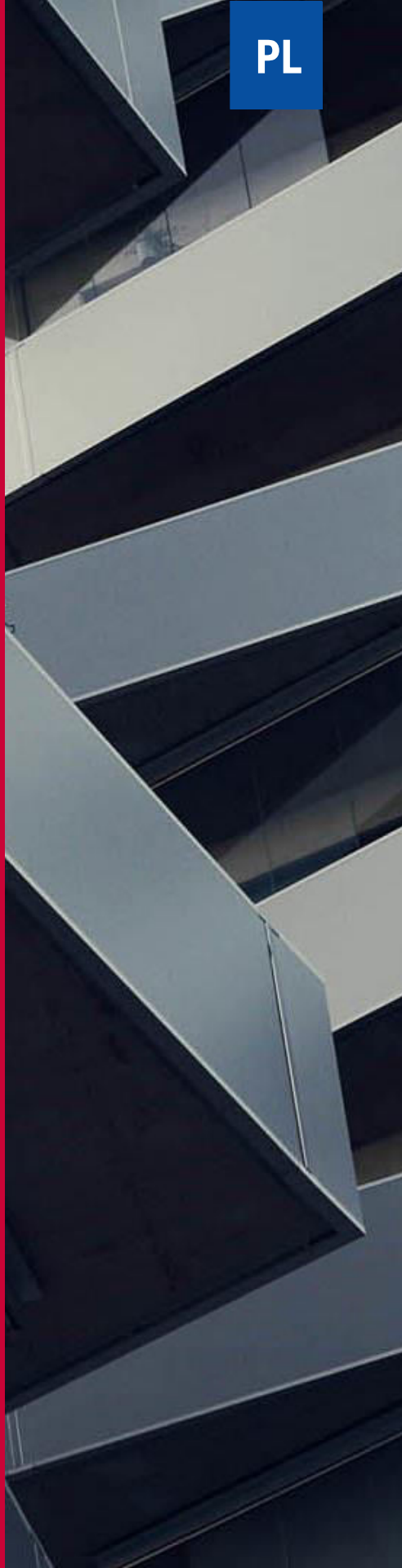
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

PL



Od stycznia 2019 r. do kwietnia 2020 r.

# Naruszenie bezpieczeństwa danych

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

# Informacje ogólne

Naruszenie bezpieczeństwa danych to incydent związany z cyberbezpieczeństwem polegający na uzyskaniu dostępu do danych (lub części systemu informatycznego) bez odpowiedniego upoważnienia i zwykle w przestępczych zamiarach, co mogło potencjalnie doprowadzić do utraty lub niewłaściwego wykorzystania takich danych. Naruszenia takie mogą też wiązać się z „błędami ludzkimi", które często mają miejsce przy okazji konfiguracji i wdrażania niektórych usług i systemów, i mogą skutkować nieumyślnym narażeniem bezpieczeństwa danych[1].

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[2]. Badania wskazują, że wykrycie naruszenia bezpieczeństwa danych w organizacji zajmuje około 206 dni[3]. Powrót do normalności po opanowaniu naruszenia bezpieczeństwa, podjęciu środków zaradczych i odzyskaniu danych trwa więc znacznie dłużej.

Pomimo wiążącego się z tym ryzyka organizacje coraz więcej danych[4] przechowują w chmurze i w złożonych systemach lokalnych. Środowiska te są coraz bardziej narażone na nowe, odmienne zagrożenia – proporcjonalnie do tego, jak wrażliwe są przechowywane dane. Nie jest więc zaskoczeniem, że w latach 2019 i 2020 liczba naruszeń bezpieczeństwa danych wzrosła. Nowe ustalenia wskazują, że skutki odczuwalne są nie tylko w momencie odkrycia naruszenia danych – konsekwencje finansowe mogą trwać ponad dwa lata po pierwotnym incydencie.

# Wnioski

**54%_wzrost łącznej liczby naruszeń bezpieczeństwa w połowie 2019 r. w porównaniu z rokiem 2018.**

**71%_ naruszeń bezpieczeństwa danych miało motywację finansową.** Niemal 25% wiązało się z długofalowymi celami strategicznymi (kwestie państwowe / szpiegostwo)[5].

**32%_naruszeń bezpieczeństwa danych wiąże się z działaniami phishingowymi (IOCTA 2019)[6].** Jak wynika z jednego z raportów, phishing jest jednym z czołowych czynników powodujących naruszenia bezpieczeństwa danych. W raporcie wspomniano również, że podstawową metodą dostarczania złośliwego oprogramowania w łańcuchu zdarzeń prowadzących do naruszenia bezpieczeństwa danych jest poczta e-mail (94%)[3].

**52%_naruszeń bezpieczeństwa danych wiązało się z łamaniem zabezpieczeń[5].** Inne metody obejmowały inżynierię społeczną (33%), złośliwe oprogramowanie (28%) oraz wykorzystywanie pomyłek lub błędów (21%). Od 2016 r. podstawową przyczyną naruszeń bezpieczeństwa danych w opiece zdrowotnej jest łamanie zabezpieczeń. W roku 2019 metoda ta stała za niemal 59% zgłoszonych naruszeń bezpieczeństwa danych[7].

**70%_naruszeń bezpieczeństwa danych dotyczy poczty elektronicznej.** Nazwę/e-mail użytkownika i hasła (tj. dane uwierzytelniające) najłatwiej jest zmienić, w przeciwieństwie do danych osobowych (takich jak data urodzenia), jednak to na poczcie e-mail koncentrują się najczęściej próby naruszenia bezpieczeństwa danych[8].

**55%_respondentów badania Eurobarometr odpowiedziało, że obawia się o to, że przestępcy i oszuści uzyskają dostęp do ich danych.**

# Chronologia

## 2019

### _ Styczeń

Naruszenie bezpieczeństwa danych chmury MEGA w Nowej Zelandii spowodowało ujawnienie 770 milionów wiadomości e-mail i 21 milionów haseł[9]

### _ Luty

620 milionów kont skradzionych z 16 zhakowanych witryn internetowych na sprzedaż w „ciemnej sieci" – chwali się sprzedawca[10].

### _ Marzec

Ujawnienie dokumentacji medycznej 12,5 mln kobiet w ciąży, sięgającej wstecz aż do 2014 r., znajdującej się w państwowym ośrodku opieki zdrowotnej w Indiach[11].

### _ Październik

Narażenie danych kont ponad 7,5 mln użytkowników Adobe (USA) wskutek niezabezpieczenia bazy danych online[18].

### _ Wrzesień

Firma Mastercard w Belgii doznała naruszenia bezpieczeństwa danych, które dotknęło ok. 90 tys. klientów w Europie[17]

### _ Sierpień

Poważne naruszenie bezpieczeństwa wykryte w systemach biometrycznych wykorzystywanych przez banki, policję (UK) oraz firmy odpowiadające za obronę[16].

### _ Listopad

Włoski UniCredit stał się ofiarą wycieku danych – ujawnieniu uległy 3 miliony rekordów[19].

### _ Grudzień

Dostawca inteligentnych kamer Wyze (USA) pada ofiarą dwóch naruszeń bezpieczeństwa pod koniec grudnia, kiedy to bazy danych pozostawały narażone przez ponad dwa tygodnie[20].

## 2020

### _ Styczeń

Naruszenie bezpieczeństwa 250 milionów rekordów dotyczących obsługi i wsparcia klienta z firmy Microsoft (USA), sięgających wstecz aż do 2005 roku[21].

## _ Kwiecień

Facebook (USA) zgłasza naruszenie bezpieczeństwa danych dotyczące 540 mln rekordów użytkowników na narażonych serwerach[12].

## _ Maj

Wyciek setek milionów rekordów ubezpieczeń kredytów hipotecznych First American Financial Corp. (USA)[13].

## _ Lipiec

Naruszenie bezpieczeństwa danych osobowych użytkowników kart kredytowych Capital One (USA)[15].

## _ Czerwiec

100 milionów rekordów narażonych wskutek nieupoważnionego dostępu do magazynowanych danych klientów firmy Evite[14].

## _ Luty

Niechroniony serwer chmurowy firmy Google (USA) zawierający dane osobowe 200 milionów mieszkańców Stanów Zjednoczonych[22].

## _ Marzec

Wyciek danych z firmy Antheus Tecnologia (BR) zajmującej się rozwiązaniami biometrycznymi[23].

## _ Kwiecień

W styczniu 2020 r. hakerzy uzyskali dane logowania dwóch pracowników firmy Marriott (USA) i włamali się do systemu[24].

# Trendy

## _Za naruszenia bezpieczeństwa danych organizacje płacą przez wiele lat

Jak stwierdzają analitycy bezpieczeństwa, jedna trzecia kosztów związanych z naruszeniem bezpieczeństwa danych ponoszona jest ponad rok po incydencie. W ujęciu szczegółowym: około 22% tych kosztów przypada na drugi rok, a 11% księguje się przez ponad dwa lata po pierwotnym incydencie. W przypadku organizacji podlegających ścisłym regulacjom, takich jak organizacje związane z usługami finansowymi i opieką zdrowotną, odsetek ten był jeszcze wyższy niż w innych branżach[3].
Rozwiązania chmurowe lub wielochmurowe są stosowane coraz częściej i gwałtownie wzrasta też ilość danych przechowywanych i przetwarzanych w tych środowiskach.

## _Drobne pomyłki mogą prowadzić do dużych problemów

Zabezpieczenie środowiska chmurowego tak, by nie utracić elastyczności, jaką wnosi ono do infrastruktury i zasobów, może być niełatwe. Jeden błąd w konfiguracji może doprowadzić do narażenia całej bazy zawierającej dane wrażliwe. Jak twierdzi analityk, większość naruszeń bezpieczeństwa danych w chmurze jest wynikiem błędów w konfiguracji, na ogół nieumyślnych. Incydenty w firmach Netflix, Ford i TD Bank to tylko kilka przykładów spośród wielu. Jeśli spojrzeć na to z innej perspektywy – wprawdzie naruszenia bezpieczeństwa danych spowodowane atakami o charakterze przestępczym kosztują więcej, ale błędy w systemach i błędy ludzkie również generują znaczne koszty – średnio 3,24 mln USD (ok. 2,74 mln EUR)[3].

## Małe firmy ponoszą większe koszty naruszeń bezpieczeństwa danych

Koszt naruszeń bezpieczeństwa danych w przypadku dużego przedsiębiorstwa lub organizacji zatrudniającej ponad 25 000 pracowników to 204 USD (ok. 173 EUR) na pracownika. Łącznie stanowi to około 5,11 mln USD (ok. 4,33 mln EUR). Z kolei w małych firmach (500–1000 pracowników) średni koszt to 3533 USD (ok. 3000 EUR) na pracownika. Łącznie zatem dla małych przedsiębiorstw stanowi to 2,65 mln USD (ok. 2,24 mln EUR)[3].

## Podstawowa motywacja to zysk finansowy

Za naruszenia bezpieczeństwa danych, jak wiadomo, odpowiadają sprawcy szkodliwych działań / zagrożeń (należy jednak pamiętać, że w niektórych przypadkach naruszenia te mogą być efektem pomyłek). W tym sensie głównymi sprawcami naruszeń bezpieczeństwa danych są podmioty zewnętrzne – może to obejmować na przykład botnety. Główną motywacją naruszeń bezpieczeństwa danych dokonywanych przez te grupy sprawców jest zysk finansowy. Szpiegostwo również okazało się istotną motywacją naruszeń bezpieczeństwa danych, ale nie znalazło się tak wysoko na liście, jak korzyści osobiste czy finansowe. Mamy tu do czynienia z niemal takimi samymi trendami, jak w latach 2010–2011[5].

# Trendy

## Komputery kwantowe a bezpieczeństwo danych

W erze komputerów kwantowych zasadniczą rolę pełnią wymagania kryptograficzne – i pojawiają się krytyczne problemy z bezpieczeństwem. 72% organizacji uważa, że wprowadzenie komputerów kwantowych będzie mieć strategiczny wpływ na ich działalność związaną z szyfrowaniem (w ciągu najbliższych pięciu lat). Jak wskazują wyniki badania, 92% respondentów obawia się o narażenie danych wrażliwych wskutek wykorzystywania tej technologii w branży informatycznej. Główne sugerowane strategie w zakresie radzenia sobie z tymi problemami obejmowały zmianę architektury zabezpieczeń i wdrożenie kluczowej infrastruktury zarządzania[26].

## Opieka zdrowotna – stały przedmiot zainteresowania sprawców szkodliwych działań

Opieka zdrowotna pozostaje jednym z najatrakcyjniejszych celów dla cyberprzestępców wykorzystujących oprogramowanie typu ransomware oraz techniki phishingu, co kosztuje te organizacje miliony euro konieczne do ograniczenia nasilenia ataku i opanowania jego skutków. W 2019 r. naruszenia bezpieczeństwa danych w dokumentacji pacjentów zgłosiło 400 firm związanych z opieką zdrowotną. Dla organizacji ochrony zdrowia był to rekord[7].

## Rozwiązania wielochmurowe – nowe wyzwanie dla bezpieczeństwa danych

Jak wykazało badanie przeprowadzone przez analityka bezpieczeństwa, 9 na 10 firm rozważa wykorzystanie środowiska chmurowego lub już je wykorzystuje. Około 44% respondentów uważa również, że środowiska te stanowią wyzwanie w zakresie wdrażania odpowiednich środków bezpieczeństwa danych[25].

# Typy narażonych danych (%)

| Typ danych | 2019 | 2018 | 2017 |
|---|---|---|---|
| E-mail | 70 | 44 | 32 |
| Hasło | 64 | 39 | 27 |
| Imię i nazwisko / Nazwa | 23 | 37 | 41 |
| Różne | 18 | 19 | 15 |
| Numer ubezpieczenia społecznego | 11 | 22 | 27 |
| Karta kredytowa | 11 | 16 | 19 |
| Adres | 11 | 22 | 30 |
| Konto | 10 | 7 | 4 |
| Nieznany | 8 | 13 | 18 |
| Data urodzenia | 8 | 13 | 12 |
| Dane medyczne | 5 | 9 | 7 |
| Dane finansowe | 5 | 13 | 19 |

Tabela 1 – źródło: Cyber Risk Analytics[8]

# Trendy

## _Coraz mniej zdarzeń związanych z okazywaniem karty

Jak wynika z raportu dotyczącego bezpieczeństwa, w 2019 r. spadła liczba zgłoszonych naruszeń w punktach sprzedaży oraz związanych ze skopiowaniem danych karty, tzw. skimmingiem (tam, gdzie fizycznie okazuje się kartę). Odzwierciedla to zmianę ukierunkowania działalności przestępczej z tradycyjnego kopiowania danych karty w bankomatach oraz naruszeń przy płatnościach kartami na aplikacje internetowe w handlu detalicznym.Mimo że w tym obszarze liczba incydentów spadła, nie można z tego wyciągać wniosku, że naruszeń bezpieczeństwa danych jest teraz mniej – oznacza to raczej zmianę wektorów. Spadek ten może jednak być związany z upowszechnieniem się kart/terminali odczytujących chipy i wymagających kodu PIN (zwanych EMV)[6].

## _Czego można się spodziewać w najbliższej przyszłości?

Jak twierdzi analityk bezpieczeństwa, organizacje ochrony zdrowia powinny przygotować się na 10 – 15% wzrost liczby naruszeń bezpieczeństwa danych, których głównym celem będą ich usługodawcy[7].
W ogólności na podstawie wyników z pierwszego półrocza 2019 r. można oczekiwać, że liczba naruszeń bezpieczeństwa danych będzie wzrastać w alarmującym tempie pomimo świadomości niebezpieczeństwa wśród kierownictwa wyższego szczebla i wysiłków, jakie wiele organizacji wkłada w zabezpieczenie danych[8].

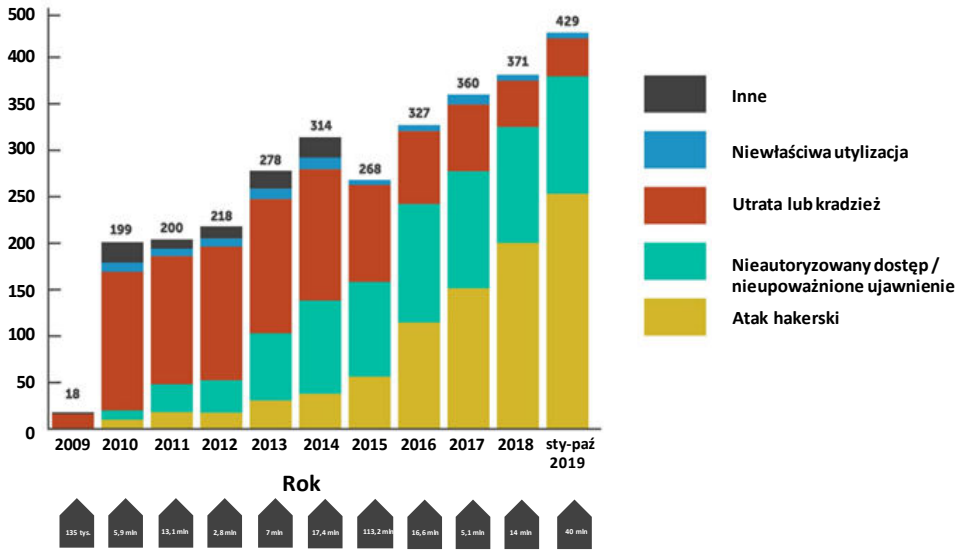
## Naruszenia bezpieczeństwa danych w zależności od branży i rozmiaru organizacji

| Incydenty | Naruszenia | Małe | Duże | Nieznane |
|---|---|---|---|---|
| Usługi noclegowe | 61 | 34 | 7 | 20 |
| Administracja | 17 | 6 | 6 | 5 |
| Rolnictwo | 2 | 2 | 0 | 0 |
| Budownictwo | 11 | 7 | 3 | 1 |
| Edukacja | 99 | 14 | 8 | 77 |
| Rozrywka | 10 | 2 | 3 | 5 |
| Finanse | 207 | 26 | 19 | 162 |
| Opieka zdrowotna | 304 | 29 | 25 | 250 |
| Przetwarzanie informacji | 155 | 20 | 18 | 117 |
| Zarządzanie | 2 | 1 | 1 | 0 |
| Produkcja | 87 | 10 | 22 | 55 |
| Górnictwo | 15 | 2 | 5 | 8 |
| Inne usługi | 54 | 6 | 5 | 43 |
| Usługi specjalistyczne | 157 | 34 | 10 | 113 |
| **Usługi publiczne** | **330** | **17** | **83** | **230** |
| Nieruchomości | 14 | 6 | 3 | 5 |
| Handel detaliczny | 139 | 46 | 19 | 74 |
| Handel | 16 | 4 | 8 | 4 |
| Transport | 36 | 3 | 9 | 24 |
| Usługi komunalne | 8 | 2 | 0 | 6 |
| Nieznane | 289 | 0 | 109 | 180 |
| Ogółem | 2013 | 271 | 363 | 1379 |

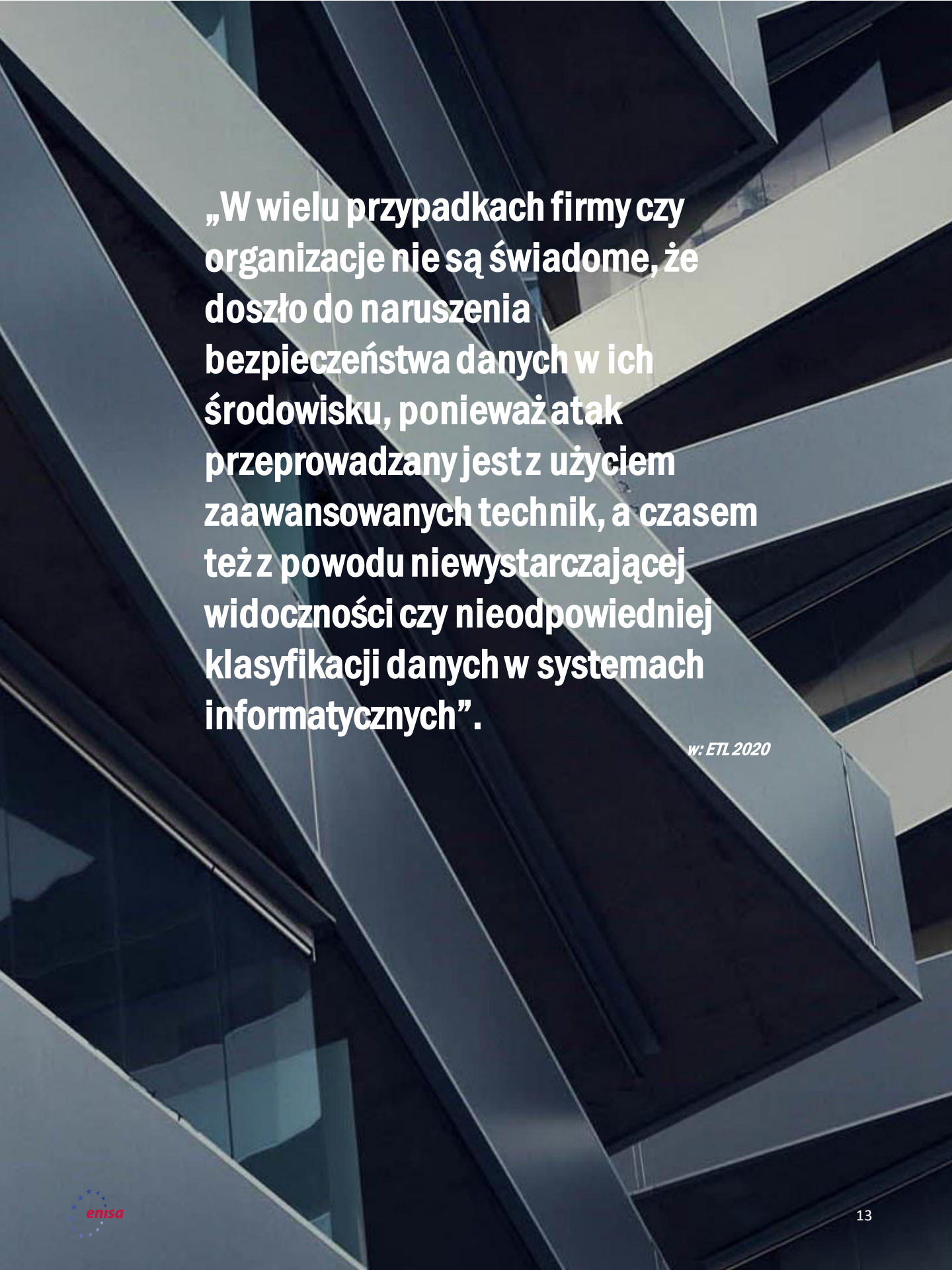
Tabela 2 – źródło: Verizon DBIR, 2019[5]

# Wektory ataku

- **E-MAIL/PHISHING.** Podszywanie się pod dostawcę zewnętrznego lub partnera przy pomocy e-maila to dla sprawców szkodliwych działań łatwe rozwiązanie przynoszące szybkie korzyści. Ten wektor jest najczęściej używany przez cyberprzestępców do atakowania ofiar i jest wykorzystywany przy większości naruszeń bezpieczeństwa danych (w opiece zdrowotnej to ponad 40% przypadków)[7].
- **APLIKACJE CHMUROWE/INTERNETOWE.** Odzwierciedla to wykorzystywanie aplikacji internetowych jako wektora dla prób ataku dokonywanych przez sprawców szkodliwych działań w celu naruszenia bezpieczeństwa danych lub zakłócenia kluczowej działalności. Głównym przykładem jest kradzież danych uwierzytelniających w celu uzyskania dostępu do serwisów e-mailowych dostępnych przez przeglądarkę. Innymi przykładami wykorzystywania podatności w serwerach aplikacji jest iniekcja/dostarczanie złośliwego oprogramowania kradnącego dane lub ataki techniką przechwytywania danych z formularzy, tzw. formjacking.
- **ZAGROŻENIE WEWNĘTRZNE.** Obejmuje to przede wszystkim nieupoważnione lub mające przestępcze intencje próby wykorzystania zasobów. Należy zauważyć, że w analizach i raportach błędy w konfiguracji i pomyłki (błędy ludzkie) popełniane przez wewnętrzne zespoły również bywają określane jako „zagrożenie ze strony wtajemniczonych". Większość naruszeń bezpieczeństwa danych spowodowanych jest przez sprawców z zewnątrz, jednak kluczową rolę w nich pełnią osoby z wewnątrz, również takie, które mają uprzywilejowany dostęp do danych[5].




Rysunek 1: Podmioty dotknięte naruszeniem bezpieczeństwa danych. Źródło: Horizon[7]



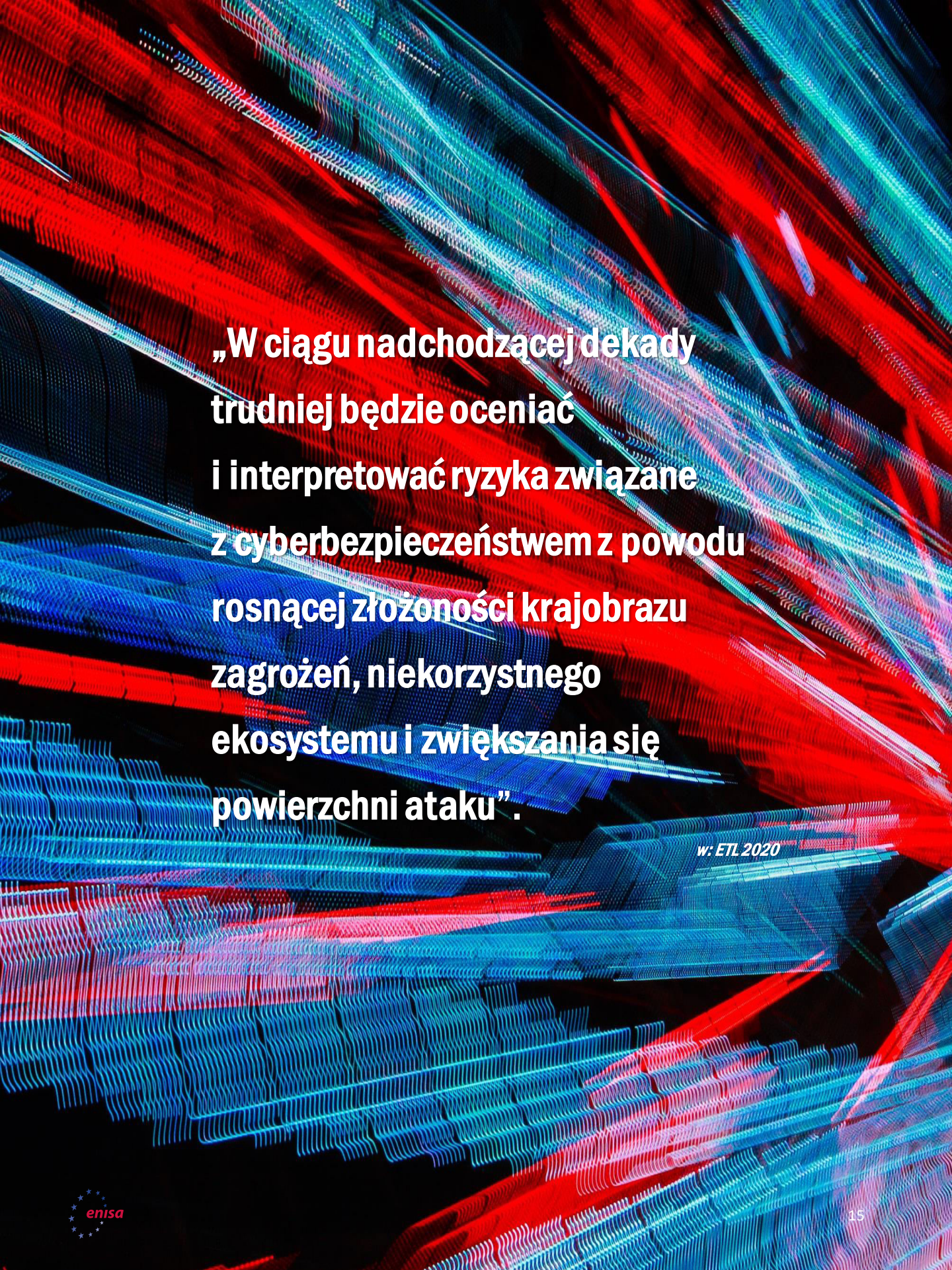
„W wielu przypadkach firmy czy organizacje nie są świadome, że doszło do naruszenia bezpieczeństwa danych w ich środowisku, ponieważ atak przeprowadzany jest z użyciem zaawansowanych technik, a czasem też z powodu niewystarczającej widoczności czy nieodpowiedniej klasyfikacji danych w systemach informatycznych”.

*w: ETL 2020*

# Ograniczenie ryzyka

## Proponowane działania

- Naruszenie bezpieczeństwa danych jest zazwyczaj skutkiem innych zagrożeń i środki zaradcze pokrywają się częściowo z innymi omawianymi w niniejszym raporcie.
- Rozważenie inwestycji w hybrydowe narzędzia do zabezpieczenia danych, które ukierunkowane są na działanie w modelu współdzielonej odpowiedzialności w środowisku chmurowym[26].
- Opracowanie i aktualizacja planu świadomości cyberbezpieczeństwa. Opracowanie szkoleń i scenariuszy symulacji mających na celu nauczenie personelu identyfikacji prób inżynierii społecznej i akcji phishingowych[7].
- Utworzenie i utrzymywanie zespołu reagowania na incydenty oraz częste ocenianie planów reagowania[3].
- Identyfikacja i klasyfikacja danych wrażliwych/osobowych i zastosowanie środków pozwalających na szyfrowanie takich danych w trakcie ich przekazywania i magazynowania[3]. Innymi słowy – wdrożenie ochrony przed utratą danych.
- Zwiększenie inwestycji w narzędzia pozwalające na wykrywanie naruszeń i alarmowanie o nich oraz na opanowanie skutków naruszenia i odpowiednie reagowanie.
- Opracowanie i utrzymywanie ścisłych zasad wymuszania mocnych haseł (zarządzanie hasłami) oraz wykorzystywania uwierzytelniania wieloskładnikowego.
- W celu zapewnienia bezpieczeństwa zasobów znajdujących się zarówno w obiektach firmy, jak i poza nimi, należy rozważyć modele obejmujące podejście „najmniejszych uprawnień” (tj. modele zerowego zaufania).
- Stworzenie zasad i planów współpracy z zespołami kierowniczymi, ds. zarządzania ryzykiem oraz ds. zgodności z przepisami[26].


„W ciągu nadchodzącej dekady
trudniej będzie oceniać
i interpretować ryzyka związane
z cyberbezpieczeństwem z powodu
rosnącej złożoności krajobrazu
zagrożeń, niekorzystnego
ekosystemu i zwiększania się
powierzchni ataku”.
w: ETL 2020

# Bibliografia


1. „What is data breach?" Norton. https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html

2. „What is data breach?" Malwarebytes. https://www.malwarebytes.com/data-breach/

3. „Cost of Data Breach Report". 2019. IBM Security, Ponemon Institute. https://www.ibm.com/security/data-breach

4. Dhritimaan Shukla, Kush Wadhwa. „Data breach – threat landscape. Unauthorised exposure of an organisation's critical data". PWC India. https://www.pwc.in/consulting/forensic-services/data-breach-threat-landscape.html

5. „Verizon Data Breach Investigations Report". 2020. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

6. Catherine De Bolle. „Internet Organised Crime Threat Assessment (IOCTA)". 2019. European Cyber Crime Centre (EC3), Europol. https://www.europol.europa.eu/iocta-report

7. „2020 Healthcare Cybersecurity Horizon Report". 2020. Fortified Health Security. https://fortifiedhealthsecurity.com/wp-content/uploads/2019/12/Fortified-Health-Security-2020-Horizon-Report.pdf

8. Inga Goddijn. „2019 Midyear QuickView Data Breach Report – Cyber Risk Analytics". Sierpień 2019 r. https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20MidYear%20Data%20Breach%20QuickView%20Report.pdf

9. Troy Hunt. „The 773 Million Record "Collection #1" Data Breach". 17 stycznia 2019 r. Troy. https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

10. Chris Williams. „620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts". 11 lutego 2019 r. The Register. https://www.theregister.com/2019/02/11/620_million_hacked_accounts_dark_web/

11. 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/

12. „Losing Face: Two More Cases of Third-Party Facebook App Data Exposure". 3 kwietnia 2019 r. UpGuard. https://www.upguard.com/breaches/facebook-user-data-leak

13. „First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records". 24 maja 2019 r. KrebsonSecurity. https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

14. „Data Incident, Evite". 14 maja 2019 r. Evite. https://www.evite.com/security/update

15. „Information on the Capital One Cyber Incident". 23 września 2019 r. CapitalOne. https://www.capitalone.com/facts2019/

16. 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

17. Neil Hodge. „Mastercard reveals data breaches in third-party loyalty program". 27 sierpnia 2019 r. Compliance Week. https://www.complianceweek.com/data-privacy/mastercard-reveals-data-breaches-in-third-party-loyalty-program/27614.article

18. Catalin Cimpanu. „Adobe left 7.5 million Creative Cloud user records exposed online". 26 października 2019 r. ZDNet. https://www.zdnet.com/article/adobe-left-7-5-million-creative-cloud-user-records-exposed-online/

**19.** Charlie Osborne. „UniCredit reveals data breach exposing 3 million customer records". 28 października 2019 r. ZDNet. https://www.zdnet.com/article/unicredit-reveals-data-breach-exposing-3-million-customer-records/

**20.** Chris Isidore. „Smart camera maker Wyze hit with customer data breach". 30 grudnia 2019 r. CNN. https://edition.cnn.com/2019/12/30/tech/wyze-data-breach/index.html

**21.** Davey Winder. „Microsoft Security Shocker As 250 Million Customer Records Exposed Online". 22 stycznia 2020 r. Forbes. https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/#2d3f9dca4d1b

**22.** Paul Bischoff. „US property and demographic database of 200 million records leaked on the web". 5 marca 2020 r. comparitech. https://www.comparitech.com/blog/vpn-privacy/200-million-us-database-leaked/

**23.** Jim Wilson. „Brazil: Millions of Records Leaked, Including Biometric Data". 11 marca 2020 r. Safety Detectives. https://www.safetydetectives.com/blog/antheus-leak-report/

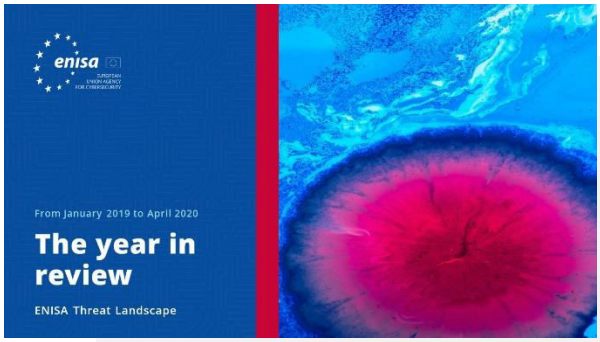
**24.** Zack Whittaker. „Marriot says 5.2 million guest records were stolen in another data breach". 1 kwietnia 2020 r. Techcrunch. https://techcrunch.com/2020/03/31/marriott-hotels-breached-again/?renderMode=ie11

**25.** „2019 Thales Data Threat Report – Global Edition" Thales Security, 2019. https://cpl.thalesgroup.com/data-threat-report

**26.** „2020 Thales Data Threat Report – Global Edition" Thales Security, 2020. https://cpl.thalesgroup.com/data-threat-report

**27.** Laura Paine. „2019 Verizon DBIR Shows Web Applications and Human Error as Top Sources of Breach". 8 maja 2019 r. Veracode. https://www.veracode.com/blog/security-news/2019-verizon-dbir-shows-web-applications-and-human-error-top-sources-breach

# 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**

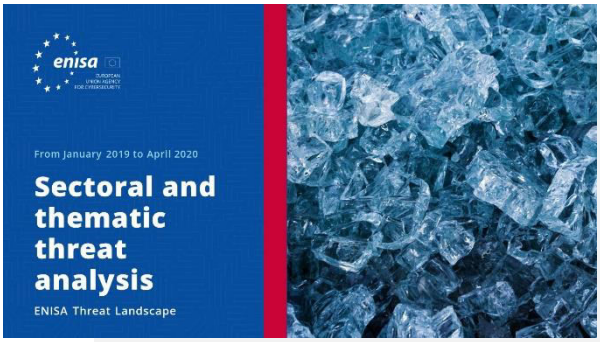
Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

**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**




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.

**PRZECZYTAJ RAPORT**

# 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 odpornością 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.

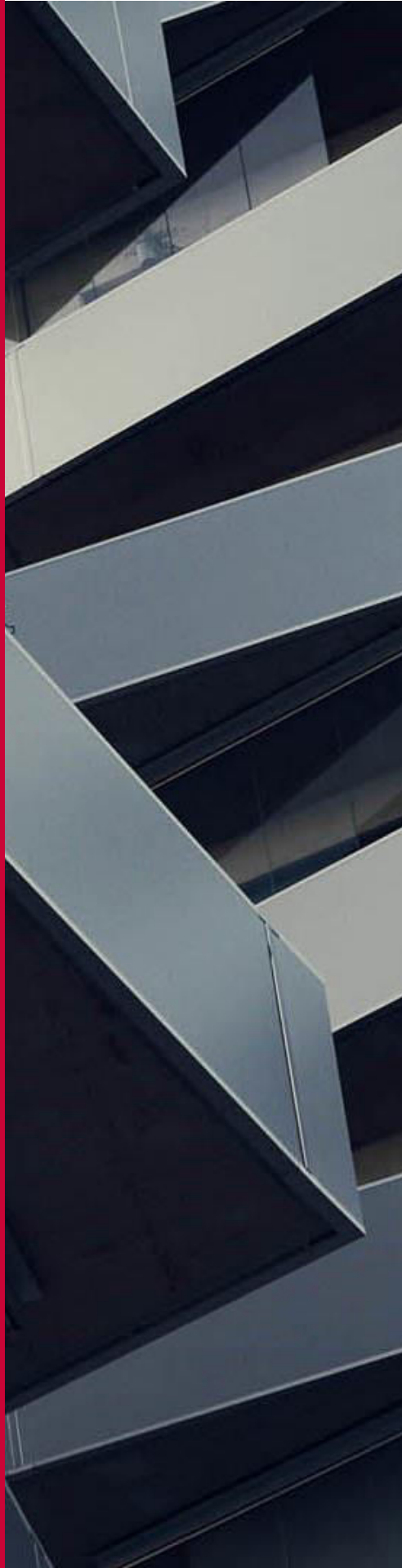
Źródła zewnętrzne zostały odpowiednio zacytowane. ENISA nie ponosi odpowiedzialności za treść źródeł zewnętrznych, w tym zewnętrznych stron internetowych, do których odniesienia znajdują się w niniejszej publikacji.

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