Sababa Expert Services

Per le esigenze specifiche delle aziende

Gli Expert Services di Sababa Security forniscono alle aziende una visione chiara e inequivocabile del loro stato di sicurezza e aiutano a comprendere meglio i loro bisogni e le aree di miglioramento. Il processo può richiedere tempistiche diverse, pochi giorni o anche mesi, a seconda della verticalità, la dimensione e la complessità delle aziende e comprende diverse fasi di intervento:

- *Fase preliminare di colloquio per definire le richieste, gli obiettivi e i timori in termini di sicurezza aziendale*
- *Strutturazione degli oggetti di rete e mappatura delle loro relazioni*
- *Test della sicurezza aziendale*
- *Verifica della conformità alle normative vigenti e sviluppo di policy di sicurezza*
- *Programma di training per incrementare le competenze di sicurezza informatica dei professionisti IT e OT*

Al giorno d'oggi le tecnologie digitali supportano le aziende a prescindere dalla grandezza o dalla verticalità del business. Andando bel oltre le reti aziendali tali innovazioni trasformano radicalmente i processi OT ed industriali, integrando veicoli connessi, droni, piattaforme IoT e sistemi cyber-fisici alle loro infrastrutture connesse. Gli obiettivi principali della cyber security sono quelli di implementare misure efficaci per prevenire incidenti di sicurezza e contrastare gli attacchi informatici, garantendo la continuità, la protezione dei dati dei clienti e la conformità alle normative vigenti. Dal momento che le reti aziendali possono essere complesse e presentare difficoltà di interazione, servono competenze specifiche e grande esperienza per identificare i gap di sicurezza, e implementare efficacemente le soluzioni corrette. Gli Expert Services di Sababa Security foniscono supporto per implementare la cyber security secondo modalità elaborate su misura per ciascuna azienda, anche in ambienti particolari e sensibili. L'attività di diagnostica è completa e include servizi di security assessment e penetration test e altri servizi di consulenza utili a costruire una solida base per un

percorso virtuoso all'insegna del miglioramento continuo. Infatti, con i servizi di Sababa Security, le aziende ottengono dei benefici immediati:

- riescono ad articolare meglio i loro obiettivi e a comprendere le necessità in relazione alla cyber security
- Smettono di tirare ad indovinare e ottengono una fotografia attendibile della loro "cyber security posture", incluse le vulnerabilità, le problematiche relative a configurazioni approssimative e alle conformità con le normative vigenti evidenze di cyber attacchi in corso o avvenuti in passato
- Dimostrano di essere conformi agli standard industriali e di mettere in atto le migliori pratiche in termini di sicurezza informatica
- Ottengono un supporto da parte di esperti per eliminare in modo organizzato tutte le lacune e sviluppare adeguate policy di sicurezza
- Migliorano le competenze dei dipendenti in termini di sicurezza informatica

Fase 1. Investigazione

Colloquio. La prima fase di diagnostica di sicurezza informatica inizia con un'analisi tecnica e un colloquio con il reparto IT dell'azienda allo scopo di collezionare le informazioni iniziali sull'infrastruttura aziendale, gli obiettivi del progetto operativo, i timori sullo stato della security attuale e le considerazioni sui potenziali attacchi informatici. Ciò fornisce una panoramica della situazione, delle pratiche in atto relative alla sicurezza informatica e il livello di consapevolezza all'interno dell'azienda. Al fine di definire al meglio gli obiettivi a dar loro la corretta priorità, viene coinvolto in tale fase il personale in rappresentanza dei diversi team all'interno dell'azienda.

Security maturity model. Basato sulle informazioni raccolte, gli attributi e gli indicatori, viene valutata la maturtà della sicurezza della rete. Questo dato riflette il livello di sicurezza corrente e permette di definire il livello di sicurezza desiderato insieme al progresso costante delle misure di sicurezza implementate.

Fase 2. Strutturazione e mappatura

Inventario. Metodi attivi e passivi vengono utilizzati per valutare i target analizzati, stabilirne dinamiche di funzionamento e gerarchie nella rete. Quando è necessario valutare ambienti critici come quelli industriali, è fondamentale adoperara con cautela strumenti di indagine che potrebbero causare problemi all'operatività. Tutti i dispositivi

non gestiti devono essere analizzati prontamente per capire come interagiscono con la rete.

Mappatura. Quando gli oggetti di rete sono noti è necessario individuare i loro punti di accesso esistenti, sia quelli fisici che quelli remoti, incluse le persone e le loro credenziali di accesso. Per alcuni ambienti, come quelli industriali dove l'eccessiva fiducia è una causa comune di problematiche legate alla security, è importante capire la disponibilità di questi oggetti ad interagire con altri oggetti.

Fase 3. Testare La Security

Security Assessment. Una cattiva gestione della configuazione della security che si traduce in punti di accesso aperti vulnerabili agli exploit è uno dei pi comuni problemi di sicurezza insieme agli errori umani e agli attacchi informatici. Il security Assessment contribuisce a identificare i gap di sicurezza esistenti e potenziali attraverso le reti IT e OT, le comunicazioni, le piattaforme IoT. Basato su differenti scenari di minaccia, fornisce visibilità sulle vulnerabilità di hardware e software, le lacune e i pericoli per l'infrastruttura con lo scopo di valutare i rischi e le tempistiche per mitigarli.
Penetration Test. Una dimostrazione pratica di quanto forti siano le misure di sicurezza adottate e può essere condotto con diversi metodi di violazione. Lo scopo è quello di ottenere i massimi privilegi del sistema informatico e della rete aziendale, partendo da credenziali di accesso iniziali differenti. Le tecniche utilizzate per eseguire il pentest sono molteplici e variano a seconda della criticità dell'ambiente in cui viene condotto. Per la conduzione degli attacchi è possibile simulare sia quelli one-way che quelli di red team.

Fase 4. Valutazione

Controllo di conformità. Le policy di sicurezza vigenti vengono valutate in base alle best practices e agli standard di conformità locali e internazionali, comprese le specifiche normative di settore e quelle generali, come il GDPR. Viene analizzato il contesto aziendale, si definiscono le sottocategorie standard obbligatorie, si identificano i profili di rete e si conduce un'analisi sui gap di sicurezza.

Sviluppo delle Policy. Le nuove policy e quelle aggiornate si basano sui risultati del percorso di valutazione e degli standard di conformità richiesti. Oltre a framework specifici relativi agli ambienti automotive, industrial, telco e altri settori verticali, vengono utilizzati quelli generali come il NIST Cybersecurity Framework. Quest'ultimo è ampiamente utilizzato ed accettato in settori diversi e in più territori, fornendo linee guida tecniche e organizzative, basate sul sistema di gestione del ciclo della cybersecurity rappresentato dal modello: "Identify-Protect-Detect-Respond-Recover".

Definire una roadmap di intervento. Il Security Assessment e i risutati del Penetration Test, nonché i requisiti normativi sono di fondamentale importanza e presenti in una roadmap dettagliata che descrive le fasi per l'eliminazione dei gap di sicurezza e le relative tempistiche.

Fase 5. Formazione

Formazione. I training di Security Awareness sono concepiti per ridurre la quantità degli incidenti di sicurezza causati dall'errore umano. La formazione può essere erogata sia ai professioni dei reparti di Information Tecnology (IT, operational tecnology (OT e information Security (IS che agli altri dipendenti aziendali di reparti differenti. Consiste in una combinazione di approcci formativi differenti che includono diversi tecniche di apprendimento, attacchi simulati e un'approfondita formazione interattiva per incrementare le competenza di sicurezza informatica. L'obiettivo è di modificare l'atteggiamento dei dipendenti stimolandoli a lavorare in modo sicuro e responsabile per dare solide fondamenta alla cultura della sicurezza a livello aziendale.