Cybercrime, come prepararsi a un Data Breach?

Sfortunatamente l'incidenza e la frequenza dei **Data Breach** sono in sensibile aumento, logica conseguenza della smaterializzazione "fisica" dei record presenti in tutte le organizzazioni.

Ma nonostante l'aumentare del fenomeno non è ancora chiaro per tutti come adeguatamente prepararsi ad affrontare questo scenario.

In questo articolo affronteremo la fase di preparazione all'eventualità di un Data Breach.

È importante stressare come la prima fase sia spesso la più cruciale, ma può facilmente essere trascurata o sottovalutata per mancanza di consapevolezza, supporto o risorse.

L'analisi del rischio

Il primo step per essere opportunamente preparati è quello di stabilire la criticità delle proprie risorse chiave e strategiche, analizzare le minacce alle quali sono esposte e attuare una serie di controlli complementari per garantire un adeguato livello di protezione.

Considerando le implicazioni per persone, processi, tecnologie e informazioni, si può aggiornare la propria capacità di risposta ai Data Breach e valutare il proprio grado di prontezza nel reagire.

Le azioni da compiere sono quelle di:

1. Definire le informazioni critiche;

2. Determinare quali minacce alla Cyber Security hanno maggior probabilità di influire su queste informazioni critiche;
3. Attuare attività periodiche e di Security Prevention (Vulnerability Assessment, Network Scan e Penetration Test);
4. Applicare i controlli gestionali e tecnici del caso per ridurre la probabilità e l'impatto dei Data Breach sulle loro informazioni critiche;
5. incrementare la consapevolezza dei rischi cyber attraverso attività incentrate su awareness e formazione;
6. determinare quanto il Data Breach possa incidere in modo probabile o effettivo sull'attività dell'impresa.

Ma non dobbiamo fermarci qui, è sicuramente consigliato identificare con la massima urgenza dove si trovano le informazioni critiche e chi ne è responsabile e definire le aspettative, in modo da essere consapevoli delle misure attuabili con il tempo, le risorse e il denaro a disposizione.

La Business Impact Analysis

Attuare una **Business Impact Analysis** permette di valutare le perdite, qualitative e quantitative, per il business a seguito di una prolungata interruzione dei propri servizi.

Determinare il danno potenziale che sarebbe recato alla propria organizzazione in caso di Data Breach concentrandosi sulla riservatezza, sull'integrità e sulla disponibilità, determinando il livello di impatto sull'impresa qualora:

- informazioni sensibili fossero divulgate a terzi non autorizzati (riservatezza)
- informazioni importanti venissero compromesse (ad es. dati chiave elaborati in modo poco preciso o errato)
- i sistemi o le infrastrutture critiche non fossero più disponibili.

Quando si determina l’impatto sull’impresa, spesso è utile considerare vari scenari e identificare tutte le implicazioni più gravi nel caso in cui un Data Breach compromettesse le proprie risorse critiche, come:

- perdita finanziaria potenziale ed effettiva
    - implicazioni per la conformità (ad es. sanzioni, restrizioni aziendali o altre penali)
    - danno alla reputazione
    - perdita del controllo amministrativo
    - perdita leva competitiva.

Una volta identificate le proprie risorse critiche, occorre stabilire dove sono collocate nella propria organizzazione (e al di fuori della stessa) e registrare dettagli importanti sul loro livello di criticità (ad es. critico, significativo, minore o trascurabile). Infine è necessario attribuire la responsabilità della protezione di queste risorse a soggetti capaci e opportunamente designati.

L’analisi delle Minacce

Il passo successivo nel processo di preparazione per un Data Breach consiste nel comprendere il livello di minaccia a cui è esposta l’organizzazione a causa delle diverse sfaccettature che può assumere il fenomeno; spesso lo si può fare effettuando un’analisi delle minacce.

Al fine di contestualizzare l’analisi delle minacce alla Cyber Security è necessario ben definire:

- la natura della propria attività, la strategia d’impresa, i processi aziendali e la propensione al rischio;
- le principali dipendenze della propria organizzazione, per esempio nei confronti di persone, tecnologie, fornitori, partner e l’ambiente in cui si opera;
- i beni che possono essere presi di mira, come le

infrastrutture, il denaro, la proprietà intellettuale o le persone, nonché i sistemi informatici di supporto;
- la possibile compromissione della riservatezza delle informazioni sensibili, dell'integrità di importanti informazioni e applicazioni aziendali, o della disponibilità delle infrastrutture critiche.

Tenendo a mente questi importanti elementi aziendali, si può quindi incentrare l'analisi della minaccia su:

- l'infrastruttura tecnica che supporta i beni critici dell'organizzazione;
- lo scenario di Cyber Security che interessa la propria organizzazione;
- i diversi tipi di minacce alla Cyber Security a cui si può essere esposti;
- le fonti di queste minacce, come la criminalità organizzata, le organizzazioni finanziate dallo Stato, i gruppi estremisti, gli hacktivisti, gli insider, o una combinazione di questi;
- i vettori che possono essere sfruttati per gli attacchi (ad es. download da Internet, chiavette USB non autorizzate, sistemi configurati in modo errato, accesso inadeguato o collusione);
- le vulnerabilità per ogni minaccia particolare (ad es. controlli carenti o circostanze straordinarie).

Parlando di vulnerabilità per particolari minacce, può essere utile tenere a mente l'acronimo **PLEST**, che prende in considerazione le vulnerabilità associate a:

- ambiente Politico, a livello macro e micro;
- ambiente Legale e normativo, compresi i requisiti di compliance (ad es. denuncia);
- ambiente Economico;
- ambiente Socio-culturale, compreso l'aspetto importante delle persone;
- ambiente Tecnico (ad es. registrazione).

Infine, l’analisi delle minacce alla Cyber Security andrebbe condotta su base regolare a fronte dell’evoluzione dello scenario delle minacce e delle indicazioni utili fornite dalle indagini.

Sarebbe quindi opportuno effettuare **un addestramento periodico basato su simulazioni** con una serie di scenari di attacco adattati alle minacce e alle vulnerabilità che deve affrontare l’organizzazione in questione. Questi scenari aiutano anche i soggetti coinvolti a comprendere il loro ruolo e a prepararsi per affrontare un incidente.

Il Cyber Framework

Per predisporre un corretto piano di preparazione alla gestione di un Data Breach è necessario definire il Cyber Framework in termini di:

1. Tecnologia
2. Governance
3. Dati
4. Competenze

L’approccio strategico in questo caso non solo deve essere più che adeguato e supportato da un processo formale di risposta in grado di eseguire l’identificazione dell’attacco in corso, l’indagine della situazione (compreso il “triage”), l’adozione di provvedimenti adeguati (ad es. contenendo l’incidente ed eliminandone la causa) e il ripristino di sistemi, dati e connettività.

Il processo dovrebbe idealmente indicare il responsabile di ciascuna fase, le modalità di esecuzione e i soggetti da contattare per ricevere supporto. Infine occorre fare in modo che il processo sia sottoscritto dai dirigenti pertinenti e che sia testato completamente con cadenza regolare attraverso scenari diversi.

Qualunque sia l’approccio adottato, occorre stabilire una metodologia e un piano chiari che aiutino a rispondere ai Data Breach in modo rapido, efficace e coerente.

Benché ogni situazione sia specifica, ci sono degli aspetti comuni che permettono di stilare un piano standardizzato da implementare in modo proattivo e da adattare in base alle necessità. Il piano deve essere sufficientemente esaustivo e versatile da contemplare molti scenari diversi, e spesso questo significa che dovrà essere stilato a un livello superiore.

Dal punto di vista delle competenze è essenziale istituire un team responsabile della risposta ai Data Breach, con un referente. Questo team deve necessariamente essere sostenuto dai principali soggetti interessati, come l’alta dirigenza, i reparti PR, HR, legale, IT e di gestione delle business unit. Inoltre deve avere l’autorità di confiscare o scollegare le apparecchiature e di monitorare le attività sospette, poter comunicare esternamente e condividere le informazioni (ad es. sapere cosa può essere condiviso con chi, quando e attraverso quali canali) e chiarire le fasi di escalation nel processo di gestione dei Data Breach.

Per quanto riguarda gli strumenti, è opportuno predisporre un kit ready made per la risposta ai Data Breach che comprenda:

- un metodo adeguato a registrare tutti gli aspetti dell’incidente;
- i dati di contatto di tutti i principali soggetti coinvolti;
- risorse di analisi degli incidenti;
- strumenti di forensic imaging.

Dal punto di vista della tecnologia, molte organizzazioni presentano capacità di registrazione, archiviazione, correlazione e simulazione assolutamente insufficienti. Per esempio, quando si gestisce un Data Breach i dati storici

possono essere molto importanti, dal momento che spesso gli attacchi possono svolgersi nell'arco di un periodo di tempo prolungato, mentre i file di registro e Logs (ammesso che contengano i dati giusti) sono spesso incompleti o non coprono adeguatamente gli eventi passati.

Quando si affronta un Data Breach, disporre di dati storici efficaci fa risparmiare tempo e denaro. Pertanto occorre:

- fissare standard e procedure di registrazione;
- configurare i sistemi per registrare gli eventi giusti;
- monitorare tali eventi efficacemente;
- conservare sufficienti dati storici (dal momento che i file di log possono essere sovrascritti o avere uno spazio di memoria insufficiente);
- Avere a disposizione gli asset e software inventory;
- Struttura della rete aggiornata;
- Mappatura dei sistemi di sicurezza software, hardware e sistemi presenti in azienda.

È necessario raggruppare le informazioni chiave provenienti da quanti più file di log possibili in un archivio centrale, come un sistema di S**ecurity Information and Event Management (SIEM)**. Per esempio, le prove di un incidente possono essere reperite in diversi file di log, ciascuno contenente diversi tipi di dati:

- un log di firewall potrebbe contenere l'indirizzo IP sorgente che è stato utilizzato, mentre il log di un'applicazione potrebbe contenere un nome utente
- un dispositivo di rilevamento delle intrusioni (IDS) nella rete può identificare un Cyber Security attack contro un particolare host, senza tuttavia fornire informazioni sull'esito dell'attacco.

Esaminare i file di log per risalire a tali informazioni e correlare gli eventi provenienti da sorgenti multiple può essere molto utile per confermare se si è verificato un

particolare incidente.

È essenziale assicurarsi che la propria organizzazione abbia rapido accesso alle informazioni che aiuteranno il team responsabile della risposta al Data Breach (inclusi gli esperti esterni) a operare velocemente ed efficacemente. A seconda del contesto, il tipo di informazioni che gli esperti solitamente richiedono rientrano in quattro categorie principali:

- gestione aziendale
- infrastruttura IT (ad es. diagrammi di rete, architettura di sistema e layout)
- dati (ad es. tipo di informazioni elaborate, dove e come)
- registro eventi (ad es. quali tipi di dati ed eventi sono registrati, su quali sistemi, come e quando; modalità di recupero e analisi dei dati).

Non da ultimo è la questione dei dati. La quantità di informazioni richieste da un'organizzazione differisce in base a vari fattori, come le sue dimensioni, il settore di mercato, le capacità interne e la natura del particolare Data Breach oggetto dell'indagine.

Le organizzazioni talvolta non comprendono la necessità di avere rapido accesso alle strutture dei loro service provider esterni (ad es. ai locali o alle attrezzature). Spesso hanno difficoltà a ricevere dai fornitori esterni (ad es. fornitori di servizi in cloud, di infrastrutture e di servizi gestiti) informazioni importanti (ad es. registri eventi) che riguardano il Data Breach, talvolta con tempi di attesa di più giorni.

Una volta identificati questi soggetti esterni, i loro recapiti devono essere conservati e messi a disposizione del personale responsabile, compresi i tecnici specialisti di sicurezza, i rappresentanti aziendali e il Crisis Management

Team.

https://www.key4biz.it/cybercrime-come-prepararsi-a-un-data-breach/277455/