TEMATICARESEARCH

Rize etf

Vol /01

A Whitepaper on Cybersecurity and Privacy

A Whitepaper on Cybersecurity and Privacy

Preparato Novembre, 2019

TEMATICA RESEARCH, LLC
research@tematicaresearch.com

TABLE OF CONTENTS

TEMATICARESEARCH®

A Whitepaper on Cybersecurity and Privacy

EXECUTIVE SUMMARY 3

EVOLUZIONE STORICA DELLA SICUREZZA 4

- AUTENTIFICAZIONE – IL DIGITALE È PIÙ SICURO? 5
- COME SI È EVOLUTA LA COMUNICAZIONE 6
- DALLA COMUNICAZIONE AL DATA-GATHERING 7
- IL MONDO STA PRENDENDO COSCIENZA DEL PROBLEMA DELLA SICUREZZA 7

CYBERSECURITY 8

- ESEMPI DI RECENTI CYBER-ATTACKS 10
- MAGGIORE CONNETTIVITÀ SIGNIFICA MAGGIORE VULNERABILITÀ 11

PRIVACY DEI DATI - LA PROSSIMA AREA DI INTERVENTO PER LA SPESA INFORMATICA 12

- LE NORME SULLA PRIVACY STIMOLANO LA SPESA INFORMATICA 13
- STA ARRIVANDO ULTERIORE REGOLAMENTAZIONE DELLA PRIVACY, A LIVELLO GLOBALE 14

LA CYBERSECURITY CONTINUERÀ A CRESCERE 16

CONCLUSIONE 18

ENDNOTES 19

EXECUTIVE SUMMARY

Il tema dell'investimento Tematica Research® Cybersecurity & Data Privacy mira a beneficiare delle criticità generati dalla crescente minaccia di attacchi informatici, dalle violazioni dei dati sulla privacy e dall'impatto dell'evoluzione del contesto normativo. Abbiamo già visto una crescita importante degli investimenti globali nella sicurezza informatica, definita come la pratica di difesa di sistemi, reti, programmi, dispositivi e dati da attacchi informatici dannosi. I cyber-attack sono di solito finalizzati all'accesso (e alla vendita), alla modifica o alla distruzione di informazioni sensibili; ad estorcere denaro agli utenti; o ad interrompere i normali processi aziendali.

Nel mondo sempre più digitalizzato di oggi, la quantità di dati disponibili, utilizzati e condivisi continua a crescere così come il numero e la tipologia di dispositivi collegati. Il marcato aumento delle vulnerabilità informatiche e delle violazioni della privacy rappresenta però il lato oscuro della robusta crescita della connettività. Per le persone, questa connettività digitalizzata facilita le transazioni, rendendole rapide e comode. Per imprese e istituzioni, viene utilizzata per aumentare l'efficienza, ridurre i costi e far crescere aziende data-driven che si adattano meglio alle esigenze del mondo moderno. La questione diventa pertanto piuttosto evidente: al crescere dell'utilizzo dei dati informatici, sia individui che imprese diventano via via più vulnerabili a ciber-attacchi.

Come molti aspetti del 21 ° secolo, ciò che stiamo facendo essenzialmente non è cambiato. Come stiamo facendo queste cose, tuttavia, è dove diventa interessante e spesso complicato.

Oltre agli investimenti per combattere gli attacchi informatici, le imprese stanno investendo somme ingenti sulle misure di sicurezza IT che rispondono alle nuove normative sulla privacy, come il GDPR General Data Protection Regulation) europeo. Il problema degli attachi informatici e violazioni della privacy sembra essere ulteriormente aggravato dalle nuove tecnologie, quali il cloud computing, intelligenza artificiale, IoT e 5G. Queste tecnologie renderanno nel loro complesso i nostri sistemi più vulnerabili, e consentiranno nuove forme di attacco. Come molti altri aspetti del XXI secolo, quello che stiamo facendo in sostanza non è cambiato. Il modo in cui facciamo queste cose, tuttavia, è cio' che diventa interessante e spesso complicato.

Non c'è dubbio che la sicurezza informatica sia un mercato in crescita con persone, aziende e altre istituzioni che cercano di scongiurare futuri attacchi, rafforzare le difese informatiche esistenti, valutare l'analisi degli attacchi e delle intrusioni, alzare i livelli di sicurezza. Tutto questo si traduce in una sola cosa: investimenti in sicurezza informatica. Quello che segue è un manuale introduttivo sugli elementi di base in materia di sicurezza.

EVOLUZIONE STORICA DELLA SICUREZZA

Per oltre un millennio gli esseri umani hanno cercato di migliorare il modo di salvaguardare le merci e le informazioni, compresa la consegna sicura e la ricezione verificata. Dall'argilla alla cera, i sigilli sono stati utilizzati in tutto il mondo dal 7.000 a.C. fino al XIX secolo come mezzo per garantire che i documenti fossero originali, non manomessi e ricevuti dal destinatario (tramite ricevuta di ritorno sigillata di corso). Un aspetto chiave di questa evoluzione comprendeva non solo un mezzo per mettere al sicuro le informazioni, ma anche per aumentare la velocità di consegna.

Sebbene inizialmente concepito nel XVIII secolo, il telegrafo elettrico è stato commercializzato ed è stato ampiamente utilizzato solo nel XIX secolo. A prima vista, la comunicazione via telegrafo era la più veloce possibile e, essendo una rete cablata, offriva la sicurezza di una comunicazione diretta, end-to-end. Tuttavia, intercettare i messaggi era relativamente semplice: bastava intercettare fisicamente il cavo e creare un'altra stazione ricevente.

All'inizio del XX secolo, mentre Guglielmo Marconi stava testando il suo telegrafo senza fili, sabotatori riuscirono a dirottare la frequenza utilizzata nella dimostrazione e a trasmettere il proprio messaggio, insultando Marconi (in senso figurato e letterale) con la sua stessa creazione. Più avanti nel XX secolo, mentre il telefono si affermava come il passo successivo nell'evoluzione della tecnologia della comunicazione, restavano ancora irrisolti gli stessi problemi di sicurezza dei suoi predecessori. Per intercettare una telefonata, bastava indiviudare un qualsiasi punto lungo i chilometri e chilometri di cavo, collegarvi un dispositivo di ascolto e catturare tutto il traffico lungo il cavo stesso.

La sicurezza delle comunicazioni wireless può essere compromessa con altrettanta facilità, semplicemente impostando una stazione ricevente e identificando quale frequenza monitorare.

A publicity photo of Italian radio pioneer Guglielmo Marconi posing in front of his early wireless telegraph

In realtà, la comunicazione moderna presenta molteplici rischi e problemi di sicurezza, e gli utenti si sono sempre più spesso rivolti ad un altro antico mezzo per proteggere le comunicazioni: la crittografia. La crittografia si basa sull'uso di un codice per decifrare un messaggio criptato. L'implementazione della soluzione crittografica può essere semplice come il "codice" di Cesare che si limitava a spostare le lettere dell'alfabeto di un numero fisso di posizioni, numero noto a chi riceveva i messaggi. Un codice cifrato può anche essere complicato quanto moderna chiave a 128 bit, che ha circa 3,4e+38 chiavi o 340 miliardi di miliardi di miliardi di miliardi di soluzioni possibili![1]

AUTENTIFICAZIONE – IL DIGITALE È PIÙ SICURO?

Storicamente, l'autenticazione del destinatario di un messaggio era abbastanza semplice, poiché i messaggi importanti venivano consegnati a mano o almeno la consegna seguiva un qualche protocollo di catena di custodia.

Nel 1993, The New Yorker pubblicò un ormai famoso cartone animato di due cani in ufficio, uno seduto alla scrivania con una zampa sulla tastiera che dice al suo dirimpettaio: "su internet nessuno sa che sei un cane". Mentre questo può essere vero per gli utenti di Internet, la tecnologia di autenticazione per quanto riguarda i diritti di accesso ai sistemi e alle informazioni garantisce che l'utente appropriato (umano, cane o altro) abbia un accesso approvato.

Oggi, l'autenticazione comporta non solo la conferma che l'utene dell'account abbia i diritti di accesso alle informazioni, ma anche che il dispositivo utilizzato abbia i diritti sulla rete in cui sono memorizzate le informazioni e inoltre che l'utente stesso sia l'utente approvato. Questo diventa importante se si pensa alla privacy dei dati nel mondo moderno.

COME SI È EVOLUTA LA COMUNICAZIONE

Come i metodi di comunicazione si sono evoluti nel tempo, così si sono evolute anche le informazioni che stiamo comunicando. Fino a circa 50 anni fa, i messaggi si limitavano in genere a informazioni utilizzabili, tra cui indicazioni, istruzioni, previsioni e simili. Da allora, la proliferazione dei dati digitali ha fatto sì che oggi i "messaggi" comprendano quasi tutto, dalle preferenze, alle foto, ai filmati, alle transazioni, alle cartelle cliniche e ad altre informazioni personali.

Per quanto riguarda i messaggi più tradizionali, non molto tempo fa le informazioni disponibili al pubblico erano in qualche modo limitate, almeno secondo gli standard attuali. Si potevano trovare l'indirizzo e il numero di telefono di una persona solo ottenendo una copia dell'elenco telefonico locale. Se la persona che si cercava aveva un nome comune, si diventava matti a cercare la persona giusta chiamando le n voci dell'elenco telefonico con lo stesso nome.

Per quanto riguarda i dati privati e personali, i dati bancari erano in uno dei tre posti: (a) la vostra banca, (b) la vostra casa se conservavavte gli estratti conto, o (c) nella discarica locale se gettavate gli estratti conto nella spazzatura. Un documento identificativo statale si può trovare presso l'ufficio di registrazione appropriato o nel vostro portafoglio/borsetta. Allo stesso modo, i dati medici si potrebbero trovare nell'ufficio del vostro medico e, se ne avete richiesta una copia, a casa vostra. Altre informazioni personali, come ad esempio quando e dove potreste andare per la vostra corsa mattutina, i vostri gusti in fatto di musica, i vostri gusti in fatto di film o programmi televisivi, ristoranti frequentati e altri elementi potrebbero essere determinati solo intervistando la persona o interrogando i testimoni (ammesso di trovarli).

Mentre le biblioteche sono state a lungo una fonte ed archivio di informazioni, l'avvento dei motori di ricerca da Infoseek a Yahoo ad Alta Vista a Google hanno permesso alle aziende e, per estensione, ai governi di avere registrazioni di ogni argomento ricercato da ogni utente, compreso il momento in cui è accaduto e, con qualche estrapolazione, il luogo in cui è accaduto. Per quanto i motori di ricerca siano un mezzo per discernere ciò a cui le persone sono o non sono interessate, il mondo dei social media ha completamente stravolto la qualità e la quantità di informazioni personali disponibili in rete. La cosa più incredibile è che tutte queste informazioni sono state fornite su base puramente volontaria.

Il punto è che, man mano che le nostre vite diventano sempre più digitalizzate, sempre più informazioni su "noi" - alcune delle quali piuttosto personali - esistono nel ciberspazio, dove sono potenzialmente accessibili a chi ha intenzioni nefaste.

Man mano che le nostre vite diventano sempre più digitalizzate, sempre più informazioni su "noi" esistono nel cyberspazio dove sono potenzialmente accessibili a coloro che hanno intenti nefasti.

DALLA COMUNICAZIONE AL DATA-GATHERING

Un altro aspetto della digitalizzazione moderna è che, fino all'inizio del secolo, la generazione spontanea e autonoma di dati era generalmente limitata a iniziative commerciali come i sensori di produzione utilizzati per monitorare i processi di fabbrica, o i dati di posizione utilizzati per facilitare il corretto funzionamento delle reti di comunicazione. I sistemi e i sensori che in passato registravano quantità limitate di dati commercialmente critici, ora catturano enormi quantità di dati che fino all'inizio del secolo erano considerati effimeri.

I sistemi di nuova generazione includono il lancio di Facebook nel 2004[2], Twitter nel 2006[3], Instagram nel 2010[4] e Snapchat nel 2011[5]. I sensori di nuova generazione includono dispositivi come Fitbit (2007), Amazon Alexa (2014) e tutti i loro imitatori successivi. A cavallo tra sistemi e sensori si trova lo "smartphone". Mentre i cellulari hanno avuto a lungo la capacità di fornire informazioni sulla localizzazione, è stato solo con il lancio del primo iPhone nel 2008 che i consumatori, le aziende e i governi hanno iniziato a capire il potenziale di tutti i dati che venivano generati dagli smartphone.

La trasformazione digitale della nostra società - o la digitalizzazione di tutto attraverso l'internet delle cose (IoT - Interet of things) come viene chiamata - va oltre l'individuo. Diversi settori, tra cui quello aerospaziale, manifatturiero e sanitario, hanno utilizzato la digitalizzazione per migliorare i loro processi e la risposta dei clienti per ottenere una serie di vantaggi operativi. Inoltre tocchiamo ogni giorno con mano come le aziende tecnologiche e le loro attività finiscono per impattare altri settori, come i servizi finanziari e la sanità. In entrambi i casi, la crescente pervasività della digitalizzazione dà origine a un numero sempre più grabde di vettori di attacco e minacce che hanno il potenziale di creare enormi danni a persone, aziende, governi e altre istituzioni.

IL MONDO STA PRENDENDO COSCIENZA DEL PROBLEMA DELLA SICUREZZA

Nel mondo di oggi, sempre più digitalizzato, la quantità di dati accessibili, utilizzati e condivisi continua a aumentare, così come il numero di dispositivi interconnessi. In questo mondo in evoluzione, i consumatori sono sempre più preoccupati per la privacy dei loro dati personali, soprattutto data la crescente adozione di conti online con fornitori di servizi finanziari come banche, broker o utility. Sono inoltre preoccupati della loro vulnerabilità, di quella delle aziende che gestiscono le loro informazioni private, nonché delle istituzioni pubbliche. Tutto questo sta dando luogo a iniziative mirate alla sicurezza e alla privacy dei dati scambiati tra persone, aziende, governo e altre istituzioni per scongiurare attacchi informatici.

CYBERSECURITY

Come sopra riportato, la sicurezza informatica è definita come la modalità di difesa di sistemi, reti, programmi, dispositivi e dati da attacchi informatici. In sostanza possiamo dire che la cybersecurity si occupa di:

- Rendere sicure le infrastrutture di comunicazione, fisiche o meno;
- Rendere sicuro il contenuto delle comunicazioni; e
- Autentificare gli approvati destinatari di tali comunicazioni.

Sintetizziamo qui sotto i principali tipi di attacchi:

Attacchi alle infrastrutture:

- **Attacco Denial-of-Service (DoS) -** In un attacco Denial-of-Service (DoS) un aggressore inonda sistemi, server o reti con traffico che esaurisce le risorse e la larghezza di banda, con conseguente interruzione del servizio (o negazione del servizio). In un attacco Distributed Denial-of-Services (DDoS), l'attacco viene lanciato da un gran numero di macchine host che sono state infettate da software nocivo controllato dall'aggressore. A differenza di altri tipi di attacco, gli attacchi DoS e DDoS non forniscono vantaggi diretti all'aggressore, al di fuori del negare il servizio. Tuttavia, si è visto che vengono utilizzati nella "guerra della concorrenza" business-to-business, in cui un'azienda cerca di trarre un vantaggio del danno subito da un concorrente.
- **Man-in-the-Middle (MitM) Attack** – Un attacco Man-in-the-Middle (MitM) si verifica quando un aggressore si inserisce tra una comunicazione bilaterale. Una volta che l'aggressore interrompe il traffico, può filtrare e rubare i dati. Il punto di ingresso più comune per un attacco MitM è una rete Wi-Fi pubblica non sicura. L'aggressore imposta una connessione Wi-Fi con un nome apparentemente legittimo e tutto ciò che deve fare è attendere che qualcuno si connetta. Una volta effettuata la connessione, l'aggressore otterrà l'accesso immediato al dispositivo connesso.

Attacchi al Contenuto dei Messaggi:

- **SQL Injection** – Una SQL Injection, o Structured Query Language injection, si verifica quando un aggressore inserisce un codice dannoso in un server che utilizza SQL (un linguaggio specifico del dominio) e costringe il server a rivelare informazioni che normalmente non rivelerebbe.[4] Le SQL Injection hanno successo solo quando esiste una vulnerabilità di sicurezza nel software di un'applicazione.
- **Malware** – Malware è un termine usato per descrivere software dannoso come ransomware, spyware, adware, virus, infector e worm. Gli attacchi malware utilizzano un codice che viene sviluppato per colpire furtivamente un sistema informatico compromesso senza il consenso o la conoscenza dell'utente. Tipicamente, questi attacchi violano una rete attraverso alcune vulnerabilità, come quando un utente fa clic su un link pericoloso o su allegati di posta elettronica, installando involontariamente software dannoso.
- **Drive-By Attack** – Un Drive-By attacca gli utenti attraverso il loro browser Internet, installando malware sul loro computer non appena accedono su una pagina web infetta. Questi attacchi possono anche verificarsi quando un utente visita una pagina web legittima che è stata compromessa, infettando direttamente l'utente o reindirizzandolo verso un'altra pagina web dall'aspetto legittimo che è stata a sua volta compromessa.
- **Ransomware** – Secondo il rapporto Verizon's 2018 Data Breach Investigations Report, il Ransomware si verifica nel 39% delle violazioni di dati legate al malware.[1] Il rapporto evidenzia inoltre che il ransomware è diventato così comune che gli aspiranti criminali hanno ora accesso a toolkit off-the-shelf che consentono loro di creare e distribuire il ransomware in pochi minuti.

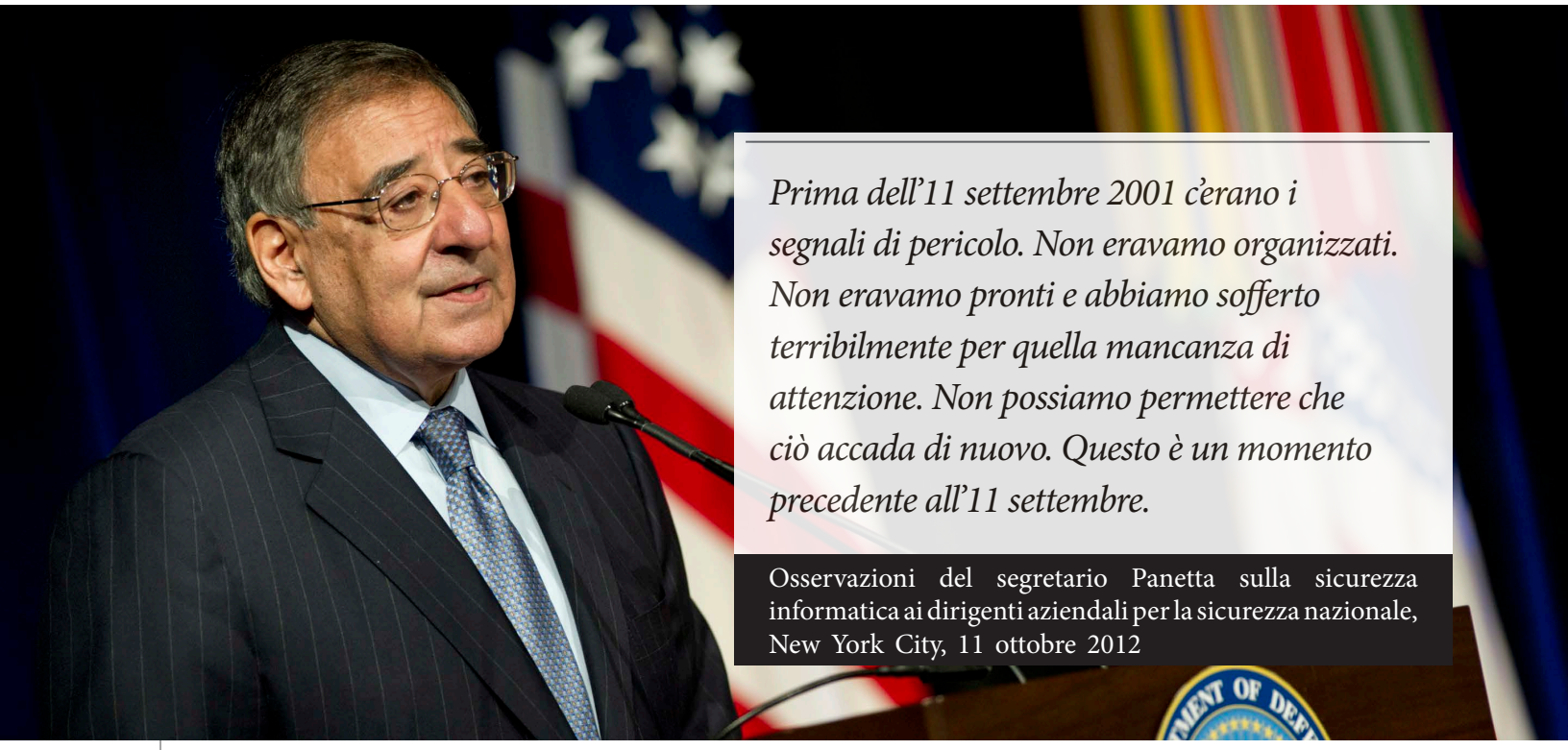
Attacchi all'autenticazione:

- **Phishing** – Il phishing è la pratica di inviare comunicazioni fraudolente che sembrano provenire da una fonte attendibile, generalmente via e-mail. L'obiettivo dell'aggressore è quello di rubare dati sensibili come le credenziali di accesso e i numeri di carta di credito o di installare malware sulla macchina della vittima.
- **Social Engineering** – Nell'era delle password, i dati personali sono spesso la chiave per decifrare le password. A tal fine, elementi apparentemente innocui come le informazioni sulla famiglia, gli animali domestici, gli hobby, i viaggi, ecc. forniscono l'opportunità di capire come una persona può pensare o dare priorità alla creazione di una password.
- **User Error** – Anche se non si tratta di un attacco di per sé, un errore utente, talvolta definito negli ambienti tecnologici come errori "ID-10.T", può essere responsabile della divulgazione pubblica involontaria di informazioni riservate. Tra gli esempi si possono citare gli utenti che lasciano le password scritte all'aperto, che lasciano i sistemi sensibili non protetti, che perdono dispositivi prototipo, che discutono informazioni sensibili in aree pubbliche. L'elenco è apparentemente infinito.

ESEMPI DI RECENTI CYBER-ATTACKS

Nell'ottobre 2012, l'allora Segretario alla Difesa Leon E. Panetta annunciò che gli Stati Uniti rischiavano di dover far fronte ad un "Cyber Pearl Harbor", sottolineando la crescente vulnerabilità del Paese nei confronti degli hacker stranieri che hanno le capacità potenziali di danneggiare reti elettriche, sistemi di trasporto, reti finanziarie e persino il Governo. In realtà, il Segretario Panetta ha molto probabilmente sottostimat quanto i cyber-attacchi diventeranno comuni negli anni a venire, man mano che imprese, governi e istituzioni si trasferiranno sempre più nel mondo digitale.

- Nel maggio 2017, il famigerato ransomware "WannaCry" si è diffuso a macchia d'olio in tutto il mondo in quello che è stato definito il peggiore attacco informatico della storia. L'attacco ha preso di mira i computer con Microsoft Windows, infettando e criptando i file sul disco rigido del PC (a sua volta rendendoli impossibili da accedere) e chiedendo poi un pagamento di riscatto (in bitcoin!) per decifrarli.[6]
- Quasi un quarto degli americani afferma di aver subito il furto di informazioni personali, carte di credito o informazioni finanziarie da parte di hacker nel 2018.[7]
- Nel 2018, Singapore ha subito un attacco senza precedenti ai sistemi informatici della sanità pubblica che ha compromesso i dati di circa 160.000 pazienti. L'attacco ha fatto seguito a simili tentativi di furto di dati sensibili in altri Paesi dell'area, compresa la massiccia violazione dei dati che ha colpito le telecomunicazioni Malesi nel 2017.[8]
- Nella primavera del 2018 la città Atlanta ha subito un ransomware attack da parte di SamSam, crypto malware che, secondo il Dipartimento di Giustizia Americano, ha causato perdite per $30 milioni a ospedali, comuni e altre istituzioni pubbliche. Il cyber-attack ha colpito più di un terzo delle computer application utilizzate dalla città, bloccando o rallentando una parte importante dei servizi pubblici erogati da Atlanta.[9]



Prima dell'11 settembre 2001 c'erano i segnali di pericolo. Non eravamo organizzati. Non eravamo pronti e abbiamo sofferto terribilmente per quella mancanza di attenzione. Non possiamo permettere che ciò accada di nuovo. Questo è un momento precedente all'11 settembre.

Osservazioni del segretario Panetta sulla sicurezza informatica ai dirigenti aziendali per la sicurezza nazionale, New York City, 11 ottobre 2012

- Nel giugno 2019, alcuni hacker lanciarono un cyber-attack a Lake City, in Florida, che ha messo fuori uso i sistemi informatici della città. L'attacco è durato diversi giorni fino a quando la giunta comunale non ha convocato una riunione di emergenza e approvato il pagamento del riscatto richiesto dagli hacker: 42 Bitcoin, all'epoca del valore di circa 460.000 dollari. Questo fu il secondo attacco del genere segnalato in altrettante settimane - la settimana precedente, Rivera Beach, Florida, approvò un pagamento straordinario di 600.000 dollari, sempre in Bitcoin.[10]
- Più recentemente, i server del fornitore di consegna pasti Door Dash è stato violato, con la conseguente potenziale fuga di informazioni relative a 4,9 milioni fra clienti, fattorini e ristoranti.[11]

MAGGIORE CONNETTIVITÀ SIGNIFICA MAGGIORE VULNERABILITÀ

All'inizio del 21° secolo, Internet aveva meno di 250 milioni di utenti globali. Nei 20 anni successivi, questa base di utenti è esplosa a 4,5 miliardi a giugno 2019, circa il 59% della popolazione globale, secondo i dati pubblicati da Internet World Stats.[12] Negli ultimi due decenni, i consumatori e le imprese si sono rivolti sempre più alla rete per effettuare transazioni, acquistare, vendere, trasmettere in streaming, comunicare e scambiare informazioni e altri contenuti. L'attuale indice di rete Cisco Visual Networking Index (VNI), che misura e proietta la crescita del volume di traffico IP, stima che tale traffico globale triplichi tra il 2017 e il 2022.[13]

Un fattore chiave di questa crescita sarà l'aumento esponenziale del numero di dispositivi collegati per famiglia e per persona. Entro il 2022, il numero di dispositivi collegati in rete e di connessioni per persona dovrebbe raggiungere la media di 3,6 - in aumento da 2,4 nel 2017.[14]

Ogni anno vengono introdotti e adottati dal mercato diversi nuovi dispositivi capacità di memoria e calcolo sempre maggiori. Un numero crescente di applicazioni Machine-to-Machine (M2M), come i contatori intelligenti, la videosorveglianza, il monitoraggio sanitario, il trasporto e la tracciabilità dei pacchetti o degli asset, stanno contribuendo in modo significativo alla crescita dei dispositivi e delle connessioni. Si stima che entro il 2022, le connessioni M2M saranno il 51% del totale dei dispositivi e delle connessioni.[15]

Il rovescio della medaglia di questa robusta crescita della connettività è il marcato aumento delle vulnerabilità informatiche e delle violazioni della privacy. Per le persone, questa connettività digitalizzata facilita le transazioni, rendendole rapide e comode. Per imprese e istituzioni, viene utilizzata per aumentare l'efficienza, ridurre i costi e far crescere aziende data-driven che si adattano meglio alle esigenze del mondo moderno. La questione diventa pertanto piuttosto evidente: al crescere dell'utilizzo dei dati informatici, sia individui che imprese diventano via via più vulnerabili a ciber-attacchi. Queste preoccupazioni in materia di sicurezza e privacy sono alcune delle ragioni per cui il 22% degli utenti della banda larga del Regno Unito non ha ancora installato un dispositivo per la domotica intelligente e non prevede di acquistarne uno, secondo Park Associates.[16]

PRIVACY DEI DATI - LA PROSSIMA AREA DI INTERVENTO PER LA SPESA INFORMATICA

La spesa dei consumatori nel campo della sicurezza informatica comprende:

- Servizi di protezione contro il furto di identità personale.
- Servizi di riparazione di computer e telefoni cellulari specifici per la rimozione di malware e virus.
- Installazione di software antivirus e di protezione da malware.
- Servizi post-infrazione, compreso il recupero dei dati, e l'educazione degli utenti sulle migliori pratiche per la difesa cibernetica personale.

Le preoccupazioni sulla privacy dei dati sono diventate un fattore chiave per i consumatori e si prevede che porteranno il mercato globale del software per la gestione della privacy a 1,6 miliardi di dollari entro il 2027, in aumento rispetto ai 521 milioni di dollari del 2018, secondo una ricerca pubblicata da ResearchAndMarkets.[17]

Una ricerca pubblicata da Statista ha recentemente rilevato che il 53% degli utenti in tutto il mondo è preoccupato per la loro privacy online.[18] Secondo il nuovo studio Deloitte US Consumer Data Privacy, quasi la metà dei consumatori statunitensi (47%) ritiene di avere poco o nessun controllo sui propri dati personali, e uno su tre ha avuto i propri dati compromessi. Non è quindi sorprendente che la stragrande maggioranza (86%) dei consumatori vorrebbe avere la possibilità di bloccare la vendita delle proprie informazioni digitali.[19]

Secondo il nuovo studio Deloitte sulla privacy dei dati dei consumatori negli Stati Uniti, quasi la metà dei consumatori statunitensi (47%) ritiene di non avere quasi nessun controllo sui propri dati personali e uno su tre ne ha compromesso i dati.

LE NORME SULLA PRIVACY STIMOLANO LA SPESA INFORMATICA

. . . mentre il 56% delle aziende ha riferito di avere maggiori problemi di sicurezza, il 37% è stato impegnato a concentrarsi sul rispetto delle modifiche alle normative.

Oltre agli investimenti per combattere gli attacchi informatici, le imprese stanno investendo molto in misure di sicurezza IT anch per rispondere alle nuove normative sulla privacy, come il regolamento generale europeo sulla protezione dei dati (GDPR). Una recente indagine di Spiceworks ha dimostrato che i leader IT concordano con un recente sondaggio pubblicato da Gartner, secondo il quale i due principali fattori alla base dei budget IT sono l'aumento delle preoccupazioni in materia di sicurezza e i cambiamenti del quadro normativo di riferimento. Altri dati, tra cui alcuni pubblicati da Proofpoint, una società di sicurezza informatica aziendale, hanno mostrato che, mentre il 56% delle aziende ha riferito di aver affrontato sempre maggiori problemi di sicurezza, il 37% era impegnato a concentrarsi sul rispetto delle modifiche alle normative. I recenti risultati di Cisco Systems, un'altra importante azienda di sicurezza informatica, indicano inoltre che i dirigenti considerano sempre più le normative e la conformità come fattori chiave per il futuro della spesa per la sicurezza informatica.[20]

Poiché le normative GDPR coprono qualsiasi azienda che opera nell'UE, esse impattano le aziende di tutto il mondo, ritenendole responsabili del trattamento improprio delle informazioni personali delle cittadini europei. Negli ultimi anni ci sono state decine di massicce violazioni di dati, tra cui milioni di dati di Yahoo!, LinkedIn e MySpace. Secondo GDPR, la "distruzione, perdita, alterazione, divulgazione non autorizzata o accesso ai" dati delle persone deve essere segnalata all'autorità di regolamentazione della protezione dei dati di un paese.

L'aspetto più discusso del GDPR è rappresentato dalla possibilità delle Autorità Europee di multare le imprese che non rispettano le norme. Se un'organizzazione non salvaguarda o non elabora correttamente i dati di un individuo, può essere multata. Se è richiesto, e un'organizzazione non ha un responsabile della protezione dei dati, può essere multata. Se c'è una violazione della sicurezza, può essere multata. Le multe GDPR (multe amministrative) possono arrivare fino a 20 milioni di euro o al 4% del fatturato globale annuo. Prima dell'applicazione della GDPR, la multa massima per ogni violazione della protezione dei dati era stata pari a 500.000 sterline ($624.000) - quando Facebook fu multata per tale importo nel luglio 2018.[21]

Le multe GDPR (ammende amministrative) possono raggiungere i 20 milioni di euro o il 4% del fatturato globale annuo, a seconda di quale sia il più elevato.

Finora sono state inflitte diverse multe di alto profilo da parte del GDPR. British Airways ha dovuto far fronte ad una multa record di 230 milioni di dollari dopo che il fallimento del suo sito web ha compromesso i dati personali di circa 500.000 clienti. La multa di 230 milioni di dollari rappresenta circa l'1,5% del fatturato annuale di British Airways. In un altro caso di alto profilo, Marriott International ha ricevuto una multa di poco più di 124 milioni di dollari per aver esposto una serie di dati personali di 339 milioni di record di clienti a livello globale.[22]

STA ARRIVANDO ULTERIORE REGOLAMENTAZIONE DELLA PRIVACY, A LIVELLO GLOBALE

La legge CCPA richiederà un pulsante di "opt-out" su ogni pagina di ogni sito Web, consentendo ai consumatori di comunicare facilmente alle aziende che non desiderano che nessuno dei loro dati venga raccolto, gestito e / o venduto.

Negli Stati Uniti, un regolamento simile è stato approvato dal California Consumer Privacy Act (CCPA). Una bozza è in fase di consultazione pubblica, che comprende diverse audizioni pubbliche, le cui proposte sono aperte fino al 6 dicembre 2019. La CCPA entrerà in vigore il 1° gennaio 2020, con le linee guida definitive previste per il 1° luglio 2020.[23]

Il CCPA porta con sé una serie di nuove normative che limitano in modo significativo il modo in cui le aziende raccolgono e gestiscono i dati dei consumatori che hanno alimentato la crescita della pubblicità digitale. La legge richiederà un pulsante "opt-out" su ogni pagina di ogni sito web, permettendo ai consumatori di impedire facilmente alle aziende che i loro dati siano raccolti, gestiti e/o venduti. I consumatori potranno anche richiedere alle aziende, agli editori o ai brand di cancellare i loro dati. Le persone potranno infine rinunciare alle condizioni di servizio di un'azienda senza perdere l'accesso alle sue offerte. Alle aziende sarà inoltre vietato vendere i dati di chiunque abbia meno di 16 anni senza un esplicito consenso.

In termini di contravvenzioni per coloro che violeranno queste norme, il CCPA stabilisce una multa per utente pari a $100 - $750 o danni effettivi (il maggiore tra i due) anche per violazione non intenzionale. Ciò significa che un servizio web relativamente piccolo con 1 milione di conti potrebbe essere multato di 100-750 milioni di dollari, una somma che potrebbe portare rapidamente una piccola società al fallimento.

E mentre il CCPA marcia verso la finalizzazione e l'attuazione, ulteriori leggi americane si stanno facendo strada in vari stati degli Stati Uniti. Il prossimo stato da tenere d'occhio sarà New York con il suo Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) che entrerà in vigore nel marzo 2020.[24] La legge SHIELD amplia la definizione di "informazioni personali". Prima della legge SHIELD, le informazioni personali comprendevano "qualsiasi informazione riguardante una persona fisica che, a causa del nome, del numero, del marchio personale o

di altri identificatori, può essere utilizzata per identificare tale persona fisica". La definizione ampliata della legge SHIELD comprende le informazioni personali che consistono in qualsiasi informazione in combinazione con uno o più dei seguenti elementi di dati, quando l'elemento di dati o la combinazione di informazioni personali più l'elemento di dati non è criptato o è criptato con una chiave di criptazione che è stata anche aperta o acquisita:

- Numero di previdenza sociale;
- Numero di patente di guida o numero di carta d'identità;
- Numero di conto, numero di carta di credito o di debito, in combinazione con qualsiasi codice di sicurezza, codice di accesso, password o altre informazioni che consentano l'accesso al conto finanziario di un individuo; numero di conto, numero di carta di credito o di debito, se esistono circostanze in cui tale numero può essere utilizzato per accedere al conto finanziario di un individuo senza ulteriori informazioni di identificazione, codice di sicurezza, codice di accesso o password;
- Informazioni biometriche, ossia dati generati da misurazioni elettroniche delle caratteristiche fisiche uniche di un individuo, come un'impronta digitale, un'impronta vocale, un'immagine della retina o dell'iride, o altre rappresentazioni fisiche uniche o rappresentazioni digitali di dati biometrici che vengono utilizzati per autenticare o accertare l'identità dell'individuo; oppure
- Un nome utente o un indirizzo e-mail in combinazione con una password o una domanda di sicurezza e una risposta che consentirebbe l'accesso a un account online.[25]

Lo Stato di New York non è l'unico Stato ad ampliare la definizione di "informazione privata". Anche l'Illinois, l'Oregon e il Rhode Island hanno ampliato le loro definizioni per includere non solo informazioni mediche ma anche alcuni codici di identificazione relative alle assicurazioni sanitarie.[26]

Siamo agli albori di quello che sembra essere un quadro normativo sempre più ampio e stringente, che porterà a una forte domanda di prodotti per la sicurezza e la privacy, in quanto le aziende cercano di contrastare attacchi sempre più sofisticati e di proteggere i dati da violazioni che potrebbero tradursi in pesanti sanzioni.

LA CYBERSECURITY CONTINUERÀ A CRESCERE

Tutto quanto sopra significa che la spesa per la sicurezza informatica è destinata a crescere. Siamo nel bel mezzo di un boom informatico, mentre emergono nuovi vettori di attacco e si sviluppano nuove contromisure. Questo si riflette nelle previsioni che suggeriscono che la criminalità informatica costerà 6 trilioni di dollari all'anno entro il 2021, in aumento rispetto ai 3 trilioni di dollari del 2015, secondo Cybersecurity Ventures.[27] Tale previsione include i costi associati al danneggiamento e alla distruzione dei dati, il denaro rubato, la perdita di produttività, il furto di proprietà intellettuale, il furto di dati personali e finanziari, l'appropriazione indebita, la frode, le interruzioni post-attacco, le indagini forensi, il ripristino dei dati e dei sistemi hackerati, nonché il danno alla reputazione.

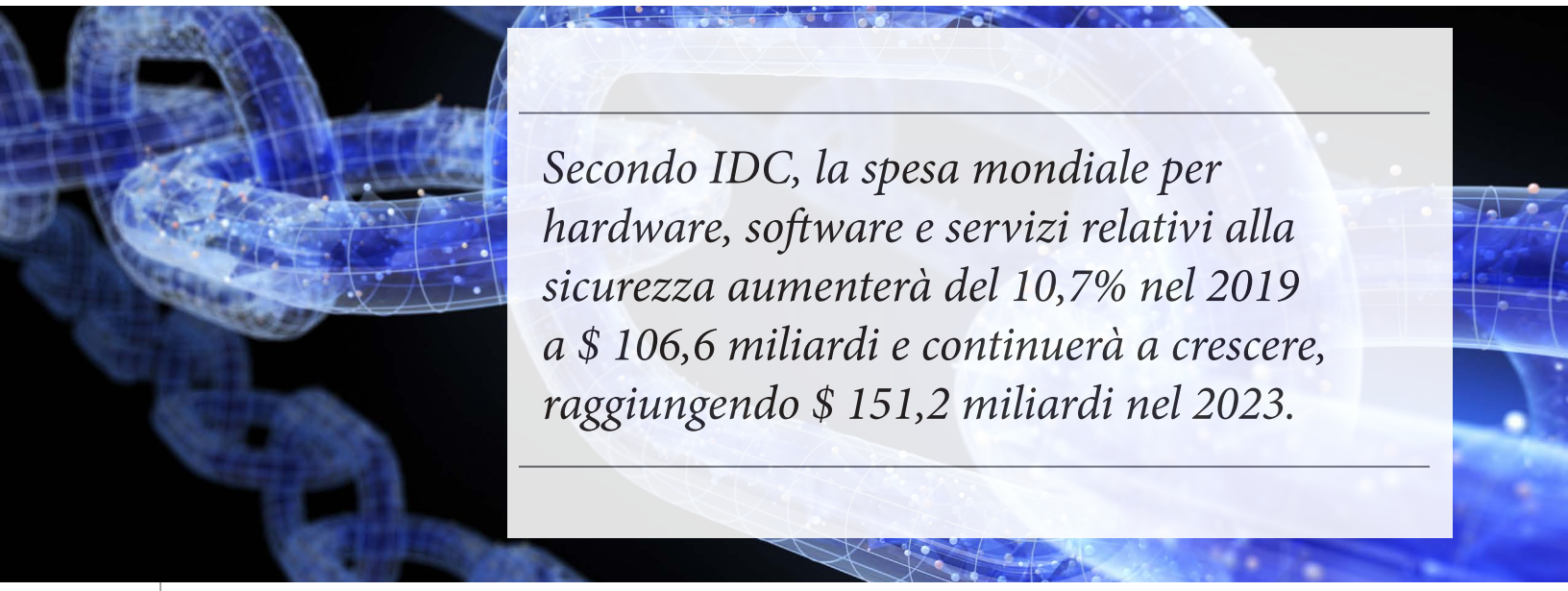
La questione dei cyber-attacchi e delle violazioni della privacy sarà ulteriormente aggravata dalle nuove tecnologie, come il cloud computing, l'intelligenza artificiale, l'interet of things (IoT) e il 5G. Queste tecnologie apriranno collettivamente nuovi punti di vulnerabilità e permetteranno nuove forme di attacchi. In termini di vulnerabilità potenziali, il solo mercato dell'IoT, che comprende dispositivi collegati che vanno dalle auto e dalle linee di assemblaggio di fabbrica ai baby monitor e ai semafori dovrebbe raggiungere i 25 miliardi di dispositivi entro il 2021, secondo i dati raccolti da Gartner.[28] Per mettere questi dati in prospettiva, Cybersecurity Ventures si aspetta che, nel 2021, ogni 11 secondi un'azienda cadrà vittima di un attacco informatico, rispetto ad uno ogni 14 secondi nel 2019 e uno ogni 40 secondi nel 2016.[29]

La questione degli attacchi informatici e delle violazioni della privacy sarà ulteriormente aggravata dalle nuove tecnologie, come il cloud computing, l'intelligenza artificiale, l'IoT e il 5G.

Questo inquadra bene il motivo per cui i cyber-attacks sono stati considerati il rischio principale alla stabilità del business da parte dei dirigenti delle aziende negli Stati Uniti, in Canada e in Europa, secondo un sondaggio tra i leader aziendali pubblicato dal World Economic Forum, in collaborazione con Zurich Insurance Group e Marsh & McLennan.[30]

Questa comprensibile preoccupazione si riflette in diverse previsioni di spesa per la sicurezza informatica:

- Gartner prevede che nel 2019 la spesa per la sicurezza IT in tutto il mondo sia cresciuta dell'8,7%, raggiungendo i 124 miliardi di dollari rispetto al 2018. Gartner prevede inoltre che i servizi di sicurezza rappresenteranno il 50% dei budget per la sicurezza informatica entro il 2020, con aree di investimento chiave per i servizi di sicurezza, la protezione delle infrastrutture e le attrezzature di sicurezza della rete.[31]
- La spesa mondiale per la sicurezza delle informazioni (un sottoinsieme del più ampio mercato della sicurezza informatica) ha superato i 114 miliardi di dollari nel 2018 e, secondo Gartner, nel 2022 tale mercato raggiungerà i 170,4 miliardi di dollari.[32]
- Si prevede che la spesa globale per la formazione sulla consapevolezza della IT security e i programmi di simulazione di phishing per i dipendenti - una delle categorie in più rapida crescita nel settore della sicurezza informatica - raggiungerà i 10 miliardi di dollari entro il 2027, rispetto a circa 1 miliardo di dollari nel 2014.[33]
- MarketsandMarkets prevede che il mercato della sicurezza informatica raggiungerà i 248,3 miliardi di dollari entro il 2023, crescendo ad un CAGR del 10% nel periodo 2018-2023.[34]
- Cybersecurity Ventures ha previsto che la spesa globale per la sicurezza informatica supererà i 1.000 miliardi di dollari cumulativamente dal 2017 al 2021.[35]
- Secondo una previsione aggiornata della International Data Corporation (IDC) Worldwide Semiannual Security Spending Guide, la spesa mondiale per hardware, software e servizi legati alla sicurezza aumenterà del 10,7% nel 2019 fino a raggiungere 106,6 miliardi di dollari nel 2019 e continuerà a crescere, raggiungendo i 151,2 miliardi di dollari nel 2023.[36]



Secondo IDC, la spesa mondiale per hardware, software e servizi relativi alla sicurezza aumenterà del 10,7% nel 2019 a $ 106,6 miliardi e continuerà a crescere, raggiungendo $ 151,2 miliardi nel 2023.

CONCLUSIONE

A nostro avviso, non c'è dubbio che la sicurezza informatica sia un mercato in crescita, con persone, aziende e istituzioni che cercheranno di scongiurare attacchi futuri, rafforzare le loro difese informatiche esistenti, valutare gli attacchi e monitorare/analizzare le intrusioni.

Tutto questo si traduce in una sola cosa: maggiore spesa per la sicurezza. Mentre gli importi effettivi in dollari possono variare, ciò che tutte queste previsioni hanno in comune è un vettore verso l'alto e una velocità crescente, con la spesa per la sicurezza informatica che rappresenta la parte maggiore del budget complessivo di spesa IT. Per Gartner, la spesa IT generale è destinata a crescere del 3,2% nel 2019 rispetto all'8,7% per la sicurezza informatica.[37]

Queste traiettorie indicano una continua crescita della spesa informatica, dato che la sicurezza informatica è una corsa agli armamenti contro hacker sempre più sofisticati che cercano di sfruttare nuove vulnerabilità tramite nuove forme di attacco. La storia suggerisce tuttavia che le previsioni di spesa dell'industria sono state troppo prudenti. Ad esempio, nel 2017, Gartner prevedeva che nel 2018 la spesa sarebbe salita a 93 miliardi di dollari. A metà del 2018, Gartner ha rivisto tale previsione di spesa a 114 miliardi di dollari per tutto il 2018.[38] I dati per Gartner mostrano che anche quella revisione al rialzo è scesa modestamente al di sotto dei 114,1 miliardi di dollari spesi nel 2018. Tutto ciò è di buon auspicio per il tema di investimento Cybersecurity & Data Privacy di Tematica Research.

Endnotes

1 "128-Bit Encryption" Available at https://www.techopedia.com/definition/29708/128-bit-encryption

2 "From Alibaba to Google, here are the 10 biggest tech IPOs of all time" Available at https://yourstory.com/2018/02/biggest-tech-ipo-of-all-time/

3 Ibid

4 "Our story" Available at https://instagram-press.com/our-story/

5 "From Alibaba to Google, here are the 10 biggest tech IPOs of all time" Available at https://yourstory.com/2018/02/biggest-tech-ipo-of-all-time/

6 CSO, "The 6 biggest ransomware attacks of the last 5 years", 2019. Available at https://www.csoonline.com/article/3212260/the-5-biggest-ransomware-attacks-of-the-last-5-years.html

7 Gallup, "One in Four Americans Have Experienced Cybercrime", 2018. Available at https://news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx

8 The Straits Times, "Info on 1.5m SingHealth patients stolen in worst cyber attack", 2018. Available at https://www.straitstimes.com/singapore/info-on-15m-singhealth-patients-stolen-in-worst-cyber-attack

9 The New York Times, "A Cyberattack Hobbles Atlanta, and Security Experts Shudder", 2019. Available at https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

10 Ibid

11 CNBC, "DoorDash hack leaks data of 4.9 million customers, restaurants", 2019. Available at https://www.cnbc.com/2019/09/27/doordash-hack-leaks-data-of-4point9-million-customers-restaurants.html

12 Internet World Stats. Available at https://www.internetworldstats.com

13 Cisco Systems, "Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper" Available at https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

14 Ibid

15 Ibid

16 Park Associates, "U.K. smart home adoption lagging compared to the U.S.", 2018. Available at https://www.parksassociates.com/newsletter/article/ca-nov18

17 ResearchAndMakets, "Privacy Management Software Market to 2027", 2019. Available at https://www.researchandmarkets.com/reports/4762324/privacy-management-software-market-to-2027#pos-0

18 Statista, "Online privacy - Statistics & Facts", 2109. Available at https://www.statista.com/topics/2476/online-privacy/

19 Chain Store Age, "Deloitte: Consumers seek control of personal data", 2019. Available at https://chainstoreage.com/deloitte-consumers-seek-control-personal-data

20 Cisco System, "Maximizing the value of your data privacy investments", 2019. Available at https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf

21 The Guardian, "UK fines Facebook £500,000 for failing to protect user data", 2018. Available at https://www.theguardian.com/technology/2018/oct/25/facebook-fined-uk-privacy-access-user-data-cambridge-analytica

22 Compliance Week, “Marriott reveals $124M GDPR fine for data breach”, 2019. Available at https://www.complianceweek.com/data-privacy/marriott-reveals-124m-gdpr-fine-for-data-breach/27373.article

23 CNBC, “California AG tells businesses like Facebook and Google how they must comply with the state’s new landmark privacy law”, 2019. Available at https://www.cnbc.com/2019/10/11/california-attorney-general-outlines-rules-for-state-privacy-law-ccpa.html

24 JD Supra, “SHIELD Act Overhauls New York’s Data Privacy Framework”, 2019. Available at https://www.jdsupra.com/legalnews/shield-act-overhauls-new-york-s-data-33724/

25 Workplace Privacy, Data Management & Security Report, “New York Enacts the SHIELD Act”, 2019. Available at https://www.workplaceprivacyreport.com/2019/07/articles/data-breach-notification/new-york-enacts-the-shield-act/

26 Ibid

27 Cybersecurity Ventures, “Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021”, 2018. Available at https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

28 Network World, “Gartner’s top 10 IoT trends for 2019 and beyond”, 2018. Available at https://www.networkworld.com/article/3322517/a-critical-look-at-gartners-top-10-iot-trends.html

29 Cybersecurity Ventures, “Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021”, 2018. Available at https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

30 Insurance Journal, “Cyber-Attacks Named as Top Business Risk in U.S., Canada and Europe, by WEF Survey”, 2019. Available at https://www.insurancejournal.com/news/international/2019/10/01/541672.htm

31 Security Intelligence, “11 Trends to Inform Your 2020 Cybersecurity Budget”, 2019. Available at https://securityintelligence.com/articles/11-stats-on-ciso-spending-to-inform-your-2020-cybersecurity-budget/

32 Cybersecurity Ventures, “Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021”, 2018. Available at https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

33 Ibid

34 MarketsandMarkets, “Cybersecurity Market worth $248.3 billion by 2023”, 2019. Available at https://www.marketsandmarkets.com/PressReleases/cyber-security.asp

35 Cybersecurity Ventures, “Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021”, 2018. Available at https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

36 IDC, “New IDC Spending Guide Sees Solid Growth Ahead for Security Products and Services”, 2019. Available at https://www.idc.com/getdoc.jsp?containerId=prUS45591619

37 Gartner, “Gartner Says Global IT Spending to Grow 3.2 Percent in 2019”, 2019. Available at https://www.gartner.com/en/newsroom/press-releases/2018-10-17-gartner-says-global-it-spending-to-grow-3-2-percent-in-2019

38 Gartner, “Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019”, 2018. Available at https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019