



S.A.C.B.O. S.p.A.

Orio al Serio, International Airport

Panoramica

Settore

- Trasporti

Sfida

- Cyber-attacchi sofisticati e minacce in rapida evoluzione
- Digitalizzazione delle procedure aeroportuali
- Visibilità limitata della rete
- Minacce dall'interno

Risultati

- Rilevamento delle minacce di nuova generazione, in tempo reale
- Capacità di effettuare analisi approfondite e di mitigare i rischi
- Visibilità totale della rete
- Interfaccia Threat Visualizer con grafica 3D

Profilo aziendale

L'aeroporto internazionale "Il Caravaggio Bergamo Orio al Serio", chiamato a volte "Aeroporto di Milano Bergamo", si trova alle porte di Bergamo, città del Nord Italia, a 70 chilometri a nord-est del capoluogo lombardo. Gestito da SACBO SpA (Società per l'Aeroporto Civile di Bergamo - Orio al Serio), è il terzo aeroporto italiano con oltre 11 milioni di passeggeri in transito ogni anno. Dopo Londra Stansted, questo aeroporto internazionale è il secondo hub di Ryanair in Europa.

“

Il livello senza precedenti di visibilità e le capacità di rilevamento delle minacce di nuova generazione rendono la tecnologia di Darktrace unica nel suo genere.

Ettore Pizzaballa, ICT Manager, SACBO SpA

”

La sfida

Le più recenti innovazioni tecnologiche utilizzate in campo aeroportuale, comprese le reti Wi-Fi, il check-in online, i sistemi automatizzati per il bagaglio, i passaporti elettronici e i controlli di frontiera senza personale, hanno migliorato l'efficienza e l'organizzazione degli scali. Tuttavia la digitalizzazione delle pratiche aeroportuali è anche fonte di vulnerabilità e di possibili punti di breccia per gli avversari informatici. Questa è una preoccupazione costante per i gestori degli aeroporti, strutture già di per sé esposte agli attacchi informatici.

Come parte delle infrastrutture critiche nazionali in Italia, l'Aeroporto di Milano Bergamo rappresenta un obiettivo interessante per molti cyber-attaccanti. Come tale, la struttura ha voluto rafforzare la propria strategia di difesa informatica adottando la tecnologia più recente e innovativa attualmente disponibile.

Inoltre, l'aeroporto ha voluto dotarsi di una visibilità di rete completa, al fine di conoscere in maniera approfondita i comportamenti dei propri dipendenti e degli utenti con l'obiettivo di rilevare qualsiasi potenziale minaccia proveniente dall'interno. Dato il numero di dispositivi che quotidianamente accedono alla rete principale dell'aeroporto, era fondamentale disporre della massima trasparenza su tutte le attività.

La Soluzione

Dopo aver completato una Proof of Value di 4 settimane con l'Enterprise Immune System di Darktrace, i responsabili dell'Aeroporto di Milano Bergamo sono rimasti colpiti dalla capacità di questa soluzione di garantire il rilevamento delle minacce in tempo reale.

Alimentata da potenti funzioni di "machine learning" e da algoritmi matematici sviluppati da specialisti dell'Università di Cambridge, la tecnologia self-learning della piattaforma si ispira ai principi biologici del sistema immunitario umano. Essa ha permesso di modellare i comportamenti di ogni utente, di ogni dispositivo e della rete nel suo complesso, stabilendo un "pattern of life" specifico dell'infrastruttura informatica dell'Aeroporto di Milano Bergamo.

Utilizzando la comprensione dinamica di ciò che è da considerare "normale", la tecnologia è in grado di rilevare automaticamente qualsiasi attività che devia dalla norma e di contrassegnarla come sospetta, segnalando le anomalie al team di sicurezza dell'aeroporto; il tutto, senza dover utilizzare regole o firme. Tutti gli alert vengono presentati tramite il Threat Visualizer di Darktrace, un'interfaccia grafica 3D che fornisce anche una rappresentazione topologica della rete dell'Aeroporto di Milano Bergamo e delle attività al suo interno.

“

I Threat Intelligence Report sono preziosi per noi. Siamo in grado di condividere facilmente i risultati con il management aziendale, permettendo a tutti di comprendere cosa sta succedendo e come vengono gestiti i problemi.

Ettore Pizzaballa, ICT Manager, SACBO SpA

”

I benefici

Grazie alla tecnologia "immune system" di Darktrace, l'Aeroporto di Milano Bergamo può ora essere allertato in tempo reale in merito a comportamenti anomali che possono essere indicativi di cyber-minacce. Le funzioni di Threat Visualizer permettono al team di sicurezza dell'aeroporto di analizzare gli eventi e le loro cause andando indietro nel tempo nonché di indagare più in profondità in specifici dispositivi e di adottare qualsiasi azione di mitigazione del rischio per prevenire gravi danni.

Subito dopo l'implementazione dell'Enterprise Immune System, l'aeroporto è stato informato della presenza di alcune minacce potenzialmente pericolose. Tra queste, un proxy flash (che in precedenza era passato inosservato) e vari punti deboli nella rete che, inconsapevolmente, erano accessibili al pubblico. L'aeroporto dispone ora di una visibilità totale della rete e, di conseguenza, di una migliore comprensione dei comportamenti dei dipendenti e degli utenti.

L'aeroporto riceve inoltre dei report settimanali - Threat Intelligence Report (TIR), redatti da analisti esperti di Darktrace - che riassumono e classificano le potenziali minacce rilevate. "I TIR sono preziosi per noi. Siamo in grado di condividere facilmente i risultati con il management aziendale permettendo a tutti di comprendere cosa sta succedendo e come vengono gestiti i problemi", ha dichiarato Ettore Pizzaballa, ICT Manager, SACBO SpA. "Questo, oltre a un livello senza precedenti di visibilità e alle potenti capacità di rilevamento delle minacce di nuova generazione, rende la tecnologia di Darktrace unica nel suo genere".

Contact Us

North America: +1 415 229 9100

Europa: +44 (0) 1223 394 100

Asia-Pacific: +65 6804 5010

info@darktrace.com

darktrace.com