

## CYBERBEZPIECZEŃSTWO JAKO WSPÓŁCZESNE WYZWANIE W ZARZĄDZANIU MAŁYM I ŚREDNIM PRZEDSIĘBIORSTWEM

Anna Elżbieta Sawicka<sup>1\*</sup>


<sup>1</sup> Eduexpert Sp. z o.o., Toruń, Polska

**Streszczenie:** Wraz z rozwojem technologii i narzędzi komunikacyjnych istotne z perspektywy zarządzania organizacją stało się zagadnienie bezpieczeństwa cybernetycznego. Celem artykułu jest analiza funkcjonowania przedsiębiorstw MŚP w celu identyfikacji najczęściej występujących ataków cybernetycznych oraz sposobów przygotowania przedsiębiorstwa MŚP do funkcjonowania w związku z ryzykiem wystąpienia zagrożenia cybernetycznego. Analizę przeprowadzono w oparciu o artykuły naukowe z lat 2017-2022 dostępne online, najnowsze raporty publikowane przez korporacje technologiczne oraz audytowe, a także pozostałe źródła internetowe. Informacje pozyskane zostały również z krajowych aktów prawnych oraz dokumentów publikowanych przez organy Unii Europejskiej. Ograniczeniem badawczym jest brak uwzględnienia branż MŚP i traktowanie tej grupy jako całości. W związku z tym, że zarządzanie MŚP w coraz większym stopniu opiera się na wykorzystaniu systemów informatycznych i przetwarzaniu różnego rodzaju danych, w ramach badania zwrócono uwagę na problematykę związaną z cyberzagrożeniami i wyzwaniami stojącymi przed zarządzającymi przedsiębiorstwami MŚP. Jednym z nich jest konieczność wdrożenia stałego monitorowania bezpieczeństwa cybernetycznego w firmie, niezależnie od wielkości i etapu rozwoju, a także uwzględnianie czynnika ludzkiego na każdym etapie obsługi systemów informatycznych.

**Słowa kluczowe:** cyberbezpieczeństwo, cyfryzacja procesów biznesowych, ochrona danych, zarządzanie bezpieczeństwem

**Kod klasyfikacji JEL:** G32, F50, K24

---

<sup>1</sup> Anna Elżbieta Sawicka, mgr, ul. Kociewska 22A, 87-100 Toruń, Polska, [sawicka.a.e@gmail.com](mailto:sawicka.a.e@gmail.com),  <https://orcid.org/0000-0002-5090-6957>

\* Autor korespondencyjny: Anna Elżbieta Sawicka, [sawicka.a.e@gmail.com](mailto:sawicka.a.e@gmail.com)

## Wprowadzenie

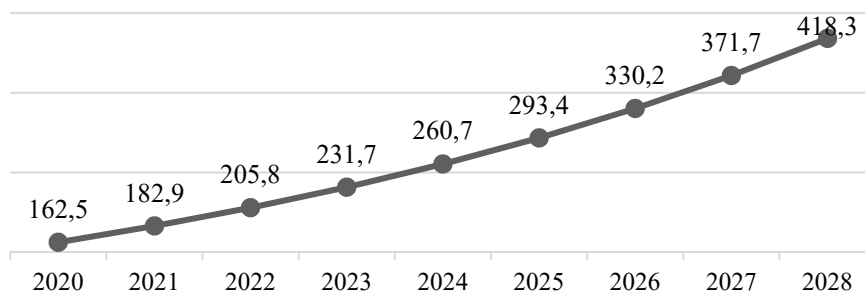
Jednym z aspektów zarządzania współczesną organizacją jest obszar związany z cyfryzacją procesów biznesowych. Wspiera ją m.in. transformacja związana z przechodzeniem na Przemysł 4.0, podczas której znaczące środki inwestycyjne przeznaczane są na cyfryzację, robotyzację i automatyzację procesów w przedsiębiorstwach (Komisja Europejska, 2019). Poza wyraźnymi korzyściami, takimi jak np. podniesienie konkurencyjności, większe możliwości w komunikacji z klientem, obniżenie kosztów czy możliwość szybkiego wprowadzenia innowacyjnych rozwiązań, cyfryzacja niesie też za sobą zagrożenia. Do wirtualnego środowiska przenoszone są zettabajty informacji (Komisja Europejska, 2019), które dotyczą działalności przedsiębiorstw oraz ich klientów. Ten ogrom danych to również środowisko, w którym poruszają się cyberprzestępcy.

Problem cyberbezpieczeństwa dotyka nie tylko duże organizacje, ale także MŚP (Komisja Europejska, 2014), które stanowią większość, bo aż 99,8% wszystkich przedsiębiorstw w Polsce (PARP, 2021). Podobny udział przedsiębiorstw MŚP w ich ogólnej liczbie występuje również w Unii Europejskiej (Komisja Europejska, 2021). Rozwój społeczeństwa informacyjnego podniósł rolę danych do kluczowego zasobu. Jego ochrona, nie tylko na poziomie publicznym, ale również prywatnym, staje się jednym z priorytetów z perspektywy zachowania stabilności światowej gospodarki.

Jest to widoczne chociażby w zakładanych przychodach z rozwoju rynku cyberbezpieczeństwa. Globalne analizy wskazują podwyższenie przychodów z 162,5 mld USD w 2020 roku do aż 418,3 mld USD w roku 2028, gdzie skumulowany średni roczny wzrost przychodów CAGR (Goertz, 2014) w tych latach wynosi 12,5% (Globe News Wire, 2021), gdzie  $V(t_n)$  to wartość przyszła w badanym okresie,  $V(t_0)$  to wartość początkowa w badanym okresie,  $t_n$  to rok końcowy badanego okresu, a  $t_0$  to rok początkowy badanego okresu.

$$CAGR_{t_0, t_n} = \left( \frac{V(t_n)}{V(t_0)} \right)^{\frac{1}{t_n - t_0}} - 1 \quad (1)$$

$$CAGR_{t_{2020}, t_{2028}} = \left( \frac{418,3}{162,5} \right)^{\frac{1}{8}} - 1 \approx 0,125458 \approx 12,5\%$$



**Rysunek 1. Prognozowany przychód z rozwoju rynku cyberbezpieczeństwa (w mld USD) w latach 2020-2028**

Źródło: Opracowanie własne na podstawie danych (Globe News Wire, 2021)

Prognozowane przychody w oparciu o średnią stopę zwrotu z inwestycji w wysokości 12,5% w latach 2020-2028 przedstawiono na Rysunku 1.

Obecnie trudno określić, czy prognozowane wartości znacząco zmieniają się ze względu na konflikt rosyjsko-ukraiński. Warto poczekać na aktualizację danych związaną z wahaniami kursów walutowych i wpływem wprowadzonych sankcji na ten obszar. Koronnym przykładem jest zmiana sytuacji rynkowej przedsiębiorstwa Kaspersky Lab, będącego jednym z liderów rynku oprogramowania antywirusowego na świecie. Wraz z nasileniem konfliktu rosyjsko-ukraińskiego zostały nałożone sankcje (MSWiA, 2022) na założyciela pochodzącego z Rosji, a organizacja mierzy się z problemami związanymi z odpływem partnerów i klientów.

## Zarządzanie bezpieczeństwem – ujęcie teoretyczne

Powstaje zatem pytanie, jak zabezpieczyć się przed cyberzagrożeniami, skoro zdarza się, że oprogramowanie, służące zapobieganiu atakom cybernetycznym, może stać się furtką dla potencjalnych cyberprzestępców. Pojęcie bezpieczeństwa oznacza „stan niezagrożenia” (Słownik Języka Polskiego PWN, 2022). Definicja w kontekście zarządzania przedsiębiorstwem jest niewyczerpująca, gdyż na zarządzanie bezpieczeństwem składa się nie tylko trwanie w braku zagrożenia, ale szereg działań konceptualnych, organizacyjnych i analitycznych w celu przewidywania i zapobiegania potencjalnym niebezpieczeństwom (Kwieciński, 2016). Ponadto bezpieczeństwo należy do wartości warunkujących optymalne funkcjonowanie człowieka, a zaburzenie poczucia bezpieczeństwa będzie skutkowało osłabieniem więzi społecznych i zawężeniem współpracy (Huczek, 2010), co dotyczy zarówno pracowników organizacji, jak również klientów, korzystających z produktów i usług przedsiębiorstwa. Zarządzającym powinno zależeć na utrzymywaniu wysokiego poczucia bezpieczeństwa wśród interesariuszy, jednak za tym powinny iść konkretne działania realnie potwierdzające wysoki poziom bezpieczeństwa w organizacji w różnorodnych obszarach, w tym związanych z cyberbezpieczeństwem.

Encyklopedia PWN przychodzi z rozróżnieniem bezpieczeństwa na bierne i czynne (Encyklopedia PWN, 2022). Bezpieczeństwo bierne to stan przyczyniający się do „złagodzenia następstw awarii lub wypadku”, bezpieczeństwo czynne zaś umożliwia „zmniejszenie ryzyka lub uniknięcie awarii lub wypadków”. Z definicją bezpieczeństwa wiąże się zatem pojęcie ryzyka. Choć ze względu na kontekst pojęcie ryzyka może się różnić, w obszarze ekonomii i zarządzania ryzyko jest określane jako „zdarzenie powodujące możliwość pojawienia się straty” (Gędek, 2018). W cytowanej publikacji przytaczana jest też inna, rozszerzona definicja w odniesieniu do prowadzenia działalności według Dowgiałło (1992), gdzie „ryzyko związane z działalnością gospodarczą oznacza prawdopodobieństwo występowania zdarzeń prowadzących do nieosiągnięcia celu lub do niekorzystnych skutków ubocznych dotyczących tej działalności”. Zatem ryzyko można określić za pomocą metod ilościowych i rachunku prawdopodobieństwa, co umożliwia zarządzanie ryzykiem, a więc „planowe stosowanie polityki, procedur i praktyk zarządczych w ramach zadań dotyczących analizy, wyceny i nadzoru ryzyka” (Stanik et al., 2016).

Analiza rodzaju potencjalnych źródeł zagrożeń oraz ryzyka ich wystąpienia należy do podstawowych zadań z zakresu zarządzania bezpieczeństwem, którego celem jest zapewnienie „stabilności stanu bezpieczeństwa” (Kołodziński, 2009). Ponadto „zarządzanie ryzykiem stanowi integralną część całościowego procesu zarządzania bezpieczeństwem informacji” (Pałęga, 2017). W tym kontekście ważna jest identyfikacja ryzyka, która „obejmuje ustalenie zasobów (aktywów) informacyjnych, zagrożeń i źródeł ich powstawania, podatności oraz potencjalnych skutków i strat zidentyfikowanych incydentów” (Pałęga, 2017). Podobne stanowisko wynika z raportu Najwyższej Izby Kontroli, gdzie wskazano, że obowiązek zarządzania bezpieczeństwem informacji należy realizować „w szczególności w taki sposób, aby wszystkie aktywa informatyczne zostały zidentyfikowane, a także powinien zostać sporządzony i być na bieżąco aktualizowany spis tych aktywów” (NIK, 2019). Zarządzający przedsiębiorstwem powinni zatem zaplanować działania na wypadek zdarzenia niepożądanego oraz następnie stworzyć procedury minimalizujące skutki wystąpienia zagrożenia tak, aby jak najszybciej powrócić do maksymalnego poziomu bezpieczeństwa (Kołodziński, 2009).

Istotne z perspektywy zarządzania bezpieczeństwem w przedsiębiorstwie jest podnoszenie świadomości dotyczącej ryzyka występowania cyberzagrożeń. „Zagrożenie odnosi się do sfery świadomościowej danego podmiotu (człowieka, grupy społecznej, narodu) i oznacza pewien stan psychiki lub świadomości wywołany postrzeganiem zjawisk ocenianych jako niekorzystne lub niebezpieczne. Percepcja zagrożeń przez ten podmiot, tym samym i jego poczucie bezpieczeństwa, stanowi odzwierciedlenie w jego świadomości realnego lub potencjalnego zagrożenia. Oznacza to, że może być niezgodna ze stanem faktycznym” (Kołodziński, 2009). Analizowanie ryzyka zagrożeń i typowanie ich przez jedną osobę lub wąską grupę specjalistów np. w działach IT może być niewystarczające ze względu na ograniczoną percepcję osób pracujących w podobnych warunkach, posiadających ponadprzeciętne umiejętności techniczne w porównaniu z pozostałymi pracownikami. Zachowanie uważności na ryzyko występowania zagrożenia ze strony cyberprzestępców powinno być zatem zadaniem nie tylko specjalistów w tej dziedzinie, ale również właścicieli przedsiębiorstwa, osób zarządzających oraz pozostałych pracowników organizacji (Pławińska & Skulska, 2021). Badania na temat emocji związanych z cyberzagrożeniami wykazały, że zagadnienie cyberbezpieczeństwa niesie za sobą negatywne skojarzenia (Renaud et al., 2021). Do najczęściej wymienianych w próbie badawczej emocji należą te związane z niepewnością. Ponadto cyberzagrożenia powodują niepokój, przytłoczenie i frustrację. Przed wyzwaniem stoją zatem działy HR, dbające o jakość wdrażanych rozwiązań wraz ze szkoleniami, a także działy prawne, których zadaniem jest wdrożenie systemów bezpieczeństwa w przedsiębiorstwie zgodnie z obowiązującym prawem, które w zakresie cyberbezpieczeństwa wciąż ewoluuje.

## **Metodyka badawcza**

W artykule poruszono problematykę zarządzania bezpieczeństwem w oparciu o przegląd literatury naukowej w celu odniesienia się do obszaru bezpieczeństwa

cybernetycznego, stanowiącego nowe wyzwanie w związku z szybkim rozwojem technologii i powstającymi nowymi zagrożeniami w przestrzeni cybernetycznej.

W ramach badania skorzystano z najnowszych badań przedstawionych w dokumentach i raportach z obszaru bezpieczeństwa cybernetycznego, opublikowanych w latach 2020-2022 przez organizacje międzynarodowe, a także korporacje, działające w obszarze technologii i audytu – aby określić obecny stan świadomości zagrożeń cybernetycznych wśród menedżerów zarządzających przedsiębiorstwami MŚP. Autorka także dokonała przeglądu dokumentów legislacyjnych – w tym ustaw krajowych, rozporządzeń Unii Europejskiej – aby określić obecne i przyszłe trendy w zakresie stanowienia prawa i zaleceń w regionie.

Celem badania jest uzyskanie odpowiedzi na pytanie, w jaki sposób przedsiębiorca i kadra zarządzająca powinna przygotować przedsiębiorstwo MŚP do funkcjonowania w obliczu stałego zagrożenia cybernetycznego.

## **Regulacje prawne w zakresie cyberbezpieczeństwa w kontekście funkcjonowania małych i średnich przedsiębiorstw**

Jednym z priorytetów Unii Europejskiej i Komisji Europejskiej jest wykorzystanie potencjału cyfryzacji i technologii informacyjno-komunikacyjnych. Dążenie do wypracowania jednolitych standardów i wytycznych widoczne jest m.in. w strategii „Kształtowanie cyfrowej przyszłości Europy” ogłoszonej w 2020 roku (Komisja Europejska, 2020b). Transformacja cyfrowa będzie obejmować zarówno aspekty gospodarcze, jak i społeczne, prowadząc do wzrostu konkurencyjności, suwerenności gospodarczej i technologicznej. W naturalny sposób również kwestie cyberbezpieczeństwa znalazły się w centrum zainteresowania, zarówno organów unijnych, jak i krajowych.

Jednym z kluczowych dokumentów na poziomie europejskim jest dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, znana jako dyrektywa NIS (Network and Information System Directive), przyjęta 6 lipca 2016 r. (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r.). Był to pierwszy na poziomie Unii Europejskiej akt bezpośrednio poruszający kwestie cyberbezpieczeństwa. Dyrektywa skierowana była do krajów członkowskich, które zobligowano do powołania instytucji i wprowadzenia mechanizmów współpracy w tym zakresie.

W Polsce Dyrektywę NIS implementuje do porządku prawnego Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, która choć doczekała się kilku projektów nowelizacji, w związku z licznymi uwagami środowisk prawniczych i branży IT, wciąż posiada swój pierwotny kształt. W najnowszym projekcie nowelizacji z 25 marca 2022 r. zaproponowano m.in. procedurę uznania dostawcy za dostawcę wysokiego ryzyka, a także zapowiedziano wprowadzenie krajowych programów certyfikacji cyberbezpieczeństwa. Ustawodawca wyraźnie zaznacza potrzebę większej kontroli organów państwa nad dostępem do usług i produktów IT ze względu na wymagania związane z bezpieczeństwem. W uzasadnieniu określa

wymogi „w celu ochrony dostępności, autentyczności, integralności i poufności przechowywanych, przekazywanych lub przetwarzanych danych lub powiązanych funkcji bądź usług oferowanych lub dostępnych za pośrednictwem tych produktów, usług i procesów w trakcie ich całego cyklu życia” (MC, 2022). Ustawodawca zaznacza, że opracowanie ogólnych wymogów cyberbezpieczeństwa obowiązujących dla wszystkich przypadków jest bardzo skomplikowane, dlatego uzyskanie pozytywnej opinii ministerstwa będzie wydawane na mocy decyzji administracyjnej w oparciu o indywidualną analizę przeprowadzoną przez powołane do tego zadania organy.

Sama ustawa dotyczy tylko części przedsiębiorców, koncertując się na podmiotach kluczowych dla działania państwa i gospodarki. Można w niej zidentyfikować pojęcie cyberbezpieczeństwa, które zostało określone jako „odporność systemów informacyjnych na wszelkie działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy” (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa).

Przedsiębiorstwa MŚP najbardziej odczuły wprowadzenie regulacji związanych z ochroną i przetwarzaniem danych klientów i pracowników. Na poziomie Unii Europejskiej wprowadziło ją rozporządzenie 2016/679 (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.), na poziomie krajowym Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Rozwiązanie to objęło wszystkie rodzaje przedsiębiorstw (bez względu na wielkość), które prowadzą działalność na terenie UE, i spowodowało zmiany w ponad 130 ustawach we wszystkich sektorach gospodarki. Postawiło to przedsiębiorstwa MŚP przed dużym wyzwaniem. Wdrożenie wymogów ustawy wymaga bowiem nakładów finansowych, zarówno na fizyczne zabezpieczenie danych osobowych, jak i wirtualne.

Komisja Europejska i Europejska Służba Działań Zewnętrznych (ESDZ) w grudniu 2020 r. przedstawiła strategię UE w zakresie cyberbezpieczeństwa (Komisja Europejska, 2020a). Za główny cel postawiono wzmocnienie odporności Europy wobec cyberzagrożeń oraz zapewnienie przedsiębiorcom i obywatelom możliwości korzystania z godnych zaufania i niezawodnych usług oraz narzędzi cyfrowych. W strategii wskazano konkretne rozwiązania dotyczące wdrażania instrumentów regulacyjnych, inwestycyjnych i politycznych.

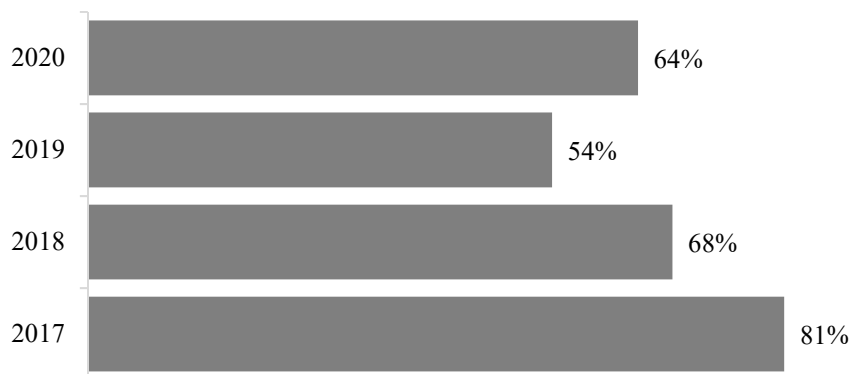
W kontekście MŚP istotny był raport Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA, 2021a), opublikowany listopadzie 2021 r., w którym ogłoszono zalecenia dotyczące bezpieczeństwa właśnie dla tej grupy podmiotów. Określono obszary cyberzagrożeń oraz obszary, które wymagają poprawy poziomu.

Istnieje także wiele inicjatyw nieformalnych, które mają podnosić świadomość związaną z cyberbezpieczeństwem, których zadaniem jest wsparcie przedsiębiorstw w tym zakresie, przede wszystkim w pogłębianiu wiedzy w tej tematyce w czterech podstawowych zakresach: edukacja, badania naukowe, wsparcie dla start-upów i tworzenie partnerstw europejskich (Komisja Europejska, 2020c).

## Obszary cyberzagrożeń w przedsiębiorstwach MŚP

W 2012 roku były dyrektor FBI Robert Mueller wskazał, że w podstawowym wymiarze istnieją dwa rodzaje przedsiębiorstw – te, które już zostały zhakowane, oraz te, które będą zhakowane (Mueller, 2012).

Potwierdzenie tych poglądów można znaleźć w danych o liczbie cyberataków. Z raportu KPMG wynika, że 64% polskich przedsiębiorstw w 2020 roku odnotowało przynajmniej jeden incydent (sytuacja), który był związany z naruszeniem bezpieczeństwa (Rysunek 2). Jest to o 10 punktów procentowych więcej w stosunku do 2019 roku (KPMG, 2021).



**Rysunek 2. Udział przedsiębiorstw, które zarejestrowały przynajmniej jeden incydent bezpieczeństwa w latach 2017-2020**

Źródło: Opracowanie własne na podstawie raportu (KPMG, 2021)

Z kolei według raportu Sophos (2022) ponad 54% polskich przedsiębiorstw odnotowało wzrost liczby cyberataków w pierwszym roku pandemii. Przy czym tylko 22% przedsiębiorstw zgłaszało, że ataki są zbyt zaawansowane jak na ich możliwości. W raporcie CERT Polska z 2020 roku można odszukać informację o 10 420 zarejestrowanych (zgłoszonych) incydentach cyberbezpieczeństwa, co stanowi wzrost o 60,7% w porównaniu z rokiem ubiegłym (CERT Polska, 2020).

Rodzajów cyberzagrożeń jest wiele i ich lista jest wciąż uzupełniana (Wasilewski, 2017; Nowak, 2010). Raport ENISA z 2021 roku wyróżnia dziewięć podstawowych typów (ENISA, 2021d):

- ransomware – cyberszantaż, ataki z użyciem złośliwego oprogramowania na sieci w celu blokowania danych z żądaniem okupu;
- malware – złośliwe oprogramowanie;
- cryptojacking – kradzież kryptowalut, przestępca wykorzystuje komputer ofiary do generowania kryptowalut;
- zagrożenia związane z pocztą elektroniczną;
- ataki na dane – naruszenie danych, wyciek danych, wyłudzenie danych (phishing);

- zagrożenia dla dostępności i integralności danych, np. ataki typu DDoS – czyli uniemożliwienie dostępu do strony/usługi poprzez sztuczne generowanie wzmożonego ruchu przez boty czy przejęcie kontroli (botnety);
- dezinformacja – fałszywe wiadomości;
- zagrożenia inne niż złośliwe oprogramowanie – błędy ludzkie, nieprawidłowe konfiguracje systemów, wypadki mające wpływ na systemy informatyczne;
- ataki na łańcuchy dostaw.

Według danych CERT Polska w 2020 roku najczęstszym typem ataków był phishing, który stanowił aż 73,15% wszystkich obsługiwanych incydentów i dotknął 29% polskich przedsiębiorstw (CERT Polska, 2020).

Raport przygotowany przez korporację Siemens we współpracy z Ministerstwem Cyfryzacji wskazuje, że jednym z głównych zagrożeń dla przedsiębiorstwa jest to płynące od wewnątrz, czyli płynące z najbliższego otoczenia (Siemens, 2020). Zagrożeniem mogą być pracownicy, zarówno obecni, jak i byli, partnerzy oraz podwykonawcy (Rysunek 3). Działania te mogą być umyślne, nieumyślne lub spowodowane zaniedbaniem.

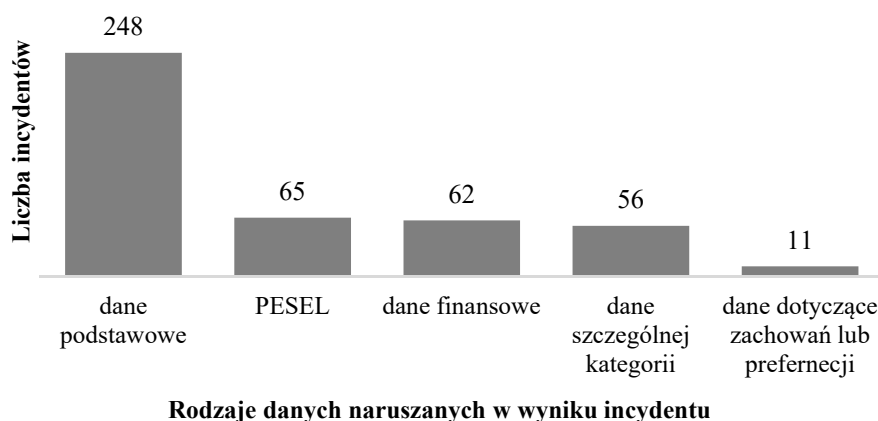


**Rysunek 3. Źródła zagrożeń wewnętrznych dla bezpieczeństwa przedsiębiorstwa**

Źródło: Opracowanie na podstawie danych z raportu (Siemens, 2020)

Dotkliwe pod kątem prawnym, finansowym i wizerunkowym dla przedsiębiorstw są wycieki danych osobowych. W rocznym sprawozdaniu za rok 2020 Prezes UODO poinformował o wpłynięciu 6442 skarg, z czego 2519 dotyczyło przedsiębiorstw z sektora prywatnego (UODO, 2021). Niosły one ze sobą różne konsekwencje, od upomnień do kar grzywny przekraczających milion złotych. Warto wspomnieć, że wdrożenie polityki związanej z RODO deklarują praktycznie wszystkie przedsiębiorstwa (Cyfrowa Polska, 2022). Wśród typów incydentów związanych z naruszeniem ochrony danych osobowych według raportu ZFODO za 2021 rok aż 83,17% wynika z działań pracowników lub współpracowników organizacji (ZFODO, 2022). Do najczęściej naruszanych danych należały dane podstawowe – 248 incydentów (Rysunek 4).





**Rysunek 4. Rodzaje naruszanych danych i częstość występowania incydentów w 2021 roku**

Źródło: Opracowanie na podstawie (ZFODO, 2022)

Naruszenie danych związanych z bazą numerów PESEL nastąpiło 65 razy, natomiast dane finansowe były przedmiotem incydentu aż 62 razy. Bezpieczeństwo danych szczególnej kategorii – czyli tzw. danych wrażliwych, wśród których znajdują się informacje szczególnie chronione, tj. dane o stanie zdrowia, preferencjach seksualnych czy przekonaniach politycznych bądź religijnych (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r.) – było naruszone aż 56 razy w 2021 roku.

### **Wyzwania w przedsiębiorstwach MŚP w zakresie zarządzania cyberbezpieczeństwem**

Dynamiczne zmiany ostatniej dekady postawiły przedsiębiorstwa MŚP przed wieloma nowymi wyzwaniami. Dostosowanie się do wymogów RODO, proces transformacji do Przemysłu 4.0, przyspieszona cyfryzacja związana z pandemią COVID-19 – wszystko to wymagało od osób zarządzających podjęcia kroków mających przystosować przedsiębiorstwa do nowej rzeczywistości.

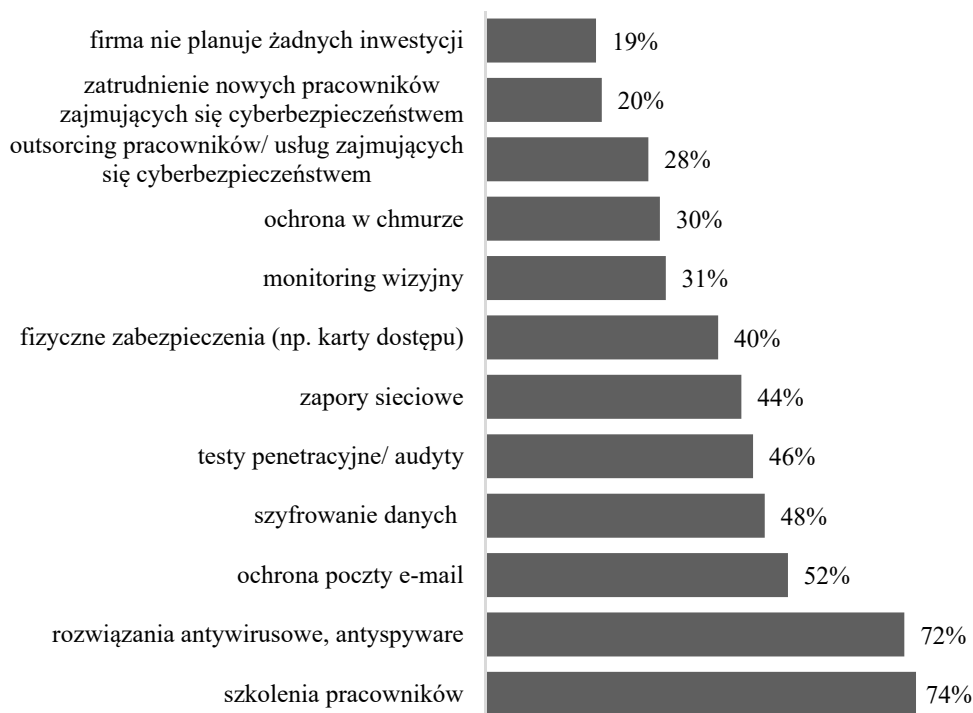
W latach 90. XX wieku uczelnia wojskowa United States Army War College wprowadziła koncepcję VUCA, jako określenie sytuacji po zakończeniu zimnej wojny. Na początku XXI wieku termin ten coraz częściej był stosowany do ogólnego określenia sytuacji w kontekście przywództwa strategicznego, w tym w odniesieniu do przedsiębiorstw. Akronim VUCA (USAHEC, 2021, za: Barber, 1992) pochodzi od słów:

- Volatility – zmienność;
- Uncertainty – niepewność;
- Complexity – złożoność;
- Ambiguity – niejednoznaczność.

Określenie to dobrze wpisuje się w realia, w jakich przyszło działać współczesnym menedżerom, również pod kątem cyberbezpieczeństwa. Przyspieszona cyfryzacja wymaga planowania kosztów, dobrej organizacji zespołu i nowych kompetencji pracowników.

Zwiększona aktywność przedsiębiorstw w ostatnich dwóch latach w sferze cyfrowej wymuszona została również przez kryzys związany z COVID-19 (ENISA, 2021a). Wiele podmiotów musiało wprowadzić zmiany w organizacji swojej działalności i przenieść pracowników do pracy zdalnej. Pociągnęło to za sobą szereg komplikacji, chociażby szybkie dostosowanie się do logowania do systemów organizacji spoza siedziby. Organizowanie w pośpiechu stanowisk pracy zdalnej bez przygotowania nowoczesnych systemów do uwierzytelniania użytkownika, często opartych na przestarzałych formach opierających się na statycznych danych dostępowych, takich jak chociażby hasła, nazwy użytkownika, SMS-y czy nawet kody QR, otworzyło wiele możliwości do przeprowadzenia cyberataków.

Trend pracy zdalnej ukazał też potrzebę stworzenia nowych procedur i rozwiązań, które zabezpieczyłyby przedsiębiorstwa w dłuższym okresie przed zagrożeniami. Pociągnęło to również za sobą zwiększenie wydatków na cyberbezpieczeństwo. W raporcie *Cyberbezpieczeństwo polskich przedsiębiorstw 2021* przygotowanym przez CyberMadeInPoland wskazano, w jaki sposób w najbliższym roku środki na cyberbezpieczeństwo zamierzają wydatkować przedsiębiorstwa MŚP (Computerworld, 2022). Fundusze planowe są przewidywane głównie na szkolenia pracowników, a także rozwiązania antywirusowe oraz antyspyware (Rysunek 5).



**Rysunek 5. Planowane wydatki MŚP w zakresie cyberbezpieczeństwa**

Źródło: Opracowano na podstawie danych (CyberMadeInPoland, 2021)

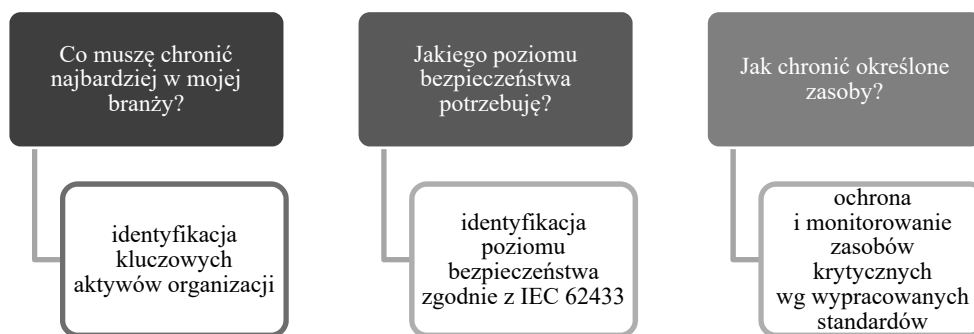
Wyzwania w obszarze cyberbezpieczeństwa według poradnika ENISA z 2021 roku podzielono na trzy główne obszary (ENISA, 2021b):

- Ludzie – jako kluczowy zasób w ochronie przedsiębiorstwa. W rekomendacji wskazano szkolenia z zakresu cyberbezpieczeństwa oraz technik bezpiecznego dzielenia się z poufnymi informacjami i danymi z partnerami biznesowymi.
- Procesy – obejmujące procedury takie, jak m.in. audyty, reagowanie na incydenty, politykę tworzenia bezpiecznych haseł, aktualizację oprogramowania, ochronę danych.
- Aspekty techniczne – oprogramowanie antywirusowe, szyfrowanie, monitorowanie bezpieczeństwa, tworzenie kopii zapasowych.

W raporcie Siemens przedstawiono z kolei holistyczne podejście (Holistic Security Concept) do obszarów wymagających ochrony w organizacji, które obejmuje poniższe aspekty (Siemens, 2020):

- infrastruktura IT,
- obsługa incydentów,
- usprawnienie procesów,
- funkcje bezpieczeństwa,
- zwiększenie świadomości.

W tym ujęciu istotna jest odpowiedź na trzy pytania przedstawione na Rysunku 6.



**Rysunek 6. Podstawowe pytanie dotyczące cyberbezpieczeństwa w organizacji**

Źródło: Opracowanie własne na podstawie danych (Siemens, 2020)

Aby zbudować efektywny system zarządzania bezpieczeństwem cybernetycznym, należy celnie wytypować aktywa przedsiębiorstwa, które wymagają ochrony, a następnie przeprowadzić analizę ilościową i jakościową w celu oszacowania ryzyka występowania zagrożenia, a także potencjalnych konsekwencji wystąpienia ataku. Ważne jest też stałe monitorowanie potencjalnych luk w systemie ze względu na zmieniające się czynniki wewnętrzne w organizacji, a także czynniki zewnętrzne (Pałęga, 2017).

Wśród czynników wewnętrznych można zidentyfikować:

- zmiany kadrowe,
- wpływ kultury organizacyjnej,
- nowe kluczowe aktywa,

- zmiany w zakresie strategii rynkowej,
- zmiany struktury właścicielskiej.

Wśród istotnych czynników wewnętrznych, które zarządzający przedsiębiorstwem powinni monitorować w celu ciągłego poprawiania systemu bezpieczeństwa cybernetycznego, znajdują się takie, których występowanie będzie sporadyczne (jeden raz na kilka lat) lub bardzo częste (codziennie lub kilka razy w ciągu miesiąca). Zmiany struktury właścicielskiej dokonują się rzadko, ale w istotny sposób wpływają na zarządzanie bezpieczeństwem cybernetycznym przedsiębiorstwa. Wraz z fuzją, sprzedażą czy inną transformacją struktury właścicielskiej pojawia się wiele wyzwań związanych z ochroną danych, dostępem do kluczowych aktywów w formie fizycznej lub wirtualnej. Dołączenie nowego pracownika, podwykonawcy lub ich odejście powinny powodować uruchomienie odpowiedniej procedury związanej z dostępem do kluczowych aktywów na odpowiednim poziomie. Przynieszone do organizacji nawyki związane z użytkowaniem nowych sprzętów lub oprogramowania należą do czynników związanych z kulturą organizacyjną przedsiębiorstwa, które również powinny podlegać cyklicznej ocenie ryzyka. Wszelkie zmiany dotyczące ekspansji lub wycofywania się z rynku, a także związane z pojawieniem się nowych kluczowych aktywów, które podlegają ochronie, wymagają weryfikacji istniejących procedur bezpieczeństwa.

Nie mniej ważna z punktu widzenia zarządzania przedsiębiorstwem jest analiza otoczenia zewnętrznego, w obszarach takich, jak:

- zmiany stopnia dla bezpieczeństwa cybernetycznego państwa,
- zmiany legislacyjne,
- zmiany rynkowe,
- postęp technologiczny.

Obserwowanie standardu działań innych przedsiębiorstw, podwykonawców czy partnerów biznesowych, szczególnie z tej samej branży, może stanowić dobrą praktykę, którą warto wprowadzić do własnego przedsiębiorstwa. Postęp cywilizacyjny spowodował trend wdrażania nowych rozwiązań technologicznych do organizacji zarówno jako nowe produkty czy usługi, jak również jako systemy wspierające zarządzanie procesami w przedsiębiorstwie. Wdrażane do organizacji nowinki technologiczne powinny zostać przeanalizowane pod kątem bezpieczeństwa cybernetycznego (Mirtsch et al., 2021).

Ponadto procesy zarządcze w obszarze cyberbezpieczeństwa mogą wymagać ulepszenia wraz ze zmianami legislacyjnymi, nakładającymi na właścicieli przedsiębiorstw oraz zarządzających nimi menedżerów nowe obowiązki. Warto również śledzić informacje rządowe dotyczące alertów o zagrożeniu terrorystycznym (Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych). W przypadku możliwości wystąpienia takiego zagrożenia, na mocy ustawy, rządzący wprowadzają jeden z czterech stopni alarmowych lub stopni alarmowych CRP dla zagrożeń w cyberprzestrzeni. Wprowadzenie stopnia alarmowego lub stopnia alarmowego CRP stanowi podstawę do wprowadzania procedur bezpieczeństwa, a także związanych z zarządzaniem kryzysowym, zarówno wśród instytucji publicznych, organizacji, jak i przedsiębiorstw.

ENISA w raporcie na temat cyberbezpieczeństwa wskazała również największe wyzwania, jakie stoją przed cyberbezpieczeństwem (ENISA, 2021c):

- niska świadomość cyberzagrożeń,
- nieodpowiednia ochrona wrażliwych i mających kluczowe znaczenie dla przedsiębiorstwa informacji,
- brak budżetu na wdrażanie środków cyberbezpieczeństwa,
- brak dostępu do fachowej wiedzy i personelu,
- brak odpowiednich wytycznych dostosowanych do MŚP,
- przejście na tryb pracy zdalnej,
- niskie wsparcie dla kadry zarządzającej.

Według Coleman Parkes Research głównymi barierami na drodze do poprawy bezpieczeństwa w IT w przedsiębiorstwach MŚP są koszty zatrudnienia specjalistów ds. cyberbezpieczeństwa oraz koszty technologii i usług (Rysunek ) (Platforma Przemysłu Przyszłości, 2022; Coleman Parkes Research, 2021).



**Rysunek 7. Główne przeszkody na drodze do poprawy bezpieczeństwa IT w przedsiębiorstwach MŚP**

Źródło: Opracowanie na podstawie danych (Coleman Parkes Research, 2021)

Dla zarządzających przedsiębiorstwami MŚP problemem zatem jest wyodrębnienie budżetu na poprawienie jakości i bezpieczeństwa infrastruktury technologicznej w organizacji. Z danych GUS za 2019 rok (GUS, 2020) wynika, że MŚP to 99,8% wszystkich przedsiębiorstw w Polsce, jednak aż 97% wszystkich przedsiębiorstw w Polsce stanowią mikroprzedsiębiorstwa, 2,2% to przedsiębiorstwa małe, zaś jedynie 0,7% to przedsiębiorstwa średnie. Ponadto w roku 2020 w aż 73,54% mikroprzedsiębiorstw zatrudniona była tylko jedna osoba, a nadwyżka przychodów nad kosztami na

jedno mikroprzedsiębiorstwo wyniosła 87,3 tys. zł (GUS, 2021). Obawa dotycząca niewystarczających środków na wdrożenie systemów bezpieczeństwa cybernetycznego jest zatem uzasadniona, szczególnie w gronie mikroprzedsiębiorców.

## Podsumowanie

MŚP w Polsce, jak i w Europie stoi przed sporym wyzwaniem. Dynamika zmian związanych z cyberbezpieczeństwem jest na tyle duża, że wymaga stałych działań po stronie osób zarządzających. Głównym elementem powinno być ogólne wypracowanie strategii możliwej i realnej do wdrożenia w strukturze danej organizacji. Za nią powinny pójść wytyczne i procedury, jasne i precyzyjne dla osób, które mają je wdrażać. W samym funkcjonowaniu należałoby postawić na wyrobienie nawyków w pracownikach, gdyż oni są najczęściej narażeni na ataki. Oparcie się wyłącznie na zabezpieczeniu systemów informatycznych nie wystarczy do osiągnięcia pożądanego efektu.

Z tego rodzi się pytanie – który z działów przedsiębiorstwa powinien wziąć na siebie główny ciężar wprowadzania, monitorowania i korygowania działań związanych z cyberbezpieczeństwem. Sam impuls do działania powinien wyjść od właściciela i zarządu. Jednakże w działaniu operacyjnym istotne jest stałe monitorowanie i reakcja na zagrożenia. Przy większych podmiotach część tych zadań mogą realizować działy kadrowe we współpracy z działem IT. Przy mniejszych organizacjach to zadanie bez wątpienia spoczywać będzie na osobach zarządzających lub właścicielach.

Z tej perspektywy tylko podejście systemowe w powiązaniu ze specyfiką danej branży, kultury organizacyjnej i już zastanych procesów pozwoli na stworzenie planu efektywnej ochrony przed cyberzagrożeniami.

## Literatura

- Barber, H. F. (1992). Developing Strategic Leadership: The US Army War College Experience. *Journal of Management Development*, 11(6), 4-12. DOI: 10.1108/02621719210018208
- CERT Polska. (2020). *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska*. <https://cert.pl/raporty-roczne/>
- Coleman Parkes Research. (2021). *Telcos: Protect Your SMB Customers*. Allot.
- Computerworld. (2022). *Cyberbezpieczeństwo polskich firm 2021*. CyberMadeinPoland, Polski Klaster Cyberbezpieczeństwa. <https://www.computerworld.pl/whitepaper/3727-Cyberbezpieczenstwo-polskich-firm-2021.html>
- Cyfrowa Polska. (2022). *Cyberbezpieczeństwo w Polsce w 2021 r.: cyberataki na urządzenia końcowe*. [https://cyfrowapolska.org/pl/raport\\_cyber2021/](https://cyfrowapolska.org/pl/raport_cyber2021/)
- Dowgiałło, Z. (1992). Pojęcie, podział i kierunki eliminowania ryzyka w działalności przedsiębiorstwa rolniczego. W: Z. Dowgiałło (Red.), *Niepewność i ryzyko w działalności przedsiębiorstwa rolniczego. Wybrane problemy* (s. 17-21). Polska Akademia Nauk – Instytut Badań Systemowych.
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194/1, 19.7.2016).
- Encyklopedia PWN. (2022). *Bezpieczeństwo*. <https://encyklopedia.pwn.pl/encyklopedia/bezpiecze%C5%84stwo.html>
- Encyklopedia Zarządzania. (2022). *CAGR*. z <https://mfiles.pl/pl/index.php/CAGR>

- ENISA. (2021a). *Cybersecurity for SMEs – Challenges and Recommendations*. Europejska Agencja ds. Cyberbezpieczeństwa ENISA. <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>
- ENISA. (2021b). *Przewodnik po cyberbezpieczeństwie dla MŚP*. Europejska Agencja ds. Cyberbezpieczeństwa ENISA. <https://www.gov.pl/web/baza-wiedzy/cyberbezpieczna-firma--mamy-poradnik>
- ENISA. (2021c). *Raising Awareness of Cybersecurity*. Europejska Agencja ds. Cyberbezpieczeństwa ENISA. <https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity>
- ENISA. (2021d). *Threat Landscape 2021*. Europejska Agencja ds. Cyberbezpieczeństwa ENISA. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>
- Gędek, S. (2018). Definiowanie ryzyka. *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, 513, 119-130. [https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-e19274fc-72f8-49e6-a092-47b61e8cc835/c/PN\\_513\\_Nowak\\_Rachunkowosc\\_Czesc12.pdf](https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-e19274fc-72f8-49e6-a092-47b61e8cc835/c/PN_513_Nowak_Rachunkowosc_Czesc12.pdf).  
DOI: 10.15611/pn.2018.513.11
- Globe News Wire. (2021). *Global Cybersecurity Market Size to Grow at a CAGR of 12.5% from 2021 to 2028*. <https://www.globenewswire.com/en/news-release/2021/03/17/2194254/0/en/Global-Cybersecurity-Market-Size-to-Grow-at-a-CAGR-of-12-5-from-2021-to-2028.html>
- Goertz, R. K. (2014). *Encyclopedia of Education Economics & Finance*. SAGE Publications. <https://sk.sagepub.com/reference/encyclopedia-of-education-economics-and-finance/i2379.xml>  
DOI: 10.4135/9781483346595
- GUS. (2020). *Działalność przedsiębiorstw niefinansowych w 2019 r.* Główny Urząd Statystyczny. [https://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5502/2/16/1/dzialalnosc\\_przedsiębiorstw\\_niefinansowych\\_w\\_2019.pdf](https://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5502/2/16/1/dzialalnosc_przedsiębiorstw_niefinansowych_w_2019.pdf)
- GUS. (2021). *Działalność przedsiębiorstw o liczbie pracujących do 9 osób w 2020 r.* Główny Urząd Statystyczny. [https://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5502/21/9/1/dzialalnosc\\_przedsiębiorstw\\_o\\_liczbie\\_pracujacych\\_do\\_9\\_osob\\_w\\_2020\\_roku.pdf](https://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5502/21/9/1/dzialalnosc_przedsiębiorstw_o_liczbie_pracujacych_do_9_osob_w_2020_roku.pdf)
- Huczek, M. (2010). Problematyka zarządzania bezpieczeństwem w organizacjach samorządu terytorialnego i szkołach wyższych. *Zeszyty Naukowe Wyższej Szkoły Humanitas. Zarządzanie*, 2/2010, 96-102.
- Incydenty ochrony danych osobowych 2021 (2022). *Związek Firm Ochrony Danych Osobowych ZFODO*. [https://www.zfodo.org.pl/wp-content/uploads/2022/01/raport\\_zfodo\\_2021-1.pdf](https://www.zfodo.org.pl/wp-content/uploads/2022/01/raport_zfodo_2021-1.pdf)
- Kołodziński, E. (2009). *Wprowadzenie do zarządzania bezpieczeństwem*. <http://www.uwm.edu.pl/mkzk/download/wprowadzenie.pdf>
- Komisja Europejska. (2014). *Rozporządzenie Komisji (UE) Nr 651/2014*. <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:02014R0651-20170710&from=EN>
- Komisja Europejska. (2019). *Priorytety Komisji Europejskiej*. [https://ec.europa.eu/info/strategy/priorities-2019-2024\\_pl](https://ec.europa.eu/info/strategy/priorities-2019-2024_pl)
- Komisja Europejska. (2020a). *Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Nowa strategia przemysłowa dla Europy*. <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0102&from=EN>
- Komisja Europejska. (2020b). *Kształtowanie cyfrowej przyszłości Europy*. <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52020DC0067>
- Komisja Europejska. (2020c). *Strategia MŚP na rzecz zrównoważonej i cyfrowej Europy*. [https://ec.europa.eu/transparency/documents-register/detail?ref=COM\(2020\)103&lang=pl](https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2020)103&lang=pl)
- Komisja Europejska. (2020d). *Wspólny komunikat do Parlamentu Europejskiego i Rady. Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę*. <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020JC0018&from=EN>
- Komisja Europejska. (2021). *Annual Report on European SMEs 2020/2021*. <https://op.europa.eu/pl/publication-detail/-/publication/849659ce-dadf-11eb-895a-01aa75ed71a1>
- Komisja Europejska. (2022). *Europejski akt w sprawie chipów*. [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-chips-act\\_pl](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_pl)
- KPMG. (2021). *Barometr cyberbezpieczeństwa. COVID-19 przyspiesza cyfryzację firm*. <https://home.kpmg/pl/pl/home/insights/2021/04/raport-barometr-cyberbezpieczenstwa-2020-covid-19-przyspiesza-cyfryzacje-firm.html>

- Kwieciński, M. (2016). Zarządzanie bezpieczeństwem działalności przedsiębiorstwa – zarys problematyki. *Prace Naukowo-Dydaktyczne Państwowej Wyższej Szkoły Zawodowej im. Stanisława Pigoń w Krośnie*, 70, 149-170.
- MC. (2022). *Uzasadnienie nowelizacji ustawy z dnia 25 marca 2022 r.* Ministerstwo Cyfryzacji. <https://legislacja.rcl.gov.pl/projekt/12337950/katalog/12716639#12716639>
- Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021). *Information Security Management in ICT and Non-ICT Sector Companies: A Preventive Innovation Perspective*. *Computers & Security*. <https://www.sciencedirect.com/science/article/pii/S0167404821002078>. DOI: 10.1016/j.cose.2021.102383
- MSWiA. (2022). *Lista osób i podmiotów objętych sankcjami*. <https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami>
- Mueller, R. S. (2012). *Speech. RSA Cyber Security Conference San Francisco, 1.03.2012*. <https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies>
- NIK. (2019). *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego*. <https://www.nik.gov.pl/plik/id,20027,vp,22647.pdf>
- Nowak, M. (2010). Cybernetyczne przestępstwa – definicje i przepisy prawne. *Biuletyn EBIB* 4/2010(113).
- Siemens. (2020). *Od audytu do bezpiecznej infrastruktury. Cyberbezpieczeństwo w praktyce*. <https://www.2ee.pw.edu.pl/wp-content/uploads/2020/06/Graniszewski-siemens-white-paper.pdf>
- Słownik Języka Polskiego PWN. (2022). *Bezpieczeństwo*. <https://sjp.pwn.pl/slowniki/bezpiecze%C5%84stwo.html>
- Pałęga, M. (2017). Zarządzanie ryzykiem bezpieczeństwa informacji w świetle wymagań normatywnych. *Systems Supporting Production Engineering*, 6(9), 58-70.
- PARP. (2021). *Raport o stanie sektora małych i średnich przedsiębiorstw w Polsce 2021*. <https://www.parp.gov.pl/component/publications/publication/raport-o-stanie-sektora-malych-i-srednich-przedsiębiorstw-w-polsce-2021>
- Platforma Przemysłu Przyszłości. (2022). *Cyberprzestępstwa w MŚP*. <https://przemyslprzyszlosci.gov.pl/cyberprzestepstwa-w-msp/>
- Pławińska, W., & Skulska, J. (2021). *Człowiek jako najsłabsze ogniwo bezpieczeństwa informacyjnego*. <https://nsz.wat.edu.pl/pdf-134812-65745?filename=Man%20as%20the%20weakest%20link.pdf>. DOI: 10.37055/nsz/134812
- Renaud, K., Zimmermann, V., Schürmann, T., & Böhm, C. (2021). Exploring Cybersecurity-Related Emotions and Finding That They Are Challenging to Measure. *Humanities and Social Sciences Communications*, 8(75), 1-17. DOI: 10.1057/s41599-021-00746-5
- 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) (Dz. Urz. UE L 119/1, 4.5.2016). <https://uodo.gov.pl/pl/404/224> <https://uodo.gov.pl/pl/file/727>
- Sophos. (2022). *The IT Security Team: 2021 and Beyond. Badanie na 100 firmach z Polski*. <https://www.sophos.com/en-us/whitepaper/sophos-it-security-team-2021>
- Stanik, J., Napiórkowski, J., & Hoffman, R. (2016). *Zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem organizacji*. Wojskowa Akademia Techniczna. [https://www.researchgate.net/publication/310607359\\_Zarządzanie\\_ryzykiem\\_w\\_systemie\\_zarządzania\\_bezpieczeństwem\\_organizacji](https://www.researchgate.net/publication/310607359_Zarządzanie_ryzykiem_w_systemie_zarządzania_bezpieczeństwem_organizacji). DOI: 10.18276/epu.2016.123-30
- USAHEC. (2021). *Who First Originated the Term VUCA (Volatility, Uncertainty, Complexity and Ambiguity)?*. US Army Heritage & Education Center at Carlisle Barracks. <https://usawc.libanswers.com/faq/84869>
- Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. 2016 poz. 904).
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000).
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).
- Wasilewski, J. (2017). *Cyberprzestępczość – wybrane aspekty prawnekarne i kryminalistyczne*. Praca doktorska. [https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/6538/1/J\\_Wasilewski\\_Cyberprzestepczosc.pdf](https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/6538/1/J_Wasilewski_Cyberprzestepczosc.pdf)



**Wkład autorów:** 100%.

**Konflikt interesów:** Brak konfliktu interesów.

**Źródła finansowania:** Brak finansowania zewnętrznego badań.

## **CYBERSECURITY AS A CONTEMPORARY CHALLENGE IN THE MANAGEMENT OF SMALL AND MEDIUM ENTERPRISES**

**Abstract:** With the development of technology and communication tools, the issue of cyber security has become relevant from the perspective of organizational management. The purpose of the article is to analyze the functioning of SME enterprises to identify the most common cyberattacks and how to prepare an SME enterprise to function in relation to the risk of a cyber threat. The analysis was based on academic articles from 2017-2022 available online, recent reports published by technology and audit companies, and other online sources. Information was also extracted from national legislation and documents published by European Union bodies. The limitation of the research is the lack of consideration of SME industries and the treatment of this group as a whole. With SME management increasingly relying on the use of information systems and the processing of various types of data, the study highlighted the issues related to cyber threats and the challenges facing SME business managers.

**Keywords:** cybersecurity, digitization of business processes, data protection, security management

Articles published in the journal are made available under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License. Certain rights reserved for the Czestochowa University of Technology.

