dr inż. Marta Chodyka
Akademia Bialska im. Jana Pawła II
ORCID: 0000-0002-8819-2451
https://doi.org/10.29316/9788368103199_10

BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH A FUNKCJONOWANIE PRZEDSIĘBIORSTW W POLSCE

CYBERSECURITY OF INFORMATION SYSTEMS AND ITS IMPACT ON BUSINESS OPERATIONS IN POLAND

Streszczenie

W dobie intensywnej cyfryzacji bezpieczeństwo systemów informatycznych stanowi fundament sprawnego funkcjonowania współczesnych przedsiębiorstw. Rozdział podejmuje problematykę wpływu poziomu cyberbezpieczeństwa na działalność firm w Polsce, koncentrując się na analizie danych za rok 2024. Celem badania było określenie, w jakim stopniu inwestycje w bezpieczeństwo IT przekładają się na ciągłość działania, wyniki ekonomiczne i odporność organizacyjną. Zastosowano metodę mieszaną – analizę danych wtórnych (raporty CERT Polska, GUS, KPMG) oraz studia przypadków rzeczywistych incydentów (ransomware, wycieki danych, ataki łańcuchowe). Pytanie badawcze dotyczyło zależności między poziomem zabezpieczeń a zakłóceniami działalności operacyjnej.

Summary

In the era of widespread digitalization, information systems security has become a cornerstone of effective business operations. This chapter addresses the impact of cybersecurity maturity on the functioning of enterprises in Poland, focusing on data from 2024. The objective of the study was to assess how investments in IT security influence operational continuity, financial performance, and organizational resilience. A mixed-method approach was applied, combining secondary data analysis (reports from CERT Polska, GUS, KPMG) with case studies of real incidents (ransomware, data breaches, supply-chain attacks). The research question explored the relationship between cybersecurity readiness and operational disruptions. Findings indicate that

Wyniki wskazują, że rosnąca liczba incydentów oraz ich złożoność stanowią realne zagrożenie, szczególnie dla sektorów finansowego i handlu. Rozdział potwierdza, że systemowe podejście do cyberbezpieczeństwa stanowi kluczowy element strategii zarządzania ryzykiem i warunek stabilności przedsiębiorstw.

Słowa kluczowe: analiza ryzyka, ataki hakerskie, cyberbezpieczeństwo, ochrona danych, systemy informatyczne

the increasing frequency and complexity of incidents pose a tangible threat, especially to the financial and retail sectors. The chapter confirms that a systemic approach to cybersecurity is a critical component of risk management strategies and a prerequisite for business stability.

Keywords: cyberattacks, cybersecurity, data protection, information systems, risk analysis

Wstęp

W dobie intensywnej cyfryzacji procesów biznesowych oraz dynamicznie rozwijających się technologii informacyjnych zagadnienie bezpieczeństwa systemów informatycznych nabiera kluczowego znaczenia dla funkcjonowania współczesnych przedsiębiorstw. Wraz z rosnącą liczbą zagrożeń cybernetycznych oraz ich złożonością, kwestia zapewnienia wysokiego poziomu cyberbezpieczeństwa staje się integralnym elementem strategii zarządzania ryzykiem operacyjnym oraz warunkiem koniecznym stabilności biznesowej.

Niniejsza praca podejmuje problem wpływu poziomu zabezpieczeń systemów informatycznych na działalność przedsiębiorstw działających na terenie Polski. Przedmiotem badania jest analiza zależności pomiędzy dojrzałością organizacyjną w zakresie cyberbezpieczeństwa a zdolnością przedsiębiorstw do zapewnienia ciągłości działania, osiągania założonych wyników ekonomicznych oraz realizacji strategii rozwoju w obliczu realnych zagrożeń. Zdefiniowano następujące pytanie badawcze: W jakim stopniu poziom cyberbezpieczeństwa determinuje stabilność operacyjną i odporność organizacyjną polskich przedsiębiorstw na cyberzagrożenia? Hipotezą badawczą pracy jest założenie, że wysoki poziom zabezpieczeń informatycznych bezpośrednio przekłada się na stabilność operacyjną oraz ogranicza negatywne skutki incydentów cybernetycznych, podczas gdy niedostateczne zabezpieczenia skutkują poważnymi zakłóceniami operacyjnymi i stratami finansowymi oraz wizerunkowymi. W realizacji celów badawczych wykorzystano metodę mieszaną, obejmującą zarówno analizę danych wtórnych, jak i studia przypadków. Na etapie wstępnym przeprowadzono przegląd literatury przedmiotu, standardów międzynarodowych (głównie norm serii ISO/IEC 27000) oraz dobrych praktyk z zakresu cyberbezpieczeństwa, co umożliwiło sformułowanie podstawowych

definicji oraz ram teoretycznych pracy. Kolejnym etapem było przeprowadzenie analizy danych ilościowych pochodzących z raportów takich instytucji, jak Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający w Polsce, Główny Urząd Statystyczny oraz międzynarodowa firma doradcza KPMG, które opisują aktualny stan bezpieczeństwa informatycznego w polskich przedsiębiorstwach w roku 2024. Ostatnim elementem analizy było przygotowanie szczegółowych studiów przypadków, które ilustrują realne scenariusze incydentów bezpieczeństwa w Polsce. Wybrano trzy reprezentatywne przykłady różniące się charakterem zagrożeń (atak *ransomware*, wyciek danych osobowych oraz atak typu *supply-chain*), aby możliwie kompleksowo przedstawić spektrum konsekwencji operacyjnych, finansowych, prawnych oraz reputacyjnych.

Wyniki przeprowadzonych badań wskazują na istotne znaczenie systemowego podejścia do bezpieczeństwa informatycznego. Udowodniono, że organizacje dysponujące dobrze rozwiniętą infrastrukturą zabezpieczeń oraz procedurami ciągłości działania potrafią znacznie szybciej identyfikować zagrożenia, skutecznie je neutralizować oraz minimalizować skutki incydentów. Natomiast przedsiębiorstwa, które zaniedbały ten aspekt działalności, doświadczają poważnych, często długofalowych konsekwencji operacyjnych, finansowych i reputacyjnych. Praca potwierdza więc, że proaktywne inwestowanie w cyberbezpieczeństwo nie powinno być postrzegane jako opcjonalny koszt, lecz strategiczna inwestycja zapewniająca długoterminową stabilność biznesową.

Cyberbezpieczeństwo w zarządzaniu organizacjami – standardy, zagrożenia i dobre praktyki

Bezpieczeństwo systemów informatycznych (ang. *Information Systems Security*), często określane także jako cyberbezpieczeństwo, oznacza ochronę zasobów informacyjnych oraz teleinformatycznych organizacji przed zagrożeniami mogącymi naruszyć ich poufność, integralność oraz dostępność, co opisuje tzw. model CIA (ang. *Confidentiality, Integrity, Availability*)[1]. Klasyczne podejście oparte na tych trzech filarach często bywa rozszerzane o dodatkowe komponenty, takie jak identyfikacja i uwierzytelnianie użytkowników, kontrola dostępu, zapewnienie niezaprzeczalności działań oraz ochrona integralności

[1] J. Andress, Foundations of Information Securit, 2019.

i poufności transmisji danych[2]. Kompleksowe podejście do bezpieczeństwa obejmuje zarówno rozwiązania techniczne (np. szyfrowanie, zapory sieciowe, systemy wykrywania włamań, kopie zapasowe), jak i procedury organizacyjne (polityki bezpieczeństwa, szkolenia pracowników, zarządzanie ryzykiem). Celem jest stworzenie środowiska, w którym zasoby informacyjne są skutecznie chronione przed całym spektrum zagrożeń – od przypadkowych awarii po celowe ataki *hakerskie*.

W dobie powszechnej cyfryzacji działalności gospodarczej przedsiębiorstwa coraz bardziej uzależniają swoją efektywność operacyjną od niezawodnego działania systemów informatycznych. Transformacja cyfrowa przynosi wymierne korzyści biznesowe, ale jednocześnie zwiększa liczbę wektorów ataków wykorzystywanych przez cyberprzestępców. Zagrożenia cybernetyczne stanowią istotne wyzwanie dla organizacji ze wszystkich sektorów gospodarki – od finansowego, poprzez handel i przemysł, aż po infrastrukturę krytyczną. Incydenty takie jak, ataki typu *ransomware*, które paraliżują operacje, naruszenia danych osobowych skutkujące sankcjami regulacyjnymi, czy włamania do wewnętrznych sieci przedsiębiorstw, mogą powodować zakłócenia ciągłości działania, utratę zaufania interesariuszy oraz znaczne straty finansowe. W kontekście dynamicznie rosnącej liczby incydentów, odporność systemów informatycznych staje się nieodzownym elementem zarządzania ryzykiem operacyjnym. Elementy te wspólnie składają się na kompleksowe podejście do bezpieczeństwa systemów. Kompleksowe ujęcie bezpieczeństwa wymaga zatem zarówno rozwiązań technicznych (np. szyfrowanie, zapory sieciowe, systemy wykrywania włamań, kopie zapasowe), jak i procedur organizacyjnych (polityki bezpieczeństwa, szkolenia pracowników, zarządzanie ryzykiem). Celem jest stworzenie środowiska, w którym zasoby informacyjne przedsiębiorstwa są odpowiednio chronione przed całym spektrum zagrożeń – od przypadkowych awarii po celowe ataki hakerskie. Ważnym punktem odniesienia są tu międzynarodowe standardy, przede wszystkim ISO/IEC 27001[3] definiująca wymagania dla systemów zarządzania bezpieczeństwem informacji

[2] L. Chacko, P. Rajan, V. Anilkumar, V. Pathari, V., *Proof-of-Variable-Authority: A Blockchain Consensus Mechanism for Securing IoT Networks*, red. V. Muthukkumarasamy, S.D. Sudarsan, R.K. Shyamasundar, *Information Systems Security*, ICISS 2023, Lecture Notes in Computer Science, vol 14424. Springer, Cham, 2023.

[3] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, International Organization for Standardization, Geneva, 2022.

ISMS (ang. *Information Security Management System*). Zgodnie z normą ISO 27001 bezpieczeństwo informacji to zachowanie poufności, integralności i dostępności informacji, a także – w razie potrzeby – ich autentyczności, rozliczalności, niezawodności i przejrzystości. Standard ten, wraz z uzupełniającą normą ISO/IEC 27002[4] (zalecenia dot. zabezpieczeń) oraz powiązanymi normami (dotyczącymi ciągłości działania – ISO 22301[5], zarządzania ryzykiem – ISO 27005[6], bezpieczeństwa usług w chmurze – ISO 27017[7] i inne.), stanowi uznany zbiór dobrych praktyk. Coraz więcej polskich firm wdraża i certyfikuje systemy zarządzania bezpieczeństwem wg ISO 27001, choć nadal świadomość i dojrzałość w tym zakresie są zróżnicowane. Zgodność z międzynarodowymi standardami, takimi jak ISO/IEC 27001, ISO/IEC 27002, NIST *Cybersecurity Framework* czy powiązane normy sektorowe, pozwala organizacjom nie tylko ustrukturyzować działania ochronne, lecz także wykazać zgodność z obowiązującymi regulacjami prawnymi i branżowymi. W literaturze przedmiotu podkreśla się, że inwestycje w bezpieczeństwo informacji powinny być traktowane analogicznie do wydatków na ubezpieczenie – mogą wydawać się kosztowne, dopóki nie wystąpi incydent[8]. Ekonomiczne podejście do bezpieczeństwa informacji znajduje odzwierciedlenie w modelach optymalizacyjnych, które wskazują, że racjonalne jest inwestowanie w zabezpieczenia do poziomu, w którym marginalne ryzyko strat zrówna się z marginalnym kosztem ochrony. Oprócz teoretycznych ujęć, istotne są także dane empiryczne, m.in. coroczne raporty instytutów badawczych, które analizują finansowe skutki incydentów naruszenia danych. Zgodnie z raportem IBM *Security, Ponemon Institute*[9], średni globalny koszt pojedynczego incydentu naruszenia danych osiągnął rekordowy poziom 4,45 mln USD, co stanowi wzrost o 2,3% w porównaniu z rokiem poprzednim oraz o 15,3% od 2020 roku. Wskaźniki efektywności

[4] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*, International Organization for Standardization, Geneva, 2022.

[5] ISO 22301:2019, *Security and resilience — Business continuity management systems — Requirements*, International Organization for Standardization, Geneva, 2019.

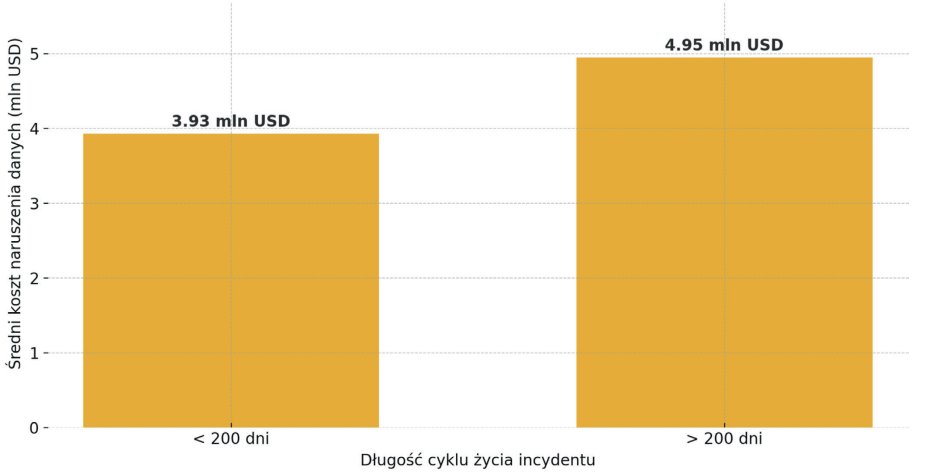
[6] ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*, International Organization for Standardization, Geneva, 2022.

[7] ISO/IEC 27017:2015, *Code of practice for information security controls based on ISO/IEC 27002 for cloud services*, International Organization for Standardization, Geneva, 2015.

[8] L.A. Gordon, M.P. Loeb, M.P., *Managing Cybersecurity Resources: A Cost-Benefit Analysis*, McGraw-Hill, 2006.

[9] IBM Security, Ponemon Institute, *Cost of a Data Breach Report,* 2023.

wykrywania pozostają niepokojące: organizacje potrzebują średnio 204 dni na identyfikację incydentu i kolejnych 73 dni na jego opanowanie, co łącznie daje 277 dni. Analiza wykazuje, że incydenty o cyklu życia krótszym niż 200 dni generowały średni koszt 3,93 mln USD, podczas gdy te trwające dłużej kosztowały średnio 4,95 mln USD, co oznacza wzrost o 1,02 mln USD. Rysunek 1 ilustruje zależność między długością cyklu życia incydentu a jego średnim kosztem, co pokazuje, że dłuższy czas identyfikacji i opanowania incydentu (powyżej 200 dni) wiąże się z wyraźnie wyższymi kosztami naruszeń danych – aż o 1,02 mln USD więcej w porównaniu z incydentami wykrytymi i opanowanymi szybciej. Szybsza identyfikacja i reakcja na incydenty są zatem kluczowe dla minimalizacji kosztów związanych z naruszeniami danych.



Rysunek 1. Zależność między długością cyklu życia incydentu a jego średnim kosztem
Źródło: opracowanie własne na podstawie danych IBM Security.

Statystyki te jasno obrazują, że szybka detekcja oraz natychmiastowa reakcja są kluczowe dla ograniczenia strat organizacyjnych. Niestety, wiele organizacji boryka się z ograniczeniami kadrowymi oraz niskim poziomem dojrzałości monitoringu. Według badania KPMG[10], ponad połowa firm wskazuje trudności z rekrutacją oraz utrzymaniem specjalistów z zakresu cyberbezpieczeństwa jako istotną barierę we wzmacnianiu swoich systemów ochronnych. Główne źródła zagrożeń nadal wiążą się z czynnikiem ludzkim – ataki

[10] KPMG, *Barometr Cyberbezpieczeństwa. Na fali czy w labiryncie regulacji?* – raport z badania ankietowego polskich przedsiębiorstw, KPMG Polska, 2024.

socjotechniczne, w szczególności *phishing*, pozostają najczęstszą formą inicjowania incydentów. Jak potwierdzają dane KPMG, kradzież danych osobowych i dostępów za pomocą *phishingu* jest nadal postrzegana jako najpoważniejsze zagrożenie cybernetyczne. Jednocześnie wzrasta liczba ataków typu *ransomware* – w 2022 r. ich częstotliwość globalnie wzrosła o około 13%, utrzymując się na poziomie uznawanym za kluczowe zagrożenie dla ciągłości działania firm[11]. Coraz powszechniejsze staje się stosowanie zaawansowanych technik inżynierii społecznej – m.in. rozmów telefonicznych lub wiadomości od przestępców podszywających się pod kadrę zarządzającą[12].

W ostatnich latach obserwuje się rosnącą świadomość organizacji w zakresie konieczności inwestowania w zaawansowane systemy ochrony zasobów informacyjnych. Coraz częściej wdrażane są rozwiązania wykorzystujące sztuczną inteligencję AI (ang. *Artificial Intelligence*) do wykrywania zagrożeń w czasie rzeczywistym, co pozwala na szybszą reakcję i ograniczenie skutków incydentów bezpieczeństwa. Pomimo tej tendencji, wdrażanie skutecznych systemów bezpieczeństwa nadal napotyka istotne bariery – w szczególności ograniczenia finansowe, niedobór wykwalifikowanych specjalistów z zakresu cyberbezpieczeństwa oraz złożoność przepisów prawnych i regulacyjnych. Na politykę bezpieczeństwa organizacji coraz większy wpływ mają regulacje normatywne na poziomie krajowym i unijnym. Do najważniejszych z nich należy dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii Europejskiej (tzw. dyrektywa NIS 2)[13] oraz ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2023 poz. 913)[14]. Ich celem jest podniesienie poziomu odporności państw członkowskich i operatorów usług kluczowych na zagrożenia cyfrowe poprzez ujednolicenie minimalnych standardów ochrony oraz obowiązków w zakresie raportowania incydentów. Zgodnie z wynikami badania przeprowadzonego przez KPMG, 45% przedsiębiorstw w Polsce deklaruje gotowość do

[11] Grant Thornton, *Cybersecurity report*, 2023.

[12] R. Chesney, D.K. Citron, D.K., *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review*, 107(6), 2019, s. 1753-1820.

[13] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii Europejskiej (Dz. Urz. UE L 333 z 27.12.2022, s. 80).

[14] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2023 poz. 913).

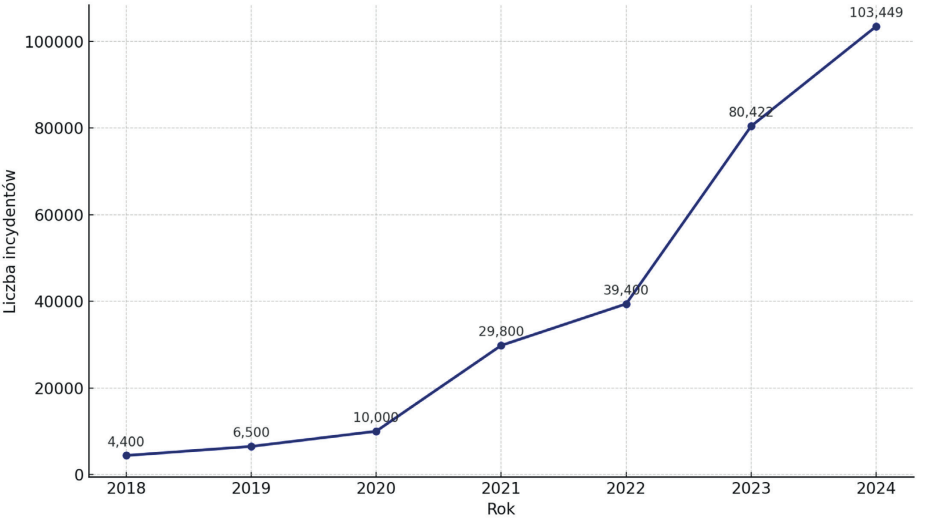
wdrożenia nowych przepisów[15]. Jednocześnie znacząca część organizacji zgłasza trudności w interpretacji obowiązków prawnych, co utrudnia skuteczne ich wdrażanie i może prowadzić do ryzyka regulacyjnego. Obowiązki takie jak konieczność zgłaszania incydentów do właściwego zespołu reagowania na incydenty bezpieczeństwa komputerowego CSIRT (ang. *Computer Security Incident Response Team*) [4] czy obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych, stanowią silny impuls do doskonalenia praktyk zarządzania bezpieczeństwem informacji. Zarówno literatura naukowa, jak i dane empiryczne wskazują jednoznacznie, że cyberbezpieczeństwo nie powinno być traktowane jako opcjonalne narzędzie ochronne, lecz jako nieodzowny element zapewnienia ciągłości działania oraz utrzymania zaufania interesariuszy.

Dane wskazują, że zagrożenia cybernetyczne są zarówno powszechne, jak i bardzo zróżnicowane – obejmują ataki socjotechniczne, złośliwe oprogramowanie, a także zaawansowane, długotrwałe kampanie realizowane przez grupy APT (ang. *Advanced Persistent Threat*), charakteryzujące się wysokim stopniem ukierunkowania i trudnością w wykryciu. Ważne jest, że ataki te dotyczą nie tylko dużych organizacji, ale również małych i średnich przedsiębiorstw, które często dysponują ograniczonymi zasobami umożliwiającymi skuteczną reakcję. Nawet pozornie drobny incydent może więc prowadzić do poważnych konsekwencji operacyjnych, finansowych i wizerunkowych. W związku z tym odporność systemów informatycznych powinna być postrzegana nie tylko w aspekcie technologicznym, lecz także jako wynik synergii rozwiązań technicznych, kompetencji kadry zarządzającej, procedur reagowania oraz organizacyjnej gotowości na sytuacje kryzysowe. Kluczowe jest wdrożenie całościowego podejścia opartego na zarządzaniu ryzykiem, obejmującego zarówno identyfikację zagrożeń, jak i ocenę ich wpływu na krytyczne procesy biznesowe. W tym kontekście zapewnienie wysokiego poziomu cyberbezpieczeństwa nie może być traktowane jako opcjonalne, lecz stanowi kluczowy warunek zapewnienia ciągłości działania organizacji.

[15] KPMG, Barometr Cyberbezpieczeństwa. Na fali czy w labiryncie regulacji? – raport z badania ankietowego polskich przedsiębiorstw, KPMG Polska, 2024.

Stan cyberbezpieczeństwa w polskich przedsiębiorstwach

Dane empiryczne zebrane na podstawie raportów dotyczących incydentów cyberbezpieczeństwa jednoznacznie potwierdzają narastającą intensyfikację zagrożeń występujących w polskiej cyberprzestrzeni. Według raportu CERT Polska[16], krajowego zespołu reagowania na incydenty bezpieczeństwa CSIRT w 2024 roku liczba odnotowanych incydentów wyniosła aż 103 449, co oznacza wzrost o około 29% względem roku poprzedniego, kiedy to liczba zgłoszeń przekroczyła 80 tys.[17] Szczególnie wymowny jest wzrost liczby incydentów w perspektywie długookresowej – pięć lat wcześniej, czyli w roku 2019, odnotowano ich zaledwie 6,5 tysiąca. Oznacza to niemal dziesięciokrotną dynamikę wzrostową, co obrazuje zarówno realny wzrost liczby ataków, jak i poprawę skuteczności procedur ich wykrywania oraz raportowania przez przedsiębiorstwa i instytucje. Tendencję tę w ujęciu chronologicznym ilustruje rysunek 2.



Rysunek 2. Liczba incydentów cyberbezpieczeństwa w Polsce w latach 2018–2024
Źródło: opracowanie własne na podstawie danych CERT Polska.

[16] CERT Polska, *Raport roczny 2024. Incydenty naruszające bezpieczeństwo teleinformatyczne obsługiwane przez zespół CERT Polska,* NASK PIB, 2025.

[17] CERT Polska, *Raport roczny 2023. Incydenty naruszające bezpieczeństwo teleinformatyczne obsługiwane przez zespół CERT Polska*, NASK PIB, 2024.

Wzrost liczby incydentów cybernetycznych jest bezpośrednio powiązany z ewolucją ich charakteru oraz rosnącym zaawansowaniem technicznym. Według raportu CERT Polska (2024), dominującą kategorią zgłoszonych incydentów były oszustwa komputerowe, których udział sięgnął aż 94,7% wszystkich przypadków. Wśród nich szczególnie często pojawiał się *phishing* – metoda manipulacji społecznej polegająca na podszywaniu się cyberprzestępców pod zaufane podmioty w celu wyłudzenia informacji poufnych (np. loginów, haseł, danych bankowych). W 2024 roku *phishing* był najczęściej realizowany poprzez masowe kampanie mailowe oraz fałszywe strony internetowe, podszywające się między innymi pod znane serwisy sprzedażowe (OLX – ok. 10 tys. przypadków, Allegro – ok. 4 tys.) oraz społecznościowe (Facebook – prawie 4 tys. przypadków). Znacznie rzadziej zgłaszano szkodliwe oprogramowanie (ang. *malware*), które odpowiadało za 1,8% przypadków (1891 incydentów), czy wykorzystanie podatności usług informatycznych (1,6%, 1634 przypadków). Pozostałe kategorie, takie jak publikacja treści nielegalnych, włamania, zakłócenia dostępności usług, próby włamań, ataki na bezpieczeństwo informacji oraz nieautoryzowane gromadzenie danych, łącznie stanowiły mniej niż 2% zgłoszeń. Szczegółowe zestawienie struktury incydentów według kategorii przedstawiono w tabeli 1.

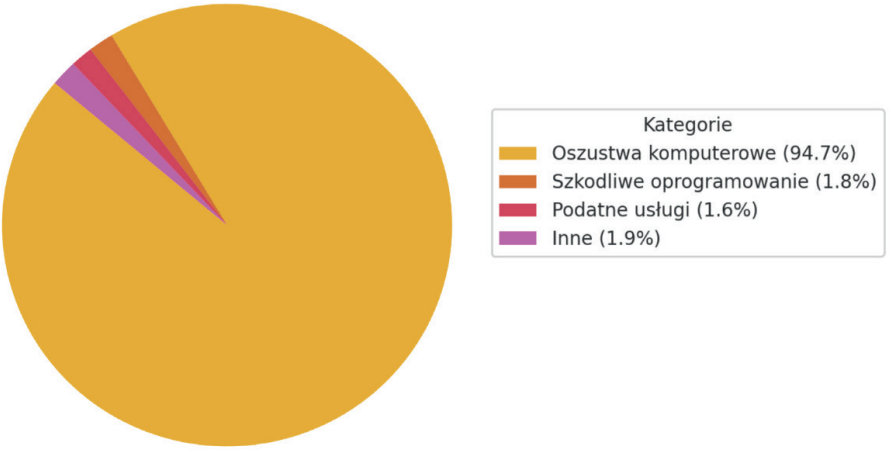
Tabela 1. Zestawienie incydentów cyberbezpieczeństwa według kategorii w Polsce za 2024 rok

Kategoria zagrożenia	Liczba incydentów	Udział procentowy
Oszustwa komputerowe	97 995	94,7%
Szkodliwe oprogramowanie	1 891	1,8%
Podatne usługi	1 634	1,6%
Obraźliwe i nielegalne treści	775	0,7%
Włamania	447	0,4%
Dostępność zasobów	426	0,4%
Próby włamań	179	0,2%
Atak na bezpieczeństwo informacji	62	0,1%
Gromadzenie informacji	26	0,0%
Inne	14	0,0%
Łącznie	103 449	100%

Źródło: opracowanie własne na podstawie danych CERT Polska.

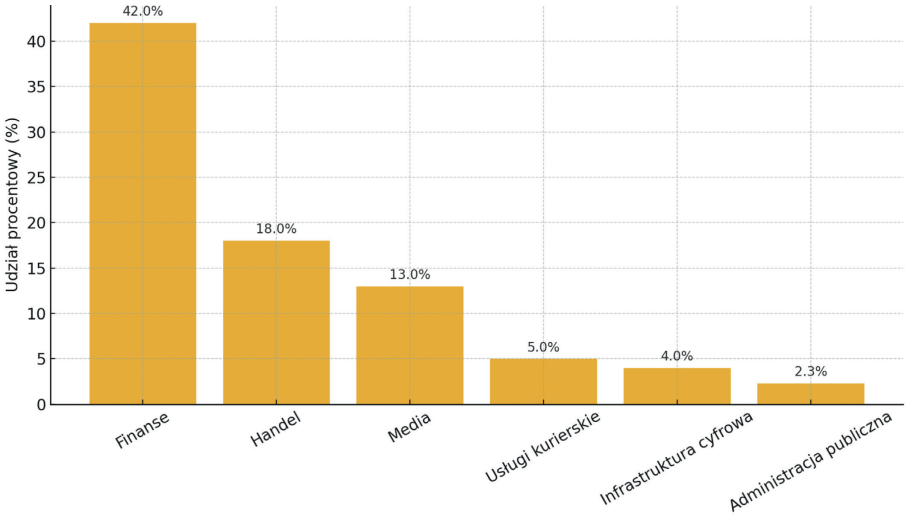
Szczegółową strukturę zgłoszonych incydentów przedstawiono na rysunku 3. Dominującą kategorią były oszustwa komputerowe, które odpowiadały za niemal 95% wszystkich zgłoszeń. Pozostałe kategorie, choć liczbowo

mniej liczne, wskazują na zróżnicowany charakter zagrożeń – od szkodliwego oprogramowania, przez nielegalne treści, po techniczne próby włamań i naruszenia dostępności usług. Dla zwiększenia czytelności, kategorie o najmniejszym udziale procentowym zostały zaszeregowane pod wspólnym mianem „Inne".



Rysunek 3. Struktura incydentów według kategorii w Polsce (2024)
Źródło: opracowanie własne na podstawie danych CERT Polska.

Analiza sektorowa wskazuje, iż poszczególne branże różnią się znacznie pod względem podatności na incydenty. Najbardziej zagrożony pozostaje sektor finansowy, na który przypada aż 42% wszystkich zarejestrowanych przez CERT Polska incydentów w 2024 roku. Kolejne sektory o wysokiej podatności to handel (18%) oraz media (13%). Niższy, lecz nadal znaczący poziom zagrożenia odnotowano w sektorze usług kurierskich (5%), infrastrukturze cyfrowej, obejmującej usługi telekomunikacyjne i centra danych (około 4%) oraz administracji publicznej (około 2,3%). Zestawienie danych zostało zaprezentowane na rysunku 4.



Rysunek 4. Udział sektorów w incydentach cyberbezpieczeństwa
Źródło: opracowanie własne na podstawie danych CERT Polska.

Te różnice sektorowe wynikają głównie ze specyfiki przetwarzanych danych oraz regulacji, które narzucają wyższe standardy ochrony na przykład instytucjom finansowym, co z kolei skutkuje lepszym raportowaniem incydentów. Jednocześnie, pomimo intensyfikacji zagrożeń, przedsiębiorstwa w Polsce wykazują coraz wyższy poziom świadomości potrzeby zabezpieczenia swoich zasobów informacyjnych. Według danych Głównego Urzędu Statystycznego[18], 94,1% przedsiębiorstw stosuje co najmniej jeden środek ochronny z technologii informacyjno-komunikacyjnych ICT (ang. *Information and Communication Technologies*). W przypadku dużych przedsiębiorstw wskaźnik ten jest jeszcze wyższy i sięga 99,6%. Najczęściej wdrażanymi zabezpieczeniami były: silne uwierzytelnianie (84% ogółu firm, 98,7% dużych), kontrola dostępu do sieci (64,5% ogółu firm, 97,9% dużych) oraz regularne kopie zapasowe w lokalizacjach zewnętrznych (71,4% ogółu, 96% dużych przedsiębiorstw). Niemniej jednak w ciągu ostatniego roku 32,5% firm doświadczyło przynajmniej jednego poważnego incydentu, z czego 10% wskazało na ponad 30 takich zdarzeń rocznie, co sugeruje konieczność dalszego doskonalenia systemów ochronnych. Najczęściej występowały incydenty techniczne związane

[18] GUS, *Społeczeństwo informacyjne w Polsce w 2024 roku.* Wyniki badań statystycznych z zakresu technologii informacyjno-komunikacyjnych w przedsiębiorstwach. Warszawa: Główny Urząd Statystyczny, 2024.

z awariami sprzętu i oprogramowania (29,7%), uszkodzeniem danych (7,7%) oraz ujawnieniem informacji poufnych w wyniku błędu ludzkiego (1%)[19].

Zgromadzone dane pozwalają stwierdzić, że rosnąca liczba incydentów oraz ich coraz bardziej zaawansowany charakter wymagają kompleksowego podejścia do zarządzania bezpieczeństwem, obejmującego techniczne, organizacyjne oraz edukacyjne aspekty ochrony danych. Szczególnego znaczenia nabiera wdrażanie strategii zapewnienia ciągłości działania BCP (ang. *Business Continuity Planning*) oraz strategii odzyskiwania danych po incydencie DRP (ang. *Disaster Recovery Planning*), jako kluczowych elementów budowania odporności organizacyjnej na cyberzagrożenia.

Analiza incydentów cyberbezpieczeństwa w polskich przedsiębiorstwach

Celem poniższej analizy jest zilustrowanie wpływu poziomu bezpieczeństwa systemów informatycznych na funkcjonowanie polskich przedsiębiorstw poprzez trzy szczegółowo zrekonstruowane studia przypadków incydentów cyberbezpieczeństwa. Wybrane przypadki dotyczą zróżnicowanych scenariuszy ataków – (1) *ransomware* na dużą firmę z branży gier wideo, (2) wycieku danych klientów popularnej platformy e-commerce oraz (3) ataku typu *supply-chain* wymierzonego w sektor finansowy. Każdy przypadek został opracowany na podstawie wiarygodnych źródeł (raportów incydentalnych, komunikatów firm, formalnych doniesień medialnych) i obejmuje opis przebiegu incydentu oraz analizę jego konsekwencji dla zaatakowanej organizacji w tym: zakłócenia operacyjne, straty finansowe, implikacje prawne, reputacyjne. Takie podejście pozwala ukazać szerokie spektrum zagrożeń cybernetycznych i ocenić, w jakim stopniu zaniedbania lub dobre praktyki w zakresie cyberbezpieczeństwa przekładają się na ciągłość działania przedsiębiorstw. Analiza tych przypadków stanowi podstawę do sformułowania wniosków na temat zależności między bezpieczeństwem systemów IT a kondycją biznesową firm oraz opracowania rekomendacji poprawy poziomu cyberbezpieczeństwa.

Przypadek 1: Atak ransomware na firmę z branży gier wideo (2021).
Na początku lutego 2021 roku doszło do jednego z najgłośniejszych cyberataków na polskie przedsiębiorstwo prywatne – ofiarą padła znana firma z branży gier wideo, producent popularnych tytułów. Atakujący włamali się

[19] CERT Polska, Raport roczny 2024. Incydenty naruszające bezpieczeństwo teleinformatyczne obsługiwane przez zespół CERT Polska, NASK PIB, 2025.

do wewnętrznej sieci tego przedsiębiorstwa i wdrożyli oprogramowanie *ransomware*, szyfrując dane na serwerach. Napastnicy pozostawili notatkę z żądaniem okupu oraz groźbą ujawnienia wykradzionych informacji, twierdząc, że pozyskali m.in. kody źródłowe flagowych gier oraz poufne dokumenty korporacyjne (finansowe, kadrowe itp.). Firma stanęła przed trudnym wyborem: zapłacić okup (bez gwarancji odzyskania danych i uniknięcia publikacji wycieku) albo odmówić i zmierzyć się z konsekwencjami. Zarząd ostatecznie postanowił nie ulegać szantażowi – spółka publicznie potwierdziła incydent, zawiadomiła organy ścigania i kategorycznie odmówiła zapłaty. W odpowiedzi sprawcy spełnili swoje groźby: w kolejnych dniach w Internecie zaczęły pojawiać się fragmenty skradzionych kodów źródłowych gier oraz firmowej dokumentacji, udostępniane na podziemnych forach i prawdopodobnie oferowane do sprzedaży na czarnym rynku. Skutki tego incydentu okazały się poważne i wielowymiarowe dla zaatakowanej spółki. Po pierwsze, zakłócenia operacyjne: znaczna część wewnętrznych systemów IT została zaszyfrowana lub prewencyjnie wyłączona. Między innymi infrastruktura deweloperska służąca do tworzenia oprogramowania przestała być dostępna, co wymusiło przerwanie prac projektowych. Firma musiała opóźnić publikację raportu finansowego za rok 2020 z powodu paraliżu wywołanego atakiem. Po drugie, straty finansowe i rynkowe: w dniu upublicznienia informacji o ataku kurs akcji spółki spadł na giełdzie o ok. 4%, a niepewność co do skali wycieku oraz potencjalnych dalszych konsekwencji dodatkowo obciążyła reputację firmy – już nadwątloną wcześniejszymi problemami z jednym z flagowych produktów. Choć nie podano dokładnych kwot strat, sam przestój operacyjny i koszty naprawy infrastruktury IT szacowano na wielomilionowe sumy. Po trzecie, implikacje prawne: wśród ujawnionych danych znalazły się m.in. dane personalne pracowników (np. dokumenty HR), co stwarzało ryzyko naruszenia przepisów o ochronie danych osobowych i zainteresowało Urząd Ochrony Danych Osobowych. Dodatkowo, jeśli w wykradzionej poufnej korespondencji wewnętrznej ujawniłyby się ewentualne zaniedbania zarządu, spółce mogły grozić pozwy od akcjonariuszy. Po czwarte, szkody wizerunkowe: paradoksalnie atak ten pokazał, że nawet firma technologiczna – od której oczekuje się najwyższych standardów w IT – miała luki w zabezpieczeniach. Publiczna dyskusja wokół incydentu wskazywała, że reputacja przedsiębiorstwa ucierpiała, a zaufanie inwestorów i partnerów biznesowych zostało naruszone. Analiza tego przypadku prowadzi do kilku ważnych obserwacji. Po pierwsze, atak *ransomware* uderza nie tylko w finansowe aspekty działalności, ale i strategiczne

– w tym wypadku napastnicy zaatakowali najbardziej wartościowe zasoby intelektualne firmy (kody źródłowe gier stanowiące jej kluczową własność intelektualną). Po drugie, odporność organizacji i plany awaryjne są kluczowe. W opisywanym przedsiębiorstwie posiadanie aktualnych kopii zapasowych oraz dobrze opracowanych procedur ciągłości działania pozwoliło stosunkowo szybko przywrócić podstawowe operacje, mimo zaszyfrowania części systemów – raportowano, że kluczowe funkcje udało się odzyskać w ciągu kilkunastu dni. Niemniej jednak sam fakt skutecznego włamania obnażył braki w prewencji, prawdopodobnie zawiódł któryś z mechanizmów ochronnych (np. atak rozpoczął się od skutecznego *phishingu* dającego dostęp do sieci albo brak segmentacji sieci pozwolił *malware* na szerokie rozprzestrzenienie). Po trzecie, incydent posłużył jako sygnał ostrzegawczy dla innych firm w Polsce – nawet rynkowi liderzy nie są w pełni bezpieczni. W branży *gamingowej* po tym wydarzeniu wiele podmiotów przeprowadziło dodatkowe audyty zabezpieczeń, testy penetracyjne oraz wdrożyło bardziej restrykcyjne polityki (typu *zero trust*) w celu zapobieżenia podobnym incydentom w przyszłości.

Przypadek 2: Wyciek danych klientów platformy e-commerce (2018-2019).

Drugie *case study* dotyczy poważnego incydentu, który dotknął jedną z czołowych polskich platform e-commerce działających w branży sprzedaży elektroniki. Pod koniec 2018 roku cyberprzestępcom udało się włamać do bazy danych klientów tego sklepu internetowego, co doprowadziło do wycieku informacji o ponad 2,2 miliona użytkowników. Skradzione dane obejmowały między innymi imiona i nazwiska klientów, adresy e-mail, numery telefonów, adresy dostawy, a także hasła (zaszyfrowane, lecz potencjalnie podatne na złamanie) oraz historię zakupów. Ujawnienie tak szerokiego zakresu danych osobowych – w tym danych kontaktowych i pośrednio preferencji zakupowych – stanowiło jeden z największych incydentów naruszenia ochrony danych w polskim e-commerce. Konsekwencje dla przedsiębiorstwa okazały się bardzo poważne i długofalowe. Bezpośrednio po wykryciu wycieku (w grudniu 2018 r.) firma musiała zmierzyć się z kryzysem wizerunkowym oraz obowiązkiem prawym powiadomienia zarówno klientów, jak i właściwego organu nadzorczego o zaistniałym incydencie. Uruchomiono procedury informowania wszystkich poszkodowanych osób (co samo w sobie stanowiło ogromne wyzwanie logistyczne przy tak dużej liczbie rekordów), a także wsparcia dla klientów – m.in. zalecono pilną zmianę haseł we wszystkich usługach, ostrzegano przed próbami *phishingu* wykorzystującymi wykradzione dane itd. Reakcja organu

nadzorczego była zdecydowana: w 2019 roku Prezes Urzędu Ochrony Danych Osobowych nałożył na spółkę administracyjną karę pieniężną w wysokości 2,8 mln zł za niewystarczające zabezpieczenie danych osobowych klientów. Była to wówczas rekordowo wysoka kara w Polsce za naruszenie przepisów RODO. W uzasadnieniu decyzji Urzędu Ochrony Danych Osobowych UODO wskazano m.in. brak stosowania dwuskładnikowego uwierzytelniania 2FA (ang. *Two-Factor Authentication*) w kluczowych procesach bezpieczeństwa – na przykład podczas logowania administratorów do systemu informatycznego lub klientów do swoich kont. Dwuskładnikowe uwierzytelnianie polega na konieczności potwierdzenia tożsamości użytkownika za pomocą dwóch niezależnych elementów (np. hasła oraz jednorazowego kodu SMS lub aplikacji mobilnej). Zaniedbanie tego mechanizmu znacząco ułatwiło atakującym przejęcie dostępu do chronionych danych[20]. Spółka odwołała się od decyzji, jednak w 2020 r. Wojewódzki Sąd Administracyjny podtrzymał nałożenie kary, a następnie w 2021 r. organ nadzorczy, odkrywszy dodatkowe obciążające okoliczności, zwiększył wymiar grzywny do 3,8 mln zł. Tak dotkliwa sankcja finansowa znacząco obciążyła wyniki firmy za dany okres i stała się wyraźnym sygnałem ostrzegawczym dla całej branży, że zaniedbania w ochronie danych klientów będą surowo karane. Oprócz konsekwencji prawnych, firma poniosła także poważne straty reputacyjne. Wielu klientów utraciło zaufanie do platformy – tym bardziej, że sprawa była szeroko komentowana w mediach, a w Internecie szybko pojawiły się bazy wyciekłych danych (narażając osoby na spam oraz kolejne ataki socjotechniczne). Konkurenci nie wahali się wykorzystać sytuacji w przekazach marketingowych, podkreślając bezpieczeństwo swoich rozwiązań. Szacuje się, że w wyniku skandalu część użytkowników przeniosła się z tej platformy do innych serwisów, a wskaźniki sprzedaży sklepu przejściowo spadły. Firma, chcąc odzyskać reputację, musiała zainwestować w kampanię odbudowy zaufania – wzmocniono obsługę klienta, oferowano poszkodowanym m.in. darmowy monitoring tożsamości oraz rabaty na kolejne zakupy. Wewnętrznie incydent stał się impulsem do gruntownego przeglądu zabezpieczeń: wprowadzono obowiązkową weryfikację dwuskładnikową 2FA dla klientów i administratorów systemu, zatrudniono dodatkowych specjalistów ds. bezpieczeństwa IT, wdrożono system DLP (ang. *Data Loss Prevention*), czyli rozwiązanie zapobiegające nieautoryzowanemu wyciekowi danych

[20] UODO – Decyzja Prezesa Urzędu Ochrony Danych Osobowych z 2019 r. w sprawie naruszenia ochrony danych osobowych w sklepie Morele.net (publikacja na stronie UODO.gov.pl) ZSPR.421.2.2019, 2019.

poza organizację, a także zaostrzono polityki dostępu do informacji uznawanych za krytyczne z punktu widzenia bezpieczeństwa operacyjnego. Systemy DLP umożliwiają monitorowanie, wykrywanie i blokowanie prób przesyłania wrażliwych danych poprzez różne kanały komunikacji (np. e-mail, nośniki USB, chmurę), minimalizując ryzyko ich niekontrolowanego ujawnienia. Głośnym echem odbił się przy tym fakt, iż atakujący najprawdopodobniej uzyskali wstępny dostęp do systemu, wysyłając do firmy zainfekowany dokument CV (życiorys) i wykorzystując podatność w oprogramowaniu pocztowym – co unaoczniło znaczenie edukacji pracowników oraz stosowania filtrów bezpieczeństwa nawet w tak rutynowych procesach, jak rekrutacja. Podsumowując, ten przypadek pokazuje, że wyciek danych osobowych klientów przekłada się na bardzo realne straty finansowe (kary administracyjne, koszty naprawy), operacyjne (czasochłonna obsługa incydentu, dodatkowe procedury) i wizerunkowe, które mogą obciążać firmę przez długi czas. Stanowi on również przestrogę, iż spełnianie jedynie minimalnych wymogów prawnych to za mało – przedsiębiorstwa muszą proaktywnie rozwijać swoje systemy zabezpieczeń i wdrażać najlepsze praktyki (choćby tak podstawowe jak dwuskładnikowe uwierzytelnianie), zanim to poważny incydent wymusi takie działania.

Przypadek 3: Atak *supply-chain* poprzez stronę regulatora finansowego (2016-2017).

Trzeci przypadek ilustruje zaawansowany incydent cyberbezpieczeństwa klasyfikowany jako atak łańcucha dostaw (ang. *supply-chain attack*), który dotknął polski sektor bankowy na przełomie lat 2016 i 2017. Incydent ten został uznany za bezprecedensowy w skali kraju ze względu na nietypowy wektor ataku oraz fakt, że jego źródłem była instytucja nadzoru finansowego. Zamiast dokonywać bezpośrednich prób naruszenia systemów bankowych, sprawcy uzyskali dostęp do infrastruktury teleinformatycznej Komisji Nadzoru Finansowego (KNF) – centralnego organu regulacyjnego rynku finansowego w Polsce. W wyniku kompromitacji serwera instytucji, napastnicy zmodyfikowali zawartość oficjalnej strony internetowej KNF, wprowadzając do niej złośliwy kod. W efekcie, w okresie od października 2016 roku do lutego 2017 roku, użytkownicy odwiedzający witrynę – w tym pracownicy instytucji finansowych – byli narażeni na automatyczne pobranie zewnętrznego pliku zawierającego złośliwe oprogramowanie (ang. *malware*). Wykorzystanie infrastruktury zaufanego podmiotu nadzorczego jako wektora ataku umożliwiło rozprzestrzenienie się zagrożenia na szereg banków komercyjnych. Dopiero w styczniu 2017 roku kilka instytucji finansowych niemal

równocześnie zaobserwowało anomalie w ruchu sieciowym oraz nieznane pliki na serwerach, których nie wykrywały stosowane dotąd rozwiązania antywirusowe. Analiza przeprowadzona przez zespoły bezpieczeństwa działające w ramach sektorowego zespołu reagowania (CSIRT KNF oraz jednostka przy Związku Banków Polskich) pozwoliła na identyfikację wspólnego mianownika – wszystkie zainfekowane stacje robocze wcześniej komunikowały się z witryną KNF. 3 lutego 2017 roku, w ramach działań zaradczych, infrastruktura informatyczna Komisji Nadzoru Finansowego została prewencyjnie wyłączona, celem przerwania ciągu infekcji oraz zabezpieczenia materiału dowodowego. Śledztwo wykazało, że incydent umożliwił napastnikom uzyskanie potencjalnie głębokiego dostępu do wewnętrznych segmentów sieci bankowych, co mogło pozwolić na dalsze działania z zakresu rekonesansu, eskalacji uprawnień lub wycieku danych. Zgodnie z oficjalnymi informacjami, incydent nie doprowadził do kradzieży danych klientów ani środków finansowych. Istnieją jednak przesłanki wskazujące, że celem ataku było cyberszpiegostwo, tj. pozyskanie informacji oraz przygotowanie gruntu pod potencjalne dalsze operacje cybernetyczne. Incydent ten uwypuklił słabość zaufanych relacji instytucjonalnych – nawet podmioty pełniące funkcje regulacyjne i nadzorcze mogą, wskutek luk w zabezpieczeniach, stać się punktem wejścia dla cyberzagrożeń. W oficjalnym komentarzu opublikowanym przez Rządowe Centrum Bezpieczeństwa (RCB), podkreślono, że podstawowym błędem było założenie, iż serwis informacyjny instytucji nie wymaga szczególnej ochrony – założenie to zostało bezwzględnie wykorzystane przez atakujących. Incydent unaocznił również kluczowe znaczenie współpracy międzyinstytucjonalnej w zakresie cyberbezpieczeństwa. Dzięki szybkiej wymianie informacji pomiędzy zespołami reagowania banków, CSIRT KNF oraz zespołami CSIRT NASK i Agencji Bezpieczeństwa Wewnętrznego, możliwe było szybkie zidentyfikowanie źródła ataku i ograniczenie jego skutków. Gdyby każda instytucja działała w izolacji, wykrycie wektora infekcji mogłoby zająć znacznie więcej czasu, zwiększając potencjalne straty. Konsekwencje tego incydentu były znaczące zarówno z perspektywy reputacyjnej, jak i operacyjnej. Komisja Nadzoru Finansowego zmuszona była do odbudowy zaufania oraz modernizacji swoich systemów, natomiast banki przeprowadziły kosztowne działania naprawcze i audyty bezpieczeństwa. W odpowiedzi na ten atak sektor finansowy zaostrzył procedury bezpieczeństwa, wprowadzając m.in. kontrolę kanałów zaufanych, audyty aplikacji dostarczanych przez podmioty trzecie oraz ćwiczenia typu „*red teaming*", symulujące podobne scenariusze zagrożeń. Atak ten stanowi

dziś klasyczny przykład incydentu łańcucha dostaw i jest często omawiany w kontekście szkoleń i konferencji branżowych. Pokazuje on, że bezpieczeństwo cyfrowe całego ekosystemu zależy od najsłabszego ogniwa – niezależnie od formalnej roli danej instytucji w strukturze rynku.

Zaprezentowane powyżej trzy studia przypadków – obejmujące atak typu *ransomware*, incydent związany z wyciekiem danych osobowych oraz atak typu łańcucha dostaw (ang. *supply-chain attack*) – obrazują złożoność oraz zróżnicowanie zagrożeń cybernetycznych, na jakie narażone są współczesne organizacje. Przypadki te uwidaczniają szerokie spektrum możliwych skutków incydentów bezpieczeństwa – od bezpośrednich strat finansowych i zakłóceń operacyjnych, poprzez konsekwencje prawne i regulacyjne, aż po długofalową utratę reputacji i zaufania interesariuszy. Analiza tych zdarzeń potwierdza tezę, że niedostateczny poziom zabezpieczeń – w tym brak mechanizmów redundancji danych (np. regularnych kopii zapasowych), brak wdrożenia mechanizmów silnego uwierzytelniania (np. dwuskładnikowego uwierzytelniania, czy też utrzymywanie nieaktualnego oprogramowania – znacząco zwiększa prawdopodobieństwo wystąpienia skutecznych ataków oraz pogłębia ich negatywne konsekwencje. Z drugiej strony, organizacje wykazujące wysoki poziom dojrzałości w zakresie zarządzania bezpieczeństwem informacji – posiadające zaktualizowane plany ciągłości działania, skuteczne strategie odzyskiwania po awarii, regularne kopie zapasowe oraz wewnętrzną kulturę bezpieczeństwa opartą na świadomości i kompetencjach pracowników – są zdecydowanie lepiej przygotowane na sytuacje kryzysowe. Tego rodzaju podejście umożliwia im szybsze przywrócenie funkcjonowania po incydencie oraz ograniczenie strat, zarówno materialnych, jak i niematerialnych. Z perspektywy zarządzania ryzykiem operacyjnym, studia przypadków te stanowią istotny materiał analityczny, wskazując, że inwestycje w cyberbezpieczeństwo należy traktować nie jako koszt, lecz jako element nieodzowny dla utrzymania odporności organizacyjnej w warunkach gospodarki cyfrowej.

Wnioski i rekomendacje dla podniesienia poziomu bezpieczeństwa

Przeprowadzone analizy potwierdzają istotną zależność: poziom bezpieczeństwa systemów informatycznych znacząco wpływa na ciągłość działania i wyniki przedsiębiorstw. Innymi słowy, hipoteza badawcza mówiąca, iż wysoki poziom cyberbezpieczeństwa jest kluczowym czynnikiem warunkującym stabilność operacyjną firm, została pozytywnie zweryfikowana. Widzimy

wyraźnie, że firmy inwestujące w zabezpieczenia IT (technologie, procedury, kadry) nie tylko zmniejszają prawdopodobieństwo wystąpienia incydentu, ale także lepiej radzą sobie w razie ataku – szybciej wykrywają zagrożenie, skuteczniej ograniczają jego rozprzestrzenianie i sprawniej przywracają normalne operacje. Z kolei zaniedbania w bezpieczeństwie prowadzą do poważnych zakłóceń działalności: atak *ransomware* może sparaliżować podstawowe procesy na wiele dni, wyciek danych klientów skutkuje kosztownymi karami oraz utratą zaufania, a atak na infrastrukturę informatyczną może przerwać ciągłość kluczowych usług. W skrajnym przypadku następstwem poważnego cyberataku bywa nawet upadłość przedsiębiorstwa – literatura odnotowuje przykłady, gdzie kumulacja kosztów i utraty reputacji po incydencie doprowadziła organizacje do bankructwa. Warto podkreślić, że koszty incydentów cyberbezpieczeństwa są bardzo wysokie. Średni globalny koszt naruszenia danych wynosi obecnie około 4,45 mln USD, a średni koszt incydentu *ransomware* sięga 5,23 mln USD[21]. Równie kosztowny bywa długi czas reakcji – firmy, które szybko wykrywają i neutralizują zagrożenie, ponoszą istotnie mniejsze straty niż te, u których atak pozostaje niezauważony przez wiele miesięcy. Niestety, jak wspomniano wcześniej, wykrycie ataku zajmuje organizacjom średnio ponad pół roku. Jakie działania powinny zatem podjąć polskie przedsiębiorstwa, aby zminimalizować ryzyko wystąpienia incydentów i złagodzić ich skutki? Poniżej przedstawiono kluczowe rekomendacje wynikające z dokonanej analizy przypadków oraz aktualnych dobrych praktyk:

- Implementacja wielowarstwowych zabezpieczeń (ang. *defence-in-depth*): Należy wdrażać wiele niezależnych mechanizmów ochronnych na różnych poziomach. Podstawą są aktualne systemy antywirusowe i zapory sieciowe, ale równie ważne jest szyfrowanie wrażliwych danych, segmentacja sieci (utrudniająca rozprzestrzenianie się złośliwego oprogramowania) oraz systemy wykrywania włamań IDS/IPS (ang. *Intrusion Detection System* / *Intrusion Prevention System*). Konieczne jest stosowanie silnego uwierzytelniania – co najmniej dwuskładnikowego (2FA) – wszędzie tam, gdzie to możliwe, zarówno dla dostępu pracowników do systemów wewnętrznych, jak i dla użytkowników usług online. Przykład

[21] IBM Security, Ponemon Institute, Cost of a Data Breach Report, 2023.

kary nałożonej przez UODO na platformę e-commerce[22] pokazuje, że brak 2FA może zostać uznany za poważne zaniedbanie.

- Regularne kopie zapasowe i plany ciągłości działania: Ataki *ransomware* oraz inne awarie wymuszają posiadanie aktualnych kopii zapasowych kluczowych danych, przechowywanych w odseparowanej infrastrukturze (zgodnie z zasadą 3-2-1: trzy kopie na dwóch różnych nośnikach, w tym jedna kopia *off-site*). Firmy powinny okresowo testować odtwarzanie systemów z backupów, by upewnić się, że kopie są skuteczne. Ponadto każdy przedsiębiorca powinien dysponować Planem Ciągłości Działania (BCP) oraz Planem Odzyskiwania po Awarii (DRP), które precyzują procedury funkcjonowania w trybie awaryjnym, dopuszczalne czasy przestoju dla krytycznych procesów oraz role i odpowiedzialności zespołów w razie poważnego incydentu. W opisanym przypadku firmy z sektora gier posiadanie sprawnych backupów pozwoliło odtworzyć systemy po ataku w akceptowalnym czasie, ograniczając długość przestoju – takie plany muszą jednak być regularnie aktualizowane i ćwiczone (np. poprzez symulacyjne testy typu *table-top*).
- Monitorowanie i szybka detekcja zagrożeń: Biorąc pod uwagę długi medianowy czas wykrywania incydentów (ponad 200 dni globalnie), przedsiębiorstwa muszą zainwestować w zaawansowane narzędzia monitoringu bezpieczeństwa. Nowoczesne systemy klasy SIEM (ang. *Security Information and Event Management*) oraz SOAR (ang. *Security Orchestration, Automation and Response*), umożliwiające zaawansowaną analizę, automatyzację i skuteczne reagowanie na incydenty bezpieczeństwa. Systemy te potrafią agregować logi z różnych źródeł i automatyzować detekcję anomalii, a dedykowane zespoły SOC (ang. *Security Operations Center*) lub usługi zarządzanego monitoringu zapewniają całodobowy nadzór nad bezpieczeństwem. Warto korzystać z mechanizmów *threat intelligence* – bieżących informacji o pojawiających się zagrożeniach – aby móc szybko reagować na nowe kampanie ataków (np. CERT Polska udostępnia listy ostrzeżeń o aktywnych *phishingach*). Współczesne rozwiązania wykorzystujące uczenie maszynowe mogą znacząco skrócić czas wykrycia subtelnych ataków. Długotrwałe niewykrycie incydentu, jak pokazał przypadek ataku na KNF trwającego kilka miesięcy w tle,

[22] UODO – Decyzja Prezesa Urzędu Ochrony Danych Osobowych z 2019 r. w sprawie naruszenia ochrony danych osobowych w sklepie Morele.net (publikacja na stronie UODO.gov.pl) ZSPR.421.2.2019, 2019.

pozwala napastnikom zadomowić się w sieci ofiary i zwiększa potencjalne szkody. Dlatego celem każdej firmy powinno być maksymalne zredukowanie czasu bytności atakującego w systemie (ang. *dwell time)* – np. poprzez stosowanie agentów EDR (ang. *Endpoint Detection and Response*) / XDR (ang. *Extended Detection and Response*) na stacjach roboczych, które wychwytują podejrzane aktywności (takie jak nieautoryzowana eskalacja uprawnień czy komunikacja z nietypowymi domenami).

- Szkolenia i podnoszenie świadomości pracowników: Czynnik ludzki jest jednym z najsłabszych ogniw bezpieczeństwa, którego nie da się w pełni wyeliminować technologią, dlatego kluczowe jest zbudowanie w organizacji silnej kultury bezpieczeństwa. Regularne szkolenia personelu z rozpoznawania ataków socjotechnicznych (ang. *phishingu, vishingu* itp.), zasad higieny haseł, bezpiecznych praktyk pracy z systemami oraz procedur zgłaszania incydentów są absolutnie niezbędne. Szkolenia powinny mieć praktyczny charakter (np. okresowo przeprowadzane symulowane kampanie *phishingowe* testujące czujność załogi) i być dostosowane do specyfiki danej firmy. Świadomy zagrożeń pracownik może okazać się najskuteczniejszą linią obrony – na przykład to czujność pracowników banków pozwoliła zauważyć anomalie wskazujące na atak przez stronę KNF, co przyczyniło się do wykrycia opisanego incydentu. Warto promować zasadę *zero trust but verify* – nawet wewnątrz organizacji personel powinien weryfikować nietypowe polecenia lub prośby (np. dotyczące transferów środków), nawet jeśli pozornie pochodzą od kadry zarządzającej, gdyż zdarzają się oszustwa typu BEC (ang. *Business Email Compromise*).
- Audyt bezpieczeństwa dostawców i partnerów (ang. *security of supply chain*): Firmy powinny oceniać ryzyka związane z podmiotami zewnętrznymi, które mają dostęp do ich systemów lub danych. Opisany atak *supply-chain* na sektor bankowy dobitnie pokazał, że słabo zabezpieczony partner (w tym wypadku strona WWW organu nadzoru) może zagrozić wielu niezależnym organizacjom. W praktyce należy uwzględniać wymagania bezpieczeństwa już na etapie zawierania umów z dostawcami – wprowadzać klauzule dotyczące standardów zabezpieczeń, prawa do audytu bezpieczeństwa, obowiązku zgłaszania incydentów itp. Dobrą praktyką jest okresowe sprawdzanie kluczowych partnerów pod kątem przestrzegania podstawowych zasad cyberbezpieczeństwa (czy regularnie aktualizują

oprogramowanie, czy nie doświadczyli ostatnio incydentu, który mógłby rozprzestrzenić się na infrastrukturę firmy). Należy również technicznie ograniczać zaufanie do dostawców: segmentować i minimalizować zakres dostępu partnerów zewnętrznych tylko do zasobów niezbędnych do realizacji usług (zasada najmniejszych uprawnień). Szczególnie wrażliwe integracje (np. połączenia z systemami regulatorów czy banków) powinny być objęte dodatkowym monitoringiem i dodatkowymi warstwami zabezpieczeń.

- Zgodność z regulacjami i standardami: Przedsiębiorstwa – zwłaszcza z sektorów kluczowych (finanse, energetyka, transport, zdrowie) – muszą spełniać wymogi krajowe i unijne w zakresie cyberbezpieczeństwa. Nowa unijna dyrektywa w sprawie bezpieczeństwa sieci i informacji NIS2 (ang. *Network and Information Security Directive*)[23], nałoży w najbliższym czasie jeszcze szersze obowiązki na tzw. podmioty istotne. Do najważniejszych z nich należą m.in. konieczność wdrożenia adekwatnych środków technicznych i organizacyjnych dostosowanych do poziomu ryzyka oraz obowiązek zgłaszania poważnych incydentów bezpieczeństwa w ciągu 24 godzin od ich wykrycia. Choć dyrektywa jest już wiążąca dla państw członkowskich UE, w Polsce nie została jeszcze formalnie implementowana do krajowego porządku prawnego. Obecnie trwają prace legislacyjne nad nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa – projekt ten znajduje się na etapie konsultacji międzyresortowych. Zakończenie procesu legislacyjnego i wejście w życie odpowiednich przepisów spodziewane jest w pierwszej połowie 2025 roku. Już teraz jednak warto przygotować się do nadchodzących wymogów, przeprowadzając analizę luk (tzw. *gap analysis*) względem przyszłych regulacji NIS2 i uzupełniając brakujące elementy – takie jak polityki i procedury bezpieczeństwa, mechanizmy zarządzania ryzykiem, czy ustalone kanały współpracy z zespołami reagowania na incydenty (CSIRT). Podobnie wymogi RODO dotyczące ochrony danych osobowych muszą być traktowane priorytetowo – przypadek wycieku danych i rekordowej kary dla omawianej platformy e-commerce dowodzi, że *compliance* przekłada się na konkretne koszty (lepiej zawczasu zainwestować w zabezpieczenia niż później płacić wysokie kary). Dobrą praktyką podnoszącą

[23] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii Europejskiej, znana jako dyrektywa NIS2, 2022.

poziom zaufania jest również uzyskanie certyfikacji zgodności z normą ISO/IEC 27001 – choć formalnie nieobowiązkowa, certyfikacja taka potwierdza dojrzałość systemu zarządzania bezpieczeństwem informacji w firmie i bywa wymagana przez niektórych kontrahentów (zwłaszcza międzynarodowych).

- Plan reagowania na incydenty oraz współpraca w ramach ekosystemu: Każda organizacja powinna posiadać sformalizowany plan reagowania na incydenty IRT (ang. *Incident Response Plan*), określający skład i role zespołu reagowania, procedury eskalacji problemu, zasady komunikacji (zarówno wewnętrznej, jak i z mediami oraz klientami) oraz współpracy z organami ścigania i odpowiednimi CSIRT-ami. Przećwiczenie potencjalnych scenariuszy (np. symulacja ataku *ransomware* w formie *war game*) pozwala uniknąć chaosu w sytuacji prawdziwego kryzysu. Bardzo istotna jest także współpraca sektorowa i udział w inicjatywach wymiany informacji o zagrożeniach (np. sieci ISAC w różnych sektorach). Przykład banków pokazuje, że dzielenie się wiedzą o zaobserwowanym ataku umożliwiło sprawne wykrycie jego źródła i ograniczenie skutków. Budowanie zaufanych kanałów współpracy (np. grupy robocze pod auspicjami Związku Banków Polskich, fora wymiany informacji między operatorami infrastruktury krytycznej itp.) zwiększa wspólną odporność całego ekosystemu na ataki. W przypadku mniejszych firm, które nie dysponują rozbudowanymi zespołami IT, warto rozważyć współpracę z wyspecjalizowanymi podmiotami zewnętrznymi (firmami doradczymi, integratorami bezpieczeństwa), aby w razie incydentu móc szybko uzyskać ekspercką pomoc. Uzupełnieniem strategii zarządzania ryzykiem może być także wykupienie ubezpieczenia cyberryzyk – polisa co prawda nie zapobiegnie atakowi, ale może częściowo złagodzić jego skutki finansowe (trzeba przy tym pamiętać, że warunkiem wypłaty odszkodowania jest zwykle posiadanie podstawowych zabezpieczeń, co stanowi dodatkową motywację do ich wdrożenia).

Reasumując, cyberbezpieczeństwo stało się nieodłącznym elementem zarządzania nowoczesnym przedsiębiorstwem. Wyniki powyższych analiz jednoznacznie wskazują, że wysoki poziom zabezpieczeń warunkuje stabilność i zrównoważony rozwój firm w cyfrowej gospodarce. Nakłady na bezpieczeństwo informacji należy traktować jak inwestycję chroniącą przed potencjalnie druzgocącymi stratami. Przedsiębiorstwa działające w Polsce powinny systematycznie podnosić poziom dojrzałości w zakresie cyberbezpieczeństwa,

obejmując działania zarówno w obszarze technologii, jak i procesów organizacyjnych oraz zasobów ludzkich. Tylko kompleksowe, proaktywne podejście do zarządzania bezpieczeństwem informacji, oparte na współpracy wszystkich uczestników ekosystemu, pozwala skutecznie minimalizować negatywne skutki incydentów bezpieczeństwa dla działalności operacyjnej organizacji. W kontekście rosnącej skali i złożoności zagrożeń, konieczne jest nie tylko wdrażanie odpowiednich narzędzi technicznych, lecz również budowanie świadomości i kompetencji wśród pracowników oraz zapewnienie gotowości decyzyjnej i operacyjnej w sytuacjach kryzysowych.

Podsumowanie

W rozdziale przeanalizowano związek pomiędzy poziomem bezpieczeństwa systemów informatycznych a funkcjonowaniem przedsiębiorstw w warunkach rosnących zagrożeń cybernetycznych. Wykorzystując podejście mieszane – łączące analizę danych empirycznych z krajowych raportów oraz studia przypadków realnych incydentów – wykazano, że dojrzałość organizacyjna w zakresie cyberbezpieczeństwa jest jednym z kluczowych determinantów ciągłości działania, stabilności finansowej i odporności operacyjnej przedsiębiorstw.

Przeprowadzone badania potwierdziły, że brak odpowiednich zabezpieczeń technicznych, organizacyjnych oraz kompetencyjnych skutkuje poważnymi konsekwencjami – zarówno w wymiarze bezpośrednich strat finansowych i operacyjnych, jak i długofalowej utraty reputacji. Przypadki takie jak ataki ransomware, wycieki danych osobowych czy kompromitacje infrastruktury pośredników zaufania, jednoznacznie ukazują, że cyberzagrożenia nie są zjawiskiem marginalnym, lecz systemowym ryzykiem wymagającym skoordynowanej odpowiedzi. Z drugiej strony, przedsiębiorstwa charakteryzujące się wysokim poziomem dojrzałości w zakresie zarządzania bezpieczeństwem informacji – wdrażające standardy branżowe, realizujące polityki ciągłości działania, monitorujące infrastrukturę w czasie rzeczywistym oraz inwestujące w edukację pracowników – wykazują wyraźnie większą odporność na incydenty i szybciej odzyskują zdolność operacyjną po ich wystąpieniu.

Wnioski płynące z rozdziału wskazują, że cyberbezpieczeństwo powinno być postrzegane jako strategiczny obszar zarządzania ryzykiem, a nie kosztowny dodatek technologiczny. Wdrażanie rozwiązań zgodnych z normami międzynarodowymi (takimi jak ISO/IEC 27001), rozwój mechanizmów

monitorowania i reagowania (SIEM, SOAR, EDR/XDR), doskonalenie planów BCP i DRP oraz systematyczna edukacja kadry stanowią podstawę budowania odporności organizacyjnej. Rozdział stanowi zatem zarówno diagnozę obecnego stanu bezpieczeństwa informatycznego polskich przedsiębiorstw, jak i zbiór praktycznych wskazówek dla decydentów odpowiedzialnych za strategię bezpieczeństwa cyfrowego.

Literatura

1. Andress, J., *Foundations of Information Security: A Straightforward Introduction*, 2nd ed., No Starch Press, San Francisco, 2019.
2. Chacko, L., Rajan, P., Anilkumar, V., Pathari, V. *Proof-of-Variable-Authority: A Blockchain Consensus Mechanism for Securing IoT Networks*, [w:] *Information Systems Security*, ed. V. Muthukkumarasamy, S. D. Sudarsan, R. K. Shyamasundar, ICISS 2023, Lecture Notes in Computer Science, vol. 14424, Springer, Cham, 2023.
3. Chesney, R., Citron, D.K. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, California Law Review, 107(6), 2019, s. 1753-1820.
4. Gordon, L.A., Loeb, M.P. Managing Cybersecurity Resources: A Cost-Benefit Analysis, McGraw-Hill, 2006.
5. CERT Polska, Raport roczny 2023. Incydenty naruszające bezpieczeństwo teleinformatyczne obsługiwane przez zespół CERT Polska, NASK PIB, 2024.
6. CERT Polska, Raport roczny 2024. Incydenty naruszające bezpieczeństwo teleinformatyczne obsługiwane przez zespół CERT Polska, NASK PIB, 2025.
7. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii Europejskiej (Dz. Urz. UE L 333 z 27.12.2022, s. 80), 2022.
8. Grant Thornton, Cybersecurity Report, 2023.
9. GUS, Społeczeństwo informacyjne w Polsce w 2024 roku. Wyniki badań statystycznych z zakresu technologii informacyjno-komunikacyjnych w przedsiębiorstwach, Główny Urząd Statystyczny, Warszawa, 2024.
10. IBM Security, Ponemon Institute, Cost of a Data Breach Report, 2023.
11. International Organization for Standardization, ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements, Geneva, 2019.
12. International Organization for Standardization, ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, Geneva, 2022.
13. International Organization for Standardization, ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls, Geneva, 2022.
14. International Organization for Standardization, ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks, Geneva, 2022.

15. International Organization for Standardization, ISO/IEC 27017:2015, Code of practice for information security controls based on ISO/IEC 27002 for cloud services, Geneva, 2015.
16. KPMG, Barometr Cyberbezpieczeństwa. Na fali czy w labiryncie regulacji? – raport z badania ankietowego polskich przedsiębiorstw, KPMG Polska, 2024.
17. UODO, Decyzja Prezesa Urzędu Ochrony Danych Osobowych z 2019 r. w sprawie naruszenia ochrony danych osobowych w sklepie Morele.net, ZSPR.421.2.2019, publikacja na stronie UODO.gov.pl, 2019.
18. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, (Dz. U. 2023 poz. 913).