enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

PL

Od stycznia 2019 r. do kwietnia 2020 r.

Wyciek informacji

Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)

Informacje ogólne

Naruszenie bezpieczeństwa danych ma miejsce, gdy dane, za które odpowiedzialna jest organizacja, są przedmiotem incydentu związanego z bezpieczeństwem, skutkującego naruszeniem ich poufności, dostępności lub integralności[1]. Naruszenie bezpieczeństwa danych często powoduje wyciek informacji, który jest jednym z głównych zagrożeń cybernetycznych, obejmujący szeroką gamę zagrożonych informacji, od danych osobowych, przez dane finansowe przechowywane w infrastrukturach IT, po dane medyczne przechowywane w repozytoriach podmiotów opieki zdrowotnej.

Kiedy naruszenia bezpieczeństwa pojawiają się w nagłówkach biuletynów, blogów, gazet i raportów technicznych, uwaga skupia się głównie na przeciwnikach lub na katastrofalnej niesprawności procesów i technik obrony cybernetycznej. Niemniej jednak jest niezaprzeczalnym faktem, że mimo wpływu lub zakresu takiego zdarzenia, naruszenie jest zwykle spowodowane działaniem jednostki lub niesprawnością procesu organizacyjnego[2].

Wnioski

2013_potwierdzonych ujawnień danych w roku 2019

W pierwszej połowie 2019 r. organizacje odnotowały wzrost ujawnień o 11% w porównaniu z 2018 r.[5,6]

14%_wszystkich incydentów w sektorze finansowym stanowiły ujawnienia danych

W 47% tych zdarzeń ofiarą był bank[9].

4,1_miliarda rekordów danych na całym świecie ujawniono w pierwszej połowie 2019 roku

Na szczycie tej listy były wiadomości e-mail i hasła[10].

5,46_mln euro to najwyższy koszt poniesiony przez sektor ochrony zdrowia[11]

Kill chain

Proces etapów ataku

Zakres działania

Rozwiązanie Cyber Kill Chain® zostało opracowane przez Lockheed Martin na podstawie wojskowej koncepcji związanej ze strukturą ataku. Aby zbadać określony wektor ataku, należy użyć poniższego schematu Cyber Kill Chain w celu stworzenia mapy każdego etapu procesu i określić narzędzia, techniki i procedury, z jakich skorzystał atakujący.

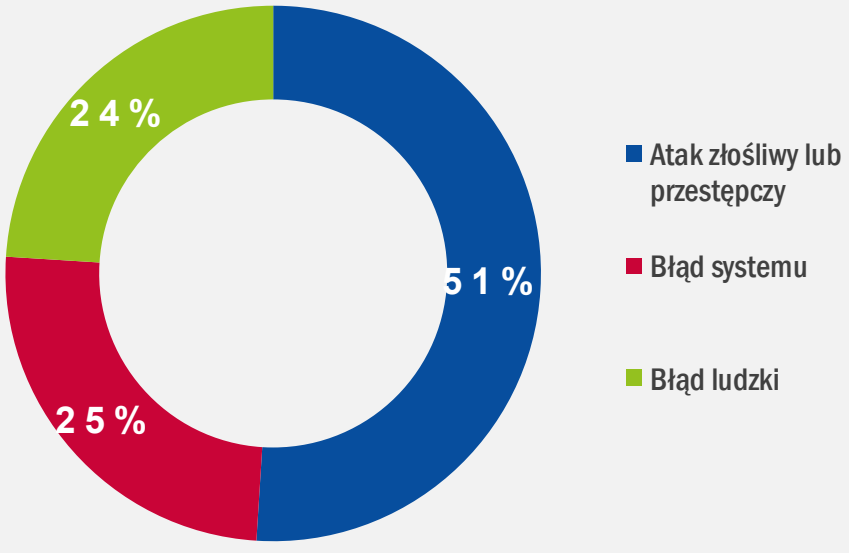
WIĘCEJ INFORMACJI

Incydenty

_Najpoważniejsze przypadki wycieków danych

- W styczniu 2019 roku niezależny analityk Troy Hunt odkrył 773 milionów adresów e-mail i haseł użytkowników **w chmurze MEGA**. Hunt nazwał ten zagrożony zbiór danych „Collection #1" i powiadomił usługę: „Have I been Pwned?", by mogła powiadomić właścicieli kont o konieczności zmiany haseł logowania do platformy MEGA[12]. W tym samym miesiącu nieuczciwe osoby ujawniły dane osobowe, prywatną korespondencję i informacje finansowe setek **niemieckich polityków**, reprezentujących każdą partię polityczną poza skrajnie prawicową AfD (Alternatywa dla Niemiec)[6].
- W lutym 2019 roku z 16 stron internetowych zostało zebranych ponad 61 milionów kont, które wystawiono na sprzedaż w „ciemnej sieci". Właściciele witryn Whitepages, Dubsmash, Armor Games, 500px i ShareThis dowiedzieli się, że skradzione dane ich użytkowników sprzedano za mniej niż 20 000 USD (ok. 17 000 euro) w kryptowalucie bitcoin[13].
- W marcu 2019 roku setki milionów użytkowników serwisów **Facebook** i **Instagram** stwierdziło, że ich dane uwierzytelniające stały się widoczne z powodu kiepskiego zarządzania przechowywaniem haseł przez operatora mediów społecznościowych[14].
- W kwietniu 2019 roku w Indiach ujawniono 12,5 miliona rekordów dokumentacji medycznej ciężarnych kobiet z powodu nieszczelności rządowego serwera należącego do agencji opieki zdrowotnej. Ujawnione informacje medyczne były związane z indyjską ustawą dotyczącą prekoncepcyjnych i prenatalnych technik diagnostycznych, zakazującą prenatalnego określania płci w celu zapobieżenia aborcji nienarodzonych dziewczynek, co zakłóciłoby równowagę płci w społeczeństwie[15].

- W maju 2019 roku dostarczająca jedzenie firma **DoorDash** doznała naruszenia bezpieczeństwa danych, które dotknęło prawie 5 milionów użytkowników. Późniejsze dochodzenie wykazało, że przestępcy uzyskali dostęp do informacji takich jak nazwiska, adresy e-mail, adresy dostawy, historia zamówień, numery telefonów i hasła. Firma poinformowała, że uzyskali oni również dostęp do ostatnich czterech cyfr numerów kart kredytowych i numerów rachunków bankowych niektórych klientów[16].
- W czerwcu 2019 roku **American Medical Collection Agency (AMCA)** zaczęła powiadamiać klientów o włamaniu do systemu, które naruszyło bezpieczeństwo danych rozliczeniowych i medycznych niektórych pacjentów, w tym 11,9 mln rekordów **Quest Diagnostics**, jednej z największych w Stanach Zjednoczonych firm zajmujących się badaniami krwi. Według niedawnego zgłoszenia 8K Komisji Papierów Wartościowych i Giełd haker miał dostęp do systemu AMCA przez prawie osiem miesięcy między 1 sierpnia 2018 r. a 30 marca 2019 r.[17]



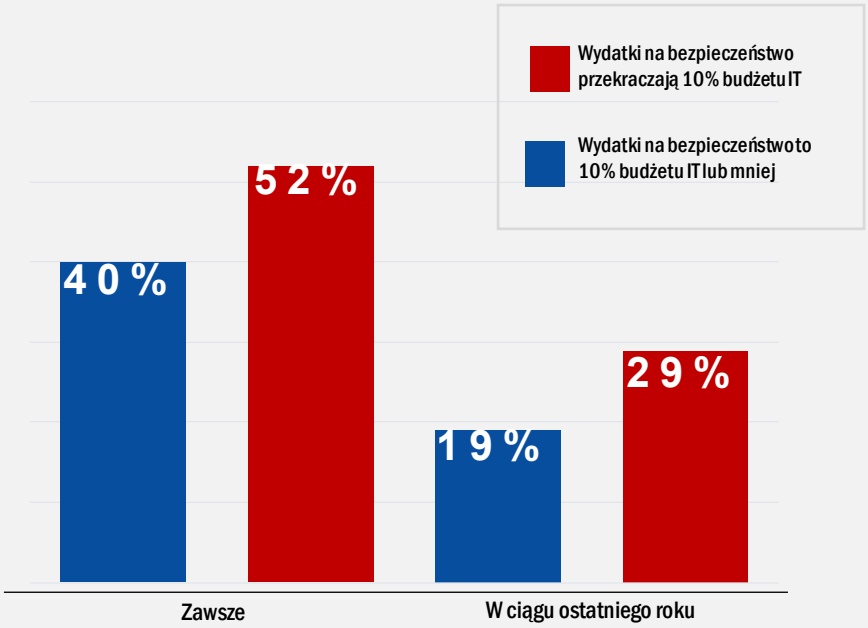
Główne przyczyny ujawnienia informacji. Źródło: Ponemon, IBM Security[22]

Incydenty

_Najpoważniejsze przypadki wycieków danych

- W lipcu 2019 r. wyciek informacji w korporacji finansowej **Capital One** objął 100 milionów wniosków o karty kredytowe, 140 tys. numerów ubezpieczenia społecznego i 80 tys. numerów kont bankowych.Capital One poinformowała, że nie ujawniono żadnych numerów rachunków kart kredytowych ani danych logowania. Jednak naruszenie ujawniło imiona i nazwiska, adresy, kody pocztowe, numery telefonów, adresy e-mail i daty urodzenia[18].
- W sierpniu 2019 roku 160 milionów rekordów **MoviePass** pozostawało niezaszyfrowanych. Ponieważ baza danych firmy nie była chroniona hasłem, widoczne były numery kart kredytowych klientów i inne szczegóły. Baza danych pozostawała online przez kilka dni[19]. W międzyczasie ogromny wyciek ujawnił 27,8 mln biometrycznych rekordów pracowników **brytyjskiej policji metropolitalnej**, banków i kontrahentów zbrojeniowych. Bazą zarządzała firma Suprema, która współpracuje z brytyjską policją[20,21].
- We wrześniu 2019 r. zhakowano ponad 218 milionów kont graczy **„Words with Friends"**. Baza danych użytkowników zawierała dane użytkowników systemów Android i iOS, którzy zainstalowali grę przed 2 września. Zespół hakerów „Gnostic players" uzyskał dostęp do informacji takich jak imiona i nazwiska graczy, adresy e-mail, dane logowania itd.[23]
- W październiku 2019 roku firma Adobe pozostawiła w niezabezpieczonej bazie danych 7,5 miliona rekordów klientów Creative Cloud. Wyciek informacji obejmował adresy e-mail użytkowników i status płatności[24].
- W listopadzie 2019 roku Facebook przyznał niewłaściwe prawa dostępu do danych profilowych 70 tys. swoich klientów około 100 twórcom aplikacji. Jeden z nich ukradł dane osobowe, a potem wykorzystał je do oszustwa[25].

- W grudniu 2019 r. **holenderski polityk** stanął wobec perspektywy 3 lat więzienia za włamanie na konta 100 kobiet w iCloud i ujawnienie nagich zdjęć. Okazało się, że polityk włamał się do osobistych kont kobiet w usłudze iCloud, korzystając z danych uwierzytelniających znalezionych podczas wcześniejszych włamań do publicznych baz danych[26]. W tym samym miesiącu na forum hakerskim ujawniono dane ponad 10,7 mln gości ośrodka wypoczynkowego **Metro-Goldwyn-Mayer (MGM)**. Informacje, które wyciekły, obejmowały imiona i nazwiska klientów, adresy domowe, numery telefonów, adresy e-mail i daty urodzenia[27].

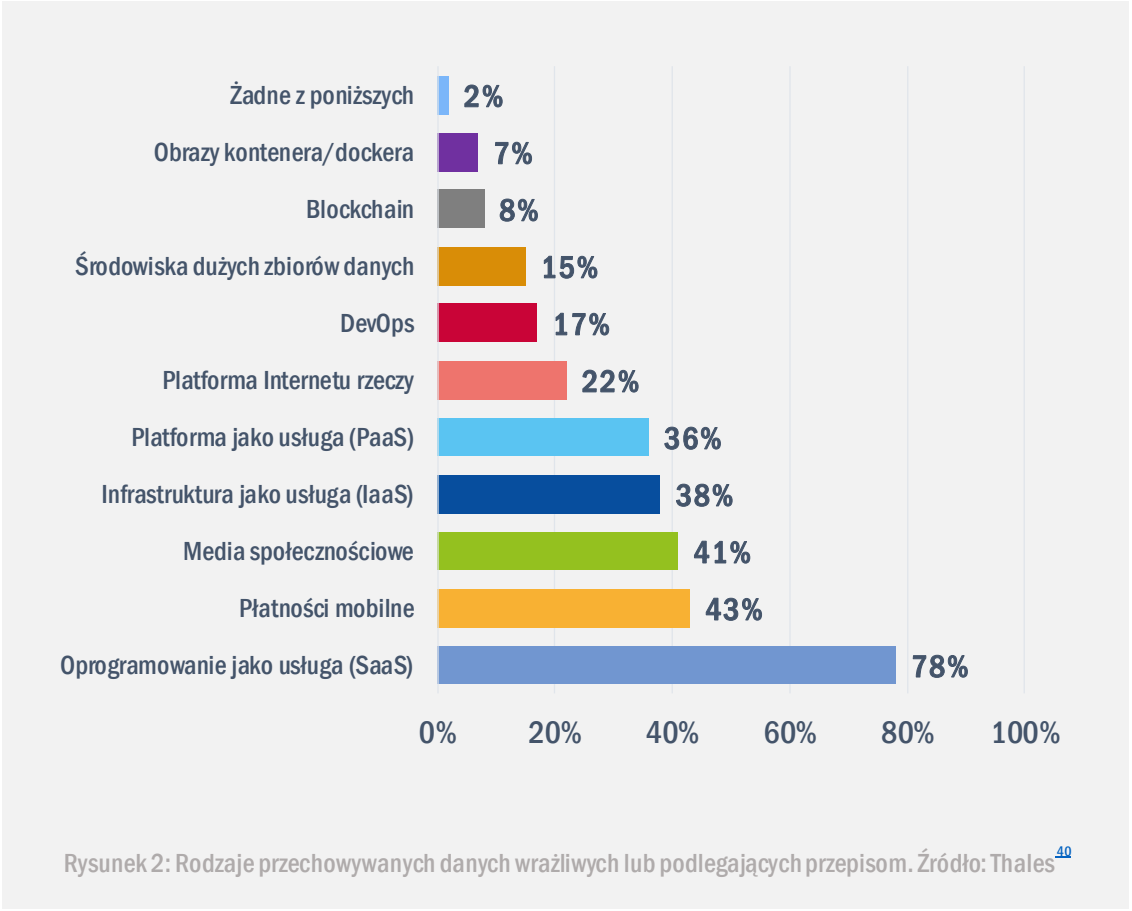


Rysunek 1: Wskaźniki incydentów naruszenia w zależności od wydatków na bezpieczeństwo. Źródło: CNET[14]

Wektory ataku

_Jak

Głównym wektorem ataków związanych z wyciekiem informacji są osoby wtajemniczone. Termin ten oznacza osoby zainteresowane „wyniesieniem” ważnych informacji wewnętrznych na potrzeby osób trzecich. Inne typowe wektory ataku wykorzystywane w związku z tym zagrożeniem to błędna konfiguracja, luki w zabezpieczeniach i błędy ludzkie.



Rysunek 2: Rodzaje przechowywanych danych wrażliwych lub podlegających przepisom. Źródło: Thales[40]

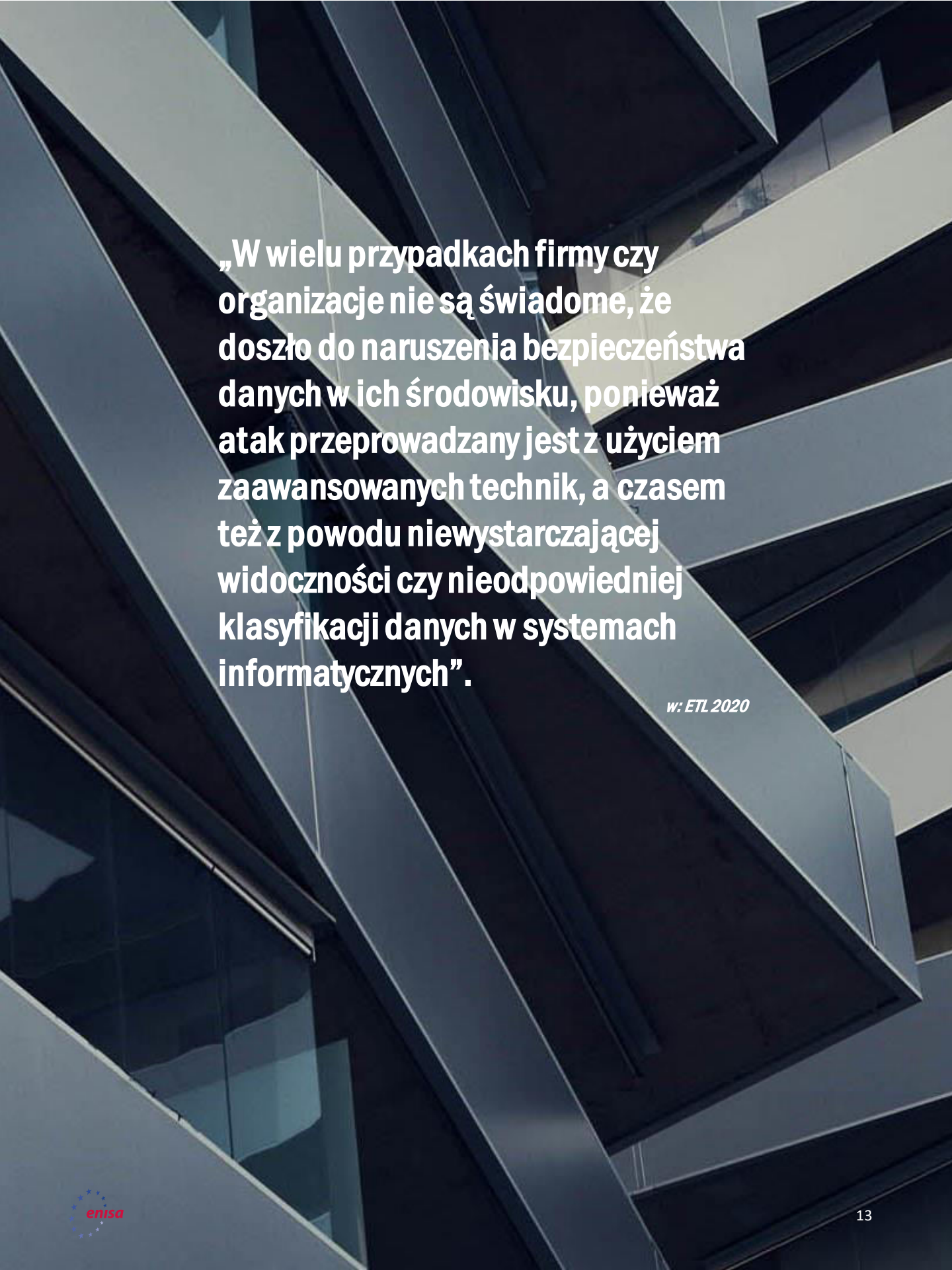
„Naruszenie bezpieczeństwa danych często powoduje wyciek informacji – jedno z głównych zagrożeń cybernetycznych, dotyczące szerokiej gamy danych”

w: ETL 2020

Ograniczenie ryzyka

Proponowane działania

- Anonimizowanie, pseudonimizowanie, minimalizowanie i szyfrowanie danych zgodnie z przepisami RODO UE, kalifornijską ustawą o ochronie prywatności konsumentów (CCPA) oraz chińską wielopoziomową ochroną bezpieczeństwa informacji (MLPS 2.0)[28,29,30,31]. Należy zawsze sprawdzać zobowiązania regulacyjne w odniesieniu do kontrahentów, którzy nie są objęci inicjatywami dwu- ani wielostronnymi[32,33,34].
- Przechowywanie danych tylko w bezpiecznych zasobach IT[35].
- Ograniczenie uprawnień dostępu użytkowników zgodnie z zasadą wiedzy koniecznej[35,36]. Należy odwołać uprawnienia dostępu każdemu, kto nie jest pracownikiem[35].
- Regularne edukowanie i szkolenie personelu[35,37].
- Korzystanie z narzędzi technicznych przeciwdziałających potencjalnym wyciekom danych, takich jak skanowanie luk w zabezpieczeniach, skanowanie złośliwego oprogramowania oraz narzędzia do ochrony przed utratą danych (DLP, data loss prevention). Wdrożenie szyfrowania danych oraz przenośnych systemów i urządzeń, a także bezpiecznych bram[36,38].
- Kluczowe znaczenie dla postępowania w przypadku naruszenia bezpieczeństwa danych ma plan ciągłości działania (BCP). Plan ten określa rodzaj przechowywanych danych i ich lokalizację oraz potencjalne zobowiązania, jakie mogą powstać podczas wdrażania działań związanych z bezpieczeństwem i odzyskiwaniem danych. Posiadanie BCP umożliwia skuteczną reakcję na incydent, której celem jest ograniczenie i naprawienie szkód przez niego spowodowanych[39].



„W wielu przypadkach firmy czy organizacje nie są świadome, że doszło do naruszenia bezpieczeństwa danych w ich środowisku, ponieważ atak przeprowadzany jest z użyciem zaawansowanych technik, a czasem też z powodu niewystarczającej widoczności czy nieodpowiedniej klasyfikacji danych w systemach informatycznych".

w: ETL 2020

Bibliografia

1. „What is a data breach and what do we have to do in case of a data breach?" Komisja Europejska. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military- intelligence-service-exposed.
2. „The human factor of cyber security". CSO. https://www.csoonline.com/article/3504813/the-human-factor-of-cyber-security.html
3. Howard Poston. „Common causes of large breaches (Q1 2019)". 1 maja 2019 r. INFOSEC Institute. https://resources.infosecinstitute.com/common-causes-of-large-breaches/#gref
4. J. Clement. „Average cost of data breaches worldwide from 2014 to 2019". 13 sierpnia 2019 r. Statista. https://www.statista.com/statistics/987474/global-average-cost-data-breach/
5. „2019 Data Breach Investigations Report". 2019. Verizon. https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf
6. „Cyber Threatscape Report". 2019. iDefense – Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf
7. „Cybercrime will cost businesses over $2 trillion by 2019". 12 maja 2015 r. Juniper Research https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019
8. „How much would a data breach cost your business?". 2019. IBM. https://www.ibm.com/security/data-breach
9. G. Dautovic. „Top 25 Financial Data Breach Statistics for 2020". 11 marca 2020 r. Fortunly. https://fortunly.com/statistics/data-breach-statistics#gref
10. Davey Winder.„Data Breaches Expose 4.1 BIllion Records In First Six Months of 2019". 20 sierpnia 2019 r. Forbes. https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#40479be4bd54
11. „Cost of a Data Breach Report". 2019. Ponemon Institute – IBM. https://databreachcalculator.mybluemix.net/executive-summary/
12. Troy Hunt. „The 773 Million Record 'Collection #1'. Data Breach", 17 stycznia 2019 r. Troy Hunt. https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/
13. Lewis Morgan. „List of data breaches and cyber attacks in February 2019 – 873,919,635 records leaked". 26 lutego 2019 r. IT Governance. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-february-2019-692853046-records-leaked
14. Rae Hodge. „2019 Data Breach Hall of Shame: These were the biggest data breaches of the year". 27 grudnia 2019 r. CNET. https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/
15. Catalin Cimpanu. „Indian govt agency left details of millions of pregnant women exposed online" 1 kwietnia 2019 r. ZDNet. https://www.zdnet.com/article/indian-govt-agency-left-details-of-millions-of-pregnant-women-exposed-online/
16. Shelby Brown. „DoorDash data breach affected 4.9M customers, drivers, merchants" 26 września 2019 r. CNET. https://www.cnet.com/news/doordash-data-breach-affected-4-9-million-customers-workers-and-merchants/
17. Jessica Davis. „11.9M Quest Diagnostics Patients Impacted by AMCA Data Breach". 3 czerwca 2019 r. HealthITSecurity https://healthitsecurity.com/news/11.9m-quest-diagnostics-patients-impacted-by-amca-data-breach
18. Alfred Ng, Mark Serrels. „Capital One data breach involves 100 million credit card applications". 30 lipca 2019 r. CNET. https://www.cnet.com/news/capital-one-data-breach-involves-100-million-credit-card-applications/
19. Shelby Brown. „Data breaches timeline: EasyJet cyberattack exposes over 9M people, and more". 19 maja 2020 r. CNET. https://www.cnet.com/how-to/equifax-mgm-resorts-beyond-every-major-security-breach-and-data-hack-update/
20. Josh Taylor. „Major breach found in biometrics system used by banks, UK police and defence firms". 14 sierpnia 2019 r. The Guardian. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

21. Guy Fawkes. „Report: Data Breach in Biometric Security Platform Affecting Millions of Users". 16 czerwca 2020 r. vpnMentor. https://www.vpnmentor.com/blog/report-biostar2-leak/

22. „Cost of a Data Breach Report". 2019. Ponemon - IBM Security. https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.148238199.1762516747.1577395260-1128561362.1577395260

23. Oscar Gonzalez. „Zynga data breach exposed 200 million Words with Friends players". 1 października 2019 r. CNET. https://www.cnet.com/news/people-rarely-change-their-passwords-after-a-data-breach-study-says/

24. John E Dunn. „Adobe database exposes 7.5 million Creative Cloud users". 28 października 2019 r. Naked Security. https://nakedsecurity.sophos.com/2019/10/28/adobe-database-exposes-7-5-million-creative-cloud-users/

25. „Insider Sold 68K Customer Records to Scammers: Trend Micro." 8 listopada 2019 r. CISOMAG. https://www.cisomag.com/insider-sold-68k-customer-records-to-scammers-trend-micro/

26. Catalin Cimpanu. „Dutch politician faces three years in prison for hacking iCloud accounts and leaking nudes". 3 grudnia 2019 r. ZDNet. https://www.zdnet.com/article/dutch-politician-faces-three-years-in-prison-for-hacking-icloud-accounts-and-leaking-nudes/

27. Corinne Reichert. „MGM Resorts confirms data breach of 10.7 million guests". 19 lutego 2020 r. https://www.cnet.com/news/mgm-resorts-confirms-data-breach-of-10-million-guest-accounts/

28. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, RODO). 27 kwietnia 2016 r. Parlament Europejski, Rada Unii Europejskiej. https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=celex%3A32016R0679

29. „AB-375 Pri.vacy: personal information: businesses, Assembly Bill No. 375, Chapter 55" 29 czerwca 2018 r. California Legislative Information. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

30. Shrub Chandrasekaran, Justin Fishman. „China's Cybersecurity Future and its Impact on U.S. Business". 31 października 2019 r. Jolt Digest. https://jolt.law.harvard.edu/digest/chinas-cybersecurity-future-and-its-impact-on-u-s-business

31. Reed Smith LLP. „MLPS 2.0: China's enhanced data security multi-level protection scheme and related enforcement updates". 9 października 2019 r. Lexology. https://www.lexology.com/library/detail.aspx?g=36c6932b-bf41-4e08-b430-e3bc839a2328

32. „Data protection if there's no Brexit deal". 13 września 2018 r. GOV. UK, Department for Digital, Culture, Media & Sport. https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal

33. Eduardo Ustaran, „Brexit and data protection: Laying the odds". 21 września 2018 r. Privacy Perspectives, iapp. https://iapp.org/news/a/brexit-and-data-protection-laying-the-odds/

34. Ibrahim Hasan. „Data protection and Brexit". 5 września 2016 r. Gazette. https://www.lawgazette.co.uk/legal-updates/data-protection-and-brexit/5057412.article

35. Eric Dosal. „5 Tips to Prevent Data Leakage at Your Company". 15 marca 2018 r. Compuquip Cybersecurity.https://www.compuquip.com/blog/5-tips-to-prevent-data-leakage-at-your-company

36. „10 ways to protect sensitive business data". 28 października 2019 r. QuoStar. https://www.quostar.com/blog/10-tips-to-help-prevent-a-data-leak/

37. „Annual Cybersecurity Report". 2018 r. Cisco https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2

38. „Cybercrime tactics and techniques: Q2 2018". 2018 r. Malwarebytes Labs

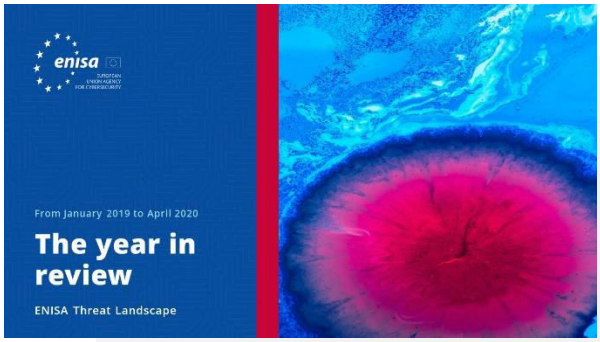
https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf

39. Mona Mangat. „81 Eye-Opening Data Breach Statistics for 2020". 27 stycznia 2020 r. phoenixNAP. https://phoenixnap.com/blog/data-breach-statistics

40. „2020 Data Threat Report – Global Edition". 2020. Thales Group. https://www.thalesesecurity.com/2020/data-threat-report

41. Oscar Gonzalez. „Zynga data breach exposed 200 million Words with Friends players". 1 października 2019 r. C|net.https://www.cnet.com/news/words-with-friends-hack-reportedly-exposes-data-of-more-than-200m-players/

Powiązany



Raport ENISA o krajobrazie zagrożeń
Przegląd roku

Zestawienie trendów w cyberbezpieczeństwie w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Wykaz piętnastu największych zagrożeń

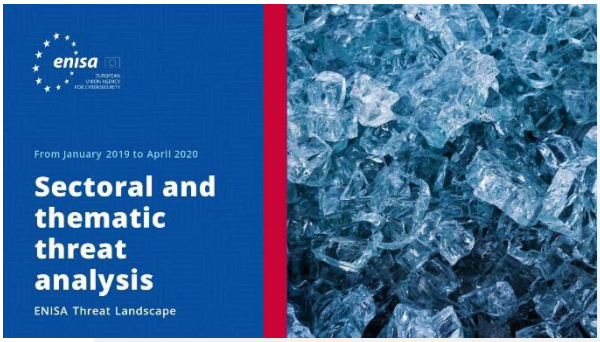
Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Tematyka badań

Zalecenia dotyczące tematów badawczych z różnych kwadrantów w dziedzinie cyberbezpieczeństwa i rozpoznawania zagrożeń cybernetycznych.

PRZECZYTAJ RAPORT



PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Sektorowa i tematyczna analiza zagrożeń

Kontekstualna analiza zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Nowe trendy

Główne trendy w cyberbezpieczeństwie w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Omówienie kwestii rozpoznawania cyberzagrożeń

Aktualny stan wywiadu dotyczącego cyberzagrożeń w UE.

Informacje o agencji

_Agencja

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) jest unijną agencją działającą na rzecz osiągnięcia wysokiego ogólnego poziomu cyberbezpieczeństwa w całej Europie. Utworzona w roku 2004 i wzmocniona przez Akt o cyberbezpieczeństwie Agencja Unii Europejskiej ds. Cyberbezpieczeństwa wnosi wkład w politykę cybernetyczną UE; zwiększa wiarygodność produktów, usług i procesów informacyjno-komunikacyjnych dzięki systemom certyfikacji cyberbezpieczeństwa; współpracuje z państwami członkowskimi i organami UE oraz pomaga przygotować Europę na przyszłe wyzwania cybernetyczne. Poprzez wymianę informacji, budowanie zdolności i pogłębianie wiedzy Agencja współdziała z kluczowymi zainteresowanymi stronami, aby zwiększać zaufanie do gospodarki opartej na łączności i odporność unijnej infrastruktury oraz w efekcie zapewnić cyfrowe bezpieczeństwo społeczeństwa i mieszkańców Europy. Więcej informacji na temat ENISA i jej działalności można znaleźć na stronie www.enisa.europa.eu.

Współautorzy

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) oraz *wszyscy członkowie ENISA CTI Stakeholders Group:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) i Thomas Hemker.

Wydawcy

Marco Barros Lourenço (ENISA) i Louis Marinos (ENISA).

Dane kontaktowe

Zapytania dotyczące tego dokumentu można kierować na adres enisa.threat.information@enisa.europa.eu.

Zapytania prasowe dotyczące tego dokumentu można kierować na adres press@enisa.europa.eu.

Chcielibyśmy poznać opinie czytelników na temat tego raportu!
Poświęć chwilę, by wypełnić kwestionariusz. Aby uzyskać dostęp do formularza, kliknij tutaj.

Zastrzeżenia prawne

Informujemy, że niniejsza publikacja przedstawia poglądy i interpretacje ENISA, o ile nie stwierdzono inaczej. Niniejsza publikacja nie powinna być interpretowana jako działanie prawne ENISA ani organów ENISA, chyba że została przyjęta zgodnie z rozporządzeniem (UE) nr 526/2013. Niniejsza publikacja nie musi przedstawiać aktualnego stanu wiedzy i ENISA może ją okresowo aktualizować.

Źródła zewnętrzne zostały odpowiednio zacytowane. ENISA nie ponosi odpowiedzialności za treść źródeł zewnętrznych, w tym zewnętrznych stron internetowych, do których odniesienia znajdują się w niniejszej publikacji.

Niniejsza publikacja ma charakter wyłącznie informacyjny. Musi ona być dostępna nieodpłatnie. Ani ENISA, ani żadna osoba działająca w jej imieniu nie ponoszą odpowiedzialności za wykorzystanie informacji zawartych w niniejszym sprawozdaniu.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecja
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu