ORGANIZZAZIONI COMMERCIALI A LIVELLO LOCALE	DIPENDENTI
195	173	16,000

Gli ostacoli

01 **Complessità e frammentazione**

La decentralizzazione delle operazioni complicava la gestione di un inventario accurato degli asset, a causa delle diverse tecnologie e tecniche utilizzate dai vari team.

02 **Esposizione ai rischi**

A causa della mancanza di visibilità centralizzata, la frammentazione ha causato delle falle e aumentato il rischio di vulnerabilità non identificate.

03 **Gestione dei rischi legati alle vulnerabilità**

Un numero elevato di falsi positivi riscontrati dai precedenti fornitori di sicurezza informatica e le problematiche legate all'identificazione delle vulnerabilità come Log4J hanno fatto emergere diversi problemi.

04 **Problemi di integrazione nei processi di fusione e acquisizione**

L'integrazione di sistemi di sicurezza eterogenei durante le fusioni ha richiesto un coordinamento unificato della sicurezza che permettesse una gestione efficace delle complessità.

Le soluzioni

✓ **Miglioramento della gestione degli asset**

Sistema centralizzato e strumenti di scansione attiva per una panoramica unificata e in tempo reale di tutti gli asset.

✓ **Miglioramento della gestione delle vulnerabilità**

Individuazione accurata, prioritizzazione e rilevamento automatico dei rischi per ridurre al minimo i falsi positivi e consentire una gestione efficiente delle vulnerabilità.

✓ **Conformità e integrazione più rigorosi**

Standard di sicurezza unificati e monitoraggio continuo per garantire la conformità a tutte le normative in tutte le unità aziendali e le acquisizioni.

✓ **Riduzione dei falsi positivi**

Riduzione significativa dei falsi positivi per consentire al team di sicurezza di concentrarsi sulle minacce reali.

Il risultato

Crescita strategica grazie alle partnership

Il gruppo, la cui sede centrale è in Spagna e le cui attività principali vengono svolte in Francia e Germania, lavora per le aziende di tutto il mondo dal suo solido quartier generale in Europa. Da gennaio 2023 a giugno 2024, l'azienda ha annunciato 25 nuove partnership nel settore dell'aviazione e non solo, migliorando le proprie competenze tecnologiche e operative. Tra le partnership di rilievo nel settore dell'aviazione figurano importanti compagnie aeree e aeroporti come TAP, Air Canada, Virgin Atlantic e il nuovo aeroporto di Sydney.

Negli altri settori, l'azienda ha stretto 14 partnership con aziende del comparto dell'ospitalità, dei viaggi e del turismo, della tecnologia e non solo, da Accor a Microsoft. Queste collaborazioni hanno ampliato il raggio d'azione e l'abilità tecnologica dell'azienda, ma hanno anche introdotto notevoli problematiche in materia di cybersicurezza a causa del maggior numero di punti di accesso al sistema e dell'integrazione di nuove tecnologie.

Risoluzione delle problematiche in materia di sicurezza informatica

L'azienda ha dovuto affrontare diversi problemi di sicurezza informatica, tra cui il mantenimento di un inventario accurato degli asset a causa delle operazioni decentralizzate e la gestione dei rischi di esposizione derivanti dalla frammentazione dei sistemi. I metodi di scansione passiva hanno ulteriormente limitato la capacità di rilevare e rispondere ai rischi in modo efficace, tanto che l'azienda si è affidata a un fornitore precedente che ha fornito numerosi falsi positivi e non è riuscito a individuare le vulnerabilità reali.

Le acquisizioni hanno introdotto domini inutilizzati che hanno aumentato il rischio di sfruttamento, e il rispetto di normative come la legge spagnola sulla Protezione dei dati e la Legge europea sulla cybersicurezza ha richiesto una gestione accorta. L'integrazione di sistemi di sicurezza eterogenei a seguito delle fusioni ha reso necessario un approccio unificato e proattivo al coordinamento della sicurezza tra le nuove entità acquisite e le operazioni esistenti.

L’effetto di Hadrian

Le soluzioni di Hadrian hanno migliorato in modo significativo la sicurezza informatica dell'azienda, sostenendone la crescita e l'innovazione nel settore dei viaggi e del turismo. L'implementazione di sistemi centralizzati di inventario degli asset e di strumenti di scansione attiva ha fornito una panoramica unificata e un monitoraggio in tempo reale degli asset, consentendo di ridurre al minimo i falsi positivi e di individuare con precisione le vulnerabilità reali.

Il miglioramento del rilevamento e della gestione dei domini inutilizzati, unito allo sviluppo di standard di sicurezza unificati e al monitoraggio continuo della conformità, ha garantito una protezione solida e il rispetto delle normative. Con il supporto di Hadrian, l'azienda ha potuto sperimentare processi semplificati, tempi di risposta più rapidi e una transizione verso una postura di sicurezza informatica proattiva, garantendo protezione completa e conformità continua.

> **“In caso di fusioni e acquisizioni, le soluzioni di rilevamento di Hadrian sono determinanti. Se un'azienda appena acquisita non ha una buona conoscenza dell'inventario degli asset e dei sistemi di sicurezza, è necessario effettuare una scansione della superficie di attacco esterna per individuare i problemi di maturità.”**
>
> Senior Network Security Engineer,
> Client Operations

La sicurezza offensiva di Hadrian svela il modo in cui gli attacchi reali potrebbero compromettere le applicazioni e le infrastrutture. La nostra piattaforma autonoma esegue costantemente dei test per valutare in modo completo gli asset esposti a Internet. La tecnologia agentless basata sul cloud viene costantemente aggiornata e migliorata dal team di hacker etici di Hadrian.

Prenota una demo