Usa 2020, taglia fino a 10 milioni di dollari sugli hacker che influenzano le elezioni

Taglia fino a 10 milioni di dollari per chi fornirà informazioni utili a identificare hacker che lavorano con governi stranieri che vogliono influenzare la campagna elettorale del 2020.

Criminal hacker: fino a 10 milioni di dollari di taglia

A offrire la ricompensa è il Dipartimento di Stato americano, a meno di 100 giorni dalle presidenziali del 2020, per provare a scongiurare le interferenze subite nelle elezioni del 2016, anche da parte di una fabbrica di troll russa.



L'offerta di ricompensa, si legge sul sito del governo, è volta a ottenere "informazioni per l'identificazione o l'ubicazione di qualsiasi persona che, mentre agisce sotto la direzione o sotto il controllo di un governo straniero, interferisce con elezioni federali, statali o locali degli

Stati Uniti aiutando o favorendo una violazione della sezione 1030 del titolo 18”, cioè la legge sulle frodi e gli abusi informatici.

Le elezioni del 2016

Durante la campagna elettorale per le elezioni presidenziali americane del 2016 alcuni hacker si infiltrano nei computer del Comitato democratico e diffusero migliaia di email riservate che testimoniano le intenzioni del partito di boicottare il candidato **Bernie Sanders** per favorire **Hillary Clinton.**

La presidente del Democratic National Committee, Debbie Wasserman Schultz, è costretta a dimettersi. È a questo punto che l’Fbi rivela l’esistenza di un’indagine top secret su possibili interferenze di Mosca nelle elezioni.

Secondo l’intelligence Usa, dietro agli attacchi hacker ci sarebbe il governo russo che cercherebbe così di influenzare il voto, screditando i democratici per favorire il repubblicano Donald Trump, considerato più vicino alla Russia. Sul caso indaga anche il Congresso. A fine anno, quando Trump è ormai presidente, Barack Obama parla di prove che portano direttamente a **Vladimir Putin**.

https://www.key4biz.it/usa-2020-taglia-fino-a-10-milioni-di-dollari-sugli-hacker-che-influenzano-la-campagna/317896/

Attacchi DDoS, pericoli e

contromisure per la difesa

Attacco DDoS: cos’è

Con il termine **DoS** (Denial of Service) o **DDos** (Distributed Denial of Service) si indica la negazione e la conseguente indisponibilità di un servizio web erogato causate da un sovraccarico anche temporaneo di risorse di rete, in seguito a un numero imprevisto di richieste scatenato rispettivamente da una o più fonti contemporaneamente, talvolta in modo non intenzionale o più solitamente attraverso un attacco informatico mirato.

Nei casi intenzionali, i criminal hacker riescono a realizzare e pianificare un attacco DDoS, individuando il punto debole di un sistema o di una rete e appena trovata la relativa vulnerabilità innescando la reazione per comprometterne l’operatività. Nei casi di attacchi DDoS più estesi ciò è reso possibile servendosi di vaste reti distribuite, le ben note **botnet** composte da migliaia di computer e sempre più di frequente da dispositivi IoT utilizzati indebitamente come vettori di attacco.



Attacco DDoS: come funziona

Gli scopi non sono dunque necessariamente quelli di hackerare un sistema, quanto piuttosto di creare disservizi (per vari motivi) o diversivi per distogliere l'attenzione dall'effettivo ultimo fine. A prescindere dalle intenzioni, le relative strategie adottate per ottenere una severa saturazione della banda di trasmissione o delle risorse di un sistema possono coinvolgere diversi livelli dello stack protocollare TCP/IP.

Ad esempio, gli attacchi ai livelli TCP e IP, generando un volume elevato di traffico mirano a colpire l'infrastruttura di rete, sovraccaricando la capacità delle risorse, dei server e delle applicazioni.

Il Flooding

Sfruttando il fatto che un server web può instaurare solo un certo numero di connessioni secondo un predeterminato dimensionamento, questo limite può venire superato con una inondazione di richieste anomale (flooding), comportando il blocco di tutti servizi erogati dal server colpito. Seguono alcune declinazioni.

Ping flooding

Attraverso l'ausilio di botnet vengono solitamente inviati in massa ai target designati dei pacchetti ICMP di echo request. Il ping flooding, se non adeguatamente gestito può innescare un processo che consuma le risorse disponibili.

SYN flooding

Questo schema di attacco sfrutta un abuso della procedura Threeway Handshake del protocollo TCP. Il protocollo di rete TCP (Transmission Control Protocol) si occupa di garantire un

traffico dati senza perdite tramite una connessione costituita da un’autenticazione in tre passaggi:

1. un client invia un pacchetto di sincronizzazione SYN a un server;
2. il server accetta e reinvia a sua volta un altro messaggio SYN e uno di risposta ACK;
3. la connessione viene chiusa da una conferma ACK lato client.

I sistemi possono paralizzarsi durante questa procedura se il server dovesse conservare diverse connessioni non concluse perché mancanti di conferme SYN e ACK. La presenza di molte di queste connessioni semiaperte e provocate da un attacco SYN flooding, se non adeguatamente gestita potrebbe rendere le risorse del server completamente occupate. Una contromisura potrebbero essere i SYN cookie: in tal caso, le informazioni inviate dai pacchetti SYN vengono salvate sui client, sotto forma di cookie criptati, utilizzando localmente solo le relative risorse senza sovraccaricare la memoria del sistema target.

UDP flooding

Anche il protocollo UDP (User Datagram Protocol) la versione connectionless del protocollo di livello trasporto può essere vulnerabile al flooding. A differenza di una trasmissione TCP, attraverso il protocollo UDP, una comunicazione dati può instaurarsi senza una connessione in tre passaggi. In questi casi per sovraccaricare i sistemi, compromettendone la relativa disponibilità, i pacchetti UDP vengono inviati in grandi quantità indicando dei numeri di porta che si riferiscono a delle applicazioni non presenti nel sistema target, il quale non riuscendo a individuare alcuna applicazione risponde ad ogni richiesta con un pacchetto ICMP “Indirizzo di destinazione non raggiungibile”.

HTTP flooding

In questo scenario d’attacco si mira a sovraccaricare le risorse di sistema, inondando il server web target con molte richieste HTTP (protocollo di livello applicazione) fino a renderlo non più raggiungibile a causa delle numerose richieste non gestite.

Lo sfruttamento di errori e falle di sicurezza

Anche falle di sicurezza nei sistemi operativi e vulnerabilità software, qualora esistenti e non risolte possono essere sfruttate per sferrare attacchi DDoS e provocare errori e crash di sistema. Ecco due casi noti:

- **Ping of Death.** I pacchetti IP vengono generalmente inviati sotto forma di frammenti che dovranno essere ricostruiti dal sistema ricevente. Se vengono inviate informazioni errate per la ricostruzione di tali pacchetti, i sistemi potrebbero generare anche pacchetti IP di dimensioni più grandi di quelle consentite causando un buffer overflow, perché la quantità di dati generata supererebbe lo spazio a disposizione. Il sistema vittima dell’attacco potrebbe così andare in crash.
- **Attacchi Land.** Sempre durante il processo di negoziazione Threeway Handshake previsto dal protocollo TCP, alterando i pacchetti SYN in modo che sia gli indirizzi mittenti che quelli destinatari corrispondano al server target, si potrebbe indurre il sistema vittima a entrare in un loop infinito, rispondendo continuamente alle sue stesse richieste ed esaurendo le proprie risorse sino ad andare in crash.

Gli attacchi DDoS amplificati

Gli attacchi DDoS che si basano su tecniche reflection/amplification colpiscono determinati obiettivi amplificando la loro portata (generando traffico dati dell'ordine dei Terabit) sfruttando le risorse di server di terze parti di tipo memcached (ovvero dotati di un sistema di gestione della memoria in forma distribuita e ad alte prestazioni per l'elaborazione di grosse quantità di dati) lasciati esposti in rete senza un'adeguata protezione. Si rammentano al riguardo gli attacchi subiti dai sistemi GitHub (con carico di picco pari a 1,3 Tbps) nel 2018 e dai sistemi AWS (con carico di picco pari a 2,3 Tbps) nello scorso mese di febbraio.

Contromisure di mitigazione

Per contrastare un sovraccarico dei sistemi informatici sono disponibili diverse soluzioni di sicurezza. Tra queste rientrano l'identificazione degli indirizzi IP critici, la risoluzione di vulnerabilità di sicurezza e la messa a disposizione di risorse hardware e software da utilizzare come bacini di espansione con cui sia possibile compensare gli effetti di eventuali attacchi DDos.

Un'altra tecnica di mitigazione potrebbe essere quella di ridurre al minimo la superficie e i relativi punti di attacco.

In alcuni casi, ciò è possibile confinando le risorse di calcolo su reti Content Distribution Network (CDN) o su sistemi di load balancing:

- **Reti CDN.** Le applicazioni Web possono utilizzare queste configurazioni di rete per fornire servizi e contenuti, agli utenti finali, sotto forma di sistemi distribuiti.
- **Load Balancing.** Anche il load balancing può essere impiegato per un'equa distribuzione del carico su

diversi sistemi ed evitare così lo sfruttamento di hardware e servizi messi a disposizione per saturare banda e sovraccaricare processi.

In altri casi, per ridurre i punti vulnerabili potenzialmente attaccabili, è possibile limitare e monitorare il traffico dei dati, provenienti da rete pubblica e diretti verso determinate zone dell'infrastruttura di rete, utilizzando blacklist o ACL (Access Control List) per identificare e bloccare indirizzi IP critici, Web Application Firewall (WAF)per prevenire richieste illegittime che tentando di sfruttare potenziali vulnerabilità nelle applicazioni, potrebbero riuscire a mascherare anche un traffico dati anomalo.

https://www.key4biz.it/attacchi-ddos-pericoli-e-contromisure-per-la-difesa/317773/

IoT botnet, al Black Hat si studia la nuova cyber minaccia per le reti energetiche globali

Le **botnet** sono ormai considerate tra le minacce più rilevanti ai sistemi di sicurezza informatici di imprese e organizzazioni pubbliche. Si tratta di una rete di *robot* (quindi anche *software* oltre che *hardware*) controllata da remoto da *botmaster* per compiere cyber attacchi

Affinchè una botnet sia efficace per un attacco informatico deve essere di grandi dimensioni. Più è grande il numero di

device “*zombie*” controllati da remoto, più grande è il danno che sono in grado di arrecare.



La minaccia delle IoT botnet

Per capire come lavora una botnet basta prendere ad esempio il celebre caso “*Mariposa*” del 2010: una rete di computer zombie che ha infettato almeno 13 milioni di pc in 190 Paesi, inclusi numerosi pc di grandi aziende (oltre la metà delle 1.000 aziende più grandi al mondo) e almeno 40 importanti banche.

Alla conferenza **Black Hat** sezione americana è stato presentato uno studio dedicato all’impiego di **botnet dell’*Internet of Things*** (IoT) nel settore della generazione e distribuzione dell’energia elettrica.

IoT botnet non solo in grado di influenzare il funzionamento delle reti energetiche, ma di condizionare anche il mercato di riferimento.

Parliamo di device connessi in rete di ogni tipo, dalle apparecchiature più sofisticate per la gestione dei flussi delle risorse energetiche ai più semplici *smart meter* (contatori) in dotazione ormai di ogni famiglia.

La domanda da porsi è la seguente, secondo i ricercatori: “*In che modo i cyber criminali utilizzeranno questa botnet IoT?*

Con quale intensità? Per causare danni o per fare profitti? O per raggiungere entrambi gli obiettivi?”.

Oggi basta una IoT botnet di 50 mila device connessi in rete e tra loro per causare danni ad imprese ed enti pubblici, quindi danni ai cittadini., secondo i ricercatori del Georgia Institute of Technology (Git).

Facili guadagni o danni sempre più grandi?

Tramite uno strumento del genere sarebbe possibile causare un **blackout energetico** in una città o in alcuni dei suoi quartieri, oppure **sottrarre energia elettrica** a migliaia di ignari cittadini senza che questi se ne accorgano, o **manipolare gli scambi di domanda-offerta sul mercato** americano, senza che nessuno se ne renda conto.

Questo tipo di azione comporterebbe un aumento dei costi in bolletta del 7% circa, un dato molto contenuto di cui in pochi si accorgerebbero su decine di milioni di utenti.

Al contrario, per i cyber criminali i guadagni sono altissimi: considerando il caso di un attacco effettuato per tre ore al giorno, per un periodo di tempo di 100 giorni in un anno, il bottino potrebbe essere di circa 24 milioni di dollari all’anno, mentre con lo stesso sistema si potrebbero anche infliggere perdite per 350 milioni di dollari l’anno.

Per questo i ricercatori suggeriscono, ad esempio, di porre maggiore attenzione agli smart device ad alto voltaggio, perché sono quelli più utilizzati nelle reti IoT impiegate nel settore energetico.

Cosa fare?

Solo casi ipotetici, purtroppo no.

Negli Stati Uniti, la Commissione federale di regolamentazione dell'energia ha indagato su 16 potenziali casi di manipolazione del mercato nel 2018, sebbene ne abbia chiusi 14 senza provvedimenti.

Inoltre, a metà maggio di quest'anno, un cyber attacco di vasta portata ha violato i sistemi IT di Elexon, la piattaforma informatica utilizzata per gestire il mercato energetico del Regno Unito.

Molto utili, a riguardo, potrebbero essere sistemi di monitoraggio in tempo reale, in grado di segnalare anche la più piccola variazione nei flussi, nei consumi e negli scostamenti di domanda e offerta.

Per anticipare le mosse dei cyber criminali odierni bisogna pensare in maniera diversa, magari iniziando ad immaginare l'impensabile. Conme ha spiegato su wired.com, il fondatore di Fortiphyd Logic: "*Chi avrebbe mai detto che i nuovi attacchi informatici avrebbero usato come porta principale la mia lavatrice connessa in rete o il frigorifero smart?*".

https://www.key4biz.it/iot-botnet-al-black-hat-si-studia-la-nuova-cyber-minaccia-per-le-reti-energetiche-globali/317629/

Garmin, pagati 10 milioni di dollari di riscatto per l'attacco informatico?

Pagare un riscatto non è mai la scelta giusta. Soprattutto quando si è vittima di un attacco informatico. Ma cosa è

successo di preciso? Andiamo con ordine.

Garmin e l’attacco informatico

Lo scorso 22 luglio, il gigante della tecnologia sportiva e del fitness **Garmin**, ha subito un grave incidente informatico per via di un attacco ransomware.



L’incidente è iniziato alla fine di mercoledì ed è continuato per tutto il fine settimana, causando il blocco dei servizi online dell’azienda per milioni di utenti, tra cui **Garmin Connect**, che sincronizza l’attività e i dati con il cloud e altri dispositivi. L’attacco ha anche messo al tappeto **flyGarmin**, piattaforma di navigazione e pianificazione delle rotte.

Parti del sito web Garmin sono rimaste a lungo offline, con la compagnia che non ha spiegato a fondo di cosa sia trattato.

Ransomware WastedLocker

La causa di tutto sarebbe il ransomware **WastedLocker**. Quest’ultimo è un nuovo tipo di ransomware, già dettagliato dai ricercatori sulla sicurezza di Malwarebytes a maggio, gestito da un gruppo di hacker noto come **Evil Corp.** Come altri malware, WastedLocker infetta i computer e blocca i file dell’utente in cambio di un riscatto, in genere richiesto in

criptovaluta.

Ciò significa che le aziende con backup potrebbero essere in grado di evitare di pagare il riscatto, mentre le altre si sono viste richiedere anche 10 milioni di dollari.

La scelta sbagliata di Garmin

Secondo Sky News, Garmin non ha risolto l'anomalia con un backup come dichiarato, ma ha ricercato e rintracciato una chiave di decrittazione per sbloccare l'effetto ransomware. Come? Pagando il riscatto multimilionario grazie all'aiuto di una società terza per la negoziazione dei riscatti chiamata **Arete IR .**

Dopo il pagamento, Garmin avrebbe quindi ricevuto la chiave di decrittazione per rientrare in possesso dei suoi file presi in ostaggio dal ransomware WastedLocker, collegato a una rete di cybercriminali russi conosciuti come **Evil Corp.**

https://www.key4biz.it/garmin-pagati-10-milioni-di-dollari-di-riscatto-per-lattacco-informatico/317440/

Gli errori commessi dagli hacker di Twitter

Sono stati arrestati in tempi record gli hacker responsabili del grave incidente informatico che ha coinvolto **Twitter** lo scorso 15 luglio.

Per le autorità statunitensi **Graham Ivan Clark**, 17enne appena diplomato proveniente dalla Florida; **Mason John Sheppard**, 19enne del Regno Unito, e **Nima Fazeli**, 22enne di Orlando

(Florida), sono i criminal hacker del maxi attacco che giorni fa hanno violato gli account degli uomini più ricchi del mondo: **Bill Gates, Jeff Bezos, Elon Musk, Warren Buffett, Michael Bloomberg.** Questi account, ciascuno con milioni di follower, sono stati compromessi per promuovere una truffa basata su **Bitcoin**.



Secondo alcuni documenti relativi all'indagine in corso e diffusi venerdì, la figura centrale dell'attacco sarebbe una persona che usava il nome Kirk, e che potrebbe essere proprio Clark. Clark è stato arrestato a Tampa (Florida), ed è accusato di oltre 30 reati tra cui frode e attacco informatico.

Gli errori dei criminal hacker

L'hack di Twitter, stando alle ricostruzioni e alla veloce cattura dei responsabili, è stato non organizzato e gestito particolarmente bene, da hacker non particolarmente esperti.

Secondo il New York Times, alcuni di loro avrebbero finito per depositare parte dei bitcoin rubati sui loro account personali di alcuni exchange crypto, in particolare **Coinbase**, e questi avrebbero prontamente segnalato alle autorità il deposito sospetto, compresa l'identità dei proprietari dell'account. Tra l'altro proprio Coinbase ha rivelato qualche giorno fa di essersi già adoperata durante l'attacco per impedire ai propri utenti di versare bitcoin all'indirizzo utilizzato dai

truffatori.

In modo particolare è stato facile tracciarli grazie ad appositi software di analisi della blockchain pubblica di **Bitcoin**, che le autorità americane hanno utilizzato.

Twitter: ‘hackerati gli smartphone dei dipendenti tramite phishing’

Twitter, tramite un comunicato ufficiale, ha spiegato che i pirati informatici hanno contattato un “numero ristretto” di dipendenti attraverso tecniche di phishing, riuscendo così ad avere accesso ad alcuni strumenti interni che poi hanno permesso agli hacker di violare il sistema di controllo degli account.

La tecnica di ingegneria sociale ha avuto successo perché i dipendenti lavorano in smart working (a causa della pandemia COVID-19), per cui non hanno potuto verificare l’identità dei (falsi) colleghi con le procedure di sicurezza presenti in ufficio.

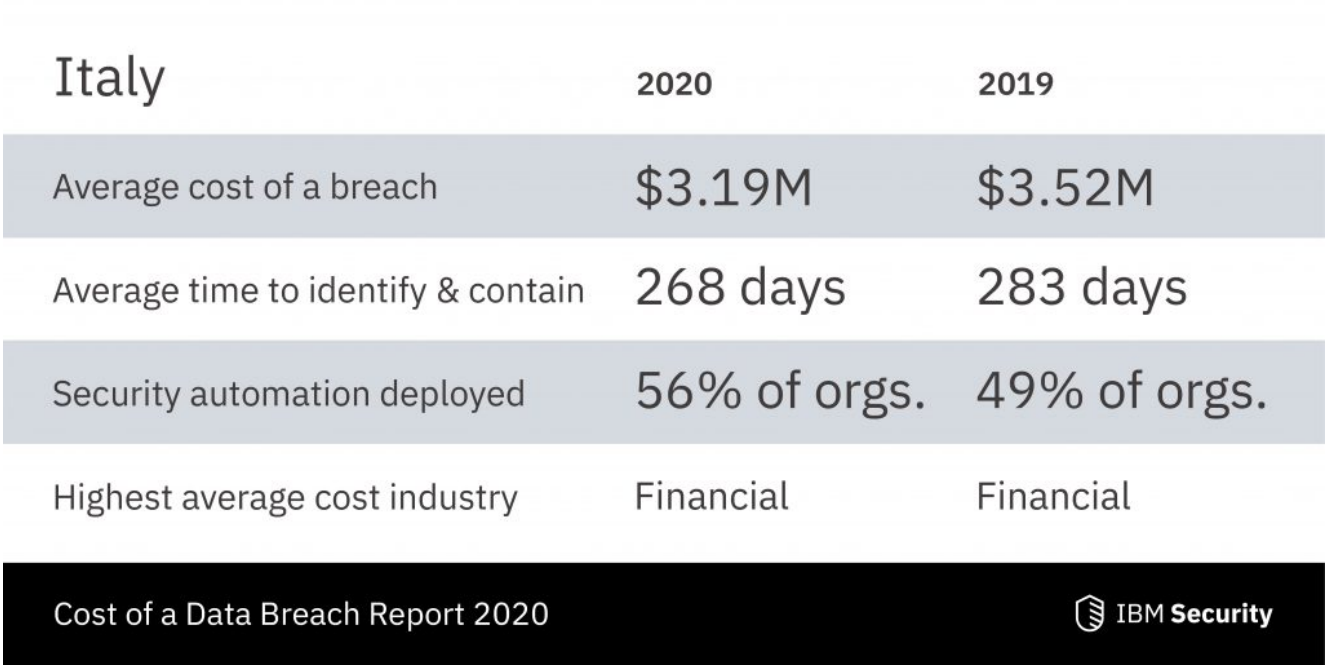
“*Questo attacco si è basato sul tentativo massiccio di ingannare alcuni dipendenti e sfruttare le vulnerabilità umane per ottenere l’accesso al nostro sistema interno*“, ha dichiarato Twitter, sottolineando come quanto è avvenuto sia “*un monito*” per ogni dipendente a mantenere le misure di protezione e sicurezza.

https://www.key4biz.it/gli-errori-commessi-dagli-hacker-di-twitter/317283/

Data breach, per ogni azienda italiana coinvolta il costo è di 2,9 milioni di euro l’anno

Ogni violazione di sicurezza costa in media all’azienda impattata 3,86 milioni di dollari a livello globale e 2.90 milioni di euro in Italia.

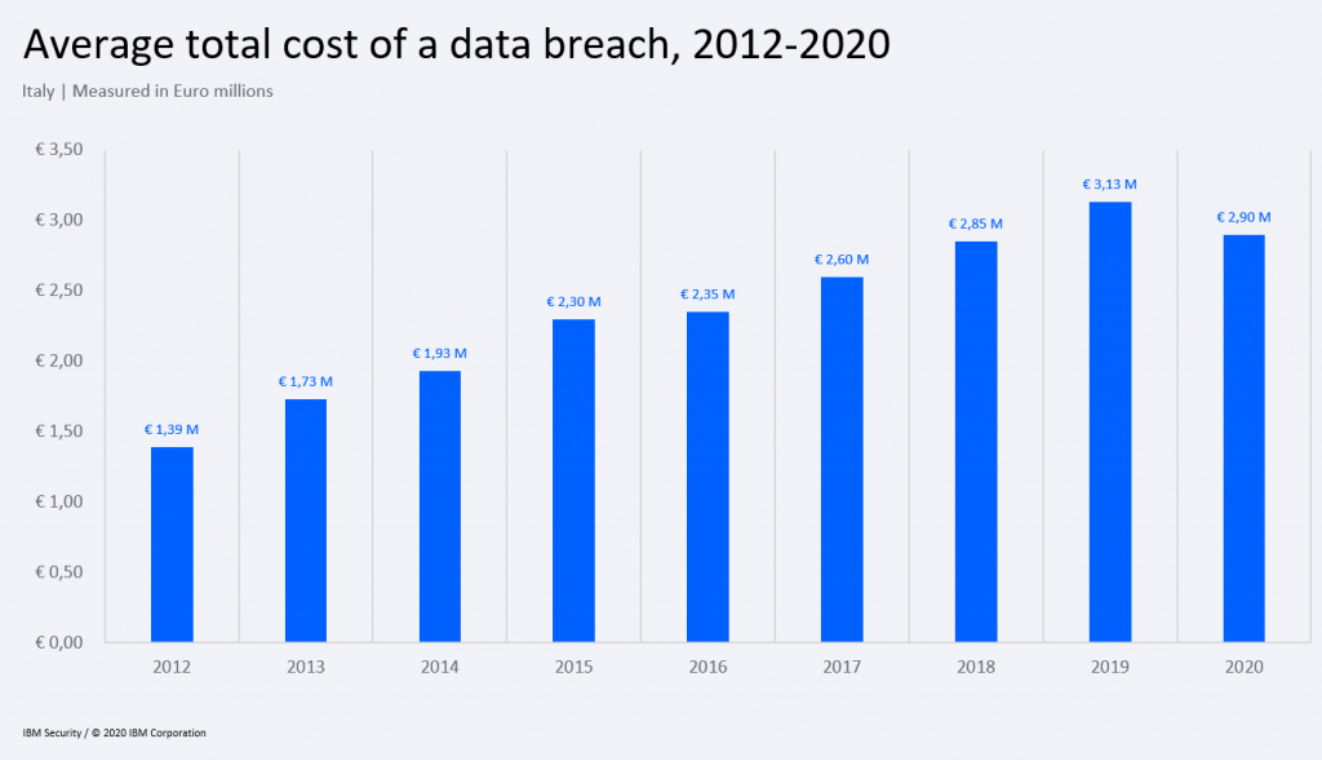
Lo rileva il nuovo studio report Cost of a Data Breach 2020, richiesto da IBM Security e condotto da **Ponemon Institute**. Il report è stato realizzato attraverso 3.200 interviste a responsabili della sicurezza di organizzazioni che hanno subito una violazione di dati nel corso dell’ultimo anno.



In Italia

L’analisi approfondita delle violazioni di dati subite da oltre 500 organizzazioni in tutto il mondo, di cui 21 italiane, rivela che la violazione dei dati dei dipendenti è quella più gravosa e che l’80% di questi attacchi ha portato

all’esposizione di informazioni di identificazione personale (Personal Identifiable Information, PII) dei clienti, causando costi ingenti per le aziende.



Data breach: furto di credenziali e cloud

Il furto e la compromissione delle credenziali, oltre alle configurazioni errate dei server cloud, rappresentano le vulnerabilità più comuni, che causano quasi il 40% dei cyberattacchi. Lo studio rivela che nel 2019 oltre 8,5 miliardi di record sono risultati vulnerabili e gli hacker, in 1 caso su 5, hanno sfruttato e-mail e password non adeguatamente protetti per sferrare i propri attacchi. Oggi le organizzazioni sono impegnate nella messa a punto di nuove strategie di sicurezza e nell’adozione un approccio a *Zero Trust*, che impone di rivedere i criteri di autenticazione e di accesso degli utenti.

Il report 2020 ha evidenziato che gli hacker hanno sfruttato proprio gli errori di configurazione dei server cloud per

violare le reti quasi nel 20% dei casi, generando un aumento dei costi di oltre mezzo milione di dollari e portando a 4,41 milioni di dollari la spesa complessiva media, che si attesta quale terza voce di costo.

Se da un lato le tecnologie forti e mature hanno reso le organizzazioni sempre più resilienti, l'accesso ai dati sensibili attraverso il lavoro a distanza e le operazioni commerciali basate sul cloud, uniti alla mancanza di una adeguata formazione, hanno reso le organizzazioni più vulnerabili.

Ciò significa che poter contare su team dedicati, predisporre e testare piani di sicurezza, adottare le più innovative tecnologie in questo ambito consente alle aziende di essere più efficienti nel prevenire e contrastare gli attacchi, ridurre i costi e conseguire ROI in tempi minori nell'area della cybersecurity.

https://www.key4biz.it/data-breach-per-ogni-azienda-italiana-coinvolta-il-costo-e-di-29-milioni-di-euro-lanno/316898/

Twitter hack, letti messaggi di 36 account tra cui un politico dei Paesi Bassi



“Crediamo che gli hacker abbiano fatto accesso ai messaggi privati di 36 account sui 130 presi di mira, incluso un account che appartiene a un politico dei Paesi Bassi. Al momento non abbiamo altre indicazioni su ulteriori ex politici o in carica di cui sono stati visualizzati i messaggi privati”.

Con questo tweet attraverso il suo account di supporto, **Twitter** ritorna a parlare dell’imponente attacco informatico che ha coinvolto l’azienda lo scorso 16 luglio.

Nell’hack i profili di utenti illustri, da **Obama e Elon Musk, da Jeff Bezos a Warren Buffett, fino agli account di Apple e Ube**r, sono stati violati per inserire un messaggio truffa mirato a raccogliere bitcoin e sfruttando, probabilmente, una falla di sicurezza di uno o più dipendenti. I criminal hacker hanno raccolto circa 120mila dollari, nelle ore successive all’attacco il titolo di Twitter è crollato in Borsa.

> *Our investigation continues, but we wanted to share more specifics about what the attackers did with the accounts they accessed. Following a complete review of all targeted*

> *accounts, here is more detail on what we know today:*
>
> *— Twitter Support (@TwitterSupport) July 22, 2020*

Sebbene Twitter non abbia rivelato l'identità del politico in questione, alcuni media olandesi hanno riportato la notizia che tra gli account violati durante l'attacco a Twitter c'era anche quello del fondatore e leader del Partito per la libertà (Pvv), **Geert Wilders**.

Secondo il quotidiano olandese **DutchNews**, l'account di Wilders, leader del PVV, sarebbe stato preso di mira modificandogli la foto del profilo e quella di copertina.

Twitter, nel 2020 ricavi in calo: abbonamento in arrivo?

Twitter ha chiuso il secondo trimestre con ricavi in calo del 19% a 683 milioni di dollari e perdite per **1,23 miliardi**, mentre il numero degli utenti giornalieri è aumentato del 12% a 186 milioni.

Per arginare il calo dei ricavi, causati dal crollo degli investimenti della pubblicità in tutto il mondo a causa della pandemia, il ceo **Jack Dorsey** parlando con gli azionisti ha fatto sapere che starebbe studiando come creare altre fonti di guadagno, oltre alla pubblicità, compreso un sistema in abbonamento.

Dorsey quindi ha confermato l'intenzione del social di cercare di diversificare la tipologia dei guadagni, ma facendo in modo di renderlo complementare comunque alle attività pubblicitarie.

https://www.key4biz.it/twitter-hack-letti-messaggi-di-36-account-tra-cui-un-politico-dei-paesi-bassi/316159/

L’app Android dei droni DJI raccoglie i dati degli utenti



L’app **DJI** per il sistema operativo **Android** raccoglie grandi quantità di informazioni personali. Lo rivela il New York Times secondo cui due società di sicurezza, che hanno diramato in due rapporti separati, segnalano la presenza di un problema di sicurezza nelle app **DJI GO 4** di controllo dei **droni** della multinazionale cinese.

Secondo le aziende che hanno documentato il problema, la francese Synacktiv e l’americana GRIMM, il produttore di droni cinese **DJI** potrebbe raccogliere quantità non necessarie di informazioni dai telefoni degli utenti, presentando un potenziale problema di sicurezza.

Le due società hanno scoperto che l’app Android utilizzata per controllare i droni DJI era anche in grado di bypassare il **Google Play Store**, che controlla le app e gli aggiornamenti per assicurarsi che le app dello store siano sicure.

Furto di dati

Nello specifico, l'applicazione ha la possibilità di accedere ai contatti della rubrica e a risorse hardware (microfono, videocamera, GPS) con il rischio di poter dare a terzi o alla stessa DJI il controllo dello smartphone di un utente.

Secondo i ricercatori GRIMM l'applicazione sarebbe anche in grado di installare app arbitrarie sfruttando il kit di sviluppo **Weibo** e aggirando ancora una volta i controlli di Google. In questo modo l'applicazione condivide le informazioni personali degli utenti con Weibo e potrebbe consentire a terzi di prendere di mira gli utenti con installazioni di app dannose.

Droni e cyberspionaggio cinese

Washington da anni sospetta che i droni della multinazionale possano facilitare lo spionaggio cinese, cosa che la compagnia ha negato con veemenza.

I ricercatori hanno sottolineato che non c'erano prove che fossero state raccolte e inviate informazioni a Pechino, né che il problema tecnico fosse una backdoor intenzionale. Tuttavia l'esistenza della vulnerabilità aumenterà le preoccupazioni per i funzionari di Washington, dato che hanno lanciato accuse di spionaggio ad aziende tecnologiche cinesi negli ultimi mesi.

Dopo Tik Tok anche la multinazione dei droni DJI

Un portavoce di DJI ha affermato al NYT che i problemi erano "*problemi tipici del software, senza prove che siano mai stati sfruttati*", aggiungendo che al momento "*non c'erano prove di connessioni impreviste di trasmissione dati dalle app di DJI*

progettate per clienti governativi e professionali“. Inoltre l’azienda ha dichiarato che i bug trovati su app che utilizzano dispositivi DJI GO4 non sono venduti per uso governativo.

Gli Stati Uniti hanno intensificato il loro assalto alle compagnie cinesi negli ultimi mesi, sostenendo che il Partito Comunista potrebbe sfruttare le debolezze del software, forse inconsapevolmente verso le aziende stesse, per trovare informazioni su utenti stranieri. Washington questa settimana ha affermato che il popolare social network **TikTok** sia uno strumento in mano a Pechino per spiare e rubare i dati di milioni di americani.

https://www.key4biz.it/lapp-android-dei-droni-dji-raccoglie-i-dati-degli-utenti-per-gli-usa-e-cyberspy-cinese/316053/

Manchester città cyber sicura per il 2021, il digitale qui contribuisce all’economia locale per 5 miliardi di sterline



Il consiglio cittadino di Manchester in Inghilterra ha votato a favore della costruzione di un *cybersecurity hub* entro la fine del 2021, con l'obiettivo di proteggere non solo le infrastrutture strategiche, ma un **business digitale che contribuisce all'economia dell'area urbana per quasi 5 miliardi di sterline**.

Le cyber difese di Manchester

Il **Manchester Digital Security Innovation Hub**, secondo il presidente del Consiglio comunale, **Richard Leese**, "*è un progetto entusiasmante che contribuirà a stimolare la crescita economica e a creare posti di lavoro in questo settore in rapida crescita, che sta emergendo come uno dei punti di forza distintivi di Manchester*".

In effetti, stando ai numeri rilasciati dall'amministrazione cittadina, parliamo di un territorio fortemente digitalizzato, con un'economia urbana a cui l'innovazione tecnologica contribuisce per 5 miliardi di sterline, a fronte di circa **10 mila imprese attive sul territorio e 86 mila occupati**.

Il centro sorgerà nella zona di Heron House, quindi nel cuore della città, e nelle intenzioni del Consiglio cittadino dovrebbe riuscire ad attrarre professionisti ed esperti non solo dal Regno Unito, ma anche dal resto del mondo.

Vi lavoreranno assieme ricercatori accademici e privati, corporation e startup, organizzazioni del settore pubblico e volontari, con l'unico scopo di prevenire, identificare e neutralizzare ogni tipo di minaccia informatica alla città e alle sue imprese.

Regno Unito Tech Nation

Nel Rapporto ***Tech Nation 2020***, la Città di Manchester è stata nominata come principale cluster tecnologico del Paese e tra quelli che crescono più rapidamente in Europa.

La cybersecurity è un argomento che negli ultimi anni sta prendendo piede nel Regno Unito. **Il Governo di Londra ha varato un piano di investimenti da 2 miliardi di sterline fino al 2021** ("*National Cyber Security Strategy 2016 to 2021*").

Ogni anno le imprese britanniche subiscono cyber attacchi per un danno medio pari a 3,8 milioni di sterline, secondo dati IBM e Ponemon.

In tutto il Paese, infine, sono attive 1.221 imprese della cybersecurity, per un mercato che vale 8,3 miliardi di sterline l'anno, secondo un recente Rapporto governativo.

> *Manchester città cyber sicura per il 2021, il digitale qui contribuisce all'economia locale per 5 miliardi di sterline*

Sventato attacco informatico ad una squadra di Premier League. L'NCSC ai club: 'Investite in cybersecurity'



L'indirizzo e-mail dell'amministratore delegato di un club di Premier League è stato violato durante una negoziazione di trasferimento di un calciatore, portando al tentativo di rubare 1 milione di sterline.

Lo ha dichiarato il **National Cyber Security Center** (NCSC) inglese, l'organizzazione governativa operativa nella sicurezza informatica, che ha spiegato come solo l'intervento della banca del club, non nominato, è riuscito a fermare la frode via email.

Per questo motivo, secondo il rapporto dell'NCSC, le

istituzioni sportive professionistiche inglesi sono state spinte a rafforzare la loro sicurezza informatica dopo che è stato rivelato che dei criminal hacker hanno tentato di sabotare un trasferimento di un giocatore di un club di Premier League.

L'NCSC ai club: 'Investite nella sicurezza informatica'

Secondo il NCSC, si tratta di uno dei numerosi incidenti evidenziati come prova che lo sport necessita di migliorare la sua sicurezza informatica. *"L'impatto dei criminali informatici che puntano questo settore è molto reale*", ha dichiarato il direttore delle operazioni **Paul Chichester.**

"*E' necessario che le istituzioni e le società investano nell'inviolabilità delle loro reti informatiche: le nostre indagini evidenziano come i tentativi di accesso degli hacker siano un evento che si ripete nel tempo, e che può avere un impatto molto grave sul settore. In un momento come questo, poi, questo tipo di investimento può essere ancora più importante: bisogna aumentare la sicurezza e fare backup dei dati*", ha concluso **Chichester**.

Phishing e furto di credenziali l'arma usata dai criminal hacker

Il dirigente è stato vittima di un attacco di phishing: cliccando su una email, è entrato in una pagina falsa di Office 365 in cui ha inserito il suo indirizzo mail e la password, con le credenziali così rubate dagli hacker.

Durante il calciomercato, spiega il rapporto governativo, hanno monitorato l'attività del dirigente e hanno messo nel mirino l'accordo per un trasferimento da 1 milione di sterline, creando un falso account mail del secondo club

coinvolto e modificando, in seguito, le coordinate bancarie su cui sarebbero dovuti essere accreditati i soldi. Il pagamento è andato a buon fine, ma il conto dei cyber criminali aveva un segnalatore di frode e la banca ha rifiutato il pagamento, mettendo in evidenza il tentativo di frode.

Il rapporto afferma anche che un club della Football League è stato preso di mira da hacker che hanno tagliato i suoi sistemi di sicurezza, bloccando i tornelli allo stadio e portando quasi al rinvio della partita.

https://www.key4biz.it/sventato-attacco-informatico-ad-un-club-di-premier-league-lncsc-ai-club-investite-in-cybersecurity/316035/