Case study ESET Italia - Audi Zentrum Alessandria per la gestione della sicurezza

Audi Zentrum Alessandria S.p.A., Gruppo guidato da Dindo Capello, pilota ufficiale Audi per 19 anni e tre volte vincitore della 24 Ore di Le Mans, comprende le quattro concessionarie Audi ufficiali di Alessandria, Asti, Alba e Cuneo. Negli anni il Gruppo si è saputo affermare come una delle realtà al top in Italia per i risultati, la personalizzazione dei servizi e l'attenzione al cliente. La validità e completezza dell'offerta, la professionalità dello staff e il ruolo fondamentale del Presidente Capello sono parte integrante del successo della struttura.

Esigenza dell'azienda cliente

Audi Zentrum Alessandria è un cliente storico di ESET: la collaborazione con il vendor risale al 2006 quando il Gruppo ha deciso di migrare l'intera infrastruttura di sicurezza dell'azienda alla piattaforma del vendor, per prevenire le problematiche di sicurezza già presenti oltre 15 anni fa. In un primo momento è stata affidata a ESET la protezione base dei singoli endpoint, poi con l'inasprirsi della diffusione delle minacce informatiche, il cliente ha deciso di innalzare ulteriormente il livello di sicurezza, arrivando ad adottare al proprio interno la soluzione **ESET PROTECT Enterprise**.

Fasi di sviluppo e realizzazione

Nel 2022, con il rilascio ufficiale dei servizi MDR – Managed Detection & Response, erogati in italiano da ESET Italia, il Gruppo Audi Zentrum Alessandria ha effettuato un ulteriore passo avanti nella sicurezza aziendale, scegliendo di affidare il monitoraggio e la fase di remediation al team di cybersecurity expert di ESET.

Il servizio **ESET Detection and Response Ultimate** ha rappresentato la risposta migliore alle esigenze del cliente.

A livello tecnologico le soluzioni presenti in ESET PROTECT Enterprise consentono di:

- gestire centralmente l'intera infrastruttura di sicurezza, con la console unica ESET PROTECT;
- proteggere i diversi dispositivi aziendali presenti nella rete, come computer e smartphone, grazie a ESET Endpoint Security;
- garantire la protezione dei dati presenti sui server aziendali, con ESET Server Security;
- bloccare le minacce zero-day e gli eventuali attacchi ransomware, analizzando i file sospetti attraverso la tecnologia di sandboxing in cloud (ESET Liveguard Advanced);
- proteggere i dati sensibili e riservati gestiti dall'azienda attuando un sistema di crittografia robusto e affidabile con ESET Full Disk Encryption

- identificare eventuali comportamenti anomali attraverso il modulo XDR - eXtended Detection and Response di ESET (ESET Inspect) che, collaborando con le altre tecnologie ESET presenti nell'infrastruttura del cliente, supporta l'erogazione dei servizi MDR di ESET.

Inoltre, per far fronte ai continui attacchi che sfruttavano l'email come vettore principale e per innalzare ulteriormente la sicurezza dei propri utenti e dipendenti, il Gruppo ha deciso di adottare anche la soluzione **ESET Cloud Office Security** che, attraverso la protezione delle app di Microsoft 365 come Teams, Exchange, OneDrive e SharePoint, consente di attuare i filtri anti-spam, anti-malware e anti-phishing e di gestire al meglio la quarantena attraverso una semplice console di gestione.

Risultati

Grazie all'adozione delle tecnologie ESET che collaborano e supportano l'erogazione dei relativi servizi MDR, il Gruppo Audi Zentrum Alessandria ha potuto migliorare nel tempo il livello di sicurezza dei sistemi aziendali e dei dati in essi gestiti.

Il basso impatto sulle risorse di sistema, e la possibilità di prevenire un'eventuale intrusione nella rete di minacce informatiche, sono i principali benefici riscontrati in oltre 15 anni di utilizzo delle soluzioni del vendor. A seguito dell'adozione dei servizi MDR, il cliente ha potuto beneficiare di un rapporto continuo e collaborativo con il team di esperti presenti presso la filiale locale che sono operativi H24 per mantenere sotto controllo lo stato di sicurezza della rete aziendale.

Evidenziando eventuali situazioni critiche solo nel momento del bisogno e gestendo direttamente le attività di incident response e remediation necessarie a riportare il sistema in sicurezza, l'adozione dei servizi MDR ha permesso al Team IT del cliente sia di ottimizzare il proprio tempo, andando a gestire attività che prima erano "secondarie" rispetto al monitoraggio della rete sia di potersi affidare a esperti del settore con un alto livello di expertise.

Infine, attraverso la migrazione dalla modalità on-premise, inizialmente adottata, alla modalità attuale in cloud, il Gruppo ha potuto estendere la protezione ESET anche ai dispositivi Android e iOS utilizzati dagli utenti aziendali, gestendo attraverso un'unica console i dispositivi presenti nella rete.


Zentrum Alessandria
P