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/

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/

Pagamenti elettronici, qual è il livello di sicurezza attuale?

In questi giorni di fervide trattative per il varo della legge finanziaria, i pagamenti elettronici sono sotto i riflettori degli organi di informazione e all'attenzione della classe politica e dei cittadini come mai avvenuto in precedenza.

E' opportuno ricordare scenari di minacce informatiche che possono inficiare il valore assicurato dall'impiego del servizio di pagamento elettronico, come il caso relativo alle carte *contactless* (senza contatto) e *mobile wallet* (portafoglio mobile)

Nuove vulnerabilità offrono agli hacker la possibilità di aggirare i limiti di pagamento sulle carte contactless **Visa** indipendentemente dal terminale della carta, secondo una ricerca di **Positive Technologies** (Visa card vulnerability can bypass contactless limits.)

In un comunicato stampa del 29 luglio, Positive Technologies ha affermato che i ricercatori hanno testato più volte i difetti con cinque principali banche del Regno Unito e con carte e terminali al di fuori del Regno Unito. Hanno scoperto che i limiti potevano essere aggirati il □□100% delle volte e

potevano consentire a un attaccante di rubare dai conti.

Scenario di attacco

L'attacco funziona manipolando due campi di dati che vengono scambiati tra la carta e il terminale durante un pagamento contactless. Soprattutto nel Regno Unito, se il pagamento necessita di un'ulteriore verifica del titolare della carta (che è richiesta per pagamenti superiori a 30 sterline nel Regno Unito), le carte risponderanno "Non posso farlo", il che impedisce di effettuare pagamenti oltre questo limite. *In secondo luogo, il terminale utilizza impostazioni specifiche del paese, che richiedono che la carta o il portafoglio mobile forniscano un ulteriore verifica del titolare della carta, ad esempio inserendo il PIN della carta o l'autenticazione tramite impronta digitale sul telefono*", si legge nel comunicato stampa.

I controlli sono stati aggirati utilizzando un dispositivo che fungeva da proxy per intercettare la comunicazione tra il terminale di pagamento e la carta, un attacco noto come man in the middle (MITM). Questi attacchi MITM possono anche essere eseguiti utilizzando i portafogli mobili, consentendo a un truffatore di caricare fino a £ 30 senza sbloccare il telefono.

La sicurezza dei pagamenti elettronici

Secondo il comunicato "*Il dispositivo dice alla carta che la verifica non è necessaria, anche se l'importo è superiore a £ 30. Il dispositivo quindi comunica al terminale che la verifica è già stata effettuata con altri mezzi. Questo*

attacco è possibile perché Visa non richiede che gli emittenti e gli acquirenti dispongano di controlli che blocchino i pagamenti senza presentare la verifica minima".

"L'industria dei pagamenti ritiene che i pagamenti contactless siano protetti dalle garanzie che hanno messo in atto, ma il fatto è che le frodi sono in aumento. Sebbene si tratti di un tipo di frode relativamente nuovo e al momento potrebbe non essere la priorità numero uno per le banche, se i limiti di verifica senza contatto possono essere facilmente aggirati, ciò significa che potremmo vedere perdite più dannose per le banche e i loro clienti.", secondo il comunicato.

Salvaguardia e raccomandazioni

I ricercatori Positive Technologies suggeriscono che gli utenti di carte contacless devono essere vigili nel monitorare i loro estratti conto bancari per rilevare tempestivamente le frodi e, se disponibili con la propria banca, implementare ulteriori misure di sicurezza come limiti di verifica dei pagamenti e notifiche via SMS.

https://www.key4biz.it/pagamenti-elettronici-qual-e-il-livello-di-sicurezza-attuale/276177/

Cybercrime, il 66% delle PMI subisce attacchi. Phishing l'arma più usata

Il sondaggio annuale **Ponemon sulle PMI** (*2019 Global State of Cybersecurity in Small and Medium-Sized Businesses)* è

interessante in quanto cerca specificamente attacchi mirati.

Ci si aspetterebbe che il numero degli attacchi alle PMI cresca su tutta la gamma possibile man mano che gli strumenti di hacking automatizzati diventano più diffusi, invece gli attacchi registrati nel sondaggio sono sofisticati e coinvolgono azioni come il phishing mirato a e-mail di un dipendente o l'ottenimento di dati aziendali specifici.

Il sondaggio di quest'anno ha incluso 2.391 professionisti della sicurezza IT e decisori di aziende situate negli Stati Uniti, nel Regno Unito e in tutta Europa. Le aziende variano da 100 a 1.000 dipendenti e i dati sono stati raccolti in agosto e settembre.

I nuovi attacchi sembrano concentrarsi sulle PMI in regioni specifiche, con gli Stati Uniti che ottengono il peggior risultato. Il numero complessivo di attacchi globali alle PMI è rimasto abbastanza stabile, forse addirittura leggermente diminuito (passando dal 67% nel 2018 al 66% nel 2019). Ciò avviene dopo anni di crescita costante e significativa; dal 55% nello studio inaugurale nel 2016 al 61% nel 2017.

Il tipo di attacco globale più comune è il phishing, di cui il 57% delle PMI globali è stato vittima nello scorso anno. Anche i dispositivi rubati e compromessi (33%) e il furto di credenziali (30%) sono vie comuni di attacco.

La perdita di dati è il risultato più comune degli attacchi informatici alle PMI. Il 69% delle aziende negli Stati Uniti che hanno risposto ha perso informazione personale sensibile appartenente a dipendenti o a clienti. È un aumento del 50% da quando è stato condotto il primo sondaggio Ponemon nel 2016.

Le tecnologie

Le nuove tecnologie sembrano essere uno dei principali fattori alla base di questi attacchi. Gli sviluppi relativamente recenti come i dispositivi Internet of Things (IoT), la biometria e l'uso di dispositivi mobili personali per il lavoro sono stati rapidamente e ampiamente adattati dalle PMI. Ma le tecnologie e le pratiche di sicurezza tendono a rimanere indietro in queste aree.

Le aziende sembrano esserne consapevoli, ma sentono di non poter fare nulla al riguardo. Il 49% degli intervistati ritiene che l'uso di dispositivi mobili con applicazioni business-critical abbia indebolito la postura di sicurezza dell'organizzazione.

L'80% ritiene che i dispositivi IoT non garantiti possano portare a un incidente catastrofico sulla sicurezza, ma solo il 21% di queste aziende sta monitorando attivamente questi dispositivi. Il 75% degli intervistati ha implementato la biometria nel proprio profilo di sicurezza o intende farlo presto.

Benefici del GDPR

Grazie all'influenza del Regolamento generale sulla protezione dei dati (GDPR), varie regioni d'Europa hanno riferito di una maggiore fiducia nella loro postura di sicurezza e hanno dovuto gestire meno attacchi informatici nell'ultimo anno.

La regione **DACH** (Austria, Germania e Svizzera) ha effettivamente la migliore postura di sicurezza dell'IoT, sebbene i numeri complessivi siano ancora relativamente bassi. DACH ha guidato tutte le altre parti del mondo con il 27% delle loro PMI che conduce formazione sulla sicurezza IoT per dipendenti e fornitori e il 25% monitora attivamente i dispositivi IoT utilizzati sul posto di lavoro per violazioni

dei dati.

Tuttavia, queste aziende hanno anche espresso la minima preoccupazione per le password dei dipendenti, con solo il 58% che ha risposto che si trattava di un problema di sicurezza.

Benelux (Belgio, Lussemburgo e Paesi Bassi) ha registrato uno dei tassi più bassi di attacchi informatici contro le PMI. Questa regione aveva un'alta enfasi sulla sicurezza delle password complesse (68%) e ha guidato gli intervistati nell'implementazione della biometria (51%).

In Scandinavia il 64% delle PMI ha subito attacchi informatici e il 71% di queste ha riferito che malware o exploit sono riusciti a superare la propria sicurezza.

La Scandinavia è stata anche l'unica regione a concentrarsi principalmente sulla protezione della proprietà intellettuale, mentre altre regioni hanno dato la priorità alla protezione dei dati dei clienti.

Futuri scenari di sicurezza per PMI

Questi rapporti annuali chiariscono che se c'è un bersaglio vulnerabile là fuori, ci sarà un hacker interessato ad esso, non importa quanto piccolo possa sembrare. Sebbene le PMI non affrontino lo stesso profilo di rischio che devono affrontare le grandi organizzazioni aziendali (come attacchi provenienti da parte di gruppi di **APT** sponsorizzate da stati), tuttavia affrontano abbastanza attacchi informatici che un piano di prevenzione e risposta è vitale.

https://www.key4biz.it/cybercrime-il-66-delle-pmi-subisce-attacchi-phishing-larma-piu-usata/275600/

Come tutelare le infrastrutture critiche e come gestire i dati degli utenti con la blockchain

Quali misure adottare in caso di disastri naturali o causati dall'uomo; come tutelare le infrastrutture critiche nazionali e in che modo gli utenti, attraverso a una piattaforma basata sulla blockchain, possono gestire i propri dati personali, in caso di cessione a soggetti terzi. Questi sono i temi principali del workshop internazionale sulla Data Protection e sicurezza nelle situazioni di emergenza, che si terrà il 24 ottobre prossimo presso la sede dello studio legale di **E-Lex** (via dei Barbieri, 6 – Roma).

Giovanni Maria Riccio, professore di Diritto comparato all'Università di Salerno e socio dello studio legale E-Lex, ci spiega nel dettaglio i 4 progetti che saranno presentati nel corso del workshop.

Key4biz. ***Su quale tema verterà il workshop internazionale?***

Giovanni Maria Riccio. Il workshop è articolato in due

sessioni. Nella prima, dopo una mia breve introduzione, saranno presentati quattro progetti finanziati nell'ambito della misura **Horizon 2020**. Si tratta di quattro progetti; in tre di questi progetti, quale partner giuridico, è presente lo studio **E-Lex**. "*Assistance*" è una ricerca che si occupa delle misure da adottare in caso di disastri, causati dalla natura o dall'uomo: un tema, quindi, molto importante, perché spazia dai cambiamenti climatici, e gli effetti che tali cambiamenti determinano in termini di situazioni catastrofiche, al terrorismo, nazionale e internazionale. "*Defender*", invece, è un progetto focalizzato sulla tutela delle infrastrutture critiche, ossia di tutte quelle infrastrutture – dalle reti di telecomunicazioni, al sistema dei trasporti, ai servizi bancari – che consentono la 'sopravvivenza' di una Nazione. Aspetti analoghi sono affrontati anche da "*Faster*". Il quarto progetto presentato, "*PoSeID-on*", mira alla creazione di una piattaforma attraverso la quale, anche per mezzo dell'uso della blockchain, gli utenti possono monitorare la 'vita' dei propri dati personali, in caso di cessione di tali dati a soggetti terzi. È un progetto sicuramente molto interessante, al pari degli altri, anche perché prevede il coinvolgimento di società che trattano dati personali, che, aderendo alla piattaforma, dimostrano una sensibilità effettiva e non solo dichiarata alla problematica del trattamento dei dati personali.

Key4biz. ***Quali sono i progetti e il ruolo della Commissione in ambito privacy?***

Giovanni Maria Riccio. L'attenzione della Commissione in materia di data protection è altissima. I progetti finanziati da Horizon 2020, anche quando non sono direttamente connessi con l'ambito privacy, hanno quasi sempre un collegamento con tale materia, a dimostrazione della sua centralità in tutti i flussi economici e sociali. I progetti che saranno presentati

nel corso del workshop, come dicevo, spaziano in ambiti differenti: eppure non sfugge come un attacco a una infrastruttura critica – ad esempio, a un operatore di telefonia o a reti di comunicazione – potrebbe essere determinato proprio dalla necessità di sottrarre dati, non necessariamente di natura personale. Discorso identico potrebbe essere fatto per lo studio degli eventi catastrofici, che impongono di soffermarsi su misure di *disaster recovery* che consentano non solo l'operatività continua dei servizi intaccati, ma altresì il recupero dei dati che potrebbero andar persi.

Key4biz. ***Quali quelli in ambito security?***
Giovanni Maria Riccio. A questa domanda, risponderei a mia volta con un'altra domanda: esiste privacy senza security? A mio avviso, ma si tratta anche dell'impostazione che mi sembra sia adottata in tutte le linee di ricerca, sono due aspetti interconnessi. Non dimenticherei, peraltro, il ruolo che sta assumendo il dibattito su *ethics e data protection*: non è un caso che il **GDPR**, nel sancire i principi applicabili al trattamento dei dati personali, parli di liceità e trasparenza, ma altresì di correttezza. A questo principio, del resto, si ispirano anche tutte le misure finalizzate a minimizzare i rischi associati al trattamento dei dati personali, quali, a titolo esemplificativo, la progettazione secondo canoni di privacy by design e privacy by default.

Speaker

Manuel Esteve – Universitat Politècnica de València – Assistance: https://assistance-project.eu

Luca Del Pizzo, Ministero dell'Economia e delle Finanze – PoSeID-on: https://www.poseidon-h2020.eu

Giuseppe Caracciolo, KPRF – Faster https://www.faster-project.eu

Gabriele Giunta, Engineering – Defender http://defender-project.eu

Dibattito

Angelo Tofalo – Sottosegretario alla Difesa

Silvia Scarpa – Università di Roma Luiss Guido Carli

Luigi Carrozzi – Autorità Garante per la protezione dei dati personali

https://www.key4biz.it/come-tutelare-le-infrastrutture-critiche-e-come-gestire-i-dati-degli-utenti-con-la-blockchain/275429/

Jack Ma: 'Alibaba subisce 300 milioni di attacchi informatici ogni giorno'

"***Alibaba*** *subisce circa 300 milioni di tentativi di attacchi informatici al giorno*". A dirlo è **Jack Ma**, il fondatore ed ex Presidente del colosso cinese del commercio elettronico, ritirato da Alibaba il mese scorso 20 anni dopo la fondazione dell'azienda.

Ieri, a Singapore, ha ricevuto il **Malcolm S Forbes Lifetime Achievement Award** per i suoi "eccezionali" contributi all'imprenditoria. E' il primo imprenditore del settore Internet a vincere il premio.

Ma, durante la premiazione, ha affermato di essere "orgoglioso" del fatto che, nonostante la sfilza di attacchi informatici, **Alipay** – la piattaforma dei pagamenti del gruppo che riporta quasi 1 miliardo di utenti ed elabora transazioni per un valore di 50 miliardi di dollari al giorno – gli hacker non sono riusciti ancora a rubare "un centesimo".

AI: Alibaba Intelligence

A febbraio Alibaba ha dovuto affrontare un vasto tentativo di attacco informatico, che ha minacciato di compromettere i conti di 20 milioni di utenti sul suo sito di eCommerce di **Taobao**.

Ma ha citato le capacità tecnologiche avanzate dell'azienda, che ha soprannominato "**AI: Alibaba Intelligence**", per il suo continuo tasso di successo, osservando che le macchine sono superiori agli umani nell'usare la logica per contrastare i criminali informatici.

"*Insegniamo alla macchina tutti i modi in cui le persone (stanno) barando*", ha detto Ma. "*La macchina ricorda milioni di modi di barare, quindi quando iniziamo a barare, la (macchina) sa già che stai barando. In questo modo stiamo proteggendo tutta la tecnologia.* "

Per raggiungere questo grado di accuratezza, tuttavia, Ma ha osservato che la società deve raccogliere ampie parti dei dati dei clienti. Ha sostenuto che ciò ha permesso ad Alibaba di sviluppare tecnologie all'avanguardia di difesa per quanto riguarda la sicurezza informatica.

https://www.key4biz.it/jack-ma-alibaba-subisce-300-milioni-di-attacchi-informatici-ogni-giorno/275341/

Ransomware, le cyber assicurazioni alimentano il cybercrime?

Il trattamento dei rischi informatici si avvale di differenti opzioni fra le quali emerge la stipula di una cyber assicurazione.

Molti assicuratori inizialmente erano riluttanti a coprire i disastri informatici, in parte a causa della mancanza di dati attuariali affidabili. Quando proteggono i clienti da rischi tradizionali quali incendi, inondazioni e incidenti automobilistici, stabiliscono una politica dei prezzi basata su informazioni autorevoli provenienti da fonti nazionali e industriali.

Come notato da **Lloyd** in un rapporto del 2017, "*non esistono fonti equivalenti per il cyber-rischio*" e i dati utilizzati per impostare i premi sono raccolti da Internet. È probabile che tali dati disponibili al pubblico sottostimino il potenziale impatto finanziario del rischio informatico per un assicuratore.

Secondo un rapporto della società di consulenza globale **PwC**, sia gli assicuratori e sia le aziende vittime sono riluttanti a rivelare violazioni a causa di preoccupazioni sulla perdita di vantaggio competitivo o danni alla reputazione.

Uno dei disastri informatici in cui può incorrere un'organizzazione e per il quale si stipulano cyber

assicurazioni è il materializzarsi di un ransomware, come altresì evidenziato dall'annuale rapporto Internet *Organised Crime Threat Assessment (***IOCTA**) di **Europol**.

Perché pagare un ransom?

Nonostante i costanti avvertimenti delle autorità di contrasto al crimine, secondo cui le organizzazioni non dovrebbero mai pagare richieste di riscatto, esiste la ragionevole possibilità che l'intero sistema di cyber assicurazioni, ora disponibile per le organizzazioni sia grandi e sia piccole, non faccia altro che aggravare il problema. Una recente ricerca di **ProPublica** (*The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks*) evidenzia tale fenomeno.

Ogni qual volta venisse erogato un pagamento tramite una assicurazione informatica, si alimenterebbe l'attività criminale e si incoraggerebbero più hacker ad attaccare le aziende e gli enti del settore pubblico per ottenere denaro portando i loro sistemi informatici offline. Di conseguenza, l'assicurazione informatica in questo scenario aumenterebbe e non diminuirebbe i rischi informatici.

Potrebbe sembrare contro intuitivo, ma le compagnie assicurative sarebbero effettivamente incentivate a pagare richieste di riscatto, anche se fossero decine e persino a centinaia di migliaia di euro. Il motivo è semplice: è più economico, più veloce e più semplice sborsare una grossa somma di denaro piuttosto che occuparsi di coprire tutti i costi d'interruzione delle attività e i ritardi del riavvio da zero di un'azienda.

In altre parole, se le compagnie assicurative non pagassero il riscatto, potrebbero essere necessarie settimane prima che un'organizzazione si rialzi e funzioni correttamente.

Nel frattempo, tali compagnie di cyber assicurazioni

dovrebbero coprire il costo dei profitti persi durante i tempi d'inattività delle società, nonché i costi dell'assunzione di consulenti IT per ripristinare dalle risorse di backup le attività operative delle società. Quindi, avrebbe più senso sistemare le cose rapidamente e facilmente con un pagamento di riscatto e andare avanti con gli affari.

Qui le cose diventano molto perverse: gli hacker che eseguono attacchi ransomware potrebbero sfruttare questa mentalità, e in particolare prendendo di mira aziende o organizzazioni che dispongono di polizze informatiche per proteggere i sistemi operativi mission-critical. Con semplice calcolo, potrebbero capire le dimensioni della polizza assicurativa informatica, la probabilità che una società debba cedere alle richieste di riscatto e quanto dovrebbero chiedere come parte del riscatto.

L'importo ottimale da richiedere in una richiesta di riscatto sarebbe di 1 € in meno rispetto al costo che una società impiegherebbe per ripristinare i suoi sistemi informatici. Da una semplice analisi costi-benefici, è razionale ed economico pagare il minore dei due mali, specialmente quando è possibile ripristinare il funzionamento dei sistemi in 24 ore o meno (e non giorni, settimane o mesi che potrebbe richiedere il ripristino da un sistema di backup).

Quale futuro per Cyber Assicurazioni?

Tutto ciò, ovviamente, solleva interrogativi sul futuro del mercato delle cyber assicurazioni. Le compagnie assicurative s'impegnando nel raccogliere più premi mensili possibili dalle aziende che acquistano l'assicurazione cyber per proteggersi dall'impatto economico degli attacchi ransomware. Ciò incentiverebbe più hacker a produrre ransomware. L'intero sistema di cyber assicurazioni sarebbe a rischio di implodere su se stesso.

Pagare il riscatto in un attacco di ransomware è la soluzione facile a breve termine, ma a lungo termine renderebbe il problema molto grave. Ora che gli hacker sanno che le aziende stanno stipulando enormi cyber assicurazioni, sanno esattamente a chi rivolgersi.

Con attenta analisi, sanno chi probabilmente pagherà e quanto. In futuro, quindi, potrebbe essere necessario che organizzazioni come l'associazione nazionale delle compagnie assicurative, intervengano e stabiliscano alcune regole di base per l'industria delle assicurazioni.

Le organizzazioni non dovrebbero mai pagare la richiesta di riscatto e gli incentivi devono essere messi in atto per assicurarsi che il pagamento del riscatto non avvenga mai.

https://www.key4biz.it/ransomware-le-cyber-assicurazioni-alimentano-il-cybercrime/274507/

Europol, il cybercrime si evolve in fretta. Il ransomware rimane la principale minaccia informatica

Il crimine informatico continua a maturare spostando la sua attenzione su obiettivi più ampi e più redditizi, per raggiungere un unico obiettivo: i dati personali.

Sono questi i risultati che emergono dalla sesta edizione

dell'*Internet Organised Crime Threat Assessment* (**IOCTA**) di **Europol**, l'agenzia anticrimine europea nata nel 1999, uno studio accurato che fornisce informazioni dettagliate sulle minacce emergenti e sugli sviluppi della sicurezza informatica.

Secondo il rapporto, le nuove minacce non derivano solo dalle nuove tecnologie, ma spesso provengono da vulnerabilità già presenti nelle tecnologie esistenti. Le forze dell'ordine – spiega il documento – devono pertanto non solo concentrarsi sul potenziale impatto dei futuri sviluppi tecnologici nel crimine informatico, come l'intelligenza artificiale, ma anche affrontare il crimine informatico in senso olistico, compresa la prevenzione, la consapevolezza e l'aumento della cyber educazione.

"*Alcune minacce di ieri rimangono rilevanti oggi e continueranno a sfidarci domani*", ha dichiarato **Catherine De Bolle**, direttore esecutivo di Europol.

"L'impatto globale che ha acquisito la sicurezza informatica ha portato la minaccia del crimine informatico ad un altro livello", spiega De Bolle. "*Serve sviluppare strumenti chiave per tenere sotto controllo i criminali informatici, considerando che altre aree criminali stanno diventando sempre più agevolate dal mondo informatico".*

Il report evidenzia come quest'anno il ransomware rimane la principale minaccia alla criminalità informatica, seguito dagli attacchi **DDoS**, dal materiale di sfruttamento sessuale dei minori e dai mercati di blockchain, incluso il deepweb. La risposta coordinata agli attacchi informatici su vasta scala rimane una sfida chiave per un'efficace cooperazione internazionale, conclude il rapporto.

Clicca qui per scaricare il report completo IOCTA 2019

https://www.key4biz.it/europol-il-cybercrime-si-evolve-in-fretta-il-ransomware-rimane-la-principale-minaccia-informatica/274370/

DarkHotel, chi sono gli Hacker del Wi-Fi e perché colpiscono gli Hotel

DarkHotel è un gruppo di Criminal hacker legati alla **Corea del Nord** che è attivo almeno dal 2007. Si tratta di un vero e proprio *omen-nomen* in quanto il gruppo ha ottenuto il suo nomignolo per aver compromesso il Wi-Fi e tutte le reti di vari hotel di lusso. A seconda delle occasioni possono anche chiamarsi **Tapaoux, Pioneer, Karba e Nemim**.

Un solo obiettivo

Il gruppo utilizza una combinazione di metodi altamente sofisticati per intrappolare le vittime, ma gli hack alberghieri continuano ad essere un obiettivo di alto valore.

La maggior parte degli hotel colpiti si trovano in Asia, ma non mancano le strutture che sono rimaste vittime di questi attacchi anche negli Stati Uniti e in Europa.

Le vittime dei Criminal hacker sono state identificate in Corea del Nord, Russia, Corea del Sud, Giappone, Bangladesh, Thailandia, Taiwan, Cina, Stati Uniti, India, Mozambico, Indonesia e Germania.

Mentre la prima campagna di spionaggio DarkHotel è stata scoperta dagli esperti di Cyber Security alla fine del 2014.

Il Modus operandi

Questo *Advanced Persistent Threat* si affida principalmente a campagne di **spear-phishing.** Il loro bersaglio? Sottrarre dati sensibili dai top executive, tra cui CEO, Senior Vice-President, direttori vendite e marketing di varie organizzazioni, mentre soggiornano negli hotel di lusso.

Questi dirigenti di alto livello provengono principalmente dai settori manifatturiero, della difesa, dei capitali, farmaceutico, delle forze dell'ordine, dagli ranghi militari e di altri settori.

Per fare tutto questo gli aggressori sfruttano diversi metodi, compresi gli exploit zero-day per penetrare nei sistemi bersaglio.

Uno dei loro preferiti è una vulnerabilità Flash. Questo inizia il suo processo di hacking compromettendo le reti Wi-Fi.

Da qui, una volta che gli utenti si connettono alla rete, vengono rappresentati con una finestra di dialogo che chiede loro di installare un falso aggiornamento.

L'aggiornamento falso è in realtà un pezzo di malware con firma digitale.

Il Malware usato dal Gruppo nord coreano, come se non bastasse, arriva equipaggiato con svariati keylogger che sottraggono tutto il rubabile e lo trasmettono direttamente alla fonte dell'attacco.

È curioso notare come negli hotel, solitamente, queste installazioni di keylogger e malware sono distribuite in modo selettivo e a individui mirati.

Questo gruppo di Criminal Hacker sembra sapere in anticipo quando le vittime prescelte arriveranno nelle strutture dai loro hotel di lusso e in che data lasceranno l'hotel.

È questo il modus operandi degli aggressori: aspettare in attesa fino a quando le loro vittime arrivano e si connettono a Internet, come è stato efficacemente analizzato dagli esperti di Cyber Security che hanno studiato le attività di DarkHotel.

Per fare questo il gruppo di Criminal Hacker viola tutti i sistemi degli hotel che mantengono tracciate e registrare le informazioni di check-in e check-out degli ospiti. Accedendo a questo all'elenco, gli aggressori sono in grado di raccogliere informazioni sui loro obiettivi principali. Gli aggressori possono accedere, tra l'altro, a informazioni quali l'orario di arrivo e di partenza previsto della vittima, il numero di camera e il nome completo.

Oltre ad inquinare le reti peer-to-peer per infettare le masse, DarkHotel utilizza una serie di certificati digitali per estendere il perimetro del loro attacco. Il gruppo sfrutta i certificati digitali scarsamente implementati per firmare il loro malcode.

Attualmente, stanno rubando e riutilizzando altri certificati legittimi per firmare il loro set di strumenti, per lo più backdoor e info stealer. La loro infrastruttura cresce e si restringe nel tempo, senza un modello coerente di configurazione. È allo stesso tempo protetta con una crittografia flessibile dei dati e mal difesa con funzionalità deboli e mal implementate.

Gli strumenti dei Criminal Hacker

Darkhotel ha solo l'imbarazzo della scelta quando si tratta di scegliere gli strumenti e le tattiche per compromettere una rete alberghiera. Tra questi:

- **Keylogger:** Visto e considerato come la maggior parte degli hotel hanno computer e reti accessibili al pubblico;
- **Malware:** li utilizzano installando un semplice downloader di malware o malware sul computer dell'ospite per raccogliere informazioni;
- **Zero day**
- **Spear-phishing:** DarkHotel utilizza questi attacchi targhettizzati ad hoc per diffondere malware

Come arginare la minaccia

Ovviamente per ogni problema sollevato dalle azioni di DarkHotel esiste una soluzione in grado di mettere dei paletti saldi e costruire il Cyber Security Framework adeguato. In primis, se la violazione è già avvenuta il primo passo da fare è seguire una procedura di Data Recovery.

Per testare la sicurezza dei propri network che, come abbiamo illustrato, sono una delle vie principali per DarkHotel di attaccare le proprie vittime è consigliata una regolare e periodica attività di *Network Scan.*

Si tratta di uno scan specifico e dettagliato che analizza l'IP di un network in modo da identificare le sue vulnerabilità e punti deboli. Questo strumento può essere usato da chiunque, che sia una multinazionale con centinaia e centinaia di computer – come una grossa catena di Hotel – o che sia una piccola azienda con un network di soli pochi dispositivi.

Assicurata la "tenuta" della rete, si deve passare a un'attenta attività di *Vulnerability Assessment*. Si tratta di un'analisi di sicurezza che ha l'obiettivo di identificare tutti le vulnerabilità potenziali dei sistemi e delle applicazioni. Come? Valutando il danno potenziale che l'eventuale "attaccante" può infliggere all'unità produttiva. Personale altamente qualificato, in un secondo momento,

integra e verifica i risultati attraverso una meticolosa attività manuale. Queste attività hanno lo scopo di rifinire la ricerca evidenziando eventuali errori commessi durante il processo. Uno degli aspetti chiave di questa tipologia di analisi è l'isolamento tempestivo delle vulnerabilità reali. Uno strumento buono di Vulnerability Assessment permette all'utente di avere un'overview aggiornata del livello di sicurezza degli asset IT. Ovviamente, questo è il punto di partenza per ottimizzare tutti gli sforzi di security management.

Da ultimo non c'è misura preventiva migliore del *Penetration Test.*

Questo, detto in parole povere, fa un "esame" dei punti deboli relativi ad una infrastruttura IT e, dopo averli scoperti, prova ad exploitarli in maniera sicura e controllata. Le vulnerabilità che sono oggetto d'esame da parte delle attività di Penetration Testing possono essere presenti nel software stesso in questi punti d'accesso:

- Flaws non intenzionali nel design del codice del software;
- Utilizzando il software in un modo per cui non è stato progettato;
- La non corretta implementazione della gestione della configurazione del software;
- Backdoor (porte sul retro) nel sistema operativo.

Le attività di *Penetration Testing* possono essere condotte sia attraverso processi automatici che manuali. Solitamente, il target di questa attività è focalizzato sui seguenti endpoint:

- Network endpoint;
- Dispositivi Mobile e Wireless;
- Network Security Device;
- Server;
- Altre aree esposte come il codice che sta dietro alle

applicazioni.

Lo scopo di un Penetration Test, tuttavia, è quello di andare il più a fondo possibile nell'infrastruttura IT aziendale per arrivare agli asset elettronici di una azienda. L'obiettivo non è quello di colpire duramente il bersaglio al primo tentativo, ma è quelli di colpire anche più duramente nei tentativi seguenti.

Prendendo questo come punto di partenza, possiamo stabilire che l'obiettivo principale di un penetration test sia quello di identificare chiaramente le vulnerabilità di sicurezza. Oltre a quanto appena detto, c'è una serie di altri obiettivi che il penetration test può raggiungere:

- Verificare la compliance delle policy di sicurezza;
- Testare la consapevolezza dello staff in materia di sicurezza;
- Controllare se e come un'organizzazione può affrontare un security breach.

Insomma, le soluzioni per arginare il fenomeno sono già presenti, ora a prendere le redini della situazione devono essere le università; il rischio dovrebbe già essere ben chiaro.

https://www.key4biz.it/darkhotel-chi-sono-gli-hacker-del-wi-fi-e-perche-colpiscono-gli-hotel/273905/