Disney+, l'anti Netflix violata dagli hacker dopo una settimana dal lancio

Un inizio pieno di problemi per Disney+, la piattaforma di streaming video della **Walt Disney**, lanciata lo scorso 12 novembre negli Stati Uniti, Canada e Paesi Bassi.

Dopo aver raccolto oltre 10 milioni di abbonati dopo poche ore dal lancio, il servizio ha avuto vari problemi tecnici a causa del flusso enorme di utenti che provavano ad accedervi.

I problemi tecnici

Sono diversi gli utenti che hanno lamentato subito la presenza di alcuni disservizi e problemi tecnici. Sono infatti tanti gli utenti che non sono riusciti ad accedere allo streaming online dei video della propria serie tv preferita o del film che desideravano guardare.

E tra i tanti qualcuno dichiarava anche di non riuscire ad accedere al proprio profilo.

Questo perché gli hacker li avevano buttati fuori dagli account, cambiando le credenziali e bloccando di fatto i legittimi proprietari.

Profili in vendita sul dark web

Secondo il sito di informazione tecnologica **ZdNet**, i profili violati sono in vendita sul dark web per cifre che vanno dai 3 agli 11 dollari.

Quest’ultimo problema deriva dal fatto che gli hacker che hanno attaccato la piattaforma hanno reperito le informazioni di login di alcuni utenti ed hanno cambiato le credenziali non consentendo più al legittimo proprietario di poter loggare con il suo account regolarmente acquistato.

La velocità con cui gli hacker si sono mobilitati per monetizzare gli account del servizio streaming è sorprendente, fa notare il sito ZdNet. I profili sono stati messi in vendita su un forum di hacking dopo poche ore dal lancio del servizio, con annunci che offrono accesso a migliaia di credenziali.

La Disney minimizza

Disney afferma di prendere molto sul serio la privacy e la sicurezza dei dati degli utenti “*e non vi è alcuna indicazione di una violazione della sicurezza su Disney +*“.

“*Molto probabilmente gli incidenti*“- ha affermato l’azienda, “*si sono verificati “a seguito di un individuo non autorizzato che riutilizzava la combinazione email / password di un cliente raccolta durante precedenti incidenti di sicurezza*“.

Disney+ l’anti Netflix

Disney + è la grande scommessa della Walt Disney Company per ribaltare il predominio di Netflix. I film di prima visione prodotti dalla media company e dalle sue filiali non finiranno sui canali TV di proprietà Disney come ABC, Disney Channel e Freeform, ma saranno tutti trasmessi in streaming su Disney +, a meno che non siano classificati come vietati ai minori. Altri film per adulti probabilmente finiranno su Hulu, sempre di proprietà della multinazionale.

Oltre al catalogo Disney e alle produzioni realizzate per lo streaming, il servizio è commercializzato come sede di film e programmi TV dall’universo Star Wars di Marvel, Pixar,

National Geographic e Lucasfilm.

Il servizio Disney + è lo streamer di più alto profilo dell'anno, dopo il lancio di **Apple TV** + il 1 ° novembre. In arrivo nel 2020 HBO Max di Warner Media e **Peacock** di NBC / Universal.

https://www.key4biz.it/disney-lanti-netflix-violata-dagli-hacker-dopo-una-settimana-dal-lancio/279542/

Cybersecurity e il Golden Power esteso al 5G, le 10 novità della legge

Con il via libera definitivo da parte della Camera, diventa legge il decreto sulla **Cybersicurezza** che ha l'obiettivo di mettere in sicurezza le infrastrutture critiche del Paese da attacchi informatici e di intervenire in modo più tempestivo ed efficace in caso di minacce e pericoli per la sicurezza nazionale provenienti dal cyberspazio.

La legge amplia anche i poteri speciali del Governo (la cosiddetta Golden power), che vengono estesi anche al **5G**.

Spetta al Premier individuare il perimetro di sicurezza nazionale cibernetica

In particolare, la legge prevede un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti

e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi di attacchi informatici.

Quali sono le amministrazioni pubbliche, gli enti e gli operatori nazionali – pubblici e privati – obbligati a tutelarsi contro le minacce informatiche e presenti nel perimetro di sicurezza nazionale cibernetica? Entro 4 mesi dall'entrata in vigore della legge, l'istituzione del perimetro di sicurezza nazionale cibernetica è demandata ad un decreto del presidente del Consiglio dei ministri, da adottare su proposta del CISR (Comitato interministeriale per la sicurezza della Repubblica), previo parere delle competenti Commissioni parlamentari.

Le procedure di notifica degli attacchi subìti

Entro 10 mesi dall'entrata in vigore della legge spetta ad un decreto del presidente del Consiglio dei ministri adottare su proposta del CISR, previo parere delle competenti Commissioni parlamentari, la determinazione delle procedure di notifica degli incidenti prodottisi su reti, sistemi informativi e sistemi informatici inclusi nel perimetro di sicurezza nazionale cibernetica e le misure di sicurezza.

Coinvolte anche le Pmi

È infine rimessa ad un regolamento – da emanarsi con decreto del Presidente del Consiglio dei ministri, entro 10 mesi dalla data di entrata in vigore della legge di conversione – la

definizione delle procedure, delle modalità e dei termini ai quali devono attenersi le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati, inclusi nel perimetro di sicurezza nazionale cibernetica, che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT, destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici individuati nell'elenco trasmesso alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico

Nasce il centro di valutazione al ministero dell'Interno

La legge prevede l'istituzione di un Centro di valutazione (**CEVA**) presso il Ministero dell'interno e i conseguenti adeguamenti nel testo, compresa la copertura finanziaria per la realizzazione, l'allestimento e il funzionamento del Centro. È stato altresì specificato che l'istituendo Centro di valutazione del Ministero dell'interno, così come quello del Ministero della difesa, siano accreditati presso il Centro di Valutazione e certificazione nazionale (**CVCN**) e sono tenuti ad impiegare metodologie di verifica e test quali definiti dal medesimo CVCN. Con decreto del presidente del Consiglio dei ministri saranno inoltre definiti gli obblighi di informativa di tali Centri con il CVCN

Gli obblighi

Sono determinati alcuni obblighi per: gli operatori dei servizi essenziali; i fornitori di servizi digitali; le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, inclusi nel perimetro di sicurezza nazionale cibernetica.

I poteri del premier

È altresì previsto che il Presidente del Consiglio – su deliberazione del CISR – possa disporre la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati.

Sanzioni

Il provvedimento reca quindi un articolato sistema sanzionatorio per i casi di violazione degli obblighi previsti ed individua le autorità competenti all'accertamento delle violazioni e all'irrogazione delle sanzioni.

L'assunzione di 87 esperti di Cybersecurity e digitale

Parallelamente è autorizzata l'assunzione a tempo indeterminato, attraverso concorsi pubblici, di un contingente massimo di 77 unità di personale, di cui 67 di area terza e 10 di area seconda, tenuto conto dell'esigenza di disporre di personale in possesso della professionalità necessaria per lo svolgimento delle funzioni del Centro di valutazione e certificazione nazionale (**CVCN**). A sua volta, la Presidenza del Consiglio è autorizzata ad assumere fino a 10 unità di personale non dirigenziale, per lo svolgimento delle funzioni in materia di digitalizzazione.

Il Golden Power esteso al 5G

La legge amplia anche i poteri speciali del Governo (la cosiddetta Golden power), che vengono estesi anche al **5G**.

Sono in particolare previste le seguenti modifiche:

- Viene in generale allungato il termine per l’esercizio dei poteri speciali da parte del Governo, con contestuale arricchimento dell’informativa resa dalle imprese detentrici degli asset strategici; si amplia l’oggetto di alcuni poteri speciali; sono modificati e integrati gli obblighi di notifica finalizzati all’esercizio dei poteri speciali;
- Viene modificata la disciplina dei poteri speciali in tema di tecnologie 5G, per rendere il procedimento sostanzialmente simmetrico rispetto a quello per l’esercizio dei poteri speciali nei settori della difesa e della sicurezza nazionale;

Ridefinito il concetto di “soggetto esterno all’Unione europea”

- Viene ridefinito il concetto di “soggetto esterno all’Unione europea” e sono precisati i criteri per determinare se un investimento estero è suscettibile di incidere sulla sicurezza o sull’ordine pubblico.

https://www.key4biz.it/cybersecurity-e-il-golden-power-esteso-al-5g-le-10-novita-della-legge/279067/

Roberto Viola (DG Connect): “Cybersecurity è parte della vita quotidiana delle

famiglie e delle nostre aziende”

Dare vita al mercato unico digitale o ***Digital single market***, significa “*garantire ai cittadini dell’Unione europea, in particolare ai giovani, le conoscenze e le competenze per proteggersi online da ogni tipo di attacco informatico. È una nostra responsabilità far diventare i cittadini europei degli utenti responsabili nell’utilizzo delle tecnologie emergenti*”.
Così **Marija Gabriel**, Commissario europeo per l’economia e la società digitali, ha presentato lo ***European Cybersecurity Month 2019***.

La cybersecurity deve diventare una buona abitudine quotidiana, come lavarsi le mani. Una routine individuale e famigliare, che passa per la metafora dell’igiene personale, utile a mantenere elevato il livello di protezione informatica dei nostri dati e dei nostri device (dal computer al tablet, dallo smartphone alle tecnologie indossabili, fino alla smart tv o i sistemi smart home).

Sempre in occasione del mese della cyber sicurezza in Europa, **Roberto Viola**, Direttore Generale DG Connect della Commissione europea, ha affermato: “*La cultura della sicurezza informatica deve far parte della vita quotidiana delle nostre famiglie e delle nostre aziende. La sicurezza informatica è una responsabilità condivisa!*”.
Una cultura che deve ancora affermarsi, però, che deve diffondersi e penetrare nella società contemporanea, troppo pigra, superficiale e a tratti ingenua difronte al pericolo della criminalità informatica e digitale.

> *Director-General of Communications Networks, Content and Technology @ViolaRoberto takes the floor for more insights on developing an ecosystem for a thriving cyber industry #EUCyber #EU2019FI pic.twitter.com/h7CFtbDuPh*

> *— EU Institute for Security Studies (@EU_ISS)* ***November 8, 2019***

"*L'Europa sta ballando sul Titanic della cybersecurity?*", si domandava provocatoriamente Viola in un suo intervento di qualche giorno ad un evento dell'Institute for Security Studies dell'Unione europea.
Parlando di tecnologie emergenti e future, il direttore della DG Connect ha dichiarato: "***Quantum, post quantum, 6G****: dobbiamo proteggere le nuove tecnologie per proteggere i nostri valori. Siamo riusciti con supercomputer, ora dobbiamo riuscire nel cyber*".

La cybersecurity quindi come fattore e valore fondamentale su cui costruire il mercato unico, ma anche la società stessa in cui viviamo. Le soluzioni tecnologiche non mancano.
Il mercato è già pronto alla sfida della sicurezza informatica e della guerra ai cyber criminali. **Entro il 2024, il settore cybersecurity potrebbe arrivare a valere a livello globale oltre 267 miliardi di dollari,** secondo stime Reportlinker.
La tecnologia ***machine learning*** offre grandi vantaggi nel rilevamento delle minacce informatiche e il suo utilizzo nella *cybersecurity* sta migliorando la protezione di molte delle tecnologie emergenti più utilizzate, come l'***Internet of Things***, la **robotica**, l'**intelligenza artificiale** e il ***cloud***.

Secondo una recente indagine pubblicata da Data connectors, a livello mondiale, il 43% delle organizzazioni è caduto preda di attacchi informatici di qualche tipo, soprattutto violazione/sottrazione di dati sensibili. I temibili ransomware quadruplicheranno i loro attacchi entro il 2022, prendendo di mira soprattutto il settore sanitario e ospedaliero.
Entro il 2030 il 50% delle *smart city* mondiali dovrà munirsi

di piattaforme cybersecurity per proteggere le proprie infrastrutture strategiche, hanno evidenziato i ricercatori, ma anche i servizi e le tecnologie alla base dell'elevato livello di connettività sul territorio.

Il numero complessivo di attacchi DDoS, nel terzo trimestre del 2019, è aumentato del 30% rispetto a quanto registrato nel periodo immediatamente precedente e del 32% rispetto al terzo trimestre del 2018, soprattutto a causa di un picco di attività malevole registrato a inizio autunno. Il 53% degli attacchi DDoS dell'intero trimestre sembra essersi concentrato nel mese di settembre, secondo dati Kaspersky.
A proposito di tecnologie emergenti di ampissima diffusione, **nei primi sei mesi dell'anno**, sempre la rete Kaspersky ha rilevato **105 milioni di attacchi su dispositivi *Internet of Things*** (IoT) provenienti da 276.000 indirizzi IP unici.
Questo dato è sette volte più grande rispetto a quella registrato nello stesso periodo del 2018: nei primi sei mesi dello scorso anno, infatti, sono stati rilevati 12 milioni di attacchi provenienti da 69.000 indirizzi IP. I cybercriminali, sfruttando la leva della scarsa sicurezza informatica che spesso caratterizza il mondo dell'internet delle cose, cercano di creare e far fruttare economicamente botnet composte da dispositivi IoT.

> *Roberto Viola (DG Connect): "Cybersecurity è parte della vita quotidiana delle famiglie e delle nostre aziende"*

Cybersecurity, in Gazzetta il

decreto con la nuova architettura nazionale

E’ stato pubblicato in Gazzetta Ufficiale il decreto del presidente del Consiglio che istituisce il ‘Computer security incident Response team’ (**Csirt**) italiano, in linea con quanto previsto dalla direttiva che per la prima volta a livello Ue affronta il tema della cybersicurity, definendo le misure standard comuni necessarie per un elevato livello di sicurezza delle reti e dei sistemi informativi nazionali.

Il Csirt è istituito presso il Dis, il Dipartimento delle informazioni per la Sicurezza, e ha il compito di:

- definire le procedure tecniche per la prevenzione e la gestione degli incidenti informativi, ricevere le notifiche sugli incidenti, fornire a chi ha effettuato la notifica le informazioni per facilitare una gestione efficace dell’evento.
- Informare gli altri Stati dell’Ue eventualmente coinvolti.
- Garantire la collaborazione nella rete Csirt, attraverso l’individuazione di forme di cooperazione appropriate, lo scambio di informazioni.

“Viene così a comporsi un altro tassello importante dell’architettura nazionale cyber – sottolinea il Dipartimento – *che, con la collocazione del Csirt presso il Dis, favorirà una più efficace gestione tecnica degli incidenti a livello nazionale e internazionale, grazie alle sinergie garantite dalle altre funzioni già assicurate dal Dipartimento in tale ambito, quali il ‘punto di contatto unico nazionale Nis’ per la gestione operativa di incidenti transfrontalieri, il ‘Nucleo per la Sicurezza Cibernetica (Nsc)’ per la gestione operativa di incidenti che hanno un impatto sulla sicurezza nazionale, e le attivazioni che deriveranno dal cosiddetto*

‘Perimetro di sicurezza nazionale cibernetica’.”

Il decreto firmato dal presidente del Consiglio **Giuseppe Conte** individua anche i tempi per una piena operatività del Csirt: entro 120 giorni il Dis, il **Mise** e l’**Agid** dovranno sottoscrivere appositi accordi per assicurare il trasferimento delle funzioni del Cert nazionale e del Cert-Pa al Csirt italiano che, per lo svolgimento dei propri compiti, si avvarrà dell’Agid ai sensi del decreto legislativo Nis. Le disposizioni del decreto istitutivo del Csirt entreranno in vigore entro 6 mesi.

Il provvedimento dispone la definizione di un ‘Perimetro di sicurezza nazionale cibernetica’ rinviando a un Decreto del presidente del Consiglio dei ministri l’individuazione dei soggetti pubblici e privati le cui reti e sistemi informativi e informatici sono necessari per l’esercizio di una funzione essenziale dello Stato. Con un emendamento del Governo sono state inoltre ‘recuperate’ le norme sul rafforzamento della ‘Golden power’, con particolare riferimento ai contratti **5G**, varate nel luglio scorso con il decreto Brexit e successivamente decaduto.

Per saperne di più: 5G

Cybersecurity, in Gazzetta il decreto con la nuova architettura nazionale

Perché i Criminal hacker amano il Social engineering?

Il 2019 ha confermato il trend di crescita delle Cyber minacce su tutti i fronti, con un aumento significativo sia nella frequenza degli attacchi sia nella loro magnitudine.

Un anno che ha visto casi di punta come **Capital One** o **Maersk** e – spesso – a margine di questi eventi di alto profilo molti hanno puntato il dito contro la scarsa resilienza nei confronti degli attacchi dei Criminal Hacker, soprattutto da parte del "comune lavoratore".

Ma siamo così sicuri che sia veramente questo l'anello debole della catena che potenzialmente potrebbe trasformare la nostra società nella prossima **Equifax**?

Non è neppure detto che anche quando l'end user si affida alle policy e alle procedure prefissate, seguendole alla lettera, riesca ad uscire indenne da una ben orchestrata campagna di phishing.

Il caso più lampante – per farci un'idea – è stato quello del'ex Capo di gabinetto della Casa Bianca, nonché campaign manager di **Hilary Clinton, John Podesta.**

Nel suo caso Podesta ha pensato che l'e-mail di reset della password di Google che aveva ricevuto avesse un aspetto ben più che sospetto, ma il responsabile IT della campagna o dando il suo lasciapassare o scrivendo male la sua risposta ha indotto il sig. Podesta a fornire le sue credenziali ai Criminal hacker.

Si tratta di un caso esemplare – e probabilmente non unico – di qualcuno che agisce in buona fede, compiendo le azioni

prescritte dagli esperti e diventando comunque una vittima.

Perché i Criminal hacker amano il Social engineering

Non è difficile capire come i Criminal hacker siano sempre molto affezionati alle tecniche di Social Engineering:

- **Ci sono molti bersagli**: Va da sé che per avere successo i Criminal Hacker hanno bisogno di una superficie d'attacco il più ampia possibile. In termini generali, ci sono sicuramente più utenti che sistemi. Inoltre, molti sistemi non sono direttamente accessibili via Internet, ma la maggior parte degli utenti finali lo sono. I siti di social-media offrono agli aggressori anche strumenti di ricognizione efficaci, difficili da prevenire, individuare o anche isolare.
- **I loro bersagli hanno già ciò che cercano:** Quando gli aggressori prendono di mira i sistemi, il loro percorso verso il bottino può essere tortuoso. Devono trovare un sistema che possono compromettere, ottenere i privilegi da amministratore e/o ruotare verso un altro sistema e continuare a mappare l'ambiente per scoprire dove si trovano i dati preziosi. Il processo può essere estremamente ripetitivo e richiedere molto tempo. I singoli utenti, invece, offrono un percorso abbastanza diretto ai dati desiderati. Se siete alla ricerca di file personali, perché non ottenerli da qualcuno delle Risorse Umane? Se cercate un rendiconto finanziario, non è il dipartimento finanziario il punto di partenza logico?
- **Gli attacchi di Social engineering sono leve molto forti:** Mentre alcune campagne si basano ancora su argomenti e oggetti molto vecchi e molto ovvi – e sono quindi molto facili da evitare (chi casca ancora nelle mail di "Sei il milionesimo cliente!) – molti attacchi

moderni di social-engineering sono così avanzati e taylorizzati da sembrare autentici. Questo è particolarmente significativo in un ambiente aziendale perché il contesto è tale che le conseguenze derivanti dal non agire potrebbero essere gravi se lo scenario fosse legittimo. Per esempio, e-mail che sembrano provenire da supervisori che richiedono azioni o informazioni, o notifiche da parte dell'IT in merito a modifiche delle password sono cose che semplicemente non possono essere ignorate nella normale conduzione degli affari interne all'azienda senza un grave impatto.

Come rimediare?

Ovviamente dinnanzi alle minacce poste dalle campagne di Social Engineering il rimedio più comunemente proposto e più efficace è una maggiore sensibilizzazione degli utenti finali. Ma se l'Awerness è sicuramente parte della soluzione, è solo uno dei diversi elementi di una difesa efficace.

Per esempio:

Implementazione di un'autenticazione (più)forte: sottrarre le credenziali è un obiettivo frequente del Social engineering e il furto di credenziali ha un ruolo di primo piano in molte violazioni di maggiore spicco negli ultimi anni. Un'autenticazione più forte – che si tratti di crittografia, autenticazione multifattoriale (MFA) o di una combinazione dei due – significa che un attacco riuscito non produrrà necessariamente nulla di utile. Vale anche la pena sottolineare che, mentre in tempi di PSD2 non è più ufficialmente raccomandabile l'SMS come secondo fattore di autenticazione, anche misure deboli di 2FA (2 factor authentication) sono meglio di 0.

White-listing delle applicazioni a rischio: l'installazione o l'esecuzione di malware è un altro obiettivo comune degli attacchi di social-engineering. Anche se la lista dei software

in White listing può essere lunga e difficile da compilare, la maggior parte delle organizzazioni dovrebbe sapere quale software stanno effettivamente eseguendo sui loro sistemi. L'applicazione di successo di tale protocollo non è mai facile, ma rende molto più difficile l'esecuzione di software dannoso e permette agli esperti di Cyber Security e ad altri membri dei team di sicurezza di concentrare i loro sforzi su una superficie di attacco molto più piccola.

Segmentare la rete aziendale: L'essere umano è fallibile e di conseguenza in una certa percentuale lo saranno anche le difese che progetta. Un certo numero di attacchi di alto profilo nel corso degli ultimi anni è stato caratterizzato da malware in grado di muoversi lateralmente attraverso le reti, aumentando significativamente sia il danno complessivo che il tempo necessario per il Data Recovery. La segmentazione di rete, come la white-list delle applicazioni, è un esercizio non banale per la maggior parte delle organizzazioni, ma è facilmente una delle migliori "polizze assicurative" per quei momenti in cui un attacco ha successo.

In un certo senso, la difesa contro gli attacchi di Social engineering deve assumere gli stessi caratteri di quella adottata tempo fa per la sicurezza sulle strade. In primo luogo devono essere formati gli utenti in modo da renderli competenti, ma al contempo dobbiamo renderci conto che gli errori saranno sempre parte del nostro essere umani e per questo si migliorano le infrastrutture e gli strumenti.

Integrare la formazione per migliorare l'Awerness con le capacità degli esperti di Cyber Security rendono più facile fare la cosa giusta e più difficile fare la cosa sbagliata; il tutto unito ad un Cyber Security Framework resiliente per eliminare o ridurre i danni durante un evento catastrofico.

https://www.key4biz.it/perche-i-criminal-hacker-amano-il-social-engineering/277772/

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/

Nel dark web 16 milioni di password rubate alle aziende di Fortune 500

Durante quest'anno si è registrato un incremento rilevante negli attacchi informatici con finalità di sottrazione illecita dei dati (***data breach***) e di conseguente esposizione nella **dark web.** Secondo stime Risk Based Security, si tratta di un 50% in più sul 2018, con 4.000 violazioni e 4 miliardi di record compromessi.
Secondo altre fonti, come Troy Hunt, sono 8 miliardi le credenziali raccolte illegalmente su internet.

Ad essere maggiormente prese di mira dai cyber criminali sono comunque le aziende. Secondo un nuovo **Report di ImmuniWeb**, **negli ultimi 12 mesi sono state rubate e riversate nella dark web oltre 16 milioni di password appartenenti alle società che fanno parte della celebre classifica Fortune 500**. (principalmente terze parti, partner esterni, fornitori).
Fortune 500 è la celebre lista annuale compilata e pubblicata

dalla rivista Fortune, all'interno della quale trovano posto le 500 maggiori imprese societarie statunitensi con il fatturato più elevato.
Complessivamente, però, sono 21 milioni le credenziali sottratte e nel 95% dei casi si tratta di password non crittografate o rinforzate. Diciamo che nella stragrande maggioranza dei casi si è trattato di "*password troppo facili*".

L'indagine ha svelato che **più di 5 milioni di credenziali sottratte appartengono a società tecnologiche**, **4,9 milioni a organizzazioni finanziarie**, quasi **2 milioni ad aziende sanitarie**, più di 1,7 milioni di password a gruppi industriali, altri 1,7 milioni ad utilities, 1,3 milioni alle telcos, 600 mila a testa alle imprese del retail e dei trasporti, circa 500 mila ad imprese aerospaziali e attive nel settore della Difesa.

Le password, come detto erano piuttosto facili e non abbastanza protette, molte di queste evidenziano una semplicità disarmante: "*password*", "*password1*", "*123456*", "*abc123*", "*benvenuto*", "*000000*", "*111111*", fino alla classica "*apritisesamo*".
Chiarissimi esempi di password spesso predefinite o create in automatico.

Le aziende che hanno mostrato eccessiva superficialità sono state quelle del commercio al dettaglio (47,29%), delle telecomunicazioni (37,57%), dell'industria, (37,36%) dei trasporti (36,19%), della finanza (35,15%), dell'aerospaziale (34,44%), dell'high tech (33,88%).

> *Nel dark web 16 milioni di password rubate alle aziende di Fortune 500*

Spyware e sorveglianza di massa: WhatsApp porta in tribunale l'israeliana NSO Group

Lo scorso maggio la notizia di **WhatsApp** "*bucato*" ha fatto il giro del mondo. Sfruttando un punto debole nella funzione di chiamata vocale, uno spyware denominato "*Pegasus*" ha sostanzialmente sorvegliato di nascosto un gran numero di utenti appartenenti a categorie di elevato profilo civile e politico.

Le vittime della "*spiata di massa*" sono state soprattutto personalità impegnate nella difesa dei diritti civili, giornalisti, avvocati, attivisti, investigatori internazionali, movimenti e gruppi di opposizione politica, manager, imprenditori, organizzazioni della società civile e altre figure chiave attive nel settore.

Ora, si legge sul profilo LinkedIn di Nicola Vanin, esperto di Data Governance and Information security, **WhatsApp ha annunciato che porterà in aula di tribunale la NSO Group**, una società israeliana leader mondiale nella creazione di malware destinati a telefoni cellulari e dispositivi.

Secondo i ricercatori WhatsApp, infatti, dietro agli attacchi subiti nei mesi scorsi spunta proprio la NSO Group con i suoi server.
L'accusa è che la NSO ha volontariamente sfruttato una vulnerabilità per colpire circa 1.400 smartphone con un malware progettato per infettare allo scopo di condurre la sorveglianza su utenti specifici di WhatsApp.

L'*hacking*, in sostanza, ha consentito a NSO Group e ai suoi clienti di spiare messaggi, email e telefonate, nonché le telecamere e microfoni dei dispositivi in questione.

La NSO, ha dichiarato sul Washington Post il vice presidente e product manager del Gruppo Facebook**, Will Cathcart**, "*ha preso di mira almeno un centinaio di difensori dei diritti umani, giornalisti e altri membri della società civile in tutto il mondo*".

La società israeliana ha quindi avuto accesso ai server WhatsApp e li ha utilizzati al fine di emulare il traffico di rete legittimo e le chiamate di WhatsApp come parte delle operazioni per infettare i dispositivi di destinazione. Un lavoro considerato dagli esperti "*di alto livello*", perché il codice dannoso era embeddato all'interno delle chiamate stesse.

La NSO si è sempre difesa affermando che il software incriminato ("*Pegasus*") è stato venduto ad agenzie governative e forze dell'ordine di vari Paesi, che sono responsabili direttamente dell'uso che ne fanno. Sostenendo anzi di contribuire ampiamente alla lotta al terrorismo e altri reati odiosi, come la pedofilia in rete, proprio grazie a questa tecnologia.

Il dubbio è che tale presunta missione *pro bono* nasconda invece torbidi interessi, legati allo spionaggio internazionale, alla sorveglianza di singoli soggetti e/o organizzazioni, attive come detto nell'ambito della tutela dei diritti umani, e alla raccolta di informazioni sensibili senza alcuna autorizzazione, anche a scopo di ritorsione e minaccia.

Una storia, tra molte altre, di spionaggio ai danni di liberi cittadini, permessa da tecnologie di utilizzo quotidiano, i nostri device personali. Un argomento delicato, che andrebbe

approfondito, soprattutto da un punto di vista giuridico, regolatorio e certamente culturale.
Un campanello d'allarme che suona da troppo tempo, sia per i Governi, sia per le stesse aziende tecnologiche, perché il solo fatto che esistano e vengano venduti regolarmente strumenti per la sorveglianza del prossimo è un fatto grave, una minaccia concreta alle libertà fondamentali di tutti noi.

https://www.key4biz.it/spyware-e-sorveglianza-di-massa-whatsapp-porta-in-tribunale-lisraeliana-nso-group/277282/

Privacy, le app di viaggio sono conformi agli standard di sicurezza?

Le app di viaggio sono tra le app più popolari da scaricare per gli utenti di smartphone, in particolare quelle che consentono di ottenere i prezzi più bassi sui viaggi o di garantire le migliori offerte possibili.

Tuttavia, la facilità e la convenienza di utilizzo di queste app di viaggio hanno un prezzo molto elevato per quanto riguarda la privacy e la sicurezza.

Secondo uno studio condotto dal fornitore di soluzioni di sicurezza mobile **Zimperium** (*A Zimperium Analysis of the Top 30 Mobile Travel Apps' Privacy and Security Risks*), la totalità delle app basate su iOS e quasi la metà delle app basate su Android non hanno ricevuto un voto positivo con riferimento alla conformità per la privacy.

Inoltre, la totalità delle app basate sia su iOS e sia su

Android non ha ricevuto un voto positivo con riferimento alla conformità per la sicurezza. In breve, quasi tutte le app di viaggio che si scaricano da **Google Play** o da **Apple Store** non soddisfano gli standard di base di sicurezza e di privacy.

Vulnerabilità su privacy

I ricercatori hanno analizzato le app di viaggio per vedere il loro comportamento rispetto ai parametri di riferimento del settore per la privacy.

Ogni singola app di viaggio per iOS ha fallito test sulla privacy – sebbene l'impegno profuso da Apple per la tutela della privacy e per evidenziare iPhone come il miglior smartphone sul mercato per chiunque sia preoccupato per la sicurezza dei dati personali.

Come esempio di non protezione della privacy degli utenti, la quasi totalità delle app basate su iOS è stata in grado di acquisire schermate dell'interfaccia utente, fornendo agli sviluppatori delle app o a terze parti sconosciute informazioni sulle app installate sul telefono, nonché le configurazioni preferite dell'utente.

Inoltre, i tre quarti delle app attuano funzionalità di localizzazione puntuale. Ci si può chiedere per quale motivo le app di viaggio che vendono pacchetti hotel e voli dovrebbero conoscere la posizione precisa dell'utente.

E le cose non sono state migliori nel caso delle app di viaggio basate su Android. I ricercatori hanno scoperto che un decimo delle app accede alla cronologia delle chiamate dell'utente e talvolta anche agli elenchi di contatti.

Vulnerabilità su sicurezza

Se i risultati sulla privacy sembrerebbero desolanti, quelli relativi alla sicurezza lo sono ancor di più. Tutte le app di viaggio basate su iOS non hanno superato i test di sicurezza e allo stesso modo ha fallito la quasi totalità delle app di viaggio basate su Android. Nel caso delle app basate su iOS, si utilizza un metodo di autenticazione che può essere utilizzato da utenti esterni per intercettare le comunicazioni inviate tra il telefono e altri utenti.

Nel caso delle app di viaggio basate su Android, nella metà dei casi si consente injection di oggetti Java in fase di esecuzione – ciò che potrebbe essere utilizzato per iniettare codice dannoso nello smartphone.

Scegliere Mobile app tenendo conto di privacy e sicurezza

Se c'è un insegnamento da trarre dal rapporto su come le app di viaggio si comportano rispetto agli standard di sicurezza e di privacy, è quello per cui sia gli sviluppatori di app e sia interi ecosistemi di app hanno fatto pochissimi progressi per indirizzare i problemi di sicurezza e di privacy.

Nel caso di Apple, ci si può domandare come mai tante app di viaggio sono state autorizzate in Apple Store quando presentano così tanti problemi con la privacy e la sicurezza.

Gli sviluppatori di app dovrebbero fare di più per garantire che le app siano conformi agli standard di sicurezza e di privacy, evitando che un utente malintenzionato possa sfruttare le vulnerabilità di sicurezza.

Per gli utenti, il fatto che le app di viaggio più popolari abbiano prestazioni così scarse in termini di standard di sicurezza e di privacy dovrebbe essere una vera e propria

sveglia per prestare maggiore attenzione a quali app si scaricano e al modo in cui si usano.

https://www.key4biz.it/privacy-le-app-di-viaggio-sono-conformi-agli-standard-di-sicurezza/277271/

Unicredit, nel 2015 accesso non autorizzato ai dati di 3 milioni di utenti

Stamattina il Gruppo Unicredit ha diffuso una nota stampa relativa ad "***un accesso non autorizzato a dati relativo a un file generato nel 2015. Questo file conteneva circa 3 milioni di records***". Una notizia riferita al "*perimetro italiano*" e che ha subito messo in allarme i tanti correntisti della banca, la quale ha peraltro assicurato "*che non sono stati compromessi altri dati personali, né coordinate bancarie in grado di consentire l'accesso ai conti dei clienti o l'effettuazione di transazioni non autorizzate*".

La scoperta dell'attacco informatico è stata fatta dal team di sicurezza interno a Unicredit, che ha identificato un accesso non autorizzato ai dati. il Gruppo ha escluso perentoriamente che siano stati violati i conti bancari, ma certo **la violazione ha interessato dati sensibili**, come nomi e cognomi di utenti, città di residenza, numero di telefono, indirizzo di posta elettronica.

"*UniCredit ha immediatamente avviato un'indagine interna e ha informato tutte le autorità competenti, compresa la polizia*".
Il comunicato informa che **saranno contattate "*tutte le persone potenzialmente interessate*"** dall'evento.

Per chi volesse ricevere informazioni su quanto accaduto può telefonare al numero verde messo a disposizione da Unicredit: **800 323285**.

Dal 2016 ad oggi, fanno sapere da Unicredit, il Gruppo ha investito 2,4 miliardi di euro per l'aggiornamento e il rafforzamento dei sistemi IT e della sicurezza informatica, mentre lo scorso giugno è stato potenziato il sistema di autenticazione ("*strong customer authentication*"), offrendo anche l'opzione dell'identificazione biometrica.

> *Unicredit, nel 2015 accesso non autorizzato ai dati di 3 milioni di utenti*