Scoprire minacce informatiche e creare opportunità d'investimento

it.allianzgi.com

Documento ad uso esclusivo e riservato di distributori di fondi ed investitori professionali

L'attacco è stato bloccato prima che potesse causare danni. L'8 febbraio 2021 gli hacker hanno avuto accesso da remoto all'impianto di trattamento delle acque della città di Oldsmar, in Florida, e hanno aumentato il livello di idrossido di sodio di 111 volte. A questi livelli, i 15.000 residenti si sarebbero ammalati seriamente. Fortunatamente, l'acqua non ha mai raggiunto le loro case; l'hacking del trattamento dell'acqua in Florida è stato sventato.[1]

Ancora più recentemente, il 9 maggio 2021, un gruppo di hacker chiamato Darkside ha lanciato un attacco ransomware che ha fermato un oleodotto essenziale per l'energia negli Stati Uniti.
La Colonial Pipeline trasporta 2,5 milioni di barili di prodotti petroliferi raffinati dalla costa del Golfo degli Stati Uniti alle principali città statunitensi della East Coast.[2] L'interruzione ha generato il panico nelle stazioni di servizio statunitensi e ha minacciato di causare un danno economico significativo. È stato riportato che l'organizzazione ha dovuto pagare un riscatto di 5 milioni di dollari per ricevere la chiave in grado di sbloccare i dati che sono stati criptati dal gruppo di hacker.[3]

Solo 3 giorni dopo, lo stesso gruppo di hacker ha attaccato la divisione nordamericana del distributore chimico tedesco Brenntag, e ha richiesto un pagamento di circa 4,4 milioni di dollari.[4]

Questi sono solo alcuni esempi della gravità dei cyberattacchi.

Per contestualizzare il tutto, secondo uno studio dell'Università del Maryland, gli hacker colpiscono in media una volta ogni 39 secondi, il che equivale a 2.244 volte al giorno.[5] Molte aziende spesso non sanno di essere state attaccate, mentre altre scelgono di non divulgare questi eventi per paura di subire danni di reputazione.[6]
La frequenza e la portata di questi attacchi è destinata ad aumentare man mano che il nostro mondo diventa sempre più connesso digitalmente.

Analizziamo alcuni dei pericoli che le aziende devono affrontare.

Gli hacker attaccano in media una volta **ogni 39 secondi**, il che equivale a **2.244 volte** al giorno

Value. Shared.

Allianz Global Investors

1 Minaccia 1
Mancanza di sufficienti capacità di cybersecurity

All'inizio della pandemia le aziende sono state costrette a organizzare le attività del personale in smart-working e di conseguenza la loro infrastruttura informatica è stata messa a dura prova, al di là di ogni previsione. È stata l'occasione perfetta a disposizione dei cyberattackers per colpire.

Gli strumenti di videoconferenza che i dipendenti hanno iniziato ad utilizzare per comunicare erano vulnerabili. Secondo Deloitte, quasi mezzo milione di lavoratori hanno subito il furto di dati personali per le vulnerabilità informatiche causate dal software di videoconferenza durante il primo lockdown.[7]

Gli attacchi di ransomware, le frodi di identità e le campagne di phishing sono aumentate significativamente durante questo periodo. Anche gli attacchi che utilizzavano strumenti di cracking delle password e tattiche di controllo dei conti, sono stati utilizzati frequentemente per accedere ai conti online. Come del resto sono aumentate le frodi bancarie e i furti d'identità.

L'importo più alto riportato per il pagamento di un ransomware ammonta a più di

4.5m USD

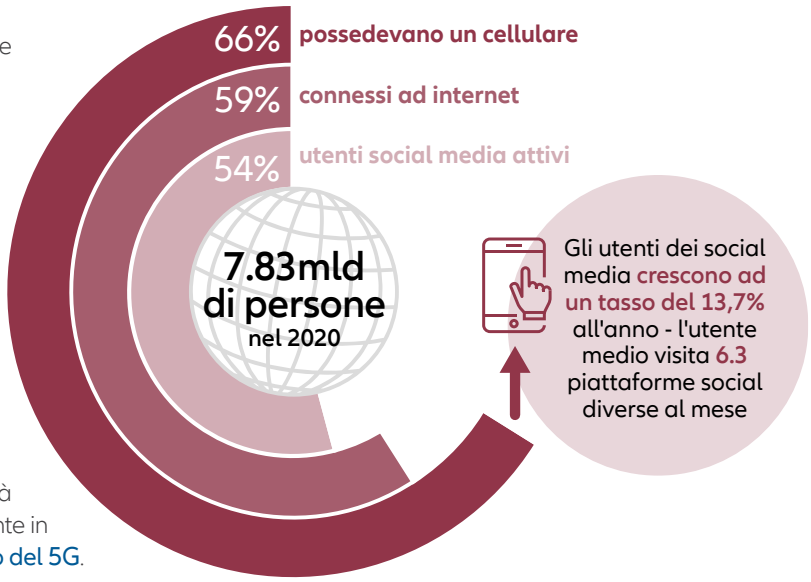
Secondo IBM, il costo medio di ogni violazione dei dati che un'azienda ha subito nel 2020 è stato di 3,86 milioni di dollari. Secondo le statistiche, ci sono voluti in media 270 giorni per individuare una violazione, mentre ci sono voluti in media 280 giorni dal momento in cui la violazione è stata indentificata fino al suo completo contenimento.[8]

Ransomware, un software che cripta i tuoi dati chiedendo un riscatto per il loro rilascio (Kaspersky) è il malware in più rapida crescita secondo il Dipartimento di Giustizia degli Stati Uniti. Questo malware, secondo il Dipartimento, inizia a criptare i file della vittima in soli tre secondi.[9] **La somma più alta ricondotta al pagamento di un ransomware ammonta a più di 4,5 milioni di dollari.[10] Questo tipo di crimine provoca danni e lascia le persone e le organizzazioni impotenti.**

2 Minaccia 2
Crescita esponenziale dei dati

È verosimile che il cybercrimine continui ad aumentare anche dopo la pandemia. La crescita esponenziale di dati non adeguatamente protetti nel mondo digitale in cui stiamo vivendo è destinata ad essere un fattore importante.

Nel 2020, sulla Terra la popolazione era di 7,83 miliardi di persone. Il 66% possedeva un telefono cellulare. Nel frattempo il 59% era connesso ad internet. Il 54% erano anche utenti attivi sui social media.[11] Queste cifre sono poi aumentate a causa della pandemia. Secondo datareportal.com, a livello mondiale, gli utenti dei social media crescono ad un tasso del 13,7% all'anno, con l'utente medio dei social media che visita o usa 6,3 diverse piattaforme social ogni mese.[12]



L'enorme mole di dati che creiamo oggi offre più opportunità di attacco ai criminali informatici. Tuttavia, questo non è niente in confronto a quello che potremmo incontrare con lo sviluppo del 5G.

3 Minaccia 3
Connettività crescente

Quando il 5G sarà effettivamente operativo, ci sarà una vera e propria impennata di dispositivi connessi ad internet che produrranno una quantità di dati ancora maggiore.

Entro il 2025, si prevede che ci saranno più di 30 miliardi di dispositivi connessi, il che equivale a quattro dispositivi per persona a livello globale.[13]

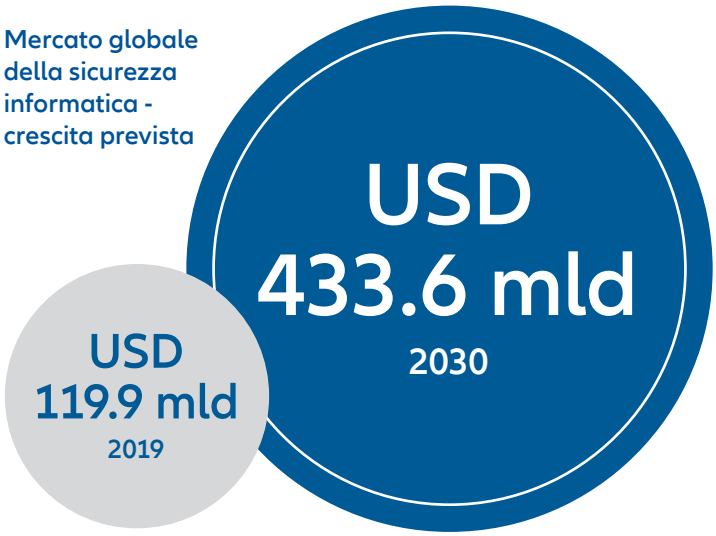
Non saranno solo gli smartphone, i portatili e i computer ad essere connessi al 5G - vedremo anche un numero crescente di auto a guida autonoma, dispositivi all'interno di case intelligenti e attrezzature industriali nelle fabbriche, che conterranno chipset 5G.

Una maggiore sicurezza è la soluzione

La sicurezza informatica sarà una componente che diventerà fondamentale nella nostra economia tecnologica emergente.

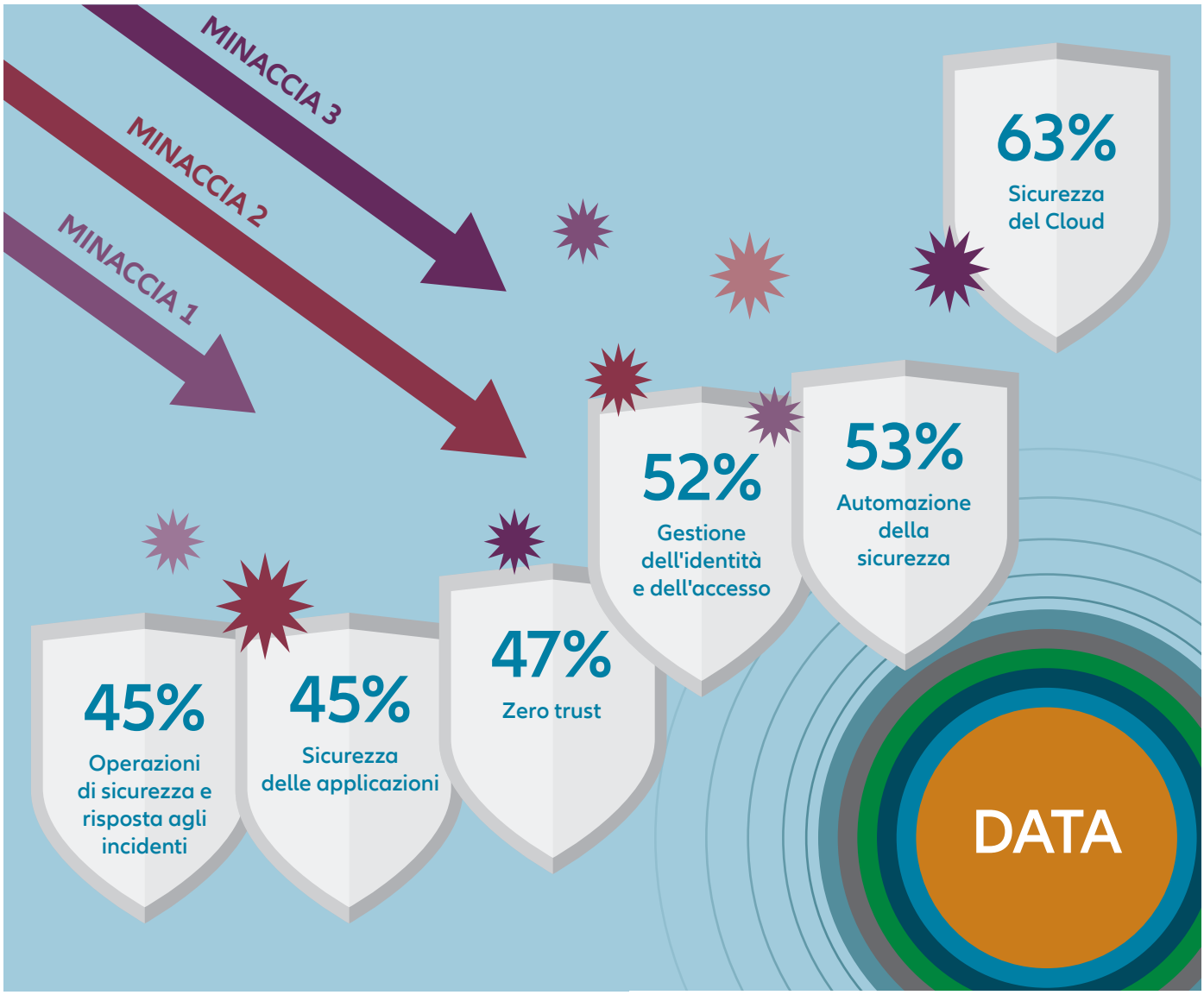
Secondo le previsioni, il mercato globale della sicurezza informatica crescerà ad un tasso del **12,6% all'anno fino al 2030, passando da 119,9 miliardi di dollari nel 2019 (prima del Covid-19) a 433,6 miliardi entro il 2030.**[14]

Infatti, secondo un recente rapporto di Accenture Security, più del 20% del budget informatico viene destinato dalle aziende leader in tecnologia avanzata, che è quasi il doppio di quanto è stato investito negli ultimi tre anni.[15]



Fonte: ResearchAndMarkets.com (2020), "Global Cybersecurity Market 2020 to 2030"

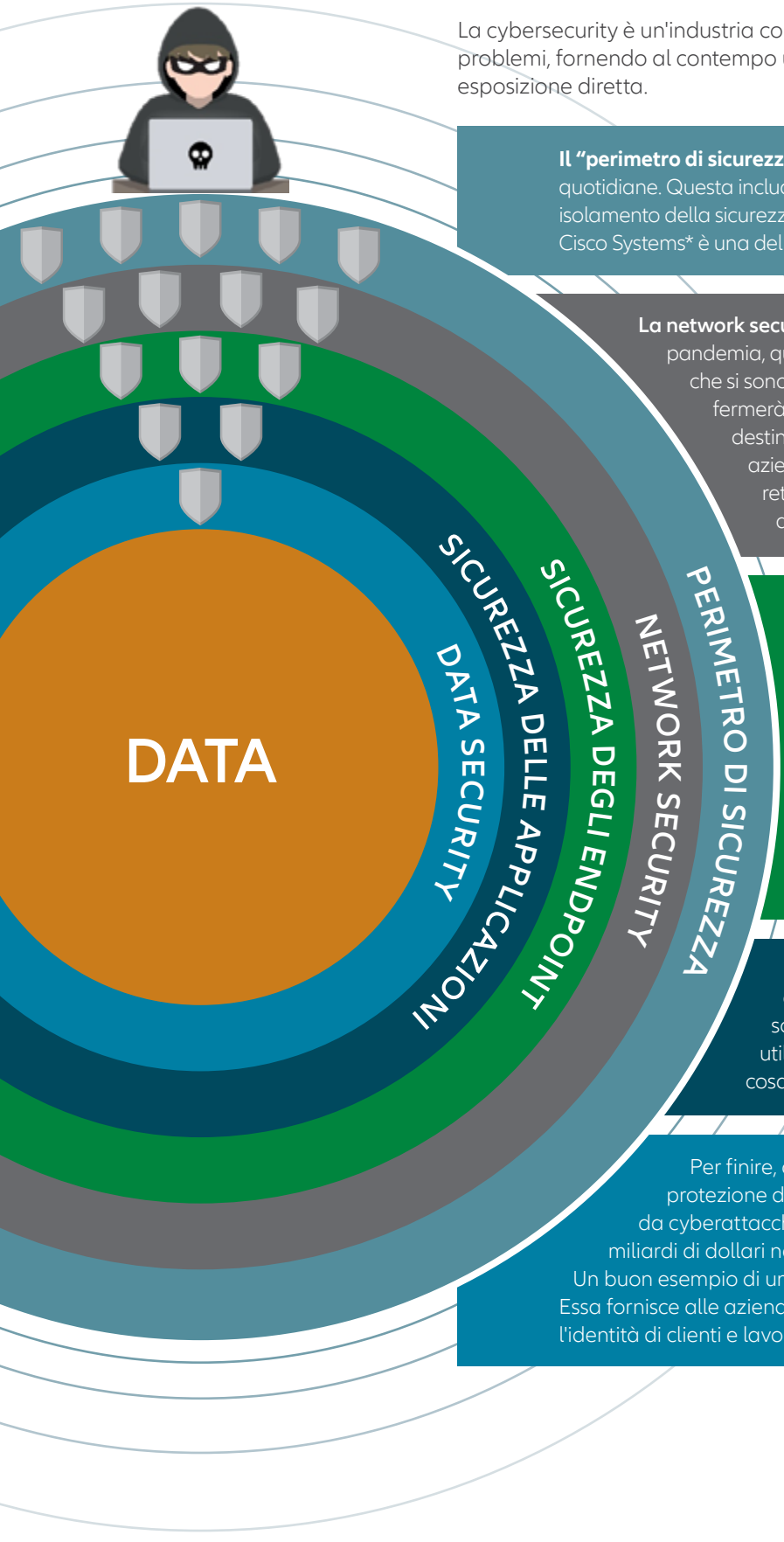
Le principali aree in cui i leader della sicurezza stanno aumentando i loro investimenti



Fonte: Team8: 2021 Cybersecurity Brief

Come investire nella crescita della sicurezza informatica?

La cybersecurity è un'industria complessa che propone soluzioni a una varietà di problemi, fornendo al contempo una grande opportunità di diversificazione e di esposizione diretta.



Il "perimetro di sicurezza" è probabilmente la più importante delle attività quotidiane. Questa include il firewall del browser, ma anche i sistemi di isolamento della sicurezza che riconoscono le minacce ad una rete di computer. Cisco Systems* è una delle aziende più conosciute che operano in questo settore.

La network security è diventata particolarmente importante durante la pandemia, quando si è verificato un enorme aumento dei lavoratori che si sono collegati da remoto. Ma questo probabilmente non si fermerà dopo che la pandemia sarà finita. Il cloud computing è destinato a vedere questa tendenza continuare in futuro e alle aziende sarà richiesto di far fronte ad una struttura ibrida di reti interne ed esterne. Le aziende, come FireEye*, ora aiutano le imprese a migliorare questo tipo di sicurezza.

C'è anche la **sicurezza degli endpoint**, che ha come scopo la protezione delle reti di computer da dispositivi come desktop, portatili e smartphone che sono collegati ad essa. Questa può essere un'area di vulnerabilità per le reti di computer ed è diventata sempre più importante dato che sempre più aziende adottano la tecnologia cloud. Un'azienda che lavora in questo spazio è CrowdStrike*, che aiuta a garantire la sicurezza degli endpoint e fornisce informazioni sulle minacce alle aziende per cui lavora.

Anche la sicurezza delle applicazioni è importante e costituisce la proprietà intellettuale di molte aziende. Le società dovranno solamente proteggere i dati e il codice utilizzato per realizzare le applicazioni di loro proprietà, cosa che aziende come Zscaler* possono aiutarle a fare.

Per finire, c'è la **sicurezza dei dati** stessi. In altre parole, la protezione dei dati digitali, come quelli memorizzati nei database da cyberattacchi. Gartner* ritiene che questo mercato crescerà da 9,8 miliardi di dollari nel 2019 a circa 14,0 miliardi di dollari entro il 2024.[14] Un buon esempio di un'azienda che opera in questo spazio è Okta*. Essa fornisce alle aziende una piattaforma che può aiutare a proteggere l'identità di clienti e lavoratori.

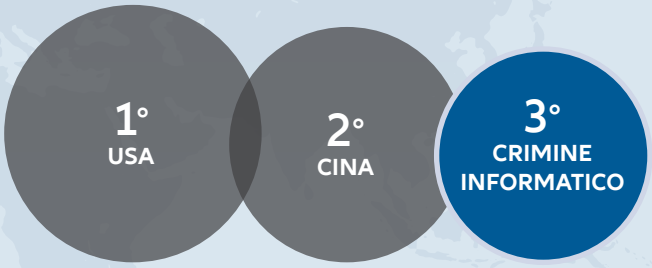
* Non si intende raccomandare o sollecitare l'acquisto o la vendita di alcun titolo specifico. Un titolo menzionato in via esemplificativa potrebbe non essere più presente nel portafoglio di investimenti della strategia alla data di pubblicazione del presente documento o ad una qualsiasi data successiva.

Cosa ci dobbiamo aspettare?

Il crimine informatico è un trend di lungo termine che ha subito un'accelerazione a causa della pandemia. Questo ha, a sua volta, consolidato l'importanza della sicurezza informatica come parte dell'economia globale in futuro.

La crescente sofisticazione del crimine informatico è allarmante e di difficile comprensione per la maggior parte delle persone non specializzate nel campo. Secondo X-Force di IBM Security* "il 35% degli incidenti investigati sfrutta le vulnerabilità [del loro obiettivo] nell'attacco".[16]

È un problema importante. Se i costi del crimine informatico nel 2021 fossero il PIL del paese, questi rappresenterebbero la terza grandezza al mondo dopo gli Stati Uniti e la Cina. Si prevede che il crimine informatico potrebbe costare 6 trilioni di dollari nel 2021.[17]



Non esiste una soluzione unica per tutti

Le aziende necessiteranno di diversi livelli di sicurezza informatica con soluzioni personalizzate. In alcuni casi, la copertura di ogni livello di sicurezza informatica dovrà essere richiesta a diversi fornitori, questo è il motivo per cui è fondamentale avere una solida industria specializzata in tale tema. Senza questo tipo di infrastruttura, sarà impossibile veder nascere una futura economia digitale.

Questa è un'industria che probabilmente registrerà una crescita considerevole in futuro. Ecco perché il momento di investire nella sicurezza informatica è adesso.

[1] Robles, F., & Perlroth, N. (2021, February 9). 'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town. The New York Times. https://www.nytimes. com/2021/02/08/us/oldsmar-florida-water-supply-hack.html.
[2] Colonial Pipeline: cyberattack draws attention to besieged US energy system. (2021, May 11). Financial Times. https://www.ft.com/content/de0be95e-fbd4-40ff-ab3a-2e8490fdcd32.
[3] Javers, E. (2021, May 14). Colonial Pipeline paid $5 million ransom to hackers. CNBC. https://www. cnbc.com/2021/05/13/colonial-pipeline-paid-ransom-to-hackers-source-says.html.
[4] https://www.washingtonpost.com/politics/2021/05/14/cybersecurity-202-biden-saysrussian-government-was-not-involved-with-colonial-pipeline-hack/.
[5] https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds University of Maryland 2007.
[6] https://www.itgovernance.co.uk/blog/data-breaches-and-cyber-attacks-quarterly-review-q1-2021.
[7] Nabe, C. (2020, December 15). Impact of COVID-19 on Cybersecurity. Deloitte Switzerland. https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html.
[8] IBM Security. (2020). Cost of a Data Breach Report 2020. https:// www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf.
[9] https://www.justice.gov/criminal-ccips/file/872771/download.
[10] https://www.itgovernance.co.uk/blog/the-5-biggest-ransomware-pay-outs-of-all- time#:~:text=The%20US%20travel%20services%20company,compromised%20two%20 terabytes%20of%20data.
[11] https://datareportal.com/global-digital-overview April 2021.
[12] Kemp, S. (2021, April 19). Digital 2021: Global Overview Report. DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2021-global-overview-report.
[13] Kenworthy, R. (2019, November 18). The 5G And IoT Revolution Is Coming: Here's What To Expect. Forbes. https://www.forbes.com/sites/forbestechcouncil/2019/11/18/the-5g-iot-revolution-is-coming-heres-what-to-expect/?sh=59e632086abf.
[14] ResearchAndMarkets.com. (2020, November 19). Business Wire. https://www.businesswire.com/news/home/20201119005835/en/Global-Cyber-Security-Market-2020-to-2030- --by-Component-Security-Type-Deployment-Enterprise-Use-Case-and-Industry---ResearchAndMarkets.com.
[15] Accenture Security. (2020). State of Cybersecurity Report 2020. https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf.
[16] Firch, J. M. (2021, May 17). 10 Cybersecurity Trends You Can't Ignore In 2021. PurpleSec. https://purplesec.us/cyber-security-trends-2021/.
[17] Morgan, S. (2021, April 27). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

AdMaster: 1729289

Luglio 2021