POTENZIARE IL MONITORAGGIO DELLA SICUREZZA PER UN IT SERVICE PROVIDER

HWG Sababa

AKITO
IT FOR CHOICE

Selda

Case study

Selda Informatica

Società consortile a responsabilità limitata costituita nel 1983; i soci sono Fasi e Previndai[1]

Realizza e gestisce le diverse componenti dei Sistemi Informativi automatizzati dei Consorziati, ma anche di clienti esterni

I principali settori di attività sono quelli previdenziale, sanitario, assicurativo, formativo e sindacale

AKITO

Fondata nel 2016

System Integrator italiano specializzato nella Security e Cybersecurity

Indirizza i suoi servizi alle PMI, alla PA centrale e locale, ad enti ed organizzazioni presenti sul territorio nazionale

"Le persone pensano sempre che gli incidenti di sicurezza siano qualcosa che può accadere solo agli altri, finché non colpiscono un settore o un'azienda a loro vicina. Questo è ciò che spesso provoca un cambiamento nell'approccio alla cybersecurity, ma a volte è già troppo tardi"

Domenico Vitulli, Head of Systems, Networks and Technological Infrastructure di Selda Informatica

[1] Fasi (Fondo Assistenza Sanitaria Integrativa), Previndai (Fondo di Previdenza a Capitalizzazione per i Dirigenti di Aziende Industriali)

Negli ultimi anni, la criminalità informatica è diventata una minaccia sempre più incombente per le aziende di tutte le dimensioni, tanto che si prevede che i costi globali derivanti da questo fenomeno aumenteranno da 8,44 trilioni di dollari nel 2022 a 23,84 trilioni di dollari entro il 2027. Per raggiungere queste cifre, i criminali informatici accedono illegalmente ai sistemi, rubano i dati e li vendono o li trattengono in cambio di un riscatto, sfruttando diversi metodi, come phishing e attacchi malware.

Pertanto, la protezione dei dati e delle infrastrutture digitali non è più un'opzione. Soprattutto se sei un'azienda che gestisce quotidianamente dati sanitari e previdenziali dei tuoi clienti.

È qui che entra in gioco **Selda Informatica**, una società consortile fondata nel 1983 che conta oltre 30 dipendenti. In parallelo alla gestione informatica dei Consorziati, Selda svolge anche attività esterne per i clienti che gravitano nel mondo dirigenziale dei settori previdenziale, sanitario, assicurativo, formativo e sindacale.

L'importanza di proteggere i dati

La cybersecurity è sempre stata un tema di primaria importanza per Selda Informatica, tanto che l'azienda ha iniziato a prendere in considerazione il monitoraggio della sicurezza già dalla fine degli anni '90. Proprio per questo motivo, quando si sono resi conto che le competenze interne in materia di security non erano più sufficienti a monitorare l'intero perimetro aziendale - reso ancora più esteso dalla pandemia - si sono rivolti al loro partner di fiducia, **Akito**, con cui collaborano da oltre 6 anni.

"A differenza di quanto è accaduto a molte aziende, non è stata la pandemia a cambiare il nostro approccio alla sicurezza. Per noi questo è sempre stato un aspetto fondamentale del nostro business, proprio perché abbiamo quotidianamente tra le mani dati sensibili."

ha commentato Domenico Vitulli, Head of Systems, Networks and Technological Infrastructure di Selda Informatica

"In Selda tendiamo a gestire tutte le attività internamente, affidandoci raramente a terze parti. Tuttavia, quando ci siamo resi conto di quanto il monitoraggio stesse diventando complesso e, allo stesso tempo, di quanto la superficie di attacco si stesse ampliando, abbiamo deciso di esternalizzare questo processo. Insieme ad Akito, nostro security partner da sempre, abbiamo iniziato a considerare il SOC."

Nella fase di scouting sono stati presi in considerazione diversi fornitori e, nonostante la giovane età e le dimensioni allora ridotte di HWG Sababa, la scelta è ricaduta sul suo servizio SOC.
La grande flessibilità e le solide competenze tecniche dimostrate sin dalle prime fasi della proposta sono stati due elementi decisivi per Selda Informatica.

Nel vivo del progetto

Nonostante la situazione geopolitica sempre più tesa e le conseguenti pressioni interne per accelerare l'attivazione del servizio, la fase di onboarding si è svolta rapidamente e senza intoppi, in un contesto di trasparente collaborazione tra HWG Sababa, Selda Informatica e Akito. Data la necessità di un rapido avvio del progetto, la fase iniziale ha visto il monitoraggio degli elementi più critici - come Active Directory e firewall - e l'avvio delle attività di Threat Intelligence.

"All'inizio di marzo 2022 abbiamo svolto il nostro primo incontro tecnico di persona. È stata una cosa che abbiamo molto apprezzato perché abbiamo avuto l'opportunità di visitare il SOC e di conoscere i nostri partner, cosa che ritengo fondamentale per poter poi lavorare bene da remoto."

ha commentato Roberto Vasari, Systems Architect di Selda Informatica

"Si è trattato di un deployment parziale, iniziato col monitoraggio dei sistemi più critici e aggiungendo gradualmente i restanti."

Il SOC in dettaglio

Fornendo un importante aiuto nell'erigere un'efficace difesa per i dati, il Security Operations Center è responsabile del monitoraggio, del rilevamento, dell'analisi e della risposta agli incidenti e alle minacce che possono prendere di mira gli ambienti IT e OT di un'organizzazione.

Grazie a tecnologie avanzate come SIEM, SOAR e Threat Intelligence, gli analisti SOC di HWG Sababa individuano gli eventi di sicurezza, ne analizzano e valutano la gravità e adottano le opportune misure per prevenire o mitigare potenziali incidenti di sicurezza, monitorando gli ambienti digitali dei clienti 24x7.

Composto da oltre 70 cybersecurity expert, il SOC è così organizzato:

- **Security Manager.**
  È il principale interlocutore per il cliente, con una visione completa e la piena responsabilità dello stato del servizio. Questo profilo è coinvolto nelle fasi di incident management e nei review meeting.

- **Proactive Detection Team (livello 1 e livello 2).**
  Team di analisti di sicurezza che identifica le minacce indirizzate all'infrastruttura digitale, monitorando continuamente l'alert queue, eseguendo il triage degli avvisi di sicurezza e svolgendo un'analisi approfondita degli attacchi. Il team gestisce gli incidenti di sicurezza, determinando se un sistema o un set di dati critici è stato colpito, occupandosi della remediation e fornendo supporto nello sviluppo di nuovi metodi analitici di rilevamento delle minacce.

- **Competence Center (livello 3).**
Disponendo di conoscenze approfondite su rete, endpoint, threat intelligence, analisi forense, reverse engineering, nonché sul funzionamento di applicazioni specifiche, il Competence Center agisce come un cacciatore di incidenti. Essendo attivamente coinvolto nello sviluppo, nella messa a punto e nell'implementazione di metodi analitici di rilevamento delle minacce, esso aiuta a risolvere gli eventi di sicurezza più complessi.

La **reportistica** è un'altra componente chiave del servizio. Giornalmente sono disponibili report generati automaticamente, mentre gli analisti di HWG Sababa forniscono in aggiunta quanto segue:

- **Report settimanale:**
descrizione dettagliata degli avvisi settimanali e report personalizzati richiesti
- **Report mensile:**
overview mensile del servizio, che include anche una sezione sugli executive members
- **Report annuale:**
overview annuale del servizio

Risultati

Il progetto è iniziato a marzo 2022 e gli analisti di HWG Sababa si sono dimostrati sempre pronti a rilevare e contrastare gli attacchi informatici.

"Attraverso i sistemi di monitoraggio sono state evidenziate su alcuni client attività anomale, ma questo comportamento non si è concretizzato in un incidente perché l'antivirus ha bloccato sul nascere ogni azione non lecita. In questo episodio abbiamo coinvolto gli analisti di HWG Sababa e abbiamo apprezzato la rapidità con cui hanno analizzato il problema e fornito le indicazioni per mettere in sicurezza i client che erano stati compromessi."

ha commentato Domenico Vitulli,

"Il SOC ha monitorato tutti gli eventi per confermare che il tentativo di compromissione era fallito e che successivamente non se ne erano verificati altri."

Nell'ambito del servizio, Selda Informatica riceve report giornalieri, settimanali e mensili, questi ultimi destinati a fornire una panoramica delle attività, verificando quanti ticket vengono aperti, quanti eventi generati, se è necessario correggere qualche fonte di log in termini di SIEM ed altro ancora.

"È un continual service improvement che tiene in considerazione anche le nuove minacce emergenti."

ha commentato Roberto Vasari,

"La disponibilità e la flessibilità di HWG Sababa ci hanno garantito un servizio su misura per le nostre esigenze, e questa tempestività da parte loro è stata una conferma di quello che avevamo capito già in fase di scouting: proprio per le sue dimensioni, HWG Sababa è in grado di fornire un'attenzione e una cura particolare ai suoi clienti, a differenza dei grandi player del mercato che a volte sono troppo rigidi."

HWG Sababa

AKITO
IT FOR CHOICE

Selda

Follow us on:

www.hwgsababa.com