Sababa Incident Response

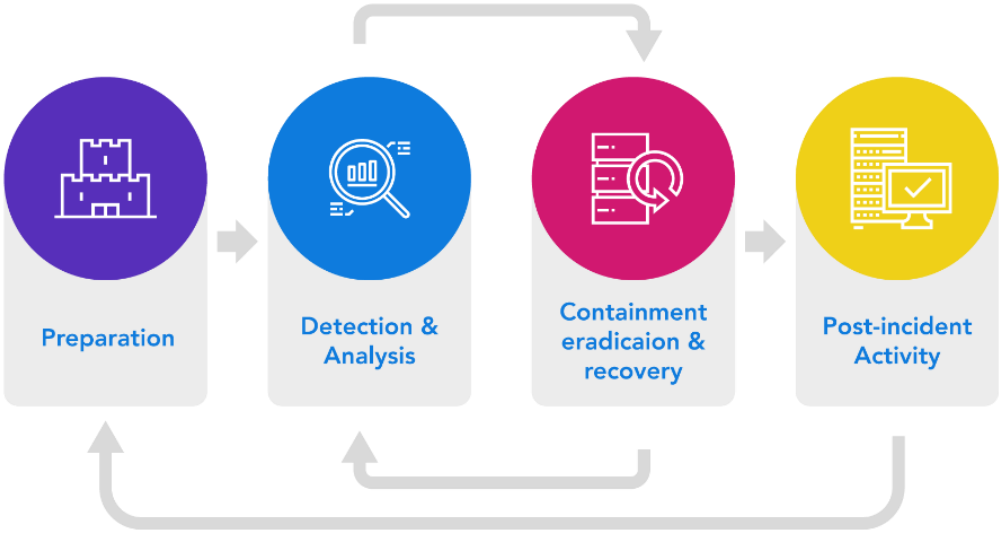
Pronto intervento per il tuo business in caso di cyber emergenza

"Se serve un medico chiama il 118", "in caso di incendio non utilizzare l'ascensore" tutti noi conosciamo queste regole. Anche se la probabilità di trovarsi in una di queste situazioni è, per fortuna, relativamente bassa, sappiamo esattamente come comportarci: abbiamo cioè un piano di emergenza."

Anche gli incidenti di sicurezza informatica necessitano di un piano di emergenza per ripristinare al più presto l'operatività aziendale, è auspicabile quindi che in azienda esistano già procedure consolidate per gestire gli incidenti informatici. Ad ogni modo, come per qualsiasi emergenza, l'obiettivo principale è quello di reagire in tempi brevi, in quanto ogni minuto è prezioso per mitigare gli impatti negativi (operativi, finanziari, reputazionali) che l'incidente potrebbe avere sul business.

Sababa Incident Response è un "pronto intervento" per supportare la tua azienda in caso di incidente informatico. I nostri analisti, con competenze specifiche nel settore dell'incident response, operativi 24 ore su 24, 7 giorni su 7, possono intervenire rapidamente per fermare un attacco e ripristinare la tua operatività. In conformità al regolamento UE 2016/679 (GDPR); al Decreto Legislativo 231/01 e al Codice Etico, sono in grado di gestire l'incidente di sicurezza secondo la linee guida del NIST coordinando tutti gli attori coinvolti nel processo (es. DPO, system integrator, i fornitori delle soluzioni di sicurezza utilizzate) e fornendo supporto anche per gli eventuali adempimenti di legge.

Il servizio Incident Response di Sababa Security può essere attivato in qualsiasi momento, anche quando l'attacco è in corso o già terminato, tuttavia è consigliabile sempre agire in anticipo, anche quando non si rilevano evidenze di un attacco imminente.



Il servizio di Incident Response prevede quattro fasi fondamentali:

- **Preparazione** – Questa fase prevede l'analisi degli asset critici, stabilire le priorità sia dal punto di vista operativo sia in merito alla protezione dei dati personali. Mettere in piedi una serie di processi e procedure che consentano di monitorare l'attività abituale e di rilevare un incidente nel minor tempo possibile. Preparare la stesura di un incident response plan che descriva le procedure da seguire per gli incidenti più probabili. All'interno dell'incident response plan vengono stabiliti anche ruoli, modalità di comunicazione e strumenti di analisi da utilizzare in caso di incidente
- **Analisi e Rilevamento** – in questa fase l'incidente viene rilevato e gli esperti di Sababa Security intervengono per analizzare le evidenze e scoprire l'eventuale vettore di attacco. I log dei dispositivi coinvolti vengono analizzati, una serie di valutazioni determinano quali azioni intraprendere nelle fasi successive.
- **Contenimento, eradication e recovery** – questa fase richiede rapidi e precisi interventi per bloccare l'attacco, contenerlo e ripristinare l'operatività nel minor tempo possibile. Questa attività prevede sostanzialmente la bonifica dei sistemi e il ritorno ad una situazione di normalità

- **L’attività di Post-Incident** – detta anche “lesson learned” è uno step molto importante perché oltre alla redazione della reportistica che spiega come è avvenuto l’attacco, prevede una serie di attività che consentono di analizzare nel dettaglio l'incidente, come è stato gestito e quali migliorie possono essere apportate al processo di incident handling e all’incident response plan.

Ecco come funziona il servizio Sababa Incident response in caso di cyber-emergenza:

Identificazione del tipo di attacco
Per prima cosa valutiamo la situazione per capire se l’attacco sia terminato o meno. Nel caso in cui l’attacco fosse ancora in corso, valutiamo in sinergia con il cliente, una strategia di contenimento per limitare l’eventuale compromissione di dati e servizi.

Stima dell’impatto e pianificazione recovery
In stretta collaborazione con il management, analizziamo l’impatto sull’operatività generale e nel dettaglio quello a breve termine, sulle attività e i servizi interessati dall’attacco. Infine stabiliamo le priorità dei processi critici, pianifichiamo le azioni di recovery e la modalità operative più adatte alla circostanza.

Valutazione dell’impatto sulla riservatezza dei dati personali
Gli esperti di Sababa Security, insieme al vostro Data Protection Officer (DPO) effettuano un’indagine per capire se eventuali dati personali siano stati violati. Se necessario offrono supporto per effettuare tempestivamente e nel modo corretto tutti gli adempimenti previsti dal GDPR.

Raccolta dei dati relativi all’incidente
In questa fase raccogliamo tutte le informazioni utili per comprendere il vettore di attacco e le vulnerabilità utilizzate, i cosiddetti movimenti laterali, l’escalation sui privilegi e altro. Per fare ciò raccogliamo i log di rete e quelli dei dispositivi coinvolti (es. endpoint, active directory, ERP ecc.). Se necessario produciamo copie forensi dei sistemi compromessi o preserviamo i log utili alla ricostruzione dell’accaduto con un’ulteriore analisi approfondita. Identifichiamo gli host da cui sono partiti gli attacchi e i possibili canali di comunicazione, analizziamo lo stato dell’attività e mettiamo in sicurezza le parti dell’infrastruttura non compromesse.

Indagine sull’attacco

Una volta individuate le risorse violate, se necessario, viene condotta l'analisi forense, studiando gli indicatori di compromissione (IOC), al fine di ricostruire in modo accurato la cronologia e gli strumenti utilizzati per condurre l'attacco. Provvediamo anche alla redazione della reportistica con tutti i risultati che possono essere utili per le fasi di ripristino e di "lesson learned".

Ripristino

In questa fase raccogliamo ogni informazione e configurazione utile al ripristino in sicurezza dei sistemi e a delle attività. La priorità è quella di ristabilire la sicurezza dell'infrastruttura nei tempi più rapidi possibili partendo da un'operatività limitata ed abilitando progressivamente i servizi e i processi in accordo con le priorità stabilite.

Lesson learned (cosa abbiamo imparato)

Una volta ripristinate le attività principali, viene organizzato un meeting detto "lesson learned" il cui obiettivo è quello di discutere dell'accaduto. In questa occasione vengono valutare le policy e le procedure da mettere in campo (o da rivedere) per evitare che si possano verificare in futuro incidenti analoghi. Durante questo incontro gli esperti di Sababa Security sono a disposizione per rispondere a tutte le domande relative all'incidente e forniscono supporto per le eventuali modifiche da apportare all'incident response plan