Gestione degli incidenti

Obiettivo:

Dopo esserti confrontato con l'analisi dei rischi informatici nell'elaborazione di un Risk Assessment, dovrai affrontare la gestione di un potenziale pericolo in azienda!

Brief progetto:

La tua SFIDA sarà infatti quella di GESTIRE UN INCIDENTE DI SICUREZZA.
Concentriamoci sull'esercizio ;)
Tra le principali responsabilità di chi ricopre ruoli di responsabilità in campo IT, c'è quella di gestire gli eventi di sicurezza che potrebbero impattare l'azienda.
Ai fini di una corretta gestione degli eventi non previsti è necessario specificare la differenza tra evento di sicurezza, incidente di sicurezza e data breach:

Evento: Un evento è un episodio osservabile in un sistema o in una rete, consistente in un cambiamento osservabile all'interno del comportamento abituale di un sistema o di un processo.

Incidente: ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi, è una violazione o una minaccia imminente di violazione delle politiche di sicurezza e di utilizzo lecito degli strumenti tecnologici, è un evento che produce effetti negativi sulla confidenzialità, integrità o disponibilità dei dati all'interno di un'organizzazione e/o che impatti negativamente sui processi dell'organizzazione stessa.

Violazione dei dati personali (Data Breach): è un Incidente, che riguarda o coinvolge, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dall'organizzazione.

Ecco la situazione in cui ti trovi:

La vostra azienda è stata attaccata!
Un Ransomware ha cifrato tutti i dati contenuti nei vostri sistemi aziendali!

Se il riscatto non verrà pagato, gli attaccanti non solo non sbloccheranno i vostri dati ma informeranno i media dell'accaduto e metteranno in vendita i vostri dati nel surface (spazi pubblici sul web) e nel dark web!

Divisione in Gruppi

Questo progetto prevede l'esecuzione in gruppi di 2 o 3 persone, nello step successivo ti spieghiamo come funzionerà la creazione dei gruppi.

Istruzioni

Il gruppo di cui fai parte dovrà gestire l'incidente di sicurezza delineando una strategia da seguire per far fronte all'evento ed identificando le attività da compiere al fine di mitigare gli impatti, sia verso l'esterno, che interni.
Ognuno dei 2 o 3 componenti del gruppo avrà un ruolo ben definito. Una suddivisione dei ruoli all'interno di un gruppo, dove ognuno si occupa di un aspetto specifico risulta fondamentale per gestire al meglio un evento di sicurezza in tutte le sue fasi.
Ciascun membro all'interno del gruppo dovrà redigere un documento (output) specifico!

Ruolo 1: IHAU (Incident Handling Assessment Unit)
Raccoglie tutte le segnalazioni ed ha la responsabilità di effettuare una prima valutazione dell'incidente e di coinvolgere le altre funzioni interessate come ad esempio il CISO e il DPO.
L'output consisterà in una identificazione ed una classificazione dell'incidente, i quali dovranno essere comunicati all'IRT e al MARIT mediante un report sintetico.

Ruolo 2: IRT (Incident Response Team)
Provvede a porre in essere le misure tecniche e organizzative al fine di mitigare e contenere l'incidente.
Inoltre si occupa di delineare le attività di recupero e ripristino.
L'output consisterà in una lista di attività di carattere tecnico e organizzativo che dovrebbero essere valutate e poste in essere al fine di mitigare l'impatto dell'incidente e ripristinare i sistemi compromessi.

Ruolo 3: MARIT (Managing and Responding Incident Team)
Provvede alla registrazione dell'incidente e alla redazione della notifica da inviare alle Autorità di controllo (es: Autorità Garante per la protezione dei dati personali, Autorità NIS, CSIRT).
L'output consisterà nella redazione di una bozza di notifica da poter inviare all'Autorità di controllo, la quale dovrà essere identificata correttamente in base alla natura dell'incidente avvenuto e alla tipologia di informazioni compromesse.
Inoltre, dovrà essere redatto il cd. Registro degli incidenti ex art. 33.4 GDPR.

In che modo sarà valutato il progetto?
Il progetto verrà valutato dal vivo, nel quale sarà riscontrato l'output relativo al vostro team!

Incidendent Hadling Assessment Unit

L'azienda Sanitaria Provinciale (ASP) di Messina, comprende diverse sedi dislocate in 108 differenti comuni della Sicilia con bacino d'utenza di circa 645 mila cittadini, è stata attaccata da un gruppo di hacker, approfittando dei ***plugin (un programma non autonomo che interagisce con un altro programma)****e* ***CMS (son delle librerie come: WordPress, Bootrap, etc****)non aggiornate mandando in tilt i sistemi informativi di varie strutture ospedaliere e sanitarie.*

COMUNICAZIONE

Durante l'orario di ufficio è pervenuta una segnalazione da un membro dello staff, che comunicava di aver ricevuto una e-mail sospetta, che ha sbadatamente aperto causando il blocco della sua postazione di lavoro e costringendo a forzare immediatamente l'arresto.

Al riavvio della macchina è comparso sullo schermo, un avviso con una richiesta di riscatto in denaro, (chiaro attacco informatico di tipo ransomware) con esfiltrazione di dati sensibili e minaccia di diffusione pubblica sul Dark Web in caso di rinuncia al pagamento richiesto.

Successivamente sono state ricevute diverse segnalazioni da parte di altre strutture ospedaliere sanitarie che dichiaravano il blocco completo dei loro client.

REPORTAGE

Tramite le segnalazioni delle diverse infrastrutture colpite, si evince quindi che un malware si è introdotto nei sistemi informatici infettando gli host e criptando tutti i dati, con lo scopo di chiedere un riscatto in denaro.

Nei desktop dei diversi utenti è apparso un avviso con un timer di 7 giorni che comunicava di provvedere immediatamente al pagamento, altrimenti tutti i dati sensibili saranno pubblicati sul dark web.

La problematica è stata tempestivamente esposta all'attenzione del CISO e del DPO per intraprendere le dovute azione necessarie al contenimento della minaccia e ridurre i danni il più possibile
Il CISO ha avviato una indagine per identificare i responsabili e capire di che tipo di attacco si tratti;

Il DPO nel frattempo ha avviato la procedura di notifica delle unità competenti.

L'incidente è stato classificato come un attacco ransomware mirato ai dati sensibili dell'azienda

Incident Response Team

Mitigazione	*Contenimento*	*Recupero*
Per mitigare la minaccia i tecnici hanno provato ad usare un software di decryptor per provare a recuperare i file decriptandoli ma senza alcun risultato. Poi, messo il sito in modalità manutenzione per impedire l'accesso ai visitatori mentre si lavora per ripristinare il sito. Successivamente abbiamo aggiornato i CMS e i plug-in alla versione più recente per correggere eventuali vulnerabilità che potrebbero essere state sfruttate dal ransomware. Dopodiché eseguito una scansione sia sui computer del ma anche sul sito visto che l'attacco è avvenuto sulle CMS e Plug-in del sito e	Per contenere la minaccia isolare il dispositivo infetto dalla rete e spegnere il dispositivo infetto. Inoltre, per proteggere l'azienda da futuri attacchi ransomware, applicare regolarmente patch per aiutare a contrastare gli attacchi ransomware che sfruttano la vulnerabilità del software e del sistema operativo e rivisto le politiche di sicurezza per identificare eventuali lacune che potrebbero aver permesso al ransomware di infettare il sistema e apportare le modifiche necessarie per prevenire future infezioni ed anche pianificato una formazione per i dipendenti per cercare di arginare e	Per recuperare i dati, i tecnici hanno provato ad usare un punto di ripristino e strumenti per il recupero dati senza ottenere risultati. Per cui, hanno analizzato se i backup erano stati danneggiati o compromessi e poi eseguito il backup precedente come era stato previsto in caso di perdita o furto dati.
rimosso il ransomware con un anti-malware.	limitare problemi di questo tipo. Per evitare ulteriori attacchi abbiamo reimpostato le password per ogni P.D.L. (postazione di lavoro).	

Non cedere al ricatto dei criminali informatici pagando il riscatto:

- Pagare significa candidarsi al ruolo di ‘’preda facile’’. I criminali saranno incentivati ad attaccare di nuovo e ‘’finanziati’’ nelle loro attività illecite.
- Si deve sempre tenere in considerazione l'ipotesi che i dati "liberati" dopo il pagamento possano essere corrotti, compromessi e inutilizzabili.
- Per etica

Managing and Responding Incident Team

L'ASP di Messina ai sensi del Regolamento Europeo 2016/679 (GDPR), è tenuta a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo (entro 72 ore) in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).

Redazione notifica: Pubblicazione sito ufficiale Asp Messina data 09/05/2023

L'Azienda è spiacente di comunicare che in data 08/05/2023 è stato segnalato dal CED di questa ASP di Messina il malfunzionamento di alcuni server aziendali a seguito di un attacco informatico subito ad opera di un gruppo di criminali informatici con conseguenze anche sui dati personali degli utenti.

Dopo diverse verifiche è risultato che tali server malfunzionanti erano compromessi da un virus informatico installato da un gruppo di hacker che avevano criptato i files di sistema rendendoli inutilizzabili, riuscendo a superare le misure di sicurezza dell'azienda, comportando il malfunzionamento del sistema e l'interruzione dei servizi. Inoltre, ransomware ha estrapolato 30 mila cartelle contenenti dati personali di utenti e dipendenti dell'ASP, patologie e annesse terapie, per poi pubblicarli sul dark web. Pertanto gli stessi dati potrebbero essere utilizzati per finalità diverse da quelle previste, in modo illecito.

Per porre rimedio alla violazione subita è stato necessario procedere alla bonifica dei sistemi compromessi, operando con il massimo impegno per cercare di limitare al minimo gli effetti dell'attacco subito.

L'ASP di Messina, in qualità di Titolare del Trattamento, ha proceduto a notificare l'evento illecito alle forze dell'ordine e all'Autorità Garante per la protezione dei dati personali in data 09/05/2023, ai sensi dell'art. 33 del Regolamento Generale sulla protezione dei dati.

Per evitare che in futuro si possano ripresentare simili situazioni, il Titolare del Trattamento ha provveduto ad un rafforzamento delle misure già adottate.

REGISTRO DEGLI INCIDENTI INFORMATICI E DELLE VIOLAZIONI DI DATI (ARTT. 33 E 34 DEL GDPR)

Data violazione	*Tipologia violazione*	*Sistema impattato*	*Tipi di dati coinvolti*	*Data notificazione DPO*	*Data notificazione a Garante per la protezione dei dati*	*Rif. Scheda violazione dei dati*
08/05/2023	Attacco ransomware ASP Messina. Si registra indisponibilità di utilizzo di tutti i servizi da questa erogati, violazione dati sensibili pazienti.	Piattaforma Asp	Dati personali e particolari di: ● pazienti ● dipedenti Dati amministrati: ● fatture ● bilanci ● cartelle cliniche	08/05/2023	09/05/2023	Comunicato ripristino delle funzionalità in data 11/05/2023.