HWG SABABA MDR PER AUMENTARE LA SICUREZZA DEGLI ENDPOINT DI UN PROVIDER DI SERVIZI DIGITALI



PROBLEM SOLVER srl
SERVIZI INFORMATICI E ORGANIZZAZIONE

HWG Sababa

Case study

Problem Solver

Offre soluzioni globali nell'ambito dei servizi ad alto valore aggiunto nel campo dell'Office Automation e della Digitalizzazione

È un importante player nel campo della Robotic Process Automation a livello nazionale

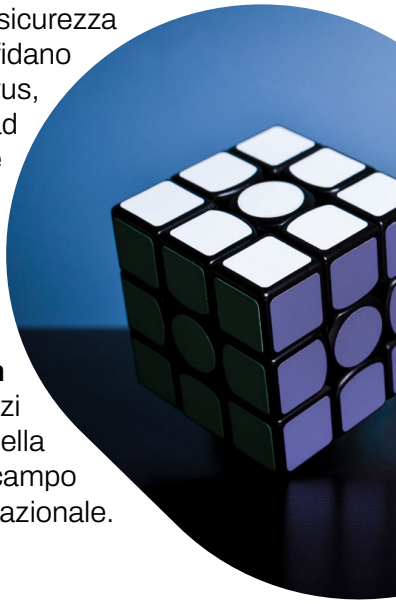
Il settore bancario rappresenta la principale area di intervento

Sfide e obiettivi

Si pensa erroneamente che le piccole e medie imprese, proprio per le loro dimensioni, siano target meno attraenti per i criminali informatici, senza considerare che gli attori malevoli sono impazienti di sfruttare proprio quelle caratteristiche che le rendono ancora più vulnerabili agli attacchi cyber.

Infatti, mentre le grandi aziende possono permettersi di assumere un team di esperti di cybersecurity per monitorare e proteggere i loro asset digitali, per le PMI - che notoriamente hanno budget limitati - questo è quasi impossibile, risultando quindi più facili da violare.

Tuttavia, dovendo rafforzare la propria sicurezza come fanno le grandi aziende, le PMI si affidano solitamente ai tradizionali software antivirus, che i cyber criminali riescono spesso ad aggirare grazie a modelli di attacco sempre più sofisticati e approfittando di team IT aziendali ridotti che non sono in grado di gestire e monitorare gli eventi di sicurezza 24 ore su 24.



La storia non è diversa per **Problem Solver**, una PMI italiana che fornisce servizi nell'ambito dell'Office Automation e della digitalizzazione, e un player importante nel campo della Robotic Process Automation a livello nazionale.

Una storia di successo

Con 150 endpoint e un team IT composto solo da tre persone altamente operative, Problem Solver ha da sempre utilizzato una soluzione antivirus di un vendor globale di cybersecurity, al punto tale da gestirla internamente ed in autonomia.

Tuttavia, per motivi legati all'attuale situazione geopolitica, l'azienda si è trovata a dover rivalutare le proprie scelte, decidendo di migrare verso una nuova soluzione.

"Nella ricerca di un nuovo provider, la nostra intenzione era innanzitutto quella di mantenere lo stesso livello di detection rate, ma al contempo di ottenere quel valore aggiunto apportato da un servizio gestito",

spiega Fabio Macchiagodena, CTO di Problem Solver.

HWG Sababa

PROBLEM SOLVER srl
SERVIZI INFORMATICI E ORGANIZZAZIONE

[1] Rapporto Clusit sulla Sicurezza Informatica 2022
[2] HWG Sababa Awareness Report 2021

hwgsababa.com

"HWG Sababa è stata una piacevole sorpresa e la proposta di migrare a HWG Sababa MDR ci è sembrata subito interessante e competitiva. La soluzione ci avrebbe permesso di monitorare e controllare molte più cose rispetto a prima e, soprattutto, di alleggerire il nostro carico di lavoro, poiché avremmo avuto a disposizione un team dedicato all'analisi degli eventi di sicurezza e alla gestione della maggior parte degli incidenti".

Dopo la POC, il progetto è andato in porto con un contratto di licenza di 3 anni e, nonostante una fase di onboarding piuttosto impegnativa a causa delle peculiarità dei sistemi operativi e delle macchine del cliente, i team di HWG Sababa e Problem Solver hanno sin da subito gettato le basi per un rapporto diretto e trasparente, che ha favorito una migrazione senza intoppi.

Ciò che è stato particolarmente apprezzato - oltre al fatto che la nuova tecnologia permetteva di mantenere il servizio di Web Reputation, la componente antivirus e il monitoraggio comportamentale già presenti nella soluzione precedente - è stato il tool di Data Loss Prevention, che ha consentito a Problem Solver di definire regole specifiche per monitorare e bloccare la trasmissione indesiderata di determinate informazioni all'esterno o addirittura all'interno dell'infrastruttura. Lavorando con le banche e gestendo molti dati sensibili, questa funzionalità ha rappresentato un vero e proprio plus per l'azienda.

HWG Sababa MDR in dettaglio: la soluzione di cybersecurity per le PMI

HWG Sababa MDR rileva costantemente malware noti e sconosciuti ed altre minacce informatiche che colpiscono le reti aziendali, riducendo così il carico di lavoro del team IT interno.
Il monitoraggio della sicurezza degli endpoint è esternalizzato ad un team di esperti SOC che analizzano gli eventi di sicurezza e gestiscono la maggior parte degli incidenti in autonomia durante l'orario di lavoro in modalità 8x5, informando semplicemente il cliente delle azioni di remediation adottate o necessarie.
In caso di un attacco di sicurezza più complesso, gli analisti sono sempre informati e applicano immediatamente le misure di contenimento, comunicando al cliente le azioni richieste di risposta all'incidente.

Qual è il valore aggiunto per l'azienda?

1. Protezione avanzata degli endpoint

- Rilevamento in tempo reale anche di attacchi complessi, invisibili alle soluzioni antivirus tradizionali
- Scansione regolare delle vulnerabilità e distribuzione degli aggiornamenti da remoto per garantire che le workstation e i server aziendali siano aggiornati

2. Monitoraggio completo della sicurezza

- Ogni cliente è supportato da un team di analisti di sicurezza, altamente qualificati nella ricerca, nel rilevamento e nella risposta al malware
- Manager personale per ogni cliente
- Supporto in italiano e risposta agli eventi di sicurezza 24x7

3. Risposta rapida agli eventi di sicurezza

- Isolamento flessibile delle macchine infette
- Notifica degli eventi di sicurezza gravi 24x7

4. Report mensile dettagliato

- Report mensile dettagliato
- Eventi malware e raccomandazioni per la remediation
- Bollettino di sicurezza con panoramica delle minacce più recenti
- Report su credenziali aziendali trapelate

Risultati

Ad oggi, il progetto è pienamente avviato. La tecnologia è supervisionata dal Managed Security Team di HWG Sababa, capace di bloccare rapidamente le minacce informatiche, di prevenire l'esfiltrazione di dati e le comunicazioni ai server C&C e di ridurre il tempo necessario per scoprire e correggere le minacce nell'ambiente dell'utente.

Inoltre, su base mensile, Problem Solver riceve report su tutti gli eventi di sicurezza rilevati.

“Ciò che apprezzo di più è il fatto di avere un team sempre disponibile. La comunicazione è rapida ed efficace e se c'è un problema viene risolto in pochissimo tempo. Il team di HWG Sababa è composto da veri professionisti e avere degli esperti a capo di una soluzione rende qualsiasi tecnologia più efficace",

ha commentato Fabio Macchiagodena,

"In caso di potenziali vulnerabilità critiche, l'avviso degli analisti è tempestivo, ma fortunatamente i pochi casi scoperti finora erano tutti falsi positivi. Questo anche perché abbiamo combinato l'introduzione di HWG Sababa MDR con una politica di firewalling completamente diversa da quella precedente, ottenendo così pochissimi alert”.

HWG Sababa

PROBLEM SOLVER srl
SERVIZI INFORMATICI E ORGANIZZAZIONE

Follow us on:

www.hwgsababa.com