Bezpieczeństwo cyfrowe w szkolnictwie: od zagrożeń do zarządzania systemowego

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU
MAŁOPOLSKA

Bezpieczeństwo cyfrowe w szkolnictwie: od zagrożeń do zarządzania systemowego

Publikacja współfinansowana ze środków Unii Europejskiej w ramach Krajowego Planu Odbudowy i Zwiększenia Odporności, inwestycja A3.1.1 Wsparcie rozwoju nowoczesnego kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie.

Przedsięwzięcie: Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych.

Członkowie zespołu badawczego

dr Bartłomiej Balsamski

dr hab. Magdalena Jelonek, prof. UEK

mgr Sylwia Kołdras

dr Piotr Kopyciński

mgr Marcin Kukiełka

mgr Magdalena Nalepa-Rybarska

mgr Wojciech Pelowski

mgr inż. Wojciech Sypek

mgr Izabela Władyka

mgr Cecylia Zięba

Rysunek na okładce został wygenerowany przy użyciu AI.

Kraków 2026

Spis treści

Wprowadzenie....4

1. Cyberbezpieczeństwo w szkolnictwie....6

2. Dokumenty strategiczne: kontekst prawny i standardy krajowe dot. cyberbezpieczeństwa w szkołach....9

   2.1. Kwestie cyberbezpieczeństwa w szkołach zawarte w aktach prawnych UE....9
   2.2. Kwestie cyberbezpieczeństwa w szkołach zawarte w aktach prawnych PL....12
   2.3. Zadania szkół wg. ustawy o krajowym systemie cyberbezpieczeństwa (KSC)....13
   2.4. Podsumowanie: mapa kompetencji decydentów szkolnych z mapowaniem do aktów UE/PL....14

3. Zagrożenia i wyzwania cyberbezpieczeństwa....16

   3.1. Skala i charakter zagrożeń cyberbezpieczeństwa....16
   3.2. Zagrożenia w szkołach....22
   3.3. Rodzaje cyberataków na szkoły....25

4. Analiza literatury i istniejących modeli kompetencji w zakresie cyberbezpieczeństwa w szkołach....28

   4.1. Podział modeli kompetencji....28
   4.2. Świadomość cyberzagrożeń i poziom kompetencji cyfrowych....30
   4.3. Wyniki badań i ich analiza: gdzie jesteśmy i dlaczego?....31
   4.4. Bariery rozwojowe....32

5. Benchmark, dobre i złe praktyki w zakresie kompetencji....34

   5.1. Estonia – model cyfrowego państwa i cyberbezpieczeństwa w edukacji....34
   5.2. Cyfrowe BHP w szkołach. Zasady i zagrożenia – spojrzenie praktyka....38

6. Analiza wyników mini audytów szkół....43

7. Propozycja standardu (model) cyberbezpieczeństwa w szkołach....60

8. Rekomendacje w zakresie poprawy kompetencji cyberbezpieczeństwa współczesnej szkoły....63

Bibliografia....65

Wprowadzenie

Postępująca cyfryzacja edukacji sprawia, że szkoły coraz częściej funkcjonują jako złożone środowiska informacyjne. Technologie cyfrowe są wykorzystywane nie tylko podczas lekcji, ale również w administracji, komunikacji z rodzicami, zarządzaniu dokumentacją, ocenianiu, rekrutacji, organizacji pracy nauczycieli oraz przechowywaniu danych uczniów. Oznacza to, że placówki oświatowe stają się częścią cyberprzestrzeni, a ich bezpieczeństwo zależy zarówno od jakości infrastruktury technicznej, jak i od świadomości oraz kompetencji osób, które z niej korzystają.

Cyberbezpieczeństwo w szkolnictwie nie może być rozumiane wyłącznie jako problem techniczny. Ochrona systemów informatycznych, sieci, danych osobowych i urządzeń jest bardzo ważna, ale równie istotne są procedury organizacyjne, odpowiedzialność kadry zarządzającej, przygotowanie nauczycieli, edukacja uczniów oraz współpraca z instytucjami zewnętrznymi. Szkoła jest miejscem, w którym codziennie przetwarzane są dane wrażliwe, a jednocześnie korzystają z niej dzieci i młodzież, czyli grupa szczególnie podatna na zagrożenia cyfrowe.

Współczesne zagrożenia obejmują między innymi ataki phishingowe, wycieki danych, przejęcia kont, złośliwe oprogramowanie, cyberprzemoc, dezinformację, naruszenia prywatności oraz nieuprawniony dostęp do szkolnych systemów. Skutki takich incydentów wykraczają poza sferę techniczną. Mogą prowadzić do zakłócenia pracy szkoły, utraty zaufania rodziców i uczniów, odpowiedzialności prawnej, strat finansowych oraz zagrożenia bezpieczeństwa psychicznego i społecznego uczniów.

Celem niniejszego raportu jest przedstawienie cyberbezpieczeństwa w szkolnictwie jako zagadnienia systemowego, wymagającego współdziałania administracji publicznej, organów prowadzących, dyrektorów szkół, nauczycieli, uczniów, rodziców oraz wyspecjalizowanych instytucji. Szczególną uwagę należy zwrócić na rolę zarządzania szkołą, ponieważ to dyrektorzy i kadra kierownicza odpowiadają za organizację bezpiecznego środowiska edukacyjnego, wdrażanie procedur, rozwijanie kompetencji pracowników oraz reagowanie na incydenty.

Cyberbezpieczeństwo w edukacji powinno być traktowane jako proces ciągły, a nie jednorazowe działanie. Skuteczna ochrona wymaga regularnej analizy ryzyka, aktualizacji zabezpieczeń, szkoleń, jasnego podziału odpowiedzialności oraz budowania kultury bezpieczeństwa cyfrowego. Tylko takie podejście pozwala szkołom nie tylko reagować na zagrożenia, lecz także przygotowywać uczniów do świadomego, odpowiedzialnego i bezpiecznego uczestnictwa w życiu społecznym, edukacyjnym i zawodowym w warunkach cyfrowej transformacji.

W pierwszym rozdziale przedstawiono ogólne założenia cyberbezpieczeństwa w szkolnictwie. Omówiono w nim podstawowe pojęcia, takie jak cyberbezpieczeństwo, cyberzagrożenie, incydent oraz cyberodporność. Rozdział wskazuje również, że

bezpieczeństwo cyfrowe szkół powinno być analizowane nie tylko przez pryzmat technologii, lecz także organizacji pracy, odpowiedzialności osób zarządzających, świadomości użytkowników oraz zdolności placówki do zapobiegania, wykrywania i reagowania na incydenty.

Drugi rozdział poświęcono dokumentom strategicznym, regulacjom prawnym oraz standardom krajowym i europejskim odnoszącym się do cyberbezpieczeństwa szkół. Przedstawiono w nim między innymi znaczenie RODO, dyrektywy NIS2, Aktu o usługach cyfrowych, Aktu o cyberodporności, AI Act, ustawy o krajowym systemie cyberbezpieczeństwa, Krajowych Ram Interoperacyjności oraz przepisów prawa oświatowego. Szczególną uwagę zwrócono na obowiązki dyrektorów szkół i innych decydentów w zakresie ochrony danych, zarządzania ryzykiem, reagowania na incydenty, nadzoru nad dostawcami usług cyfrowych oraz zapewniania bezpiecznego środowiska cyfrowego dla uczniów.

W trzecim rozdziale omówiono najważniejsze zagrożenia i wyzwania cyberbezpieczeństwa w sektorze edukacji. Przedstawiono skalę i dynamikę cyberataków na świecie oraz w Polsce, ze szczególnym uwzględnieniem placówek oświatowych. Analizie poddano najczęstsze typy zagrożeń, w tym phishing, ransomware, złośliwe oprogramowanie, ataki DDoS, przejęcia kont, cyberprzemoc oraz incydenty wynikające z błędów użytkowników. Rozdział pokazuje również, że skutki cyberataków mogą prowadzić nie tylko do problemów technicznych, ale także do zakłócenia procesu dydaktycznego, utraty danych, odpowiedzialności prawnej, strat finansowych oraz spadku zaufania do szkoły.

Czwarty rozdział zawiera analizę literatury oraz istniejących modeli kompetencji w zakresie cyberbezpieczeństwa. Omówiono w nim zarówno ogólne ramy kompetencji cyfrowych, jak i modele profesjonalne oraz sektorowe, które mogą być wykorzystane w środowisku szkolnym. Szczególne znaczenie przypisano takim rozwiązaniom jak DigComp 2.2, ENISA ECSF, NIST NICE, wytyczne CISA dla sektora K–12 oraz materiały brytyjskiego NCSC. Rozdział wskazuje, że skuteczne cyberbezpieczeństwo szkoły wymaga nie tylko kompetencji technicznych, ale również kompetencji zarządczych, organizacyjnych, prawnych, społecznych i wychowawczych.

W dalszej części raportu cyberbezpieczeństwo szkół analizowane jest więc jako zagadnienie wielowymiarowe: prawne, technologiczne, organizacyjne, edukacyjne i społeczne. Takie ujęcie pozwala pokazać, że ochrona placówek oświatowych nie może ograniczać się do zakupu sprzętu lub wdrożenia pojedynczych zabezpieczeń. Wymaga ona spójnego systemu zarządzania, jasno określonych ról, regularnego podnoszenia kompetencji, współpracy z instytucjami zewnętrznymi oraz traktowania bezpieczeństwa cyfrowego jako stałego elementu funkcjonowania szkoły.

1. Cyberbezpieczeństwo w szkolnictwie

Zwiększanie poziomu cyberbezpieczeństwa należy rozpatrywać w dwóch wzajemnie powiązanych aspektach. Transformacja cyfrowa wymaga przygotowania całego społeczeństwa do funkcjonowania w środowisku cyfrowym. Cyberbezpieczeństwo nie jest obecnie wyłącznie domeną specjalistów technologii informacyjno-komunikacyjnych, ponieważ technologie cyfrowe są obecnie wykorzystywane w niemal każdym obszarze życia społecznego i zawodowego. Z tego względu konieczne jest kształtowanie prawidłowych nawyków związanych z bezpieczeństwem cyfrowym, ochroną danych oraz odpowiedzialnym korzystaniem z technologii już od najwcześniejszych etapów edukacji.

Drugim istotnym aspektem jest świadomość, że cyberbezpieczeństwo nie stanowi stanu osiąganego jednorazowo, lecz jest procesem wymagającym ciągłego nadzoru, aktualizacji i doskonalenia. Dynamiczny rozwój technologii oraz zmieniający się charakter zagrożeń powodują konieczność stałego monitorowania ryzyka, rozwijania kompetencji cyfrowych oraz regularnego aktualizowania procedur bezpieczeństwa, także w instytucjach edukacyjnych.

Cyberbezpieczeństwo w jednostkach oświatowych stało się jednym z kluczowych wyzwań dla współczesnej administracji publicznej. Szkolnictwo jest jednym z sektorów najbardziej narażonych na cyberataki, co wynika z kilku czynników: rozproszonej struktury użytkowników (coraz to nowi uczniowie, nauczyciele i administracja), dużej ilości cennych danych, ograniczonych zasobów oraz dużej roli czynnika ludzkiego. Skala zagrożeń rośnie, a ich skutki wykraczają poza sferę IT – wpływają na funkcjonowanie całej szkoły i społeczności.

W szkołach przetwarza się coraz więcej danych oraz usług wykorzystując technologie informacyjno-komunikacyjne. Przełomowym okresem w tym zakresie była pandemia COVID-19, gdzie cały proces dydaktyczny i część spraw administracyjnych (w tym dane osobowe) zostały przeniesione do sfery cyfrowej. Szkoły – podobnie jak i inne podmioty – nie były przygotowane na tak gwałtowną i kompleksową zmianę sposobu działania z tradycyjnego na cyfrowy. Oczywiście wraz ze wzrostem aktywności szkół w cyberprzestrzeni wzrosła również liczba zagrożeń, która widoczna jest w statystykach na całym świecie, w tym i w Polsce.

Słabe strony polskich placówek edukacyjnych w zakresie cyberbezpieczeństwa[1]:

- Przestarzały sprzęt i oprogramowanie – w wielu placówkach nadal używa się starszych komputerów i systemów operacyjnych bez aktualizacji bezpieczeństwa, co zwiększa ryzyko wykorzystania znanych luk.

[1] https://system-3.com.pl/blog/cyberbezpieczenstwo-w-systemie-edukacji---wyzwania-i-rozwiazania

- Brak segmentacji sieci – komputery uczniów, nauczycieli i administracji często działają w jednej sieci. Brak podziału na strefy bezpieczeństwa ułatwia dostęp do ważnych zasobów po uzyskaniu dostępu do sieci.
- Niewystarczająca kontrola dostępu – użytkownicy często posiadają zbyt szerokie uprawnienia, a kontrola nad dostępem do danych i instalacją oprogramowania jest ograniczona.
- Brak szyfrowania danych – dane osobowe i dokumenty bywają przechowywane bez szyfrowania, co naraża je na przejęcie w przypadku kradzieży sprzętu lub cyberataku.
- Problemy z kopiami zapasowymi – część placówek nie wykonuje regularnych backupów lub nie sprawdza możliwości ich odtworzenia, co utrudnia odzyskanie danych po awarii lub ataku ransomware.
- Brak monitorowania zagrożeń – w szkołach rzadko stosuje się systemy wykrywania zagrożeń, dlatego incydenty bezpieczeństwa są często wykrywane dopiero po wystąpieniu szkód.
- Brak procedur bezpieczeństwa – w wielu placówkach nie ma jasno określonych zasad reagowania na incydenty ani osób odpowiedzialnych za cyberbezpieczeństwo.

W akcie o cyberbezpieczeństwie[2] definicja „cyberbezpieczeństwa" jest następująca: „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami".

Bardziej rozbudowana definicja przedstawia cyberbezpieczeństwo jako zbiór działań, technologii, procedur i praktyk służących ochronie systemów informatycznych, sieci, urządzeń oraz danych przed nieuprawnionym dostępem, uszkodzeniem lub kradzieżą. Obejmuje zarówno aspekty techniczne (np. zabezpieczenia systemów), jak i organizacyjne oraz edukacyjne (świadomość użytkowników)[3].

Cyberbezpieczeństwo rozumiane funkcjonalnie to sposób, w jaki osoby prywatne i organizacje ograniczają ryzyko cyberataku, którego podstawowym celem jest ochrona urządzeń, usług on-line oraz danych przed cyberatakami, które mogłyby zakłócić funkcjonowanie podmiotu.

Cyberbezpieczeństwo w obecnych czasach powinniśmy postrzegać wieloaspektowo i strategicznie. Biorąc pod uwagę nieustająco zwiększający się zakres zadań realizowanych przy pomocy urządzeń elektronicznych oraz dane, które są zapisane w wersji elektronicznej wzrasta też zakres konieczność ich ochrony.

Stanem docelowym działań osób zarządzających szkołami jest ich cyberodporność (*cyber resilience*), czyli zapewnienie zdolności szkoły do funkcjonowania mimo

[2] Rozporządzenie 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie). https://sip.lex.pl/akty-prawne/dzienniki-UE/rozporzadzenie-2019-881-w-sprawie-enisa-agencji-unii-europejskiej-ds-69192391/art-2

[3] https://aktywnynauczyciel.pl/wiedza-cyberbezpieczenstwo-w-szkole

wystąpienia incydentu cyfrowego. Nie chodzi więc wyłącznie o ochronę przed zagrożeniami, ale przede wszystkim o przygotowanie placówki na sytuację, w której część systemów, danych lub usług stanie się czasowo niedostępna. Cyberodporna szkoła potrafi szybko rozpoznać problem, uruchomić procedury awaryjne, zabezpieczyć dane, poinformować właściwe osoby i przywrócić ciągłość pracy dydaktycznej oraz administracyjnej. Obejmuje to m.in. regularne kopie zapasowe, alternatywne kanały komunikacji, jasny podział odpowiedzialności, przygotowanie kadry oraz ćwiczenie reakcji na incydenty. W takim ujęciu odporność cyfrowa staje się elementem zarządzania szkołą i warunkiem utrzymania jej podstawowych funkcji nawet w sytuacji zakłócenia.

Odpowiedzialność osób zarządzających w zakresie cyberbezpieczeństwa polega na:

- rozumieniu ryzyka i skutków, jakie cyberataki niosą dla działalności podmiotu (szkoły) oraz
- zapewnieniu odpowiedniej cyberodporności (*cyber resilience*) poprzez zapobieganie, wykrywanie i reagowanie na cyberataki.

2. Dokumenty strategiczne: kontekst prawny i standardy krajowe dot. cyberbezpieczeństwa w szkołach

2.1. Kwestie cyberbezpieczeństwa w szkołach zawarte w aktach prawnych UE

2.1.1. Rozporządzenie 2016/679 (RODO) – jest podstawowym aktem prawa UE regulującym przetwarzanie danych osobowych, w pełni obejmującym szkoły jako administratorów danych uczniów, rodziców i pracowników[4].

a. Obowiązki dla szkoły: legalność i rozliczalność przetwarzania
Szkoła musi wykazać podstawę prawną przetwarzania danych, realizować zasady przetwarzania (m.in. minimalizacja, celowość) oraz potrafić wykazać zgodność z przepisami.

b. Obowiązki informacyjne i prawa osób, których dotyczą dane – szkoła ma obowiązek przekazywać wymagane informacje (transparentność) oraz zapewnić realizację praw osób (np. dostęp, sprostowanie, ograniczenie).

c. Bezpieczeństwo przetwarzania (środki techniczne i organizacyjne) – RODO wymaga wdrożenia adekwatnych środków bezpieczeństwa (organizacyjnych i technicznych) zależnych od ryzyka, co przekłada się na zarządzanie dostępami, ochronę kont, urządzeń, sieci oraz procedur.

d. Obsługa naruszeń ochrony danych – RODO przewiduje obowiązki oceny naruszenia, ewentualnego zgłoszenia organowi nadzorczemu i – w określonych przypadkach – poinformowania osób, których dane dotyczą; praktyczne wskazówki dostarcza UODO.

e. IOD – RODO określa rolę Inspektora Ochrony Danych, a krajowe przepisy doprecyzowują ramy stosowania (w sektorze publicznym – powszechna praktyka).

f. Ocena ryzyka i ocena skutków dla ochrony danych (DPIA) – przy procesach wysokiego ryzyka (np. nowe platformy, monitoring, dane wrażliwe) szkoła powinna umieć uruchomić ocenę skutków (DPIA) i analizę ryzyka.

[4] Regulation (EU) 2016/679 (GDPR) – EUR-Lex.

2.1.2. Dyrektywa NIS2 tworzy ramy cyberbezpieczeństwa w UE, z naciskiem na zarządzanie ryzykiem, raportowanie incydentów oraz odpowiedzialność kierownictwa, a także obowiązki państw członkowskich (strategie, Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT), nadzór).

a. Obowiązki dla szkoły (najczęściej pośrednie – poprzez dostawców i ekosystem publiczny) – szkoły zwykle nie są wprost klasyfikowane jako podmioty objęte NIS2, ale korzystają z usług dostawców objętych reżimem NIS2 (np. chmura, hosting, platformy). W praktyce dyrekcja powinna potrafić przenieść wymogi bezpieczeństwa na umowy i wymagania dla dostawców.

b. Risk management jako standard działania – NIS2 wzmacnia model zarządzania ryzykiem i odpowiedzialność kierownictwa za cyberbezpieczeństwo; szkoła powinna wdrożyć prosty, ale stały proces identyfikacji i priorytetyzacji ryzyk.

c. Incydenty: eskalacja i współpraca – NIS2 promuje spójny ekosystem reagowania. Kompetencją szkoły jest umiejętność eskalacji incydentu (organ prowadzący, dostawca, CSIRT/instytucje wsparcia) i utrzymania ciągłości działania.

2.1.3. Europejska strategia cyberbezpieczeństwa ujmuje cyberbezpieczeństwo jako element odporności społeczno-gospodarczej i bezpieczeństwa publicznego, wskazując rosnącą zależność instytucji publicznych od narzędzi cyfrowych oraz potrzebę budowania odporności systemowej i kompetencji[5].

a. Zakres i cele – w centrum znajdują się: odporność usług i produktów cyfrowych, zdolność reagowania na poważne cyberataki oraz rozwój cyberodporności w UE.

b. Cyberbezpieczeństwo jako warunek zaufania do usług cyfrowych – strategia podkreśla potrzebę bezpiecznych narzędzi cyfrowych w instytucjach publicznych, co dotyczy także szkół korzystających z platform i usług online.

c. Rozwój kompetencji i odporności społecznej – w ujęciu strategii kompetencje użytkowników są częścią odporności cybernetycznej, co uzasadnia traktowanie szkoły jako kluczowego miejsca budowania kompetencji i postaw.

2.1.4. Akt o usługach cyfrowych (Digital Services Act – DSA). DSA ustanawia ramy odpowiedzialności i należytej staranności dostawców usług pośrednich (platform, hostingów), w tym mechanizmy reagowania na treści nielegalne, przejrzystość zasad oraz ochronę użytkowników (w tym małoletnich)[6].

[5] JOIN(2020) 18 final – The EU's Cybersecurity Strategy for the Digital Decade – EUR-Lex.
[6] Regulation (EU) 2022/2065 (Digital Services Act) – EUR-Lex.

a. Zakres: korzystanie z platform (także edukacyjnych) i usług pośrednich – szkoły korzystające z platform e-learningowych, wideokonferencji i narzędzi hostowanych powinny umieć egzekwować od dostawcy transparentne zasady, bezpieczne ustawienia i kanały zgłoszeń.

b. Ochrona małoletnich i bezpieczeństwo użytkowników – DSA wzmacnia ochronę użytkowników i ograniczanie ryzyk systemowych platform, co przekłada się na kompetencję szkoły w doborze narzędzi i konfiguracji środowiska ucznia (moderacja, ustawienia prywatności, zgłoszenia).

c. Procedury „notice and action" – regulacja wzmacnia procedury zgłaszania treści nielegalnych i reagowania usługodawcy; szkoła powinna umieć uruchomić ścieżkę zgłoszeń i zabezpieczyć materiał dowodowy.

2.1.5. Akt w sprawie cyberodporności (Rozporządzenie (UE) 2024/2847). CRA ustanawia wymagania cyberbezpieczeństwa dla produktów z elementami cyfrowymi (sprzęt i oprogramowanie) wprowadzanych na rynek UE, z naciskiem na bezpieczeństwo „by design" i obsługę podatności w cyklu życia[7].

a. Zakres dla szkół: czy sprzęt i oprogramowanie spełniają standardy cyberbezpieczeństwa – chociaż obowiązki spoczywają głównie na producentach, szkoły jako nabywcy otrzymują ważne kryteria zakupowe: aktualizacje bezpieczeństwa, deklaracje zgodności, informacje o okresie wsparcia.

b. Bezpieczeństwo zakupów i umów – CRA wzmacnia podejście, że cyberbezpieczeństwo zaczyna się na etapie doboru produktów i wymagań umownych (wsparcie, aktualizacje, dokumentacja).

c. Zarządzanie cyklem życia (aktualizacje, EOL, wymiana) – w praktyce szkolnej oznacza to planowanie wymiany i utrzymania infrastruktury, tak aby nie pozostawiać systemów bez poprawek bezpieczeństwa.

2.1.6. Sztuczna inteligencja i ochrona dzieci w środowisku cyfrowym. AI Act (Rozporządzenie (UE) 2024/1689) ustanawia horyzontalne zasady korzystania z systemów sztucznej inteligencji w UE, w tym podejście oparte na ryzyku, obowiązki transparentności oraz wymagania dla systemów wysokiego ryzyka. W kontekście edukacji istotny jest fakt, że szkoły coraz częściej wykorzystują narzędzia AI jako użytkownicy, a ich wybory mogą wpływać na prawa i bezpieczeństwo uczniów[8].

[7] Regulation (EU) 2024/2847 (Cyber Resilience Act) – EUR-Lex. https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

[8] Regulation (EU) 2024/1689 (AI Act) – EUR-Lex. (https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng)

a. Zakres istotny dla szkoły: zastosowania AI w edukacji i zarządzaniu – w praktyce szkolnej AI obejmuje m.in. narzędzia do tworzenia treści, wsparcia dydaktycznego, analityki edukacyjnej, a także funkcje automatyzujące pracę administracyjną. AI Act ustanawia wymóg, aby systemy były bezpieczne i nie naruszały praw podstawowych, co tworzy ramę do podejmowania decyzji o wdrażaniu takich narzędzi.

b. AI literacy (kompetencje w zakresie AI) jako obowiązek organizacyjny – AI Act przewiduje akcent na budowanie kompetencji w zakresie AI (AI literacy), co w praktyce oznacza potrzebę przeszkolenia kadry zarządzającej i nauczycieli w rozpoznawaniu ryzyk, ograniczeń i konsekwencji użycia AI.

c. Ochrona dzieci i spójność z RODO oraz DSA – użycie narzędzi AI w szkole łączy się bezpośrednio z ochroną danych (RODO) oraz ochroną małoletnich w środowisku platform (DSA). Z perspektywy decydentów szkolnych istotne jest zapewnienie minimalizacji danych, kontroli dostępu, transparentności oraz bezpiecznych kanałów zgłoszeń i moderacji.

d. Konsekwencje praktyczne dla szkoły (polityki i procedury) – włączenie AI do środowiska szkolnego powinno skutkować wdrożeniem co najmniej czterech elementów zarządczych: (1) polityki dopuszczalnego użycia AI (uczniowie/nauczyciele), (2) zasad doboru narzędzi (w tym oceny ryzyka i zgodności z RODO), (3) zasad bezpieczeństwa treści (np. deepfake / dezinformacja w szkole), (4) procedur zgłaszania incydentów i nadużyć w narzędziach platformowych.

2.2. Kwestie cyberbezpieczeństwa w szkołach zawarte w polskich aktach prawnych

W Polsce regulacje dotyczące cyberbezpieczeństwa szkół są rozproszone i obejmują: ochronę danych osobowych, bezpieczeństwo systemów teleinformatycznych w jednostkach publicznych oraz organizację krajowego systemu cyberbezpieczeństwa.

a. Ustawa z 10 maja 2018 r. o ochronie danych osobowych[9] – ustawa służy stosowaniu RODO w Polsce i doprecyzowuje elementy krajowe (ramy organu nadzorczego, procedury, sankcje), co jest istotne dla szkół jako podmiotów publicznych.
b. Prawo oświatowe: odpowiedzialność dyrektora[10] -prawo oświatowe przypisuje dyrektorowi szkoły obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych zapewniających zgodność przetwarzania danych osobowych

[9] https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/ochrona-danych-osobowych-18722262
[10] Prawo oświatowe Art. 68 (https://lexlege.pl/prawo-oswiatowe/art-68/)

z przepisami. Jest to kluczowy przepis łączący zarządzanie szkołą z cyberbezpieczeństwem (w wymiarze danych).

c. Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne[11] – ustawa tworzy ramy interoperacyjności i minimalnych wymagań dla systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych, a więc także dla szkół jako jednostek realizujących zadania publiczne.

d. Krajowe Ramy Interoperacyjności (KRI) – standard bezpieczeństwa informacji w podmiotach publicznych[12] – rozporządzenie RM z 21 maja 2024 r. (Dz.U. 2024 poz. 773) określa KRI i minimalne wymagania dla systemów teleinformatycznych, w tym sposoby zapewnienia bezpieczeństwa przy wymianie informacji. Jest to kluczowy standard dla bezpieczeństwa informacji w sektorze publicznym.

e. Materiały wdrożeniowe UODO/MEN[13] – poradnik UODO i MEN dotyczący ochrony danych w szkołach pełni rolę praktycznego przewodnika wdrożeniowego, porządkując interpretacje i przykładowe rozwiązania organizacyjne.

2.3. Zadania szkół wg. ustawy o krajowym systemie cyberbezpieczeństwa (KSC)

Ustawa o KSC organizuje krajowy system cyberbezpieczeństwa, definiuje podstawowe pojęcia (cyberbezpieczeństwo, incydent) oraz wskazuje rolę krajowych CSIRT (w tym CSIRT NASK)[14].

a. Spójne rozumienie incydentu i cyberbezpieczeństwa – dla szkoły praktycznie oznacza to konieczność posługiwania się definicjami ustawowymi oraz budowania szkolnych procedur reagowania na incydenty (od zdarzeń „użytkowych" po ataki na systemy).

b. Ścieżka eskalacji i współpraca z CSIRT – KSC wskazuje funkcjonowanie CSIRT na poziomie krajowym; szkoła powinna wiedzieć, jak uruchomić ścieżkę wsparcia i raportowania poprzez organ prowadzący i instytucje reagowania.

c. Spójność KSC z KRI i obowiązkami dyrektora – w praktyce szkolnej KSC działa najczęściej „pośrednio": szkoła wdraża standardy KRI i obowiązki organizacyjne dyrektora wynikające z prawa oświatowego, a w sytuacji incydentu korzysta z ekosystemu krajowego (CSIRT/organ prowadzący).

[11] https://eli.gov.pl/eli/DU/2005/565/ogl
[12] https://api.sejm.gov.pl/eli/acts/DU/2024/773/text.pdf
[13] www.gov.pl/web/edukacja/ochrona-danych-osobowych-w-szkole--poradnik-uodo-i-men
[14] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC) – Dz.U. 2018 poz. 1560. https://eli.gov.pl/api/acts/DU/2018/1560/text/T/D20181560L.pdf

2.4. Podsumowanie: mapa kompetencji decydentów szkolnych z mapowaniem do aktów UE/PL

Poniższa mapa pokazuje zestaw kompetencji decydentów szkolnych (dyrekcja/zarządzanie) wynikający z omówionych aktów prawnych i standardów. Każda kompetencja jest powiązana z regulacjami UE i/lub PL.

1) Zarządzanie ochroną danych

Decydent powinien umieć ustanowić zasady legalności, minimalizacji i rozliczalności przetwarzania danych, nadzorować rejestry czynności, upoważnienia, polityki retencji oraz realizację praw osób.

Mapowanie: RODO (UE); ustawa o ochronie danych osobowych (PL); praktyka UODO/MEN.

2) Organizacja systemu bezpiecznego obiegu i przechowywania informacji

Decydent powinien rozumieć i wdrożyć minimalny system zarządzania bezpieczeństwem informacji: role, procedury, polityki, przeglądy, audytowalność oraz minimalne wymagania dla systemów teleinformatycznych.

Mapowanie: KRI (PL) oraz ustawa o informatyzacji (PL) jako rama dla podmiotów publicznych.

3) Reagowanie na incydenty i naruszenia

Decydent powinien mieć kompetencję do uruchamiania procedury po wystąpieniu incydentu: klasyfikacja zdarzenia, zabezpieczenie dowodów, komunikacja, eskalacja oraz działania naprawcze, w tym obsługa naruszeń danych osobowych.

Mapowanie: RODO (naruszenia) + KSC (incydent/cyberbezpieczeństwo, ekosystem CSIRT).

4) Bezpieczne zakupy i nadzór nad dostawcami

Decydent powinien umieć formułować wymagania bezpieczeństwa w zakupach i umowach (SLA, aktualizacje, wsparcie, kopie zapasowe, role i odpowiedzialności), a także wymagać transparentności i standardów od dostawców usług.

Mapowanie: CRA (UE – cyberodporność produktów), NIS2 (UE – governance i łańcuch dostaw), RODO.

5) Ochrona małoletnich w środowisku cyfrowym

Decydent powinien umieć zarządzać środowiskiem platform z których korzystają uczniowie: ustawienia prywatności, moderacja, ścieżki zgłoszeń, reagowanie na treści nielegalne/szkodliwe oraz kontrola używanych narzędzi.

Mapowanie: DSA (UE) + RODO (UE) w kontekście danych dzieci i bezpieczeństwa przetwarzania.

6) Kompetencje i kultura bezpieczeństwa

Decydent powinien zapewnić szkolenia i podnoszenie świadomości (kadra, administracja, uczniowie), ponieważ przepisy i strategie UE akcentują rolę kompetencji jako elementu odporności.

Mapowanie: Strategia cyberbezpieczeństwa UE (skills), AI Act (AI literacy), a w Polsce – praktyka wdrożeniowa poprzez materiały UODO/MEN.

7) AI Governance w szkole (polityki użycia AI, ryzyka, zgodność)

Decydent powinien rozumieć ryzyka związane z korzystaniem z narzędzi AI (błędy, uprzedzenia, deepfake, automatyzacja decyzji), wdrożyć zasady użycia i doboru narzędzi, a także połączyć to z ochroną danych i zasadami bezpiecznego korzystania z platform.

Mapowanie: AI Act (UE) + RODO (UE) + DSA (UE).

8) Odpowiedzialność dyrektora i wdrożenia organizacyjne

Decydent powinien umieć przełożyć wymagania prawne na realne zarządzanie szkołą: procedury, role, nadzór, środki techniczne i organizacyjne oraz spójność działań z prawem oświatowym.

Mapowanie: Prawo oświatowe (PL – obowiązki dyrektora) + KRI (PL) + RODO (UE).

3. Zagrożenia i wyzwania cyberbezpieczeństwa

W akcie o cyberbezpieczeństwie zagrożenie jest definiowane jako: „wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób".

Zatem zagrożenie (cyberzagrożenie) to każde potencjalne zdarzenie lub działanie, które może spowodować naruszenie bezpieczeństwa systemu informatycznego, danych lub użytkownika. Do zagrożeń można zaliczyć:

- zagrożenia techniczne
- zagrożenia socjotechniczne
- zagrożenia organizacyjne

Akt o cyberbezpieczeństwie odsyła do Dyrektywy 2016/1148, która w art. 4[15] definiuje incydent jako „każde zdarzenie, które ma rzeczywiście niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych".

Incydent cyberbezpieczeństwa to zdarzenie, które faktycznie narusza lub zagraża bezpieczeństwu systemu, danych lub usług

3.1. Skala i charakter zagrożeń cyberbezpieczeństwa

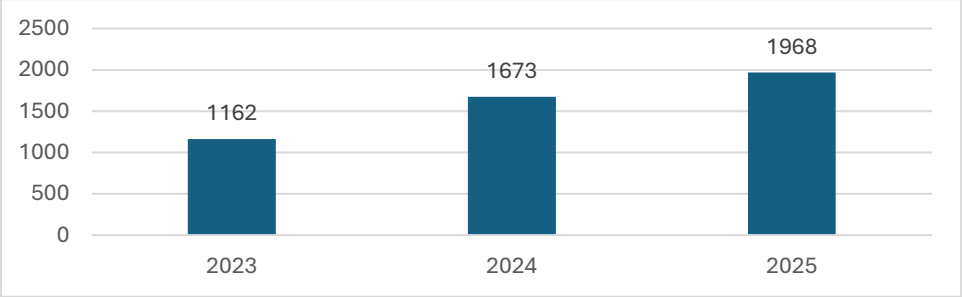
W celu lepszego zobrazowania skali, dynamiki oraz rosnącego znaczenia współczesnych cyberzagrożeń przedstawiono poniżej wybrane dane statystyczne odnoszące się do bezpieczeństwa cyberprzestrzeni, ze szczególnym uwzględnieniem sektora edukacyjnego, w tym szkół podstawowych i ponadpodstawowych. Analiza dostępnych raportów międzynarodowych i krajowych wskazuje, że placówki oświatowe należą obecnie do najczęściej atakowanych instytucji publicznych, a liczba incydentów cyberbezpieczeństwa systematycznie wzrasta zarówno w Polsce, jak i na świecie.

Liczba ataków – trend globalny

Raport Check Point 2026 wskazuje wzrost średniej tygodniowej liczby ataków na instytucję, która w 2025 r. wyniosła 1 968 i porównując ją z danymi z poprzednich okresów można zauważyć, że liczba ta wzrosła o blisko 70% w ciągu 2 lat.

[15] https://sip.lex.pl/akty-prawne/dzienniki-UE/dyrektywa-2016-1148-w-sprawie-srodkow-na-rzecz-wysokiego-wspolnego-68659478/art-4

Wykres 3.1. Średnia liczba cyberataków tygodniowo na organizację



Źródło: Check Point 2026.

Dane te pokazują, że liczba cyberataków rośnie w sposób systematyczny i dynamiczny. Coraz większa liczba usług cyfrowych, rozwój sztucznej inteligencji oraz automatyzacja działań cyberprzestępczych powodują, że organizacje publiczne i prywatne stają się coraz bardziej narażone na ataki.

Regiony świata

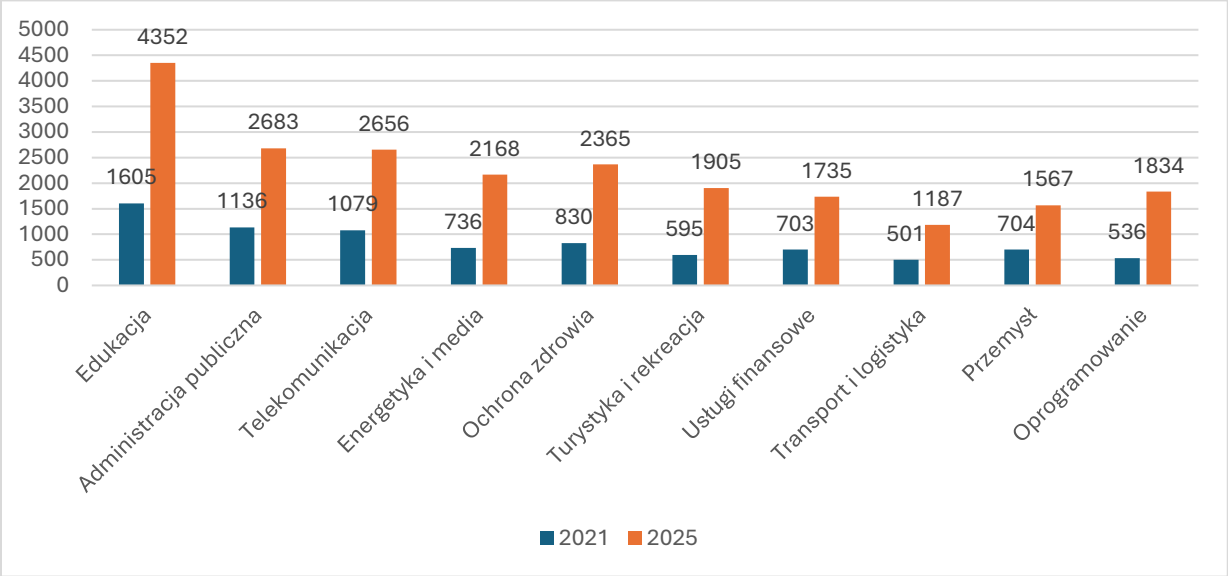
W 2025 roku najwyższą średnią liczbę cyberataków tygodniowo na 1 instytucję odnotowano w regionie Afryki (3 092 ataki tygodniowo). Niewiele niższe wartości występowały w regionie Azji i Pacyfiku (2 909). W Ameryce Łacińskiej organizacje doświadczały średnio 2 795 ataków tygodniowo. Najniższe wskaźniki zanotowano w Europie (1 642) oraz Ameryce Północnej (1 422). Dane te pokazują, że cyberprzestępcy coraz częściej koncentrują się na regionach o niższym poziomie dojrzałości cyberbezpieczeństwa oraz słabszej infrastrukturze ochronnej.

Podział ataków według sektorów gospodarki

Jak podaje Check Point[16] w marcu br. najczęstszym celem cyberataków na świecie – notując średnio 4 632 ataki tygodniowo – był sektor edukacyjny. Dla porównania warto dodać, że kolejne najczęściej atakowane branże osiągają dużo niższe wskaźniki: sektor rządowy – 2 582 ataki tygodniowo, a telekomunikacja – 2 554. Jeżeli chodzi o dynamikę zmian rok do roku – najwyższy przyrost cyberataków zanotowało rolnictwo +66%, branża turystyczna – +30% oraz branża budowlana (*construction and engineering*) – +19%. Największe spadki w porównaniu z marcem 2025 r. natomiast zanotowały branże: komputerowa (*hardware and semiconductors*) – -28%, automotive – -24% oraz medyczna – -20%.

[16] https://blog.checkpoint.com/research/march-2026-cyber-threat-landscape-shows-no-relief-as-ransomware-rebounds-and-genai-risks-intensify/

Wykres 3.2. Porównanie średniej liczby cyberataków tygodniowo na organizację w podziale na sektory gospodarki w latach 2021 i 2025

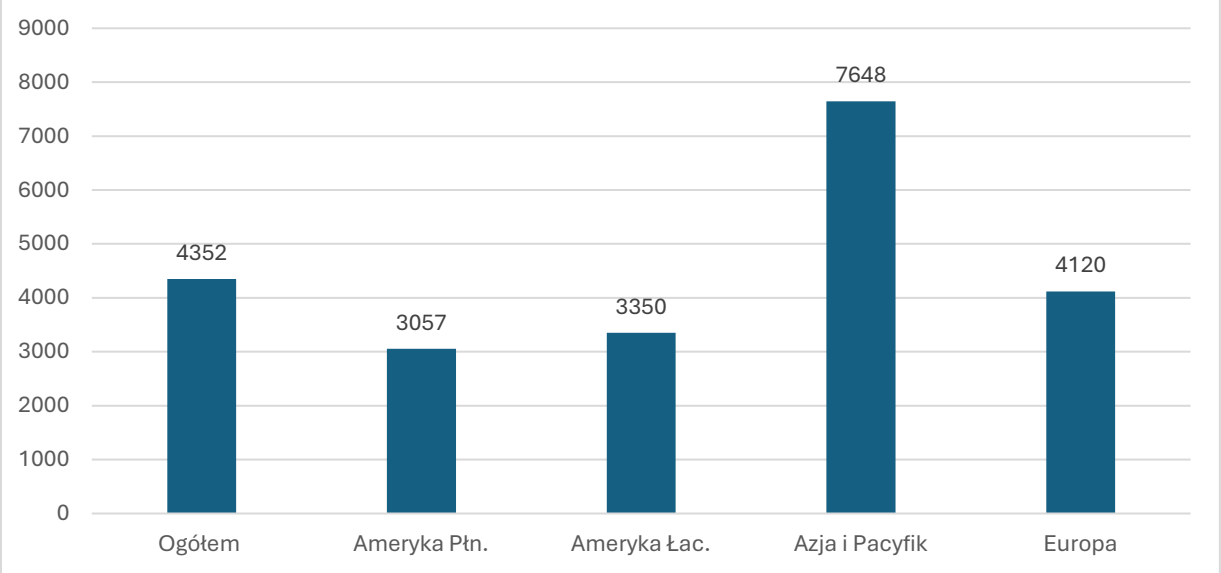


Źródło: Check Point Research (2026). March 2026 Cyber Threat Landscape Shows No Relief as Ransomware Rebounds and GenAI Risks Intensify oraz dane za 2021 ze strony Check Point.

Edukacja i badania

W większości regionów świata w 2025 r. – oprócz krajów Ameryki Łacińskiej – sektor edukacji był najczęściej atakowanym sektorem gospodarki. Najwyższą liczbę ataków odnotowano w regionie Krajów Azji i Pacyfiku, wewnątrz regionu liderem tej niechlubnej statystyki są Indie.

Wykres 3.3. Średnia liczba cyberataków na podmioty edukacyjne tygodniowo w podziale na regiony świata

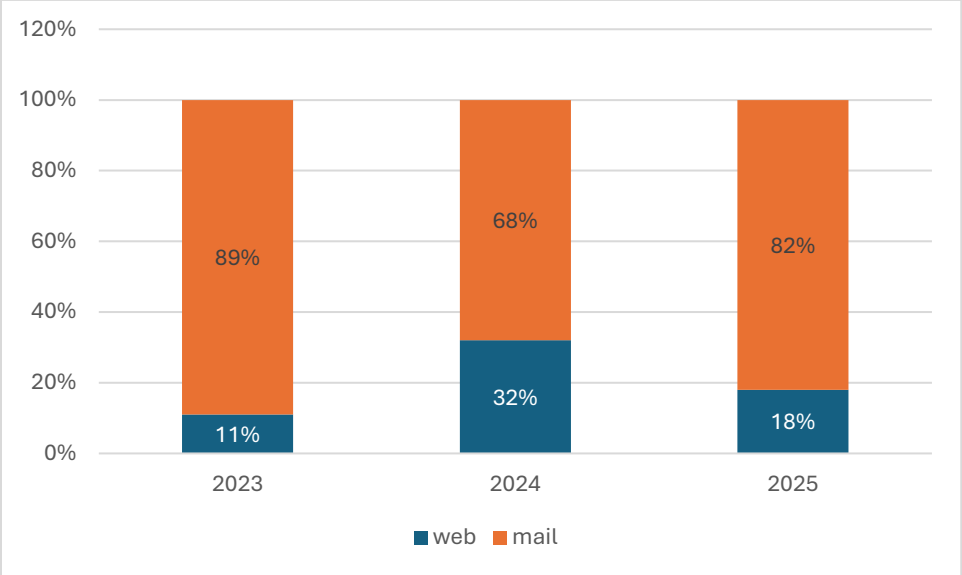


Źródło: opracowanie własne na podstawie Check Point (2026). Cyber Security Report, 2026, s. 63-68

Wektory ataku

Najczęściej wykorzystywanym wektorem ataku pozostaje poczta elektroniczna. W roku 2025 aż 82% cyberataków przeprowadzono z wykorzystaniem wiadomości e-mail. Około 18% incydentów dotyczyło podatności w aplikacjach, błędów konfiguracji systemów lub luk w zabezpieczeniach serwerów i stron internetowych.

Wykres 3.4. Wektory cyberataków

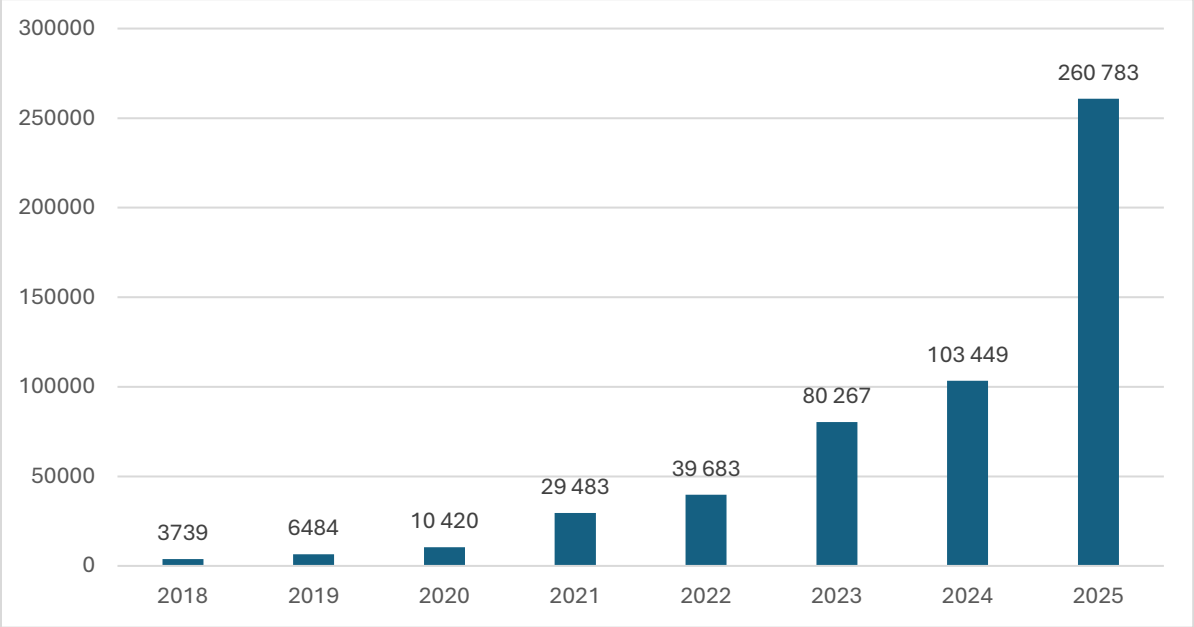


Dane te pokazują, że czynnik ludzki oraz socjotechnika nadal pozostają najskuteczniejszym narzędziem wykorzystywanym przez cyberprzestępców.

Cyberzagrożenia w Polsce

Skalę problemu obrazują statystyki zgłoszeń i incydentów rejestrowanych przez CERT – zespołu funkcjonującego w ramach instytutu badawczego NASK (Naukowa i Akademicka Sieć Komputerowa). W 2025 roku zespół CERT Polska otrzymał 658 320 zgłoszeń w zakresie cyberbezpieczeństwa oraz obsłużył 260 783 incydenty.

Wykres 3.5. Liczba incydentów obsłużonych przez CERT Polska w latach 2018-2025



Źródło: opracowanie własne na podstawie: RAPORT ROCZNY 2025 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu. CERT 2026, s. 119.

W roku 2025, w porównaniu z rokiem 2024, nastąpił wzrost liczby zgłoszeń o 10%, natomiast liczba zarejestrowanych incydentów wzrosła o 152%.

Tabela 3.1. Incydenty obsłużone przez CERT Polska w latach 2020 i 2025 w podziale na sektor gospodarki

Sektor	2020	2025
Ogółem	**10 420**	**260 783**
Osoby fizyczne	959	250 595
Administracja publiczna	388	2 801
Handel hurtowy i detaliczny	1 437	2 231
Inne	379	1 291
Oświata i wychowanie	**71**	**1 258**
Ochrona zdrowia	112	724
Infrastruktura cyfrowa	1 016	495
Usługi inne	384	255
Kultura i ochrona dziedzictwa narodowego	7	218
Bankowość	1 008	179
Transport	29	140
Wodociągi	9	95
Produkcja	57	93
Budownictwo i gospodarka nieruchomościami	29	78
Media	2 568	60
Energetyka	101	52
Logistyka i dystrybucja	27	36
Infrastruktura rynków finansowych	1 283	35
Gospodarka odpadami	1	31

Sektor	2020	2025
Rolnictwo	4	29
Hotele, restauracje, catering	19	23
Kultura fizyczna	9	18
Poczta i usługi kurierskie	500	13
Turystyka	9	10
Działalność ubezpieczeniowa	2	9
Wyznania religijne i mniejszości narodowe	8	5
Izby gospodarcze i handlowe	3	5
Rybołówstwo	1	4

Źródło: opracowanie własne na podstawie: Raport roczny 2025 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu. CERT 2026, s. 119-120 oraz Raport roczny z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu 2020, s. 26.

Liczba incydentów w sektorze edukacji wzrosła z 71 w 2020 roku do 1 258 w roku 2025, co oznacza wzrost o ponad 1 670%.

Instytucje oświatowe w Polsce w 2025 r. znalazły się na piątym miejscu w rankingu incydentów zagrażających działaniu systemów informatycznych. Jest to znaczący wzrost w porównaniu do roku 2024 r., kiedy to zanotowano 733 incydenty (14. miejsce w podziale na sektor gospodarki).

Tabela 3.2. Incydenty obsłużone przez CERT Polska w 2025 roku w podziale na kategorie

Kategoria zagrożenia	Liczba incydentów	Procent
Oszustwa komputerowe	253 238	97,1%
Złośliwe oprogramowanie	3438	1,3%
Podatne usługi	1732	0,7%
Obraźliwe i nielegalne treści	950	0,4%
Włamania	750	0,3%
Dostępność zasobów	427	0,2%
Próby włamań	139	0,1%
Atak na bezpieczeństwo informacji	76	0,0%
Inne	18	0,0%
Gromadzenie informacji	15	0,0%
Razem	**260 783**	**100,0%**

Źródło: RAPORT ROCZNY 2025 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu. CERT 2026, s. 120.

Ponad 97% wszystkich incydentów związanych było z oszustwami komputerowymi, głównie phishingiem oraz wyłudzeniami danych. Dane te potwierdzają, że najważniejszym elementem cyberbezpieczeństwa pozostaje świadomość użytkowników.

3.2. Zagrożenia w szkołach

Cyberzagrożenia w sektorze edukacji dotyczą nie tylko Polski, lecz mają charakter globalny. Statystyki brytyjskiego Departamentu Nauki, Innowacji i Technologii Ministerstwa Spraw Wewnętrznych[17] dotyczące naruszeń cyberbezpieczeństwa w Wielkiej Brytanii w 2025 r. są następujące: 60% szkół ponadpodstawowych oraz 44% szkół podstawowych zidentyfikowanych ataków lub naruszeń (dla porównania przedsiębiorstwa – 43%). Warto dodać, że 81% szkół ponadpodstawowych oraz 82% szkół podstawowych w Wielkiej Brytanii posiadało politykę cyberbezpieczeństwa. W szkołach podejmuje się działania związane z identyfikacją zagrożeń (np. ocena ryzyka): 84% szkół ponadpodstawowych oraz 84% szkół podstawowych.

Ciekawe dane przytacza CyberDefence24.pl. Brytyjskie Biuro Komisarza ds. Informacji (ICO) wskazuje, że nawet **połowa cyberataków na szkoły może być związana z działaniami uczniów**. Jedna trzecia włamań na konta szkolne była skutkiem:

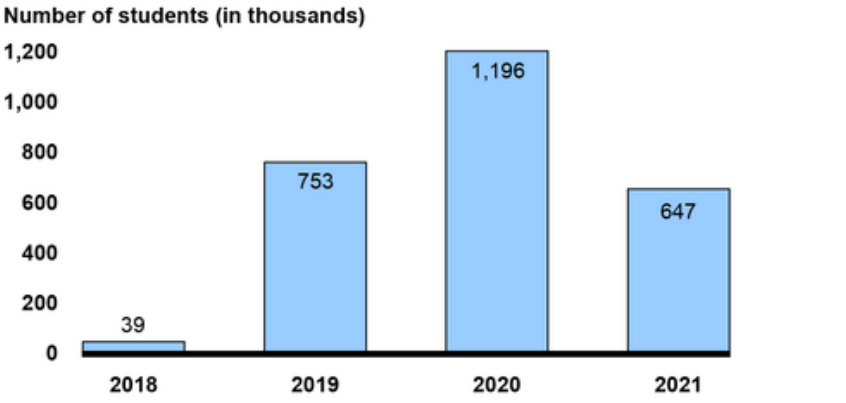
- odgadnięcia hasła,
- znalezienia hasła zapisanego na kartce,
- wykorzystania słabych zabezpieczeń przez uczniów.[18]

Biuro Komisarza ds. Informacji ujawniło, że 23 proc. incydentów w placówkach spowodowane było m.in. **zezwoleniem uczniom na korzystanie ze służbowych urządzeń czy pozostawieniu tychże bez nadzoru**, którzy łamali hasła dostępu lub wykorzystywali znalezione dane do zalogowania się do systemów szkolnych.

Dane GAO[19] pokazują, jak w trakcie pandemii i przeniesienia nauczania do internetu w USA wzrosła liczba uczniów, którzy zostali dotknięci atakami ransomware z 39 tys. w roku 2018 do 753 tys. w roku 2019, aż po 1 196 tys. w roku 2020.

[17] www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-education-institutions-findings
[18] https://cyberdefence24.pl/cyberbezpieczenstwo/cyberataki-na-szkoly-polowa-sprawcow-to-dzieci
[19] https://www.gao.gov/products/gao-23-105480

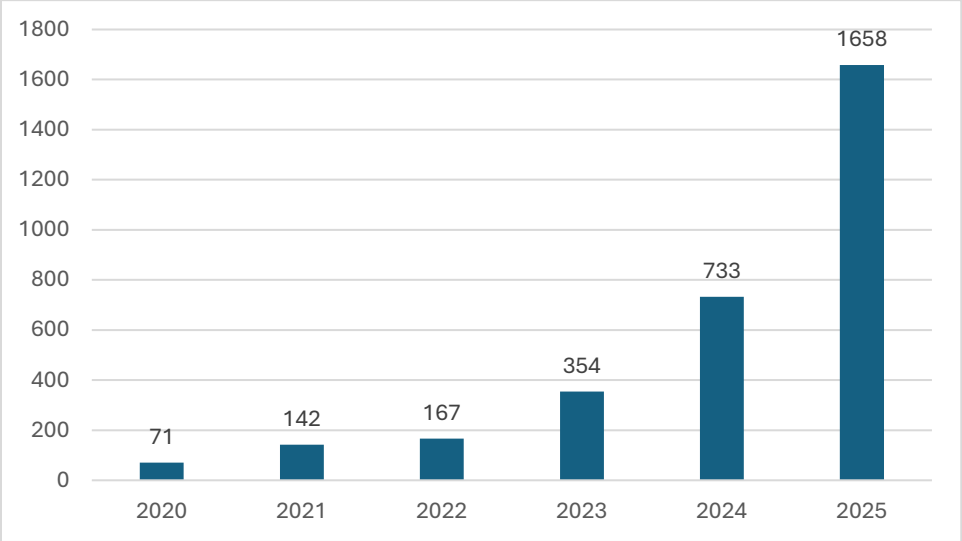
Wykres 3.6. Liczba amerykańskich uczniów dotkniętych atakami ransomware na szkoły podstawowe i ponadpodstawowe (K-12) 2018-2021



Source: GAO analysis of Comparitech study on K-12 school ransomware attacks. | GAO-23-105480

Poniższy wykres przedstawia liczbę incydentów cyberbezpieczeństwa odnotowanych w sektorze oświata i wychowanie w Polsce w latach 2020–2025. Dane pokazują wyraźny i systematyczny wzrost liczby cyberzagrożeń dotyczących placówek edukacyjnych.

Wykres 3.7. Liczba incydentów w sektorze oświata i wychowanie w Polsce w latach 2020-2025



Źródło: opracowanie własne na podstawie Raportów rocznych CERT 2020-2025.

W 2020 roku zarejestrowano 71 incydentów cyberbezpieczeństwa w placówkach edukacyjnych zgłoszonych do CERT Polska. Już w kolejnym roku liczba ta wzrosła dwukrotnie – do 142 przypadków. W 2022 roku odnotowano 167 incydentów, natomiast w roku 2023 nastąpił bardzo wyraźny wzrost do 354 zdarzeń. Szczególnie dynamiczny przyrost widoczny jest w latach 2024–2025, kiedy liczba incydentów zwiększyła się odpowiednio do 733 oraz 1 658 przypadków.

Łącznie w analizowanym okresie liczba incydentów wzrosła ponad dwudziestokrotnie. Dane te wskazują na rosnącą skalę zagrożeń cyberbezpieczeństwa w polskich

placówkach edukacyjnych oraz zwiększającą się aktywność cyberprzestępców wobec sektora oświaty. Tendencja wzrostowa może być związana m.in. z postępującą cyfryzacją szkół, rozwojem nauczania zdalnego, powszechnym wykorzystaniem dzienników elektronicznych oraz niewystarczającym poziomem zabezpieczeń i świadomości użytkowników.

Widoczny wzrost liczby incydentów potwierdza, że cyberbezpieczeństwo staje się jednym z kluczowych wyzwań funkcjonowania współczesnych placówek edukacyjnych i wymaga zarówno inwestycji technologicznych, jak i systematycznego podnoszenia kompetencji cyfrowych nauczycieli, uczniów oraz administracji szkolnej.

Zagrożenia organizacyjne w polskich placówkach edukacyjnych wynikają głównie z **braku spójnych procedur**, **niewystarczającego zarządzania informacją** oraz **ograniczonych zasobów kadrowych i finansowych**. W przeciwieństwie do zagrożeń technicznych, które dotyczą sprzętu i systemów, zagrożenia organizacyjne są efektem decyzji, zaniedbań lub braku kompetencji na poziomie zarządzania placówką. Szkoły funkcjonują w środowisku o wysokiej rotacji użytkowników, dużej liczbie urządzeń oraz ograniczonych możliwościach kontroli nad zachowaniami cyfrowymi.

Negatywny wpływ cyberzagrożeń na funkcjonowanie szkoły może być znaczący i jest wielowymiarowy. Cyberataki nie są tylko problemem technicznym i mają realny wpływ na działanie placówki:

1. Zakłócenie procesu dydaktycznego
   - brak dostępu do systemów edukacyjnych (platform edukacyjnych, e-dzienników)
   - odwołane zajęcia (nawet na kilka dni lub tygodni)
2. Problemy organizacyjne
   - niedostępność poczty, systemów administracyjnych
   - brak dostępu do dokumentacji uczniów
   - zakłócenia pracy administracji szkolnej
3. Straty finansowe
   - koszty przywracania systemów
   - koszty zakupu nowego sprzętu
   - wydatki na zabezpieczenia i modernizację infrastruktury
4. Utrata danych i konsekwencje prawne
   - naruszenie RODO
   - utrata zaufania rodziców i uczniów
5. Wpływ społeczny
   - stres uczniów i nauczycieli
   - zakłócenie funkcji społecznych szkoły (np. opieka, posiłki, wsparcie psychologiczne).

3.3. Rodzaje cyberataków na szkoły

Placówki edukacyjne należą obecnie do najbardziej narażonych na cyberzagrożenia instytucji publicznych. Dynamiczna cyfryzacja szkół, rozwój nauczania zdalnego oraz powszechne wykorzystanie platform edukacyjnych i dzienników elektronicznych powodują, że szkoły stają się atrakcyjnym celem dla cyberprzestępców. Ataki na sektor edukacyjny mają zarówno charakter techniczny, jak i socjotechniczny, a ich skutki mogą prowadzić do zakłócenia procesu dydaktycznego, utraty danych oraz poważnych problemów organizacyjnych.

Powyżej cytowane dane Check Point Research wskazują, że sektor edukacyjny pozostaje najczęściej atakowaną branżą na świecie, osiągając średnio ponad 4 352 cyberataków tygodniowo na placówkę edukacyjną (4 120 w Europie).

- **Phishing** – najczęściej występującym rodzajem cyberataków w szkołach jest phishing. Atak ten polega na podszywaniu się pod zaufane osoby lub instytucje w celu wyłudzenia danych logowania, haseł, danych osobowych lub informacji finansowych.

  Cyberprzestępcy najczęściej podszywają się pod:

  - administrację szkoły,
  - dzienniki elektroniczne,
  - platformy edukacyjne,
  - nauczycieli,
  - banki i firmy kurierskie.

  Ataki phishingowe realizowane są głównie za pomocą wiadomości e-mail, wiadomości SMS lub komunikatorów internetowych. W 2025 roku ponad 80% cyberataków przeprowadzono z wykorzystaniem poczty elektronicznej. Phishing stanowi obecnie główne źródło przejęć kont uczniów i nauczycieli.

  W szkołach szczególnie niebezpieczne są:

  - fałszywe strony logowania do dzienników elektronicznych,
  - wiadomości zawierające zainfekowane załączniki,
  - próby wyłudzenia danych dostępowych do platform edukacyjnych.

- **Ransomware** Jednym z najgroźniejszych zagrożeń dla szkół są ataki ransomware. Polegają one na zaszyfrowaniu danych lub zablokowaniu dostępu do systemów informatycznych szkoły, a następnie żądaniu okupu za ich odzyskanie.

  Ataki ransomware mogą prowadzić do:

  - utraty dokumentacji uczniów,
  - niedostępności dzienników elektronicznych,
  - przerwania zajęć dydaktycznych,

- wycieku danych osobowych,
- wielodniowych przestojów organizacyjnych.

Szczególnie niebezpieczne są obecnie ataki typu double extortion, w których cyberprzestępcy najpierw kradną dane, a następnie grożą ich publikacją.

- **Ataki typu Distributed Denial-of-Service (DDoS)** polegają na przeciążeniu infrastruktury sieciowej szkoły ogromną liczbą zapytań wysyłanych z wielu urządzeń jednocześnie. Celem ataku jest uniemożliwienie korzystania z usług cyfrowych.

  Ataki DDoS najczęściej dotyczą:
  - stron internetowych szkół,
  - platform edukacyjnych,
  - systemów egzaminacyjnych,
  - dzienników elektronicznych,
  - serwerów pocztowych.

  Skutkiem takich działań może być całkowita niedostępność systemów wykorzystywanych podczas nauki lub egzaminów online.

- **Malware i spyware** – złośliwe oprogramowanie obejmuje wirusy komputerowe, trojany, keyloggery oraz programy szpiegujące instalowane na urządzeniach szkolnych lub prywatnych komputerach uczniów i nauczycieli.

  Najczęstsze skutki infekcji malware:
  - przejęcie danych logowania,
  - kradzież danych osobowych,
  - monitorowanie aktywności użytkowników,
  - przejęcie kontroli nad urządzeniem,
  - instalacja ransomware.

  Szkoły są szczególnie podatne na tego typu zagrożenia ze względu na:
  - korzystanie z prywatnych urządzeń,
  - brak aktualizacji systemów,
  - niewystarczające zabezpieczenia antywirusowe,
  - instalowanie niezweryfikowanego oprogramowania.

- **Zakłócanie zajęć online i cyberprzemoc** – wraz z rozwojem nauczania zdalnego wzrosła liczba incydentów związanych z zakłócaniem lekcji online. Ataki te obejmują:
  - publikowanie obraźliwych treści podczas zajęć,
  - przejmowanie spotkań online,
  - rozpowszechnianie materiałów pornograficznych,
  - cyberprzemoc wobec nauczycieli i uczniów.

- **Ataki przeprowadzane przez uczniów** – coraz częściej sprawcami cyberataków na szkoły są sami uczniowie. Dotyczy to przede wszystkim:
  - prób włamań do dzienników elektronicznych,
  - przejmowania kont nauczycieli,
  - ataków DDoS,
  - cyberprzemocy,
  - zakłócania lekcji online.

Cyberzagrożenia w szkołach mają obecnie charakter wielowymiarowy i obejmują zarówno zaawansowane ataki techniczne, jak i działania wykorzystujące błędy oraz niewystarczającą świadomość użytkowników. Szczególnie istotnym problemem pozostają phishing, ransomware oraz ataki socjotechniczne, które odpowiadają za większość incydentów cyberbezpieczeństwa w sektorze edukacyjnym.

Rosnąca liczba cyberataków wskazuje na konieczność:

- wdrażania standardów cyberbezpieczeństwa,
- regularnego szkolenia nauczycieli i uczniów,
- rozwijania kompetencji cyfrowych,
- modernizacji infrastruktury IT szkół,
- tworzenia procedur reagowania na incydenty cyberbezpieczeństwa.

4. Analiza literatury i istniejących modeli kompetencji w zakresie cyberbezpieczeństwa w szkołach

Rozdział ten stanowi logiczną kontynuację wcześniejszych wątków: po zarysowaniu kontekstu prawnego (RODO/NIS2/DSA/CRA/AI Act oraz standardy krajowe) przechodzimy do analizy modeli kompetencji oraz tego, jak realnie wygląda poziom kompetencji i świadomości zagrożeń w szkołach. W warstwie krajowej punktem odniesienia jest raport „Kompetencje w zakresie bezpieczeństwa cyfrowego w polskiej szkole" (projekt Cyfrowobezpieczni.pl, 2016), a w warstwie międzynarodowej – ramy kompetencyjne i wyniki badań (m.in. DigComp 2.2[20], ENISA ECSF[21], NIST NICE[22], EU Kids Online[23], CISA K-12[24], NCSC UK[25]).

4.1. Podział modeli kompetencji

W literaturze i praktyce zarządzania cyberbezpieczeństwem w edukacji można wyróżnić kilka klas modeli kompetencji. Pierwsza to modele obywatelskie/ogólne (adresowane do każdego użytkownika technologii), druga – modele profesjonalne/z podziałem ról (w organizacjach), trzecia – modele szkolno-sektorowe (dla szkół i kadr oświaty), a czwarta – modele diagnostyczne oparte na pomiarze (testy kompetencyjne i badania). Ten podział jest użyteczny, bo pozwala dopasować narzędzie do celu: inne ramy są potrzebne do projektowania programów nauczania, inne do budowania polityk bezpieczeństwa, a z kolei jeszcze inne do audytu i rozwoju kompetencji kadry.

a. Modele ogólne (kompetencje cyfrowe obywatela) koncentrują się na umiejętnościach niezbędnych każdemu użytkownikowi: ochronie urządzeń, danych i prywatności, radzeniu sobie z ryzykami psychospołecznymi (np. dobrostan, zachowania ryzykowne), krytycznym odbiorze informacji oraz etyczno-prawnym wymiarze korzystania z treści. Najbardziej rozpowszechnioną ramą w Europie jest DigComp 2.2, która porusza temat bezpieczeństwa cyfrowego i rozpisuje przykłady wiedzy, umiejętności i postaw, w tym odnoszące się do nowych zjawisk (m.in. AI). Tego typu model dobrze tłumaczy kompetencje uczniów i rodziców na język edukacji i programów rozwojowych[26].

[20] https://www.digcomp.pl/wp-content/uploads/2023/03/DigComp2.2_TEXT_pl_.pdf
[21] https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles
[22] https://csrc.nist.gov/pubs/sp/800/181/r1/final
[23] https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf
[24] https://www.cisa.gov/topics/cybersecurity-best-practices/K12cybersecurity/protecting-our-future-cybersecurity-k12
[25] https://www.ncsc.gov.uk/information/cyber-security-training-schools
[26] Vuorikari, R., Kluzer, S., Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens*. JRC/European Commission.

b. Modele profesjonalne opisują kompetencje przez pryzmat ról i zadań w cyberbezpieczeństwie organizacji. Przykładowo, amerykański NIST NICE Framework buduje wspólny słownik zadań (tasks) oraz wymaganej wiedzy i umiejętności (knowledge/skills) dla pracy związanej z cyberbezpieczeństwem. Europejskim odpowiednikiem w wymiarze ról zawodowych jest ENISA ECSF, który opisuje 12 profili ról cyber i przypisuje im misje, zadania oraz kompetencje. Choć szkoły rzadko zatrudniają pełne zespoły cyber, te modele są bardzo przydatne do zdefiniowania minimalnej roli „koordynatora bezpieczeństwa", zakresu współpracy z administratorem IT oraz do opisu kompetencji decyzyjnych dyrekcji (governance)[27].
c. Modele szkolno-sektorowe zwykle są to zestawy priorytetów i dobrych praktyk, które budują kompetencje przez działania: szkolenia personelu, procedury, ćwiczenia reagowania, wdrożenia techniczne i kontrolę dostępu. Przykładem jest podejście CISA dla K-12, które rekomenduje skupienie się na kilku najbardziej wpływowych działaniach: MFA, łatanie podatności, kopie zapasowe, ćwiczenie planu reagowania oraz program szkoleń. Równolegle brytyjskie NCSC przygotowało dedykowany pakiet szkoleń z zakresu cyberbezpieczeństwa dla personelu szkół, adresując kluczowe ryzyka (phishing, hasła, zabezpieczenia urządzeń, zgłaszanie incydentów). Ten typ modeli buduje kompetencje przez organizację, a nie tylko przez wiedzę[28].
d. Modele diagnostyczne (pomiarowe) – takie jak raport Cyfrowobezpieczni.pl – są kluczowe, gdy celem jest ocena gdzie jesteśmy i wybór priorytetów rozwojowych. Polski raport przyjmuje wielowymiarowy układ kompetencji, łącząc komponenty techniczne i społeczne oraz testując wiedzę/umiejętności i postawy w różnych grupach (uczniowie/rodzice/nauczyciele) oraz na różnych etapach edukacyjnych. Istotne jest też to, że raport buduje model kompetencji zależnych od wieku, zakładając, iż wraz z etapem rozwojowym pojawia się inny profil ryzyk (np. seksting i cyberprzemoc w starszych grupach)[29].

W konsekwencji, w niniejszym opracowaniu zasadna jest synteza: DigComp 2.2 jako rama ogólna (dla uczniów/rodziców i nauczycieli jako użytkowników), NIST NICE/ENISA ECSF jako rama ról i zarządzania kwestiami cyberbezpieczeństwa (dla dyrekcji i osób odpowiedzialnych), oraz modele sektorowe K-12 (CISA/NCSC) jako praktyczny program (minimalny) wdrożeniowy. Krajowy raport, który powstał w ramach projektu Cyfrowobezpieczni.pl stanowi natomiast kompas diagnostyczny, wskazujący najsłabsze obszary kompetencji, których poprawa powinny stać się priorytetem.

[27] ENISA (2022). *European Cybersecurity Skills Framework Role Profiles (ECSF)*. NIST (2020). *SP 800-181 Rev. 1: Workforce Framework for Cybersecurity (NICE Framework)*.
[28] CISA (USA). *Protecting Our Future: Cybersecurity for K-12*. UK NCSC. *Cyber security training for school staff* (pakiet szkoleniowy).
[29] Tomczyk, Ł., Srokowski, Ł. (2016). *Kompetencje w zakresie bezpieczeństwa cyfrowego w polskiej szkole* (projekt Cyfrowobezpieczni.pl). Smahel, D. i in. (2020). *EU Kids Online 2020: Survey results from 19 countries*.

4.2. Świadomość cyberzagrożeń i poziom kompetencji cyfrowych

W literaturze przedmiotu cyberbezpieczeństwo w szkole jest konsekwentnie ujmowane jako splot trzech warstw: (1) warstwy technicznej (ochrona urządzeń i usług), (2) warstwy informacyjnej (weryfikacja treści, dezinformacja), (3) warstwy społeczno-wychowawczej (cyberprzemoc, seksting, kontakty z obcymi, wizerunek). Raport "Kompetencje w zakresie bezpieczeństwa cyfrowego w polskiej szkole" rozdziela obszary kompetencji na techniczno-społeczne oraz społeczne, wskazując m.in. na hasła/loginy, malware, bezpieczeństwo operacji finansowych, ergonomię, a także prawa autorskie, cyberprzemoc, kontakty online, wizerunek i seksting. Ten podział jest spójny z podejściem DigComp 2.2, które w obszarze Bezpieczeństwo, ujmuje zarówno ochronę urządzeń i danych, jak i dobrostan oraz bezpieczeństwo w interakcjach.

Różnica między kompetencjami cyfrowymi a kompetencjami z zakresu bezpieczeństwa cyfrowego polega na tym, że te drugie wymagają nie tylko sprawności obsługi narzędzi, ale także rozumienia ryzyka i zdolności do reakcji w sytuacji incydentu. Krajowy raport pokazuje to na przykładzie nauczycieli: młodsi nauczyciele mogą mieć relatywnie dobre kompetencje instrumentalne, ale słabsze kompetencje społeczne i wychowawcze, kluczowe dla radzenia sobie z zagrożeniami. Z kolei podejście NIST NICE/ENISA ECSF wskazuje, że w organizacjach cyberbezpieczeństwo wymaga warstwy „Oversight & Governance", czyli umiejętności zarządczych, które nie są tożsame z kompetencjami technicznymi. To uzasadnia tezę, że dyrekcja szkoły potrzebuje kompetencji z zakresu zarządzania cyfrowego „cyber-governance", nawet jeśli usługi IT są outsourcowane.

Świadomość cyberzagrożeń jest wprost powiązana z tym, czy szkoła traktuje bezpieczeństwo jako element codziennych praktyk. W modelach sektorowych K-12 nacisk kładzie się na trening personelu i procedury („co robić"), a nie tylko na wiedzę deklaratywną („co wiem"). CISA wskazuje, że przy ograniczonych zasobach najbardziej opłaca się wdrożyć kilka fundamentalnych praktyk (MFA, kopie, plan IR, szkolenia). NCSC UK publikuje dedykowane szkolenie dla personelu szkół, właśnie po to, by budować świadomość i minimalizować ryzyko ludzkiego błędu. Te podejścia są zbieżne z wnioskiem z polskich badań, z których wynika, że deficyty występują masowo w grupach uczniów, nauczycieli i rodziców, a więc potrzebne są działania systemowe, a nie punktowe.

Wreszcie, ważnym wymiarem świadomości są ryzyka specyficzne dla wieku i rozwoju. EU Kids Online opisuje ryzyka, umiejętności i praktyki dzieci w wieku 9-16 lat w wielu krajach Europy, pokazując, że ryzyka są powiązane z intensywnością używania technologii oraz kontekstem społecznym (rodzice/rówieśnicy/szkoła). Krajowy raport formułuje analogiczną diagnozę: wraz z wiekiem uczniów pojawiają się nowe zagrożenia, a tempo wzrostu zagrożeń bywa większe niż tempo rozwoju kompetencji. Z perspektywy modeli kompetencyjnych oznacza to, że wymagania kompetencyjne muszą być stopniowane i przypisane do poszczególnych etapów edukacyjnych.

4.3. Wyniki badań i ich analiza: gdzie jesteśmy i dlaczego?

Krajowe badanie (projekt Cyfrowobezpieczni.pl) dostarcza mocnego punktu odniesienia, ponieważ obejmuje dużą próbę: 10 720 uczniów, 1 900 rodziców i 1 233 nauczycieli, a także projektuje pomiar w 12 grupach (3 role × 4 etapy edukacyjne). Raport pokazuje ogólną diagnozę: poziom kompetencji w zakresie bezpieczeństwa cyfrowego jest niewystarczający we wszystkich grupach, a różnice między grupami są niewielkie – co wskazuje na systemowy charakter problemu.

Na poziomie wyników zbiorczych raport wskazuje średnie rezultaty w skali 0-100% (wyższy wynik oznacza, lepszy poziom wiedzy): rodzice 55%, nauczyciele 57%, uczniowie 60%. Szczególnie niskie wyniki dotyczą obszarów: prawo autorskie (ok. 36%), bezpieczeństwo transakcji finansowych oraz bezpieczne logowanie/hasła. Relatywnie najwyższe kompetencje dotyczą ochrony przeciwwirusowej i ergonomii korzystania z urządzeń. Ten wzorzec jest zgodny z logiką DigComp 2.2 i ISTE, gdzie „Safety/Digital Citizen" obejmuje zarówno kwestie techniczne, jak i prawne/etyczne (np. własność intelektualna, prywatność). W praktyce oznacza to, że braki kompetencyjne dotyczą nie tylko obszaru cyberbezpieczeństwa w sensie technicznym, ale i kompetencji społeczno-prawnych, które w szkole są kluczowe.

Kluczowym wnioskiem z krajowego raportu jest dynamika: im starsi uczniowie, tym niższe wyniki, co autorzy interpretują jako sytuację, w której „tempo wzrostu zagrożeń przewyższa tempo rozwoju kompetencji". W badaniu widać to na etapach: uczniowie klas 1-3 (wynik wysoki), później wyraźny spadek w klasach 4-6, następnie niski poziom w grupach gimnazjalnych i ponadgimnazjalnych. EU Kids Online pokazuje, że wraz z wiekiem rośnie zakres korzystania z narzędzi online, a co za tym idzie rośnie ryzyko występowania incydentów, a jednocześnie skuteczność mediacji i przeciwdziałania dorosłych bywa zróżnicowana – co przemawia za wyjaśnieniem, że brak systematycznego nabywania kompetencji jest problemem strukturalnym.

Raport wskazuje też silną nierówność kontekstową: mieszkańcy wsi (szczególnie rodzice) wypadają istotnie gorzej niż mieszkańcy miast. Jest to krytyczne, ponieważ rodzice w badaniu są najsłabszą grupą, a równocześnie pełnią kluczową rolę wychowawczą oraz pierwszą linię wsparcia dla dziecka. Ten wniosek jest spójny z analizami międzynarodowymi pokazującymi, że nierówności społeczno-ekonomiczne przekładają się na ryzyka i dostęp do wsparcia, a nie tylko na dostęp do technologii. W ujęciu modelowym oznacza to potrzebę adresowania kompetencji w sposób ukierunkowany, podkreślają to także rekomendacje CISA dla K-12 w kontekście ograniczeń zasobów i konieczności priorytetyzacji.

Istotnym elementem – dlaczego tak jest – jest rola szkoły jako środowiska, które często traktuje technologię na zasadzie „cyfrowej wyspy" (pracownia komputerowa, lekcja informatyki) zamiast integrować bezpieczeństwo cyfrowe z wieloma przedmiotami

i sytuacjami wychowawczymi. Krajowy raport krytycznie opisuje dominację modelu ograniczającego technologię do pracowni, wskazując, że nie odzwierciedla to realiów życia cyfrowego uczniów. Analogicznie, podejścia NCSC UK i CISA K-12 akcentują konieczność szkolenia całego personelu i traktowania cyberbezpieczeństwa jako elementu odporności organizacyjnej, a nie wyłącznie – działki informatyka. To przemawia na rzecz interpretacji, że brak integracji, zakorzenienia, tematu cyberbezpieczeństwa w praktyce szkoły jest czynnikiem utrwalającym luki kompetencyjne.

4.4. Bariery rozwojowe

Z krajowego raportu wyłania się zestaw barier rozwojowych, które mają charakter zarówno edukacyjny, jak i organizacyjno-społeczny.

Po pierwsze, barierą jest fragmentaryczność i nieregularność edukacji o bezpieczeństwie cyfrowym: rozmowy o zagrożeniach są prowadzone w różnej częstotliwości, a w wielu szkołach temat nie staje się stałym elementem praktyki dydaktycznej i wychowawczej.

Po drugie, barierą są deficyty dorosłych – szczególnie rodziców, którzy w badaniu wypadają najsłabiej i często nie rozmawiają z dziećmi o zagrożeniach, co ogranicza skuteczną mediację. Te bariery są spójne z wnioskami EU Kids Online, gdzie kontekst społeczny (rodzina/szkoła) silnie wpływa na ryzyka i poziom bezpieczeństwa.

Po trzecie, barierą jest niedopasowanie kompetencji kadry do realnych zagrożeń, zwłaszcza gdy kompetencje technologiczne nie idą w parze z kompetencjami społecznymi i wychowawczymi. Krajowy raport wskazuje m.in. paradoks słabszej świadomości u najmłodszych nauczycieli w obszarach społecznych zagrożeń. Z perspektywy modeli ról (NIST NICE, ENISA ECSF) oznacza to lukę w obszarze „governance/awareness/training”: organizacja może mieć narzędzia, ale bez kompetencji zarządczych i edukacyjnych nie zbuduje odporności.

Po czwarte, barierą są ograniczenia zasobów i priorytetyzacji (czas, budżet, wsparcie IT), które w szkołach często skutkują podejściem minimalistycznym w kwestii cyberbezpieczeństwa (brak MFA, brak testów kopii, brak ćwiczeń reagowania). Wprost opisują to rekomendacje CISA dla K-12, wskazując, że przy ograniczonych zasobach trzeba inwestować w najbardziej wrażliwe obszary i budować odporność stopniowo. W praktyce szkolnej oznacza to, że istotną kompetencją decydentów staje się wybór priorytetów (co wdrażać najpierw) oraz zapewnienie minimalnych standardów organizacyjnych i szkoleniowych.

Po piąte, barierą jest nierówność kompetencyjna związana z miejscem zamieszkania i wykształceniem, szczególnie widoczna u rodziców (wieś, niższe wykształcenie). Ta bariera jest krytyczna, bo oznacza, że standardowe, jednolite działania mogą nie wyrównywać deficytów. potrzebne jest zdywersyfikowane podejście. Z perspektywy DigComp 2.2 uzasadnia to projektowanie działań dopasowanych do grup (różne poziomy

wejścia, przykłady praktyczne, wsparcie w podstawach: hasła, prywatność, krytyczne myślenie). Z perspektywy EU Kids Online uzasadnia to traktowanie nierówności jako czynnika ryzyka, a nie tylko problemu edukacyjnego.

Wreszcie, narastającą barierą stają się gwałtowne zmiany technologiczne, w tym AI i automatyzacja tworzenia treści (deepfake, generowanie materiałów, wzrost skali dezinformacji), zwiększa to presję na kompetencje krytyczne i bezpieczeństwo wizerunku. DigComp 2.2 uwzględnia przykłady kompetencji odnoszące się do nowych technologii (w tym AI), a materiały edukacyjne w systemie ‘Better Internet for Kids’ podkreślają potrzebę uczenia bezpiecznych zachowań online i obywatelstwa cyfrowego w szkołach podstawowych i ponadpodstawowych. W połączeniu z wynikami krajowego raportu (deficyty w obszarach społecznych i prawnych) wskazuje to kierunek: kompetencje powinny być aktualizowane i osadzane w kontekście nowych ryzyk.

5. Benchmark, dobre i złe praktyki w zakresie kompetencji

5.1. Estonia – model cyfrowego państwa i cyberbezpieczeństwa w edukacji

Estonia uznawana jest za jedno z najbardziej rozwiniętych cyfrowo państw świata oraz europejskiego lidera w zakresie cyfryzacji administracji i edukacji. Rozwój kompetencji cyfrowych i cyberbezpieczeństwa został tam potraktowany jako element bezpieczeństwa państwa oraz długofalowej strategii rozwoju społeczeństwa informacyjnego. Estoński model edukacji cyfrowej opiera się na systemowym podejściu obejmującym uczniów, nauczycieli, administrację publiczną oraz sektor cyberbezpieczeństwa[30].

Już w 1997 roku w ramach programu Tiigrihüpe (Skok Tygrysa) rozpoczęto szeroko zakrojone inwestycje w szkolne komputery i infrastrukturę sieciową. Wszystkie szkoły zostały podłączone do internetu. Obecnie korzystanie ze smartfonów i sztucznej inteligencji jest postrzegane jako kolejny krok w rozwoju ICT [31]. Podczas gdy w wielu krajach ogranicza się korzystanie ze smartfonów w szkołach, w Estonii – kraju uważanym za lidera w zakresie edukacji – uczniowie są zachęcani przez nauczycieli do korzystania ze sztucznej inteligencji i od września 2025 r. uczniowie otrzymają dostęp do indywidualnych kont AI wspierających proces nauczania.

Wsparcie nauczycieli i uczniów w Estonii w rozwijaniu ich kompetencji cyfrowych opiera się odpowiednio na europejskich ramach Komisji Europejskiej DigCompEdu i DigComp. Ramy te są zgodne również z krajowymi programami nauczania i strategicznymi planami dotyczącymi edukacji.

Estonia opracowała ramy kompetencji cyfrowych nauczycieli oparte na DigCompEdu 2019 obejmujące sześć wymiarów:

1. Rozwój zawodowy i zaangażowanie – komunikacja, współpraca, refleksja oraz rozwój zawodowy z wykorzystaniem technologii cyfrowych.
2. Zasoby cyfrowe – wybór, tworzenie i udostępnianie cyfrowych materiałów edukacyjnych.
3. Nauczanie i uczenie się – zarządzanie i wykorzystywanie technologii cyfrowych w nauczaniu i uczeniu się.
4. Ocena – wykorzystanie technologii cyfrowych do usprawniania uczenia się.
5. Wzmacnianie pozycji uczniów – wykorzystanie technologii cyfrowych do aktywnego angażowania uczniów, wspierania zróżnicowania oraz indywidualizacji nauczania i rozwijania ogólnych kompetencji i umiejętności uczniów.

[30] www.educationestonia.org/innovation/digital-competence
[31] www.theguardian.com/education/2025/may/26/estonia-phone-bans-in-schools-ai-artificial-intelligence

6. Rozwijanie kompetencji cyfrowych uczniów – wspieranie uczniów w rozwijaniu kompetencji.

Ramy kompetencji cyfrowych uczniów zostały opracowane na podstawie DigComp 2.1 i obejmują pięć obszarów:

1. Kompetencje informacyjne i zarządzanie danymi (np. określanie potrzeb informacyjnych, ocena wiarygodności i przydatności źródeł oraz organizowanie danych cyfrowych).
2. Komunikacja i współpraca.
3. Tworzenie treści cyfrowych (np. tworzenie, ulepszanie i edytowanie treści, rozumienie zasad prawa autorskiego oraz formułowanie zrozumiałych poleceń dla systemów komputerowych).
4. Bezpieczeństwo.
5. Rozwiązywanie problemów.

Dodatkowo opracowano również dostosowaną wersję ram kompetencji cyfrowych dla uczniów ze specjalnymi potrzebami edukacyjnymi.

Estońskie ramy kompetencji cyfrowych nauczycieli i uczniów zostały uzupełnione o zestaw narzędzi wspierających ich wdrażanie. Należą do nich:

- Kryteria oceny uczniów w zakresie kompetencji cyfrowych – przygotowane dla czterech etapów edukacji ogólnej, wykorzystywane przez nauczycieli do oceny postępów uczniów w rozwijaniu kompetencji cyfrowych
- Kwestionariusz samooceny nauczyciela – internetowy kwestionariusz samooceny kompetencji cyfrowych. Umożliwia on analizę własnych kompetencji cyfrowych oraz identyfikację mocnych stron i obszarów wymagających rozwoju.
- Słownik pojęć – ramom kompetencji uczniów i nauczycieli oraz kryteriom oceniania i edukacji cyfrowej towarzyszy cyfrowy słownik pojęć, zapewniający nauczycielom i uczniom wspólny język o cyfrowym nauczaniu i uczeniu się.
- Test kompetencji cyfrowych – realizowany w krajowym systemie egzaminacyjnym (EIS). Testy nie są oceniane stopniami.
- Raport informacji zwrotnej – uczniowie przystępujący do testu kompetencji cyfrowych otrzymują raport zwrotny pokazujący ich wyniki na tle rówieśników w skali krajowej (tj. wyższy, podobny lub niższy) w każdym z pięciu obszarów kompetencji cyfrowych. Każdy obszar obejmuje szczegółowe wskaźniki, a uczniowie otrzymują jasny obraz swoich mocnych stron oraz obszarów wymagających poprawy. Nauczyciele otrzymują anonimowe raporty dotyczące swoich klas, a szkoły – raporty odnoszące się do wyników całej placówki.
- Cyfrowa baza dobrych praktyk – dobre praktyki w zakresie integrowania procesu nauczania oraz rozwijania kompetencji cyfrowych w różnych przedmiotach szkolnych publikowane w otwartym dostępie.

Cyberbezpieczeństwo jako element kultury szkoły

Estoński model zakłada budowanie kultury cyberbezpieczeństwa od najwcześniejszych etapów edukacji. Uczniowie uczą się:

- higieny cyfrowej,
- odpowiedzialnego korzystania z technologii,
- ochrony prywatności,
- bezpiecznego korzystania z mediów społecznościowych,
- rozpoznawania phishingu i dezinformacji.

Współpraca szkół z sektorem cyberbezpieczeństwa

Ważnym elementem estońskiego modelu jest ścisła współpraca szkół, uczelni oraz państwowych instytucji cyberbezpieczeństwa. Szczególną rolę odgrywa Tallinn University of Technology (TalTech), posiadający wyspecjalizowane centrum cyberbezpieczeństwa i cyfrowej kryminalistyki. Uczelnia prowadzi:

- programy studiów magisterskich z cyberbezpieczeństwa,
- szkolenia praktyczne,
- ćwiczenia typu cyber range,
- programy współpracy ze szkołami średnimi.

Ciekawym rozwiązaniem jest – finansowany przez estońskie Ministerstwo Edukacji i Badań – program rozwoju kompetencji cyfrowych „Digital Accelerator" (*Digikiirendi*), w ramach którego nauczyciele uczestniczą w szkoleniach oraz otrzymują wsparcie mentoringowe. Jednym z podstawowych założeń programu jest zaangażowanie całego zespołu danej szkoły. Organizatorzy wymagają, aby w szkoleniach uczestniczyli wszyscy nauczyciele oraz kadra zarządzająca placówki, przy czym minimalny poziom uczestnictwa został określony na 90% pracowników szkoły. Ma to zapewnić spójne wdrażanie kompetencji cyfrowych oraz budowanie wspólnej kultury bezpieczeństwa cyfrowego w placówce.

Pomimo wysokiego poziomu cyfryzacji, Estonia nadal mierzy się z problemami dotyczącymi cyberbezpieczeństwa szkół. Estoński Urząd ds. Systemów Informacyjnych (RIA) wskazuje[32], że szkoły nadal są celem: naruszeń danych, przejęć kont i stron internetowych, oszustw, ataków typu denial-of-service i ransomware oraz wielu innych zagrożeń. Przykładem może być atak ransomware na Centrum Szkolenia Zawodowego Järvamaa w sierpniu 2024 roku, w wyniku którego wszystkie dane serwerowe zostały utracone, bez dostępnych kopii zapasowych.

Eksperci RIA podkreślają, że poziom cyberbezpieczeństwa szkoły rzadko zależy od jej wielkości, a znacznie częściej od postawy kadry zarządzającej. Kluczowe znaczenie ma stopień, w jakim dyrekcja szkoły traktuje ochronę danych społeczności szkolnej oraz

[32] www.ria.ee/en/estonian-schools-should-prioritise-cybersecurity

zapewnienie bezpiecznego korzystania z nowoczesnych narzędzi edukacyjnych i organizacyjnych.

Większość estońskich placówek edukacyjnych– podobnie jak w Polsce – prowadzona i finansowana jest przez samorządy lokalne Z tego względu dyrekcje szkół powinny współpracować z władzami gmin i miast w celu podnoszenia poziomu cyberbezpieczeństwa. Ponieważ samorządy zarządzają często wieloma podległymi instytucjami korzystającymi ze wspólnych systemów informatycznych, bardziej efektywne może być scentralizowane podejście do cyberbezpieczeństwa. Może ono obejmować zatrudnienie wyspecjalizowanego personelu lub outsourcing usług cyberbezpieczeństwa do zewnętrznych podmiotów specjalistycznych.

Za przykład dobrej praktyki w zakresie cyberbezpieczeństwa można uznać estońskie Põltsamaa Coeducational Gymnasium, które w 2015 r. uruchomiło w szkole ponadpodstawowej ścieżkę kształcenia z zakresu cyberobrony. Program obejmował nie tylko zagadnienia techniczne, takie jak bezpieczne sieci, bezpieczeństwo cyfrowe i kryptografia, lecz także elementy społeczeństwa informacyjnego, etyki, cyberhigieny, ochrony osobistej oraz odpowiedzialnego zachowania w cyberprzestrzeni. Szczególnie istotna była współpraca szkoły z instytucjami publicznymi, organizacjami eksperckimi i sektorem prywatnym, dzięki której uczniowie uczestniczyli w warsztatach, spotkaniach z ekspertami i wizytach studyjnych. Model ten pokazuje, że skuteczna edukacja cyberbezpieczeństwa w szkole wymaga połączenia programu nauczania, praktycznego doświadczenia, współpracy z otoczeniem instytucjonalnym oraz kształtowania odpowiedzialnych postaw cyfrowych. Projekt został wyróżniony jako zwycięzca European Crime Prevention Award 2017[33].

Innym przykładem dobrej praktyki jest porozumienie zawarte między lokalną jednostką administracji zarządzającą szkołami publicznymi w hrabstwie Aiken w Karolinie Południowej (*Aiken County Public School District*) a Uniwersytetem Karoliny Południowej. W ramach współpracy prowadzone przez studentów Regional Security Operations Center zapewnia szkołom wsparcie w zakresie monitorowania sieci, wykrywania zagrożeń, analizy incydentów, reagowania oraz przywracania sprawności systemów po zakłóceniu. Jednocześnie współpraca przynosi korzyści uczelni i studentom, którzy zdobywają praktyczne doświadczenie w środowisku rzeczywistych zagrożeń. Rozwiązanie to pokazuje, że placówki oświatowe mogą wzmacniać cyberodporność poprzez partnerstwo z uczelniami, centrami kompetencji i instytucjami eksperckimi, szczególnie wtedy, gdy same nie dysponują wystarczającym zapleczem kadrowym lub technicznym[34].

[33] www.interregeurope.eu/good-practices/the-cyber-defence-field-of-study-at-poltsamaa-coeducational-gymnasium-poltsamaa-uhisgumnaasium; www.eucpn.org/document/the-cyber-defence-field-of-study-at-poltsamaa-coeducational-gymnasium

[34] www.usca.edu/news/2026/usca-cyber-students-protect-school-districts-computer-systems-prep-for-workforce.html

5.2. Cyfrowe BHP w szkołach. Zasady i zagrożenia – spojrzenie praktyka

W tym rozdziale postanowiliśmy oddać głos praktykom. To Małopolska Kurator Oświaty i jeden z najbardziej doświadczonych edukatorów z cyberbezpieczeństwa dla szkół.

Bez bezpieczeństwa i higieny można w tej pracy dużo stracić. Pieniądze, dobre imię, czasem zdrowie. A konkrety?

Czy w szkołach cyberbezpieczeństwo jest tematem, czy jest ważne? Gabriela Olszowska, Małopolska Kurator Oświaty *: – Jest ważne nie tylko dla szkół, ale dla każdego człowieka. Szybko przechodzimy do świata, w którym zacierają się granice między realnością, a cyfrą. Wczoraj miałam spotkanie z dyrektorami szkół w tej sprawie. Co chwilę o tym rozmawiamy. Tematów jest wiele – to m.in. kwestia państwowego dziennika cyfrowego, który będzie gwarantował te same standardy dla wszystkich szkół i będzie zintegrowany z innymi państwowymi systemami. Pracujemy nad tym w zespołach przy radzie ministrów. To też kwestia logowania dwustopniowego. Bo to ważny aspekt dla bezpieczeństwa we współczesnych systemach, ale jak to wprowadzić, kiedy nauczyciele nie mają służbowych telefonów? I nad tym pracujemy, mając świadomość, że system edukacji goni tu technologię. Zawsze będziemy tu pewnie trochę dalej, ale robimy wszystko, żeby być blisko.

***

Ważną częścią tego rozdziału opracowania będzie wiedza i konkretne przypadki jednego z najbardziej doświadczonych polskich edukatorów z zakresu bezpieczeństwa w sieci w szkołach i BHP Macieja Rakowskiego**.

Dziś bezpieczeństwo w sieci w polskich szkołach oparte jest głównie o Ogólnopolską Sieć Edukacyjną. „OSE to program publicznej sieci telekomunikacyjnej, dający szkołom w całej Polsce możliwość podłączenia szybkiego, bezpłatnego i bezpiecznego internetu. Program został zaprojektowany przez Ministerstwo Cyfryzacji, a jego założenia realizuje Państwowy Instytut Badawczy NASK” – czytamy w oficjalnych materiałach OSE.

Szkoły mają więc podpięty internet poprzez OSE. Maciej Rakowski: – Ten system od lat wyznacza granice: co wolno, a czego nie. Uczniowie nie mają dostępu do treści zakazanych, treści mogą być weryfikowane. Działa dobrze. Ale choć korzystają z niego prawie wszystkie placówki, to mają tylko 100 MB/s. To oznacza, że przy wielu pracowniach w dużych szkołach ten internet jest słaby. Z tym jest już być problem, bo programy, aplikacje potrzebują coraz szybszego internetu: to kwestia szybko przetwarzanych danych przez AI, dzienników elektronicznych, dostępu i edycji dokumentów współdzielonych, korzystania z platform do spotkań zdalnych, platform

e-learningowych, tablic elektronicznych. W małych szkołach to jeszcze nie jest problem, ale w dużych nawet dostęp do poczty może sprawiać kłopot.

W bezpieczny i bezpłatny internet poprzez OSE są wyposażone prawie wszystkie polskie szkoły. Zaczął być wprowadzany w 2018, kiedy 100 MB/s można było nazwać szybkim internetem. Co więc robią szkoły? Mogą dokupić za kilkadziesiąt złotych dodatkowe 50 MB/s. Ale to oznacza dodatkowe wydatki dla szkół, na które nie wszystkie mogą sobie pozwolić. Że by dotrzeć do 1 GB/s (system pozwala na taką maksymalną szybkość) trzeba już liczyć się z wydatkiem około 1 000 zł miesięcznie. Niektóre szkoły kupiły tzw. switche, czyli urządzenia, które łączą wiele sprzętów w jedną sieć. Zapewniają wysoką wydajność i bezpieczeństwo przesyłanych danych, pozwalają też wprowadzać ograniczenia w dostępie do wybranych treści. Ich stosowanie jest tańsze niż dokupowanie dodatkowych megabitów w OSE. Sieć OSE jest jednak podstawą funkcjonowania szkół, bo wiele ministerialnych programów i grantów zakłada, że szkoła działa w OSE.

Jakie treści blokują szkoły? Maciej Rakowski: – Pornografia, przemoc. Ale niektóre szkoły i nauczyciele ograniczają też dostęp do sztucznej inteligencji. Nowe technologie są oczywiście wyzwaniem i mogą być nadużywane, ale ja sam jestem przeciwny ograniczaniu dostępu do AI, a bardziej skłaniam się do rozumnego jej wykorzystywania, a nauczycieli do edukowania uczniów w tym obszarze, informowania, że treści, które znajdują w sieci nie zawsze są prawdziwe. Nie uciekniemy od tego, że technologia, AI będą się rozwijać. Potrzebujemy je jednak poznawać, edukować siebie i uczniów i odpowiedzialnie używać.

Według praktyków problemem polskich szkół nie jest więc brak sprzętu i systemu, który pozwala i gwarantuje cyfrowe bezpieczeństwo, a jego dostosowanie do potrzeb coraz bardziej wymagających szybkości programów. A to sprowadza się do kosztów.

***

BHP w sieci z perspektywy administracji i nauczycieli. OSE gwarantuje bezpieczeństwo, więc nie potrzeba dodatkowej administracji. Ataki hackerskie oczywiście występują, ale jeśli chodzi o bezpieczeństwo przepływu danych, OSE je gwarantuje. Czego więc musimy się obawiać? – Podstawą jest postawa uczniów i nauczycieli, musimy dbać o wyrobienie nawyku wylogowywania się. Kiedy uczniowie pracują w chmurze, muszą się do tych platform logować. Bez wylogowywania zostawiamy dostęp dla kogoś, kto może skorzystać z naszej pracy, korespondencji do wszystkich dokumentów wewnętrznych przekazywanych w sieci w sposób wyrządzający szkodę nam i całej szkole. Dotyczy to uczniów, ale też nauczycieli, którzy w trakcie dnia zmieniają sale i niekiedy zostawiając swoje dostępy do platform bez wylogowania. Znam przypadki, kiedy dane w ten sposób pozyskane służyły do zastraszania i szantażowania uczniów i nauczycieli, są przypadki wysyłania niecenzuralnych treści. Znam przykłady, że poprzez pozostawiony

niewylogowany dziennik szkoła dostawała informacje – dla jej dyrekcji wiarygodne – że występuje zagrożenie terrorystyczne, że wybuchnie bomba. Były sytuacje straszenia konkretnych nauczycieli. W dziennikach są informacje bardzo wrażliwe i kiedy uczeń, albo nauczyciel się nie wyloguje naraża się na ich wykorzystanie w złej intencji. Ktoś, kto te dane wykorzysta może użyć do – w jego rozumieniu – żartu, ale to jest przestępstwo. Tego typu sprawy są zgłaszane na policję, ale oczywiście nie wszystkie – opowiada Rakowski.

Takie sytuacje zdarzają się też nauczycielom. Na przykład nauczyciel prowadzący projekt z kilkoma uczniami i swoim komputerem z niewylogowanym dziennikiem elektronicznym zostawi przestrzeń dostępu do niego. Wtedy złośliwy uczeń może wykorzystać wrażliwe dane w dowolny sposób.

Ekspert podkreśla jak bardzo ważne jest wylogowywanie się, ale też stosowanie różnych haseł do różnych platform. W Polsce jest dużo przypadków wykorzystywania podejrzanych przez nieuprawnione osoby haseł, było również wiele wycieków haseł ze sklepów internetowych, banków. Nawet jeśli to wyciek z błahego serwisu, oszuści internetowi te hasła testują w sklepach internetowych, bankach. Jeśli zlekceważymy taki wyciek, a mamy jedno hasło do wielu serwisów, mamy też problem.

Istotne jest też korzystanie z zamkniętych, bezpiecznych sieci. Bo ktoś może przynieść do szkoły router z większą prędkością, a nauczyciel sfrustrowany słabą jakością połączenia szkolnego może się skusić na takie połączenie. Skutki mogą być bardzo bolesne, bo dane z programów w których był zalogowany mogą stać się publiczne. Logowanie się do sieci otwartych może spowodować przechwycenie danych.

Pamiętajmy też o silnych hasłach. Niektóre dzienniki elektroniczne i serwisy same wymagają silnych haseł i ich zmiany co miesiąc. To irytujące, ale pamiętajmy, że dziś 8-znakowe proste hasło jest do przełamania przez przeciętny komputer w ciągu kilku godzin.

Co ważne, brak dbałości o cyberbezpieczeństwo, o swoją higienę w sieci może sporo kosztować. Zwykle nie zwracamy na to uwagi póki sami nie wpadniemy w kłopoty, albo ktoś w naszym otoczeniu. Tu wchodzi w grę odpowiedzialność za udostępnienie danych, bezpieczeństwo związane z tożsamością, która może być wykorzystywana przez oszustów, złodziei, szantażystów.

- Niby to wiedziałem, ale dopiero teraz wiem, czym to grozi – często spotykam się z takimi reakcjami na szkoleniach, które prowadzę z cyberbezpieczeństwa – mówi Maciej Rakowski. OSE jest bezpieczne. – Ale znam przypadki, poza OSE, że ktoś wysyłał na adres IP tak duże ilości pakietów danych i zablokował internet w całej okolicy. A szkoła jest na takie ataki narażona. To na przykład absolwent szkoły, który czuł się w niej niedoceniany, a teraz pokaże, że potrafi. Blokowanie sieci w polskich szkołach występowało wielokrotnie. Dlatego tak ważna jest aktualizacja oprogramowania, stosowanie zapór i oprogramowania antywirusowego. Długo mówiło się, że aktualizacja oprogramowania

komputerów, smartfonów, tabletów, nawet tablic interaktywnych jest po to, żeby producenci wymusili wymianę produktu na nowy. Nie. To dziś kwestia zwiększenia bezpieczeństwa.

Czy nauczyciele czują, że cyberbezpieczeństwo jest istotne? Nauczyciel wczesnoszkolny z jednej z krakowskich podstawówek: – Mamy elektroniczne dzienniki. Piszemy w nich do rodziców o zachowaniach dzieci. Czasem jedno dziecko pobiło drugie. Innym razem, że dziecko sika w majtki. Jeszcze innym, że mówi „zbiję cię, jak moją mamę". To są bardzo wrażliwe dane, ale nie wiedziałem, że mogą stać się publiczne, jeśli się nie wyloguję. Nikt mnie nie szkolił.

Maciej Rakowski: – Bo tak działa ludzka psychika i takie są nasze nawyki. Działamy w schematach póki coś się nie stanie, albo ktoś sugestywnie nie powie nam, co może złego się stać. Moją rekomendacją jest szkolenie z cyberbezpieczeństwa w ramach, albo obok obowiązkowych szkoleń BHP. Dziś bezpieczeństwo w sieci bywa ważniejsze od bezpieczeństwa budynku. Nadużycia, przestępcy przenieśli się do sieci, a nasz system jeszcze tego nie widzi.

Trzeba też pamiętać o zdjęciach, które oficjalnie udostępnia szkoła. One potencjalnie są narażone na przerobienie przez AI w kontekstach zupełnie niepożądanych. Zwycięzca olimpiady matematycznej może stać się obiektem drwin ubranych w dowolną kreację AI. Tu zarządzający komunikacją szkoły powinni łączyć pozytywne emocje z sukcesów swoich wychowanków, z wiedzą o kontekście społecznym/koleżeńskim ich funkcjonowania. A z tyłu głowy mając to, że wszystko może być pretekstem do wykorzystania w niedobrych zamiarach. Maciej Rakowski: – Publikacja wizerunku i nauczycieli, i uczniów na pewno powinna być redukowana, dla bezpieczeństwa. Znam przypadki, w których montowano filmy ze szkół, mieszając konteksty, ale przedstawiały one osobę w niekorzystnym świetle. Dobrze wiemy, że kamery można dziś prawie wszędzie wnieść. Ale szkoła nie powinna ułatwiać i dostarczać materiałów do takich manipulacji.

Rakowski: – Nie powinniśmy też przenosić żadnych danych poza szkołę związanych z dokumentacją szkoły i danymi osobowymi i wrażliwymi, ale jeżeli chodzi nawet o materiały które mogą przynosić i nauczyciele i uczniowie, w podstawi prezentacji i projektów powinny być zweryfikowane czy nie zawierają wirusów lub innego szkodliwego oprogramowania które może mieć wpływ na sieć szkolna.

***

Temat jest rozwojowy, bo świat się rozwija. Bo prowokuje pytania o egzaminy, matury w przyszłości. Czy ich nie trzeba będzie przenieść do instytucji zewnętrznych? Czy jeśli nasze placówki oświatowe są obarczone instytucjonalnymi regułami, które nie nadążają

za technologią, to poradzą sobie z obiektywną oceną wiedzy? Mamy mikrosłuchawki, minikamery – ich nie widać. Mamy kalkulatory, które wyglądają retro, ale mogą być komputerami piszącymi maturę.

Coraz mniej jesteśmy w stanie weryfikować. – Mikrosłuchawka na przykład. Ktoś może prowadzić rozmowę i nikt obok nie może tego zweryfikować. Jej nie widać. Do tego dochodzą okulary, soczewki nawet – tak, w soczewkach kontaktowych możemy mieć informacje. Wszystko to wymaga nowego podejścia do bezpieczeństwa na dziś i jutro.

***

Drodzy Nauczyciele, Dyrektorzy. Bo to dla Was raport, poniżej praktyczne pytania:

- Czy gdyby korespondencja z wewnątrz systemu/elektronicznego dziennika stała się publiczną, to mogłaby kogoś narazić na nieprzyjemności?
- Czy rodzice dzieci mogliby czuć się niekomfortowo, jeśli ich rozmowy i dane dotyczące zachowań i oceny kompetencji ich dzieci stały się publiczne?
- Czy spotkaliście się z sytuacją kiedy ktoś dostał się do danych, które do niego nie powinny być dostępne?
- Jaś wysłał z Waszego konta do rodziców swojej klasy: „Pani Jola jest gupia.” A Jaś głupi nie jest.

Nie bądźmy głupi. Bo w tej pracy można się spełnić, żeby nie stracić.

* **Gabriela Olszowska**, doktor nauk humanistycznych, absolwentka polonistyki na Uniwersytecie Jagiellońskim, zarządzania w oświacie na Politechnice Krakowskiej i europeistyki w Akademii Ignatianum. Uczyła języka polskiego, przez lata była dyrektorką krakowskiego Gimnazjum nr 2. Autorka książki „O!cena. Od przepisów do sztuki oceniania”. Prowadziła szkolenia z oceniania dla dyrektorów i rad pedagogicznych.

** **Maciej Rakowski** – nauczyciel dyplomowany w Technikum nr 4 w Zespole Szkół Elektrycznych we Włocławku – szkoły z rankingu złotej 100.s Menedżer kierunku logistyki w Wyższej Szkole Bankowej w Toruniu i w Bydgoszczy. W roku 2018 roku został „Nauczycielem na medal” w konkursie „Gazety Pomorskiej”, „Expressu Bydgoskiego”. Aktywny uczestnik obrad "Okrągłego stołu edukacyjnego”. Przeszkolił kilkuset nauczycieli, m.in. w aspekcie cyfrowego bezpieczeństwa.

6. Analiza wyników mini audytów szkół

Mini audyty przeprowadzone w szkołach miały na celu rozpoznanie praktycznego poziomu organizacji cyberbezpieczeństwa w placówkach oświatowych. W odróżnieniu od klasycznego badania ankietowego, ich celem nie było wyłącznie zebranie deklaratywnych odpowiedzi, lecz uchwycenie codziennych praktyk, sposobów działania oraz potencjalnych luk organizacyjnych i kompetencyjnych występujących w środowisku szkolnym.

Zakres mini audytów obejmował zarówno kwestie formalne i organizacyjne, jak i praktyczne aspekty korzystania z narzędzi cyfrowych przez kadrę szkolną. Szczególną uwagę zwrócono na sposób zarządzania odpowiedzialnością za cyberbezpieczeństwo, korzystanie z haseł i dodatkowych metod uwierzytelniania, komunikację elektroniczną, przesyłanie danych osobowych, korzystanie z urządzeń prywatnych i służbowych, przechowywanie plików, aktualizacje systemów, dostęp do sieci Wi-Fi oraz podstawowe procedury ograniczania ryzyka.

W niniejszym rozdziale przedstawiono wybrane wyniki mini audytów w formie graficznej. Zaprezentowane diagramy odnoszą się do pytań, które uznano za szczególnie istotne z punktu widzenia diagnozy poziomu cyberbezpieczeństwa szkół.

Wykres 6.1.

Wykres 6.1 przedstawia rozkład odpowiedzi na pytanie dotyczące tego, czy w badanych szkołach funkcjonuje osoba realnie odpowiedzialna za dbanie o standardy bezpieczeństwa, w tym m.in. aktualizowanie systemów lub stron internetowych, czy też działania podejmowane są głównie reaktywnie, w odpowiedzi na incydenty.

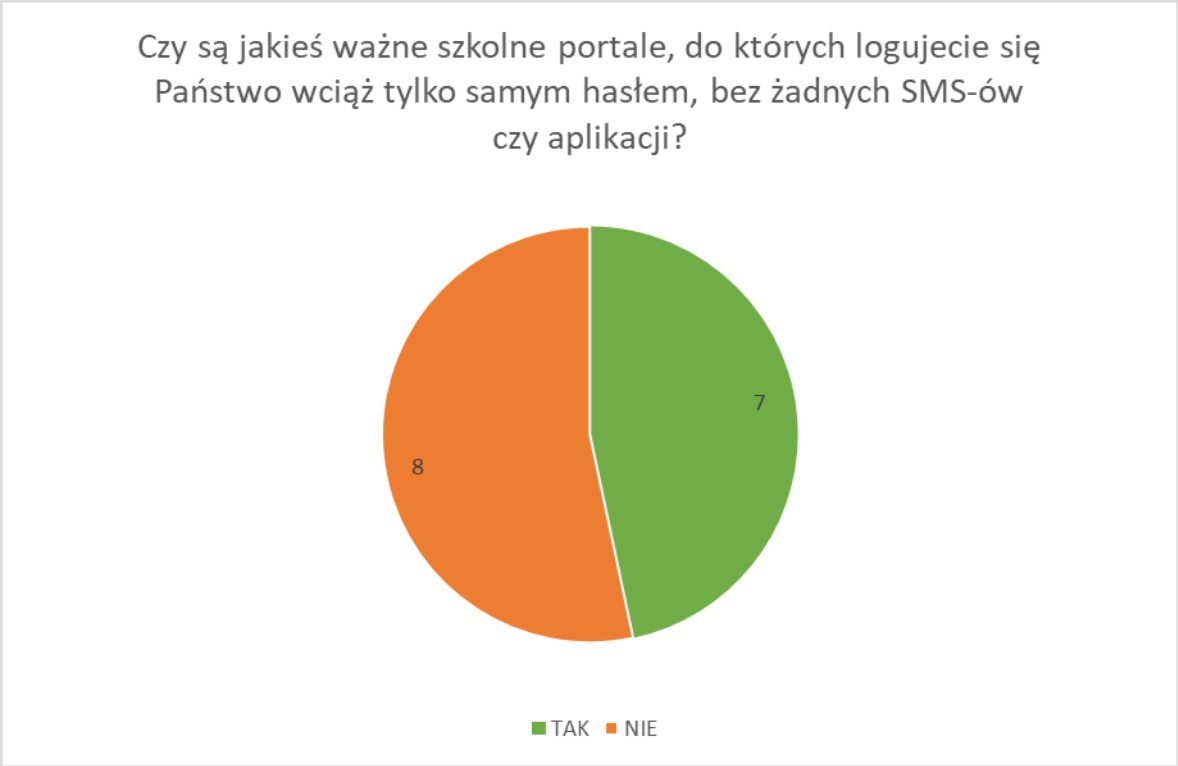
Zdecydowana większość badanych placówek zadeklarowała, że posiada taką osobę – odpowiedź „tak" wskazano w 14 z 15 przypadków, co stanowi 93,3% wszystkich odpowiedzi. Jedynie jedna szkoła, tj. 6,7% badanych, wskazała odpowiedź „nie". Wynik ten sugeruje, że w większości objętych mini audytem placówek odpowiedzialność za bieżące utrzymanie podstawowych standardów bezpieczeństwa jest formalnie lub praktycznie przypisana konkretnej osobie.

Wykres 6.2

Wykres 6.2 przedstawia rozkład odpowiedzi na pytanie dotyczące stosowania dodatkowych mechanizmów zabezpieczających logowanie do e-dziennika lub poczty elektronicznej, takich jak kod SMS, potwierdzenie w aplikacji mobilnej lub inna forma uwierzytelniania wieloskładnikowego. Większość badanych placówek zadeklarowała, że logowanie do wskazanych systemów wymaga czegoś więcej niż podania hasła. Odpowiedź „tak" wskazano w 10 z 15 przypadków, co stanowi 66,7% wszystkich odpowiedzi. Jednocześnie 5 placówek, czyli 33,3% badanych, zadeklarowało, że dostęp do e-dziennika lub poczty nadal odbywa się wyłącznie z wykorzystaniem hasła.

Wyniki te wskazują, że w znacznej części szkół wdrożono już dodatkowe mechanizmy ochrony kont użytkowników, co należy uznać za pozytywną praktykę z punktu widzenia cyberbezpieczeństwa. Jednocześnie fakt, że jedna trzecia badanych placówek nie stosuje dodatkowego zabezpieczenia logowania, pokazuje istotny obszar ryzyka. W przypadku systemów takich jak e-dziennik czy poczta elektroniczna, które mogą zawierać dane uczniów, rodziców i pracowników szkoły, opieranie dostępu wyłącznie na haśle zwiększa podatność na skutki phishingu, przejęcia konta lub wykorzystania słabych bądź powtarzanych haseł.

Wykres 6.3.

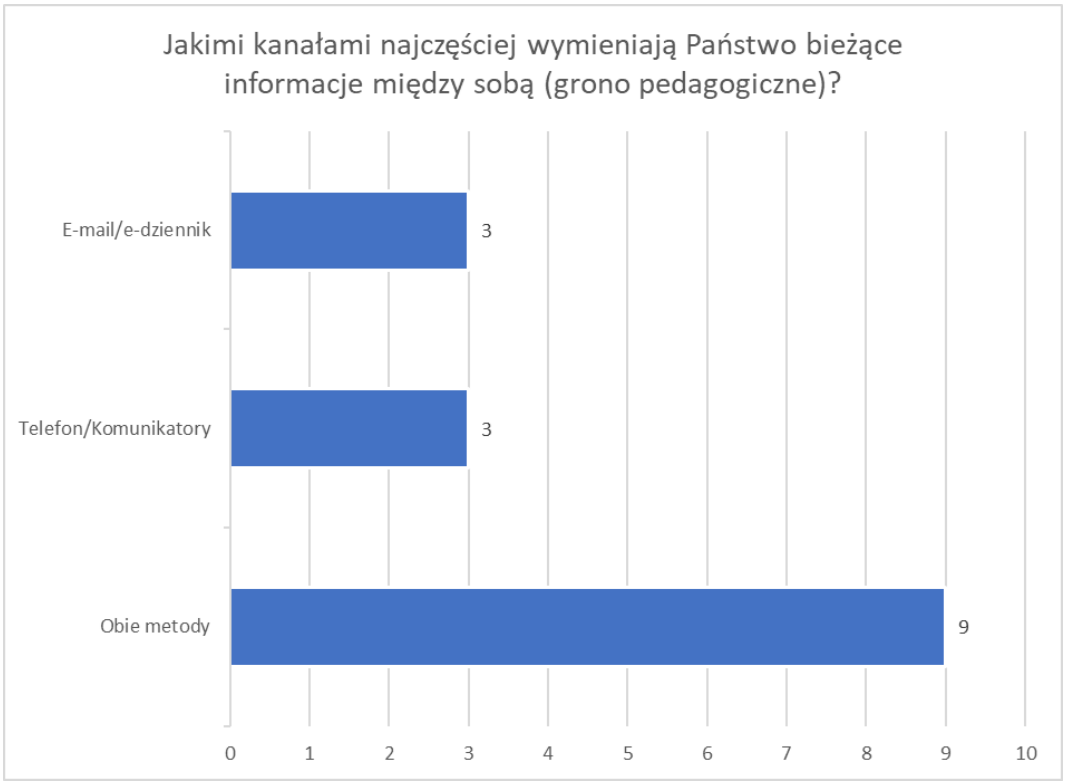


Wykres 6.3 przedstawia rozkład odpowiedzi na pytanie, czy w badanych szkołach funkcjonują ważne portale szkolne, do których logowanie nadal odbywa się wyłącznie za pomocą hasła, bez dodatkowego potwierdzenia, np. kodem SMS lub w aplikacji mobilnej. Odpowiedzi respondentów rozłożyły się niemal równomiernie. W 7 z 15 przypadków, tj. 46,7% odpowiedzi, wskazano, że w szkole nadal istnieją istotne portale, do których dostęp zabezpieczony jest wyłącznie hasłem. Z kolei 8 placówek, czyli 53,3% badanych, zadeklarowało brak takich portali lub stosowanie dodatkowych mechanizmów zabezpieczających logowanie.

Uzyskane wyniki wskazują na wyraźne zróżnicowanie praktyk w zakresie zabezpieczania dostępu do szkolnych systemów cyfrowych. Choć niewielka większość badanych placówek deklaruje, że ważne portale nie są już chronione wyłącznie hasłem, to skala

odpowiedzi twierdzących pozostaje istotna z punktu widzenia bezpieczeństwa. Oznacza to, że w niemal połowie objętych mini audytem szkół mogą nadal funkcjonować systemy, w których poziom ochrony dostępu zależy przede wszystkim od siły i poufności hasła użytkownika.

Wykres 6.4.

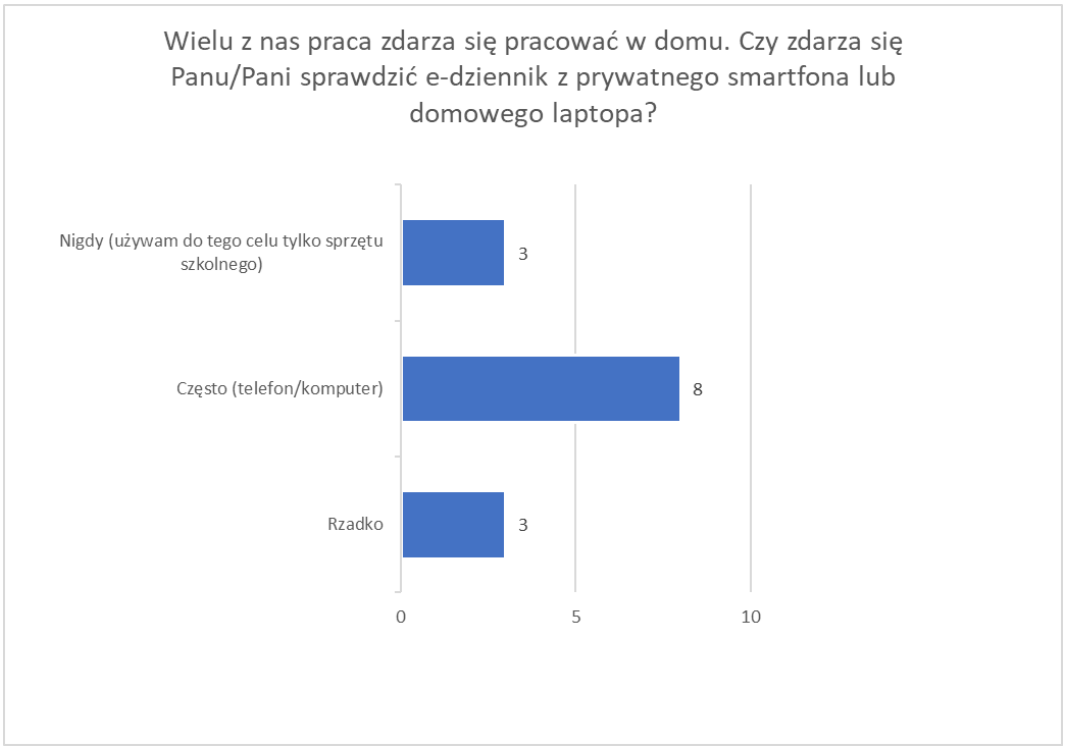


Wykres 6.4 przedstawia zagregowany rozkład odpowiedzi na pytanie dotyczące kanałów najczęściej wykorzystywanych przez grono pedagogiczne do wymiany bieżących informacji. Odpowiedzi zostały pogrupowane w trzy kategorie: komunikację za pośrednictwem e-maila lub e-dziennika, komunikację telefoniczną lub przez komunikatory oraz model mieszany, obejmujący korzystanie z obu typów kanałów. Najczęściej wskazywaną odpowiedzią był model mieszany – 9 z 15 badanych placówek zadeklarowało, że w komunikacji wewnętrznej wykorzystuje zarówno e-mail lub e-dziennik, jak i telefon lub komunikatory. Stanowi to 60% wszystkich odpowiedzi. Po 3 wskazania, czyli po 20% odpowiedzi, uzyskały kategorie obejmujące wyłącznie e-mail/e-dziennik oraz telefon/komunikatory.

Uzyskane wyniki wskazują, że w większości szkół komunikacja wewnętrzna ma charakter wielokanałowy. Oznacza to, że obok formalnych lub półformalnych narzędzi, takich jak e-mail i e-dziennik, istotną rolę odgrywają również szybsze kanały kontaktu, w tym telefon i komunikatory. Z perspektywy organizacyjnej może to zwiększać sprawność bieżącej wymiany informacji, jednak z punktu widzenia cyberbezpieczeństwa wymaga jasnego

określenia zasad, jakie informacje mogą być przekazywane poszczególnymi kanałami. W szczególności należy zwrócić uwagę na ryzyka związane z wykorzystywaniem komunikatorów lub prywatnych urządzeń do przekazywania informacji służbowych, zwłaszcza jeżeli mogą one dotyczyć uczniów, rodziców, spraw wychowawczych lub danych osobowych.

Wykres 6.5.

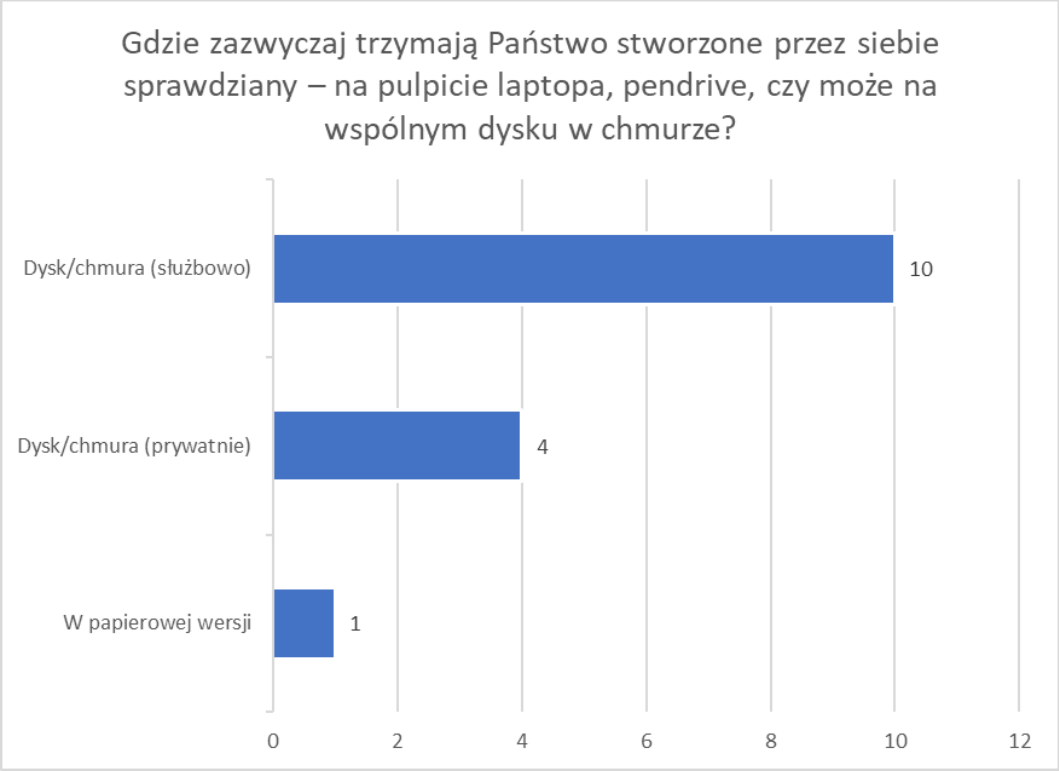


Wykres 6.5 przedstawia rozkład odpowiedzi na pytanie dotyczące korzystania z prywatnych urządzeń, takich jak smartfon lub domowy laptop, do sprawdzania e-dziennika podczas pracy poza szkołą. Największa grupa respondentów zadeklarowała, że często korzysta w tym celu z prywatnego telefonu lub komputera – taką odpowiedź wskazano w 8 przypadkach, co stanowi 57,1% odpowiedzi udzielonych na to pytanie. Odpowiedź „rzadko" wskazano w 3 przypadkach, podobnie jak odpowiedź „nigdy", oznaczającą korzystanie wyłącznie ze sprzętu szkolnego. Obie te kategorie stanowią po 21,4% odpowiedzi.

Uzyskane dane wskazują, że korzystanie z prywatnych urządzeń do obsługi e-dziennika jest w badanych placówkach praktyką stosunkowo rozpowszechnioną. Łącznie 11 respondentów, czyli 78,6% osób odpowiadających na to pytanie, zadeklarowało, że przynajmniej sporadycznie sprawdza e-dziennik z prywatnego smartfona lub domowego laptopa. Z perspektywy organizacyjnej może to wynikać z potrzeby elastycznego dostępu do informacji oraz specyfiki pracy nauczycieli, która często wykracza poza czas i miejsce pracy w szkole. Jednocześnie wynik ten wskazuje na istotny obszar ryzyka z punktu

widzenia cyberbezpieczeństwa. Korzystanie z prywatnych urządzeń może utrudniać kontrolę nad poziomem ich zabezpieczenia, aktualizacjami, ochroną antywirusową, zapamiętywaniem haseł czy dostępem osób trzecich do urządzenia.

Wykres 6.6.

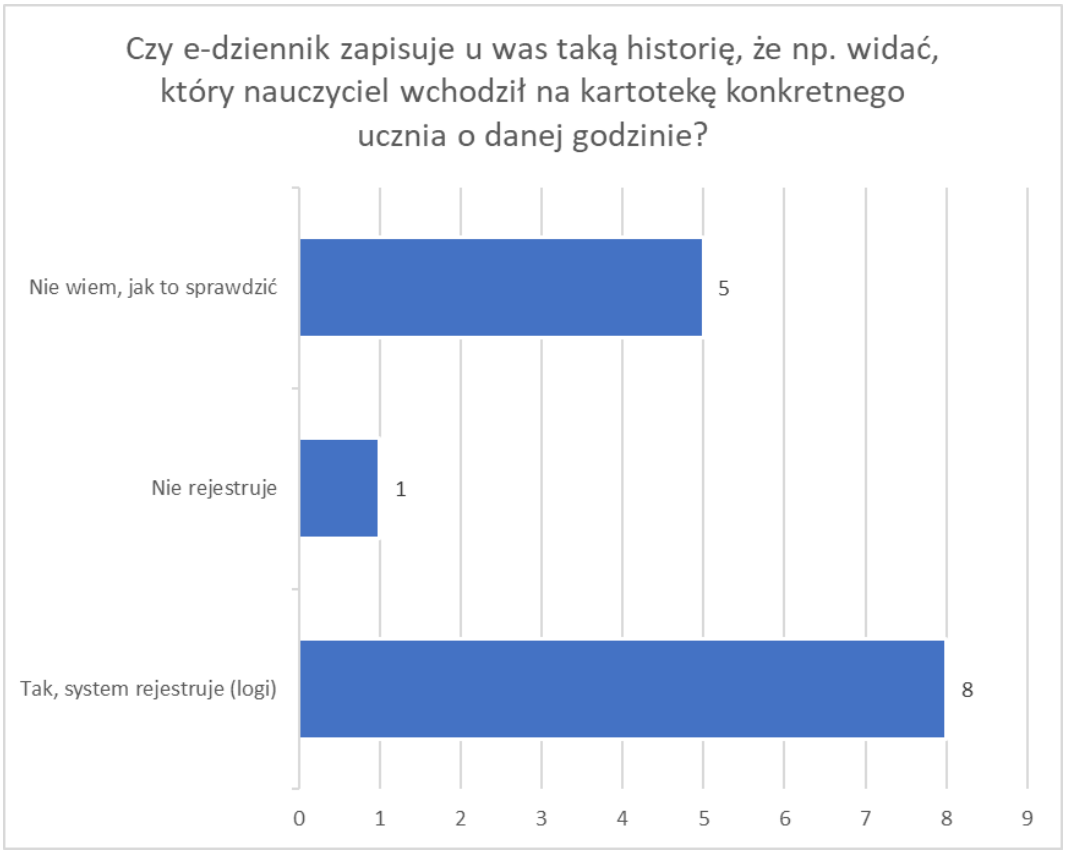


Wykres 6.6 przedstawia rozkład odpowiedzi na pytanie dotyczące miejsca przechowywania materiałów tworzonych przez nauczycieli, takich jak sprawdziany. Odpowiedzi zostały pogrupowane według trzech podstawowych kategorii: przechowywanie na dysku lub w chmurze służbowej, przechowywanie na dysku lub w chmurze prywatnej oraz przechowywanie w wersji papierowej. Największa część respondentów wskazała, że materiały tego typu przechowywane są na dysku lub w chmurze wykorzystywanej służbowo. Taką odpowiedź odnotowano w 10 z 15 przypadków, co stanowi 66,7% wszystkich odpowiedzi. Przechowywanie materiałów na prywatnym dysku lub w prywatnej chmurze wskazano w 4 przypadkach, tj. 26,7% odpowiedzi. Jedna odpowiedź, stanowiąca 6,7% ogółu, odnosiła się do przechowywania materiałów w wersji papierowej.

Uzyskane dane wskazują, że w większości badanych placówek dominują rozwiązania służbowe, co można uznać za korzystne z punktu widzenia organizacji pracy oraz bezpieczeństwa informacji. Przechowywanie materiałów na zasobach kontrolowanych przez szkołę lub organ prowadzący ułatwia zarządzanie dostępem, tworzenie kopii zapasowych oraz ograniczanie ryzyka utraty danych. Jednocześnie niemal jedna czwarta

odpowiedzi wskazuje na korzystanie z prywatnych zasobów cyfrowych do przechowywania materiałów szkolnych. Jest to istotny sygnał diagnostyczny, ponieważ prywatne dyski, konta chmurowe lub urządzenia mogą pozostawać poza kontrolą szkoły, a tym samym utrudniać zapewnienie jednolitych standardów bezpieczeństwa.

Wykres 6.7.

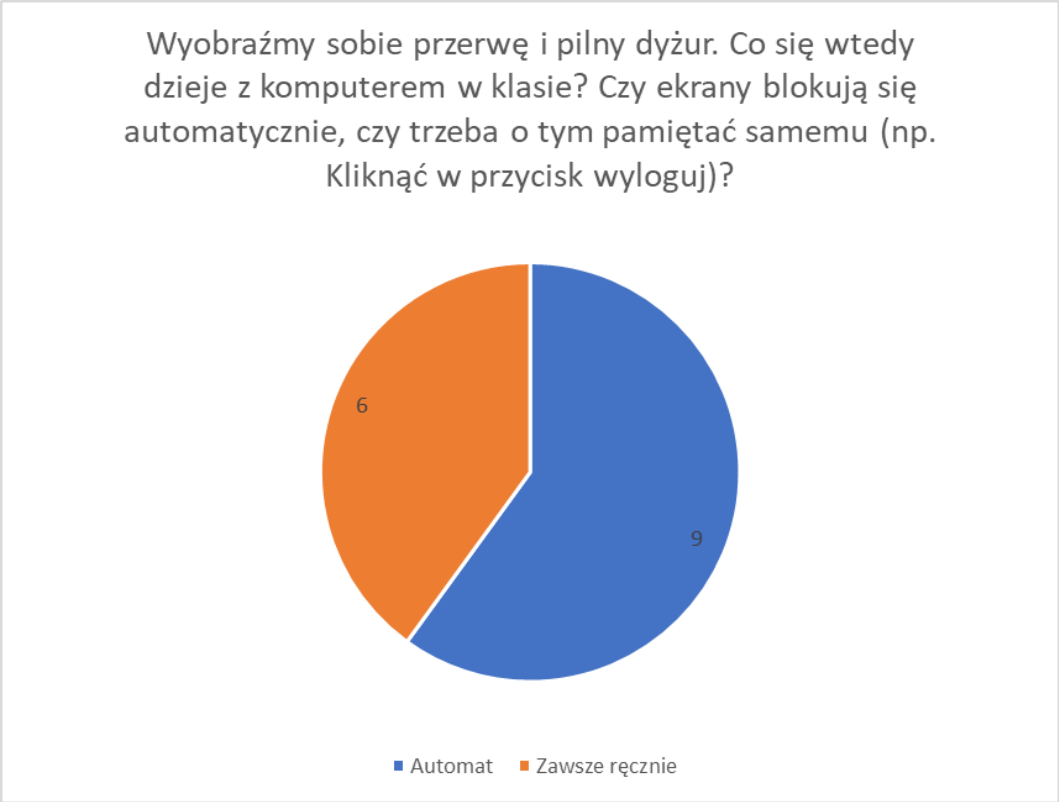


Wykres 6.7 przedstawia rozkład odpowiedzi na pytanie dotyczące tego, czy e-dziennik wykorzystywany w szkole rejestruje historię dostępu do kartoteki ucznia, tj. czy możliwe jest sprawdzenie, który nauczyciel wchodził do danych konkretnego ucznia i o jakiej godzinie. Największa grupa respondentów wskazała, że system rejestruje tego typu informacje w postaci logów. Taką odpowiedź odnotowano w 8 z 14 przypadków, co stanowi 57,1% odpowiedzi na to pytanie. Jednocześnie 5 respondentów, czyli 35,7%, zadeklarowało, że nie wie, jak sprawdzić taką informację. Tylko w jednym przypadku, tj. 7,1% odpowiedzi, wskazano, że e-dziennik nie rejestruje historii dostępu.

Uzyskane dane pokazują, że w większości badanych przypadków istnieje techniczna możliwość rejestrowania dostępu do danych ucznia, co stanowi istotny element kontroli i rozliczalności działań użytkowników systemu. Z perspektywy ochrony danych osobowych i cyberbezpieczeństwa jest to rozwiązanie korzystne, ponieważ pozwala identyfikować nietypowe lub nieuprawnione działania oraz odtwarzać przebieg zdarzeń

w przypadku incydentu. Jednocześnie relatywnie wysoki odsetek odpowiedzi „nie wiem, jak to sprawdzić” wskazuje na lukę o charakterze kompetencyjnym lub organizacyjnym.

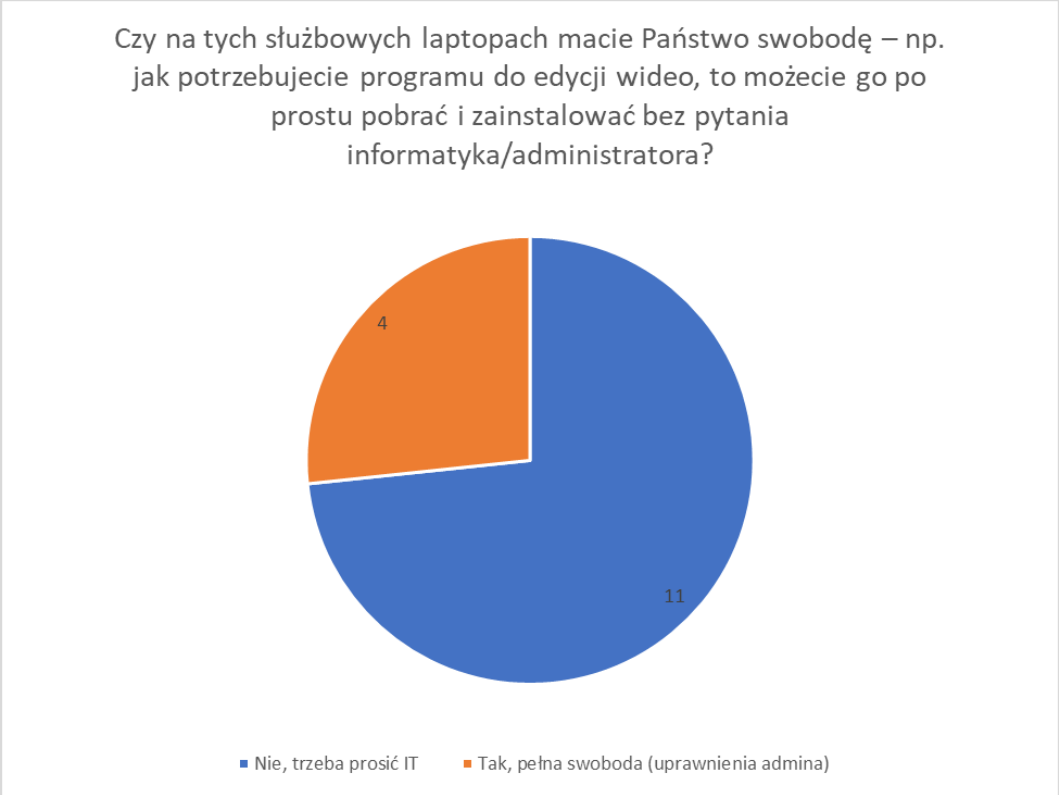
Wykres 6.8.



Wykres 6.8 przedstawia rozkład odpowiedzi na pytanie dotyczące sposobu zabezpieczania komputerów znajdujących się w salach lekcyjnych w sytuacjach, gdy nauczyciel musi opuścić stanowisko pracy, np. podczas przerwy lub pilnego dyżuru. Większość respondentów wskazała, że komputery blokują się automatycznie. Taką odpowiedź odnotowano w 9 z 15 przypadków, co stanowi 60% wszystkich odpowiedzi. Jednocześnie w 6 przypadkach, czyli w 40% odpowiedzi, wskazano, że zablokowanie komputera wymaga każdorazowo ręcznego działania użytkownika, np. wylogowania się lub samodzielnego zablokowania ekranu.

Uzyskane wyniki pokazują, że w części badanych placówek stosowane są mechanizmy automatycznego zabezpieczania stanowisk pracy, co należy uznać za korzystną praktykę ograniczającą ryzyko nieuprawnionego dostępu do danych i systemów szkolnych. Automatyczna blokada ekranu ma szczególne znaczenie w środowisku szkolnym, w którym komputery mogą znajdować się w przestrzeniach dostępnych dla uczniów lub innych osób. Jednocześnie relatywnie wysoki udział odpowiedzi wskazujących na konieczność ręcznego blokowania komputera oznacza, że w znacznej części przypadków bezpieczeństwo zależy od indywidualnej pamięci i nawyków użytkownika.

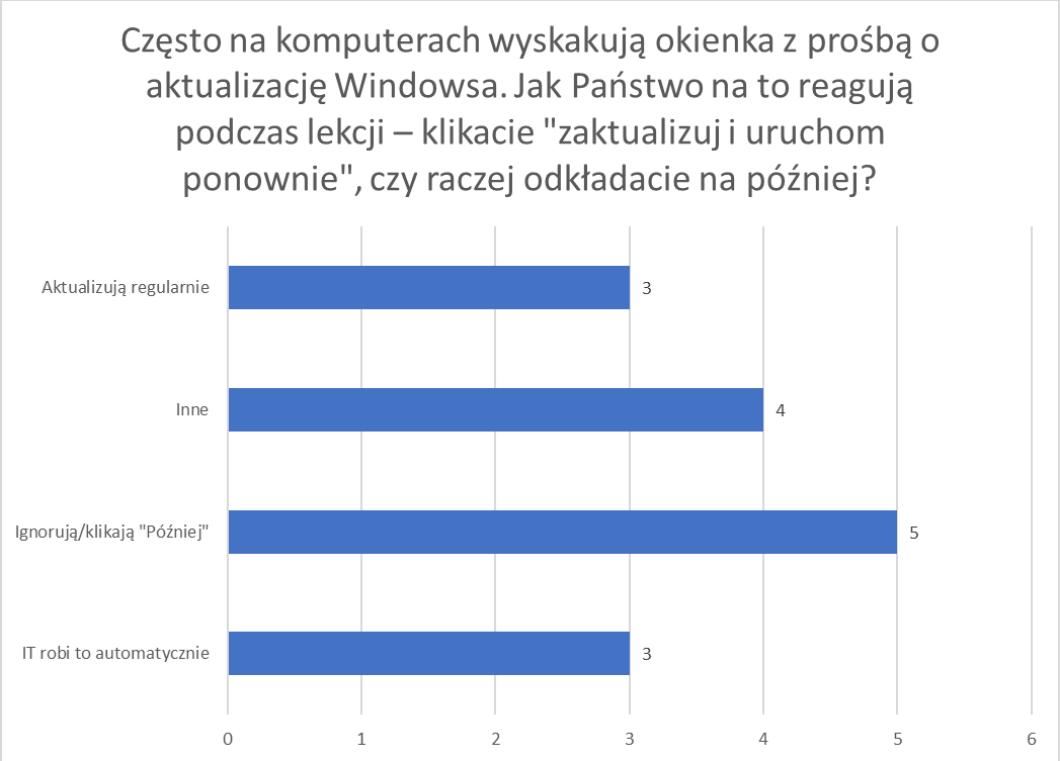
Wykres 6.9.



Wykres 6.9 przedstawia rozkład odpowiedzi na pytanie dotyczące uprawnień użytkowników na służbowych laptopach, w szczególności możliwości samodzielnego pobierania i instalowania oprogramowania bez udziału informatyka lub administratora. Zdecydowana większość respondentów wskazała, że instalacja dodatkowego oprogramowania wymaga zgody lub działania ze strony IT. Taką odpowiedź odnotowano w 11 z 15 przypadków, co stanowi 73,3% wszystkich odpowiedzi. Jednocześnie w 4 przypadkach, tj. 26,7% odpowiedzi, zadeklarowano, że użytkownicy mają pełną swobodę instalowania programów, co oznacza posiadanie uprawnień administracyjnych na służbowych urządzeniach.

Uzyskane dane wskazują, że w większości badanych placówek stosowany jest model ograniczający samodzielną instalację oprogramowania przez użytkowników. Z perspektywy cyberbezpieczeństwa jest to rozwiązanie korzystne, ponieważ pozwala ograniczyć ryzyko instalacji niezweryfikowanych, nieaktualnych lub potencjalnie szkodliwych aplikacji. Kontrola po stronie IT sprzyja również utrzymaniu większej spójności środowiska technicznego oraz ułatwia zarządzanie aktualizacjami, licencjami i konfiguracją sprzętu. Jednocześnie fakt, że w ponad jednej czwartej przypadków użytkownicy posiadają pełne uprawnienia administracyjne, wskazuje na istotny obszar wymagający uwagi. Taki model zwiększa ryzyko przypadkowego zainstalowania niebezpiecznego oprogramowania, naruszenia konfiguracji systemu lub obejścia standardowych zabezpieczeń.

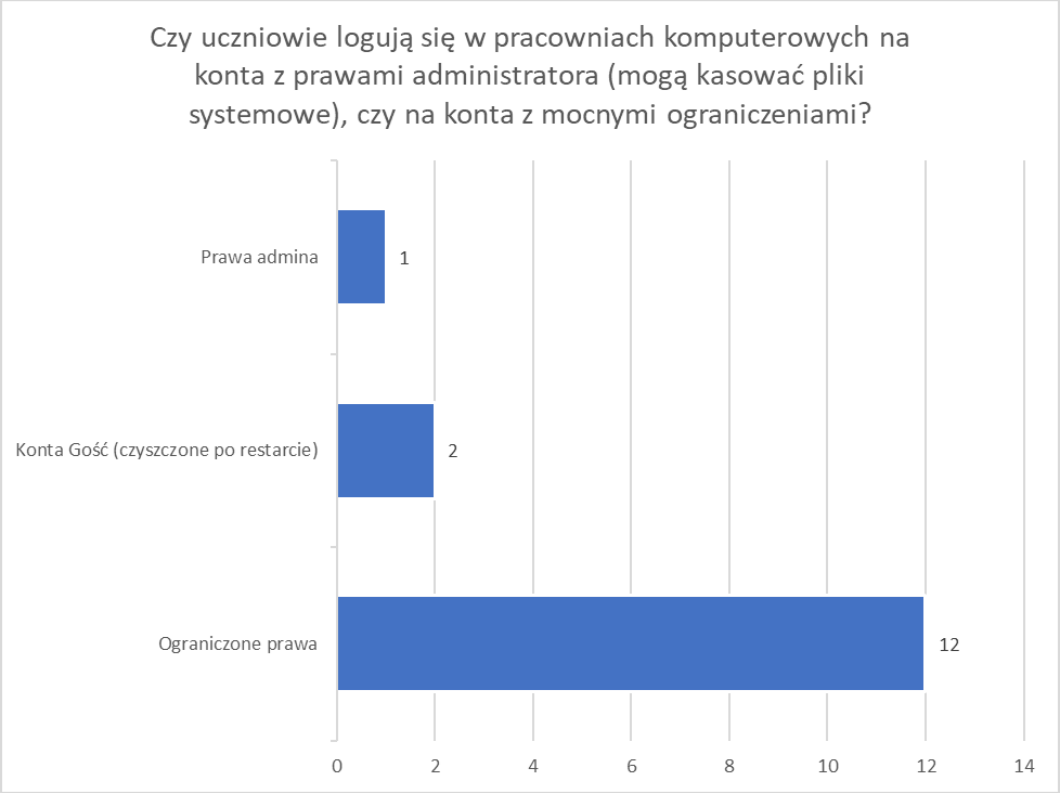
Wykres 6.10



Wykres 6.10 przedstawia rozkład odpowiedzi na pytanie dotyczące sposobu reagowania na komunikaty systemowe związane z aktualizacją systemu Windows, pojawiające się na komputerach wykorzystywanych w pracy szkolnej. Odpowiedzi respondentów są zróżnicowane. Największą grupę stanowią odpowiedzi wskazujące na odkładanie aktualizacji na później lub ich ignorowanie - taką praktykę wskazano w 5 z 15 przypadków, co stanowi 33,3% wszystkich odpowiedzi. W 3 przypadkach, tj. 20% odpowiedzi, zadeklarowano regularne wykonywanie aktualizacji przez użytkowników. Taki sam odsetek odpowiedzi — 3 wskazania, czyli 20% — dotyczył sytuacji, w których aktualizacje są wykonywane automatycznie przez IT. Pozostałe 4 odpowiedzi, stanowiące 26,7% ogółu, zakwalifikowano do kategorii „inne”.

Uzyskane dane wskazują, że praktyki związane z aktualizacją systemów nie są jednolite w badanych placówkach. Część szkół posiada rozwiązania organizacyjne lub techniczne, które sprzyjają regularnemu aktualizowaniu komputerów, w tym automatyzację po stronie IT. Jednocześnie istotny udział odpowiedzi wskazujących na odkładanie aktualizacji pokazuje, że w części przypadków bezpieczeństwo systemu może zależeć od indywidualnej decyzji użytkownika oraz od bieżących okoliczności pracy, np. trwania lekcji lub braku czasu. Z perspektywy cyberbezpieczeństwa regularne aktualizacje mają podstawowe znaczenie, ponieważ pozwalają usuwać znane podatności systemu i ograniczać ryzyko wykorzystania ich przez złośliwe oprogramowanie lub osoby nieuprawnione.

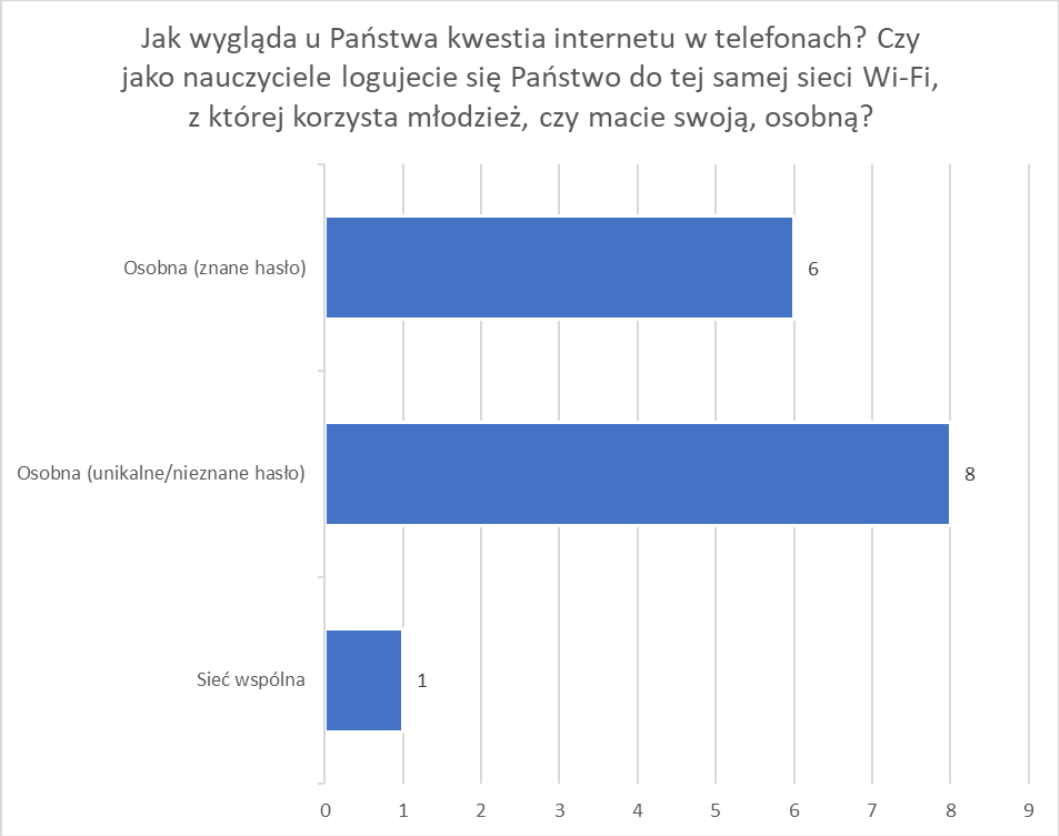
Wykres 6.11.



Wykres 6.11 przedstawia rozkład odpowiedzi na pytanie dotyczące poziomu uprawnień, z jakimi uczniowie korzystają z komputerów w pracowniach komputerowych. Pytanie odnosiło się do tego, czy uczniowie logują się na konta z prawami administratora, konta gościa czyszczone po restarcie, czy na konta z ograniczonymi uprawnieniami. Zdecydowana większość respondentów wskazała, że uczniowie korzystają z kont z ograniczonymi prawami. Taką odpowiedź odnotowano w 12 z 15 przypadków, co stanowi 80% wszystkich odpowiedzi. W 2 przypadkach, tj. 13,3% odpowiedzi, wskazano korzystanie z kont typu gość, które są czyszczone po ponownym uruchomieniu komputera. Tylko w jednym przypadku, czyli 6,7% odpowiedzi, zadeklarowano, że uczniowie logują się na konta z prawami administratora.

Uzyskane dane wskazują, że w większości badanych placówek stosowane są rozwiązania ograniczające uprawnienia uczniów na komputerach szkolnych. Jest to pozytywna praktyka z punktu widzenia cyberbezpieczeństwa, ponieważ zmniejsza ryzyko przypadkowej lub celowej ingerencji w ustawienia systemowe, instalowania niepożądanego oprogramowania, usuwania plików systemowych czy obchodzenia zabezpieczeń. Jednocześnie pojedyncze wskazanie dotyczące korzystania przez uczniów z kont administracyjnych należy traktować jako istotny sygnał ryzyka.

Wykres 6.12.



Wykres 6.12 przedstawia rozkład odpowiedzi na pytanie dotyczące sposobu korzystania z sieci Wi-Fi przez nauczycieli, w szczególności tego, czy kadra pedagogiczna korzysta z tej samej sieci co uczniowie, czy z osobnej sieci przeznaczonej dla pracowników szkoły. Największa grupa respondentów wskazała, że nauczyciele korzystają z osobnej sieci Wi-Fi, do której hasło jest unikalne lub nieznane uczniom. Taką odpowiedź odnotowano w 8 z 15 przypadków, co stanowi 53,3% wszystkich odpowiedzi. W 6 przypadkach, tj. 40% odpowiedzi, wskazano również istnienie osobnej sieci dla nauczycieli, jednak z hasłem znanym szerzej lub funkcjonującym w praktyce jako łatwo dostępne. Tylko w jednym przypadku, czyli 6,7% odpowiedzi, zadeklarowano korzystanie przez nauczycieli i uczniów ze wspólnej sieci Wi-Fi.

Uzyskane dane wskazują, że w zdecydowanej większości badanych placówek istnieje organizacyjne rozdzielenie dostępu do sieci dla nauczycieli i uczniów. Jest to rozwiązanie korzystne z punktu widzenia cyberbezpieczeństwa, ponieważ ogranicza ryzyko niepożądanego dostępu do zasobów wykorzystywanych przez kadrę szkolną oraz ułatwia zarządzanie ruchem sieciowym i uprawnieniami użytkowników. Jednocześnie istotny jest fakt, że w 6 przypadkach osobna sieć funkcjonuje przy wykorzystaniu hasła znanego szerszej grupie użytkowników. Oznacza to, że samo formalne wydzielenie sieci nie zawsze musi przekładać się na faktycznie wyższy poziom kontroli dostępu. Jeżeli hasło

jest powszechnie znane, rzadko zmieniane lub przekazywane osobom nieuprawnionym, skuteczność takiego zabezpieczenia może być ograniczona.

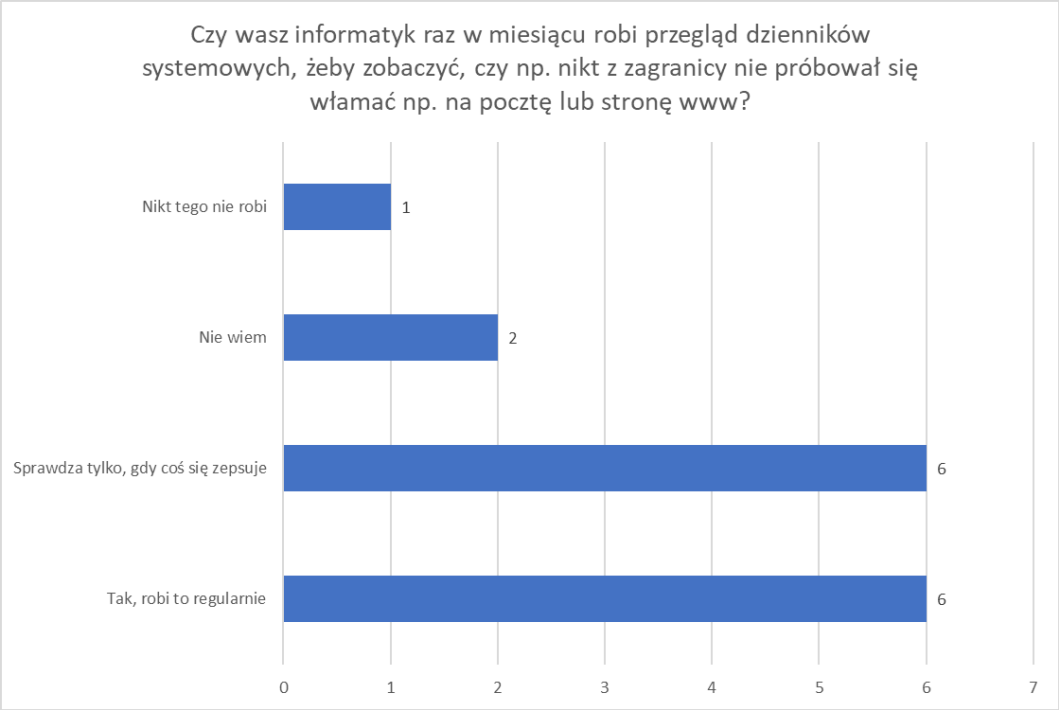
Wykres 6.13.

Wykres 6.13 przedstawia rozkład odpowiedzi na pytanie dotyczące sposobu udostępniania Internetu osobom zewnętrznym, takim jak prelegenci prowadzący warsztaty lub zajęcia w szkole. Zdecydowana większość respondentów wskazała, że w takich sytuacjach hasło do sieci wpisuje nauczyciel lub inna uprawniona osoba. Taką odpowiedź odnotowano w 12 z 15 przypadków, co stanowi 80% wszystkich odpowiedzi. W 3 przypadkach, tj. 20% odpowiedzi, wskazano korzystanie z wydzielonej sieci przeznaczonej dla gości.

Uzyskane dane pokazują, że w większości badanych placówek dostęp do Internetu dla osób zewnętrznych jest udostępniany w sposób kontrolowany na poziomie praktyki organizacyjnej - hasło nie jest publicznie wywieszone ani samodzielnie przekazywane gościowi, lecz wpisywane przez pracownika szkoły. Takie rozwiązanie ogranicza ryzyko swobodnego rozpowszechniania hasła, jednak nie jest równoważne z pełnym wydzieleniem dostępu dla użytkowników zewnętrznych. Z punktu widzenia cyberbezpieczeństwa najbardziej pożądanym rozwiązaniem jest osobna sieć dla gości, odseparowana od sieci wykorzystywanej przez pracowników szkoły i systemy wewnętrzne. Fakt, że takie rozwiązanie wskazano jedynie w 3 przypadkach, sugeruje, że

w większości placówek dostęp gości może odbywać się przy wykorzystaniu sieci, która nie zawsze jest technicznie oddzielona od zasobów szkolnych.

Wykres 6.14.

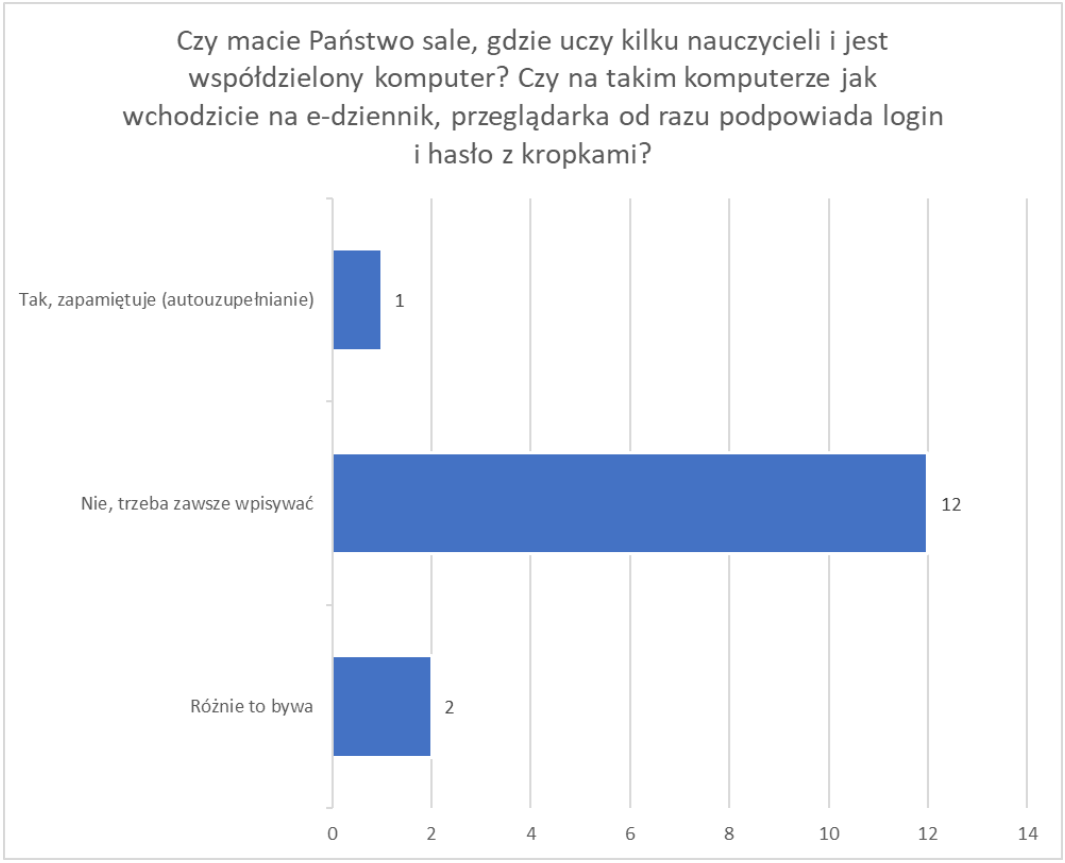


Wykres 6.14 przedstawia rozkład odpowiedzi na pytanie dotyczące regularnego przeglądu dzienników systemowych, w tym sprawdzania, czy nie występowały próby nieuprawnionego dostępu do poczty, strony internetowej lub innych zasobów szkoły. Odpowiedzi respondentów wskazują na zróżnicowany poziom praktyk w tym obszarze. W 6 z 15 przypadków, co stanowi 40% wszystkich odpowiedzi, zadeklarowano, że informatyk lub osoba odpowiedzialna za obsługę techniczną regularnie dokonuje przeglądu dzienników systemowych. Taki sam odsetek odpowiedzi – również 6 wskazań, czyli 40% – dotyczył sytuacji, w których logi są sprawdzane dopiero wtedy, gdy pojawi się problem lub coś przestaje działać. W 2 przypadkach, tj. 13,3% odpowiedzi, respondenci nie wiedzieli, czy taka kontrola jest prowadzona, natomiast w jednym przypadku, czyli 6,7%, wskazano, że nikt nie wykonuje tego rodzaju przeglądów.

Uzyskane wyniki pokazują, że jedynie część badanych placówek stosuje podejście proaktywne, polegające na regularnym monitorowaniu potencjalnych zagrożeń. Jest to praktyka korzystna z punktu widzenia cyberbezpieczeństwa, ponieważ pozwala wcześniej wykrywać nietypowe zdarzenia, próby logowania z nieznanych lokalizacji, powtarzające się błędy autoryzacji lub inne symptomy potencjalnego incydentu. Regularny przegląd logów zwiększa także możliwość szybkiej reakcji, zanim problem stanie się widoczny dla użytkowników lub doprowadzi do naruszenia bezpieczeństwa.

Jednocześnie dane wskazują, że w znacznej części szkół dominuje podejście reaktywne. Sprawdzanie dzienników systemowych dopiero wtedy, gdy coś się zepsuje, oznacza, że potencjalne sygnały ostrzegawcze mogą pozostawać niezauważone przez dłuższy czas. Z perspektywy bezpieczeństwa cyfrowego jest to istotna luka organizacyjna, ponieważ nie wszystkie incydenty od razu powodują widoczne problemy techniczne. Część zagrożeń może rozwijać się stopniowo, np. poprzez próby przejęcia kont, skanowanie podatności lub nieautoryzowane próby dostępu. Na uwagę zasługuje również grupa odpowiedzi „nie wiem", która wskazuje na ograniczoną przejrzystość procedur lub niewystarczającą komunikację dotyczącą tego, kto i w jaki sposób monitoruje bezpieczeństwo systemów.

Wykres 6.15.



Wykres 6.15 przedstawia rozkład odpowiedzi na pytanie dotyczące zapamiętywania danych logowania do e-dziennika przez przeglądarkę na współdzielonych komputerach wykorzystywanych przez kilku nauczycieli w salach lekcyjnych. Zdecydowana większość respondentów wskazała, że na współdzielonych komputerach dane logowania nie są automatycznie podpowiadane i każdorazowo trzeba je wpisać ręcznie. Taką odpowiedź odnotowano w 12 z 15 przypadków, co stanowi 80% wszystkich odpowiedzi. W 2 przypadkach, tj. 13,3% odpowiedzi, wskazano, że sytuacja bywa różna. Tylko

w jednym przypadku, czyli 6,7% odpowiedzi, zadeklarowano, że przeglądarka zapamiętuje login i hasło oraz podpowiada je przy logowaniu.

Uzyskane dane wskazują, że w większości badanych placówek stosowana jest prawidłowa praktyka polegająca na niewykorzystywaniu autouzupełniania danych logowania do e-dziennika na komputerach współdzielonych. Jest to istotne z punktu widzenia ochrony danych, ponieważ e-dziennik zawiera informacje dotyczące uczniów, ocen, frekwencji, kontaktu z rodzicami oraz innych aspektów pracy szkoły. Jednocześnie odpowiedzi „różnie to bywa" oraz pojedyncze wskazanie zapamiętywania danych logowania pokazują, że w części przypadków ryzyko nieuprawnionego dostępu nadal może występować. Nawet incydentalne zapisywanie loginów i haseł na komputerach używanych przez wielu nauczycieli zwiększa podatność na dostęp do konta przez osoby nieuprawnione, szczególnie jeśli komputer pozostaje niezablokowany lub jest wykorzystywany w sali dostępnej dla innych użytkowników.

Podsumowanie

Wyniki mini audytów wskazują, że w badanych szkołach funkcjonują już podstawowe rozwiązania organizacyjne i techniczne związane z cyberbezpieczeństwem, choć ich zakres i stopień uporządkowania są zróżnicowane. W zdecydowanej większości placówek wskazano istnienie osoby realnie odpowiedzialnej za standardy bezpieczeństwa, co stanowi istotny punkt wyjścia dla dalszego rozwijania tego obszaru. Jednocześnie dane nie pozwalają przesądzić, czy odpowiedzialność ta jest uregulowana formalnie, ani jaki jest rzeczywisty zakres zadań tych osób. Relatywnie korzystnie przedstawiają się wyniki dotyczące części podstawowych zabezpieczeń. W większości szkół logowanie do e-dziennika lub poczty wymaga dodatkowego potwierdzenia poza samym hasłem, a uczniowie w pracowniach komputerowych najczęściej korzystają z kont z ograniczonymi uprawnieniami. W większości przypadków instalacja oprogramowania na służbowych laptopach wymaga również udziału IT, co ogranicza ryzyko instalowania niezweryfikowanych aplikacji. Pozytywnie należy ocenić także fakt, że w większości szkół przeglądarki na komputerach współdzielonych nie zapamiętują danych logowania do e-dziennika.

Jednocześnie audyty wskazały kilka obszarów wymagających dalszego uporządkowania. W części placówek nadal funkcjonują ważne portale szkolne, do których logowanie odbywa się wyłącznie za pomocą hasła. Zróżnicowane są także praktyki dotyczące aktualizacji systemów - część respondentów deklarowała regularne aktualizowanie lub automatyzację po stronie IT, ale najliczniejsza pojedyncza grupa wskazywała na odkładanie aktualizacji na później. Istotnym obszarem ryzyka pozostaje również korzystanie z prywatnych urządzeń i prywatnych zasobów cyfrowych, zwłaszcza w kontekście sprawdzania e-dziennika poza szkołą oraz przechowywania materiałów dydaktycznych. Wyniki pokazują ponadto, że komunikacja wewnętrzna w szkołach ma

najczęściej charakter wielokanałowy – obok e-maila i e-dziennika wykorzystywane są także telefon oraz komunikatory. Taki model może usprawniać bieżącą wymianę informacji, ale wymaga jasnego określenia, jakie treści mogą być przekazywane poszczególnymi kanałami. Dotyczy to zwłaszcza informacji związanych z uczniami, rodzicami, sprawami wychowawczymi i danymi osobowymi. W zakresie bezpieczeństwa sieci Wi-Fi większość szkół deklaruje oddzielenie sieci nauczycielskiej od uczniowskiej. Nie zawsze oznacza to jednak pełną kontrolę dostępu, ponieważ w części przypadków hasło do sieci nauczycielskiej jest szerzej znane. Również dostęp dla gości najczęściej realizowany jest przez wpisanie hasła przez nauczyciela, a nie poprzez wydzieloną sieć gościnną. Może to wskazywać na potrzebę dalszego rozwijania zasad segmentacji i zarządzania dostępem do sieci. Najbardziej zróżnicowane wyniki dotyczą monitorowania dzienników systemowych. W części szkół logi są sprawdzane regularnie, ale równie często wskazywano, że są analizowane dopiero wtedy, gdy pojawia się problem techniczny. Oznacza to, że w części placówek nadal dominuje podejście reaktywne, a nie proaktywne wykrywanie potencjalnych zagrożeń.

7. Propozycja standardu (model) cyberbezpieczeństwa w szkołach

W krajach takich jak Finlandia, Estonia czy Norwegia kompetencje kadry kierowniczej w zakresie cyberbezpieczeństwa są traktowane jako jeden z podstawowych warunków bezpieczeństwa całej szkoły oraz ochrony danych uczniów i nauczycieli.

Na podstawie analizy systemów edukacji w krajach uznawanych za liderów w zakresie cyberbezpieczeństwa szkół oraz na podstawie audytów przeprowadzonych w ramach projektu, można wskazać kluczowe kompetencje kadry zarządzającej w tym obszarze. Kadra kierownicza nie pełni już wyłącznie funkcji administracyjnej, lecz odpowiada również za zarządzanie bezpieczeństwem cyfrowym placówki. Coraz częściej dyrektorzy i osoby zarządzające szkołami występują w roli:

1. zarządzających ryzykiem cyfrowym,
2. koordynatorów ochrony danych,
3. liderów odporności organizacyjnej,
4. osób odpowiedzialnych za ciągłość działania szkoły podczas i po cyberincydencie.

1) Zarządzanie cyberbezpieczeństwem

Osoby zarządzające szkołą powinny rozumieć:

- podstawowe typy cyberataków,
- skutki ransomware,
- ryzyko wycieku danych uczniów,
- zależności między systemami IT szkoły,
- wpływ incydentu na ciągłość nauczania.

W modelach rekomendowanych przez ENISA[35] oraz OECD kadra kierownicza odpowiada za:

- identyfikację ryzyk,
- zatwierdzanie polityk bezpieczeństwa,
- nadzór nad procedurami reagowania,
- podejmowanie decyzji kryzysowych.

2) Umiejętność zarządzania incydentem cyberbezpieczeństwa

Dyrektorzy szkół przechodzą szkolenia dotyczące:

- ransomware,
- utraty dostępu do systemów,

[35] www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management

- wycieku danych,
- komunikacji kryzysowej,
- współpracy z CERT i administracją publiczną.

Dobrą praktyką jest prowadzenie:
- ćwiczeń scenariuszowych typu tabletop – symulacji sytuacji kryzysowych,
- symulacji cyberataków,
- testów procedur awaryjnych,
- scenariuszy pracy szkoły offline.

Najbardziej rozwinięte systemy edukacyjne zakładają, że szkoła musi być zdolna do działania nawet po częściowym sparaliżowaniu infrastruktury IT.

3) Ochrona danych osobowych i prywatności

Jednym z najważniejszych standardów w krajach takich jak Finlandia czy Norwegia jest świadomość prawna i organizacyjna kadry kierowniczej.

Dyrektorzy szkół powinni rozumieć:
- zasady GDPR/RODO,
- ryzyko korzystania z usług Big Tech,
- kwestie transferu danych poza UE,
- zasady minimalizacji danych,
- kontrolę dostępu do danych uczniów.

Dobre praktyki obejmują:
- analizę ryzyka przed wdrożeniem nowych platform,
- audyty dostawców IT,
- polityki dostępu do danych,
- regularny przegląd uprawnień pracowników.

4) Budowanie kultury bezpieczeństwa

Najlepsze szkoły nie opierają cyberbezpieczeństwa wyłącznie na administratorze IT. Kadra kierownicza odpowiada za stworzenie kultury bezpieczeństwa.

W praktyce oznacza to:
- obowiązkowe szkolenia pracowników,
- procedury zgłaszania incydentów,
- edukację uczniów i rodziców,
- ograniczanie „shadow IT” (nieautoryzowanych narzędzi cyfrowych),
- regularne przypominanie zasad cyberhigieny.

Badania pokazują, że większość skutecznych ataków zaczyna się od błędu człowieka, a nie od luki technicznej.

5) Kompetencje strategiczne i organizacyjne

W nowoczesnych modelach zarządzania szkołą dyrektor powinien rozumieć:

- podstawy architektury bezpieczeństwa,
- segmentację sieci,
- kopie zapasowe,
- zarządzanie tożsamością,
- MFA,
- outsourcing usług IT,
- zależności między bezpieczeństwem a budżetem szkoły.

Nie chodzi o kompetencje administratora sieci, lecz o zdolność podejmowania świadomych decyzji strategicznych.

Według rekomendacji szkoleń dla kadry zarządzającej JST i instytucji publicznych, kluczowe są:

- zarządzanie ryzykiem,
- decyzje strategiczne,
- analiza incydentów,
- budowanie odporności organizacyjnej.

6) Stałe doskonalenie kompetencji

W modelach estońskich i skandynawskich przyjmuje się, że cyberbezpieczeństwo zmienia się zbyt szybko, aby jednorazowe szkolenie było wystarczające.

Dlatego dobre praktyki obejmują:

- cykliczne szkolenia kadry,
- ćwiczenia praktyczne,
- udział w webinarach CERT,
- współpracę szkół z ekspertami,
- aktualizację procedur po incydentach.

8. Rekomendacje w zakresie poprawy kompetencji cyberbezpieczeństwa współczesnej szkoły

1. **Zmiana paradygmatu: od wiedzy teoretycznej do aktywnego działania**

   Kluczową rekomendacją dla współczesnych placówek oświatowych jest odejście od biernego modelu kompetencyjnego. Kadra Zarządzająca nie może ograniczać się do świadomości zagrożeń. Wymagane jest aktywne stosowanie zabezpieczeń, co stanowi wypadkową trzech elementów:

   - Znajomości aktualnych standardów, procedur i przepisów.
   - Zdolności do technicznego wdrażania i konfiguracji odpowiednich narzędzi.
   - Dyscypliny w egzekwowaniu zasad, proaktywności w działaniu oraz budowania odpowiedniej kultury pracy.

2. **Zarządzanie organizacją i kultura bezpieczeństwa**
   - Wyznaczenie odpowiedzialności: Szkoła docelowo musi oddelegować wyznaczonego pracownika (koordynatora) odpowiedzialnego za codzienne, praktyczne utrzymanie polityki cyberbezpieczeństwa.
   - Kultura „Blame-free”: Należy wdrożyć procedury zgłaszania incydentów oparte na braku sankcji dyscyplinarnych dla pracowników, którzy niezwłocznie i samodzielnie zgłosili własny błąd (np. kliknięcie w link phishingowy).
   - Edukacja: Szkolenia z cyberbezpieczeństwa muszą być obowiązkowe, cykliczne i obejmować zarówno kadrę pedagogiczną, administracyjną, jak i uczniów.

3. **Zarządzanie tożsamością i dostępem (IAM)**
   - Uwierzytelnianie: Wymogiem absolutnym jest systemowe wymuszenie wieloskładnikowego uwierzytelniania (MFA) dla wszystkich systemów. Modelem docelowym jest stosowanie sprzętowych kluczy zabezpieczających (np. YubiKey) z odpowiednią procedurą backupu.
   - Zarządzanie hasłami: Należy wyeliminować zapisywanie haseł w przeglądarkach na rzecz wdrożenia i korzystania z dedykowanych, odizolowanych menedżerów haseł.
   - Zasada minimalnych uprawnień: Dostęp do danych (np. w e-dzienniku) musi być przydzielany wyłącznie w niezbędnym zakresie. Konta pracowników kończących współpracę muszą być rygorystycznie i natychmiastowo blokowane. Docelowo zaleca się wdrożenie systemów Single Sign-On (SSO) ułatwiających audyt uprawnień.

4. **Bezpieczeństwo komunikacji elektronicznej i transferu danych**
   - Ochrona kanałów przesyłu: Obowiązuje kategoryczny zakaz używania prywatnych skrzynek pocztowych do celów służbowych. Wymagane jest ponadto korzystanie z oficjalnych narzędzi ministerialnych (np. e-doręczenia) o ile jest to możliwe.
   - Szyfrowanie i separacja: Każdy załącznik zawierający dane wrażliwe musi być zaszyfrowany. Hasło do pliku należy przekazywać osobnym, odseparowanym kanałem (np. dokument e-mailem, hasło SMS-em).
   - Nośniki i chmura: Przetwarzanie danych szkolnych może odbywać się wyłącznie na sprzęcie służbowym. Wymagane jest wdrożenie oficjalnej, zabezpieczonej chmury szkolnej. Dopuszczone do użytku nośniki fizyczne (pendrive'y, dyski) muszą być bezwzględnie szyfrowane.

5. **Ochrona urządzeń końcowych i infrastruktury IT**
   - Ograniczenie przywilejów: Standardowi użytkownicy nie mogą posiadać uprawnień administracyjnych na stacjach roboczych. Należy zablokować możliwość samodzielnej instalacji nieautoryzowanego oprogramowania oraz podłączania prywatnych nośników pamięci.
   - Kopie zapasowe: Architektura backupu musi opierać się na regule 3-2-1. Tworzenie kopii zapasowych powinno być zautomatyzowane i obejmować procedurę cyklicznego testowania poprawności odtwarzania danych (w tym stacji roboczych nauczycieli).
   - Segmentacja sieci: Infrastruktura sieciowa wymaga logicznego odseparowania. Oprócz wydzielonej sieci dla gości, należy zastosować segmentację (VLAN), oddzielając ruch administracji, nauczycieli oraz uczniów.
   - Monitorowanie systemów: Kluczowe systemy (poczta, e-dziennik) muszą być skonfigurowane tak, aby generowały logi zdarzeń, które podlegają cyklicznej analizie przez wyznaczonego pracownika w celu wykrywania anomalii.

Bibliografia

1. Aktywny Nauczyciel, Cyberbezpieczeństwo w szkole. https://aktywnynauczyciel.pl/wiedza-cyberbezpieczenstwo-w-szkole
2. Altkom Akademia, Cyberbezpieczeństwo dla kadry zarządzającej – dobre praktyki JST. www.altkomakademia.pl/szkolenia/bezpieczny-samorzad-cyberbezpiczenstwo-dla-kadry-zarzadzajacej
3. CERT Polska, NASK, Raport roczny 2025 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu, Warszawa 2026.
4. CERT Polska, NASK, Raport roczny z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu 2020, Warszawa 2021.
5. CERT Polska, NASK, Raporty roczne z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu 2020–2025, Warszawa.
6. Check Point Research, Cyber Security Report 2026, Check Point Software Technologies, 2026.
7. Check Point Research, March 2026 Cyber Threat Landscape Shows No Relief as Ransomware Rebounds and GenAI Risks Intensify, Check Point Blog, 2026. https://blog.checkpoint.com/research/march-2026-cyber-threat-landscape-shows-no-relief-as-ransomware-rebounds-and-genai-risks-intensify/
8. CISA, Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats, Cybersecurity and Infrastructure Security Agency. www.cisa.gov/topics/cybersecurity-best-practices/K12cybersecurity/protecting-our-future-cybersecurity-k12
9. CyberDefence24.pl, Cyberataki na szkoły. Połowa sprawców to dzieci. https://cyberdefence24.pl/cyberbezpieczenstwo/cyberataki-na-szkoly-polowa-sprawcow-to-dzieci
10. Cyberpolicy NASK, Najnowsze wyniki badań ENISA. https://cyberpolicy.nask.pl/aktualnosci/najnowsze-wyniki-badan-enisa/
11. Department for Science, Innovation and Technology, Home Office, Cyber Security Breaches Survey 2025: Education Institutions Findings, Government of the United Kingdom, 2025. www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-education-institutions-findings
12. Education Estonia, Digital Competence. www.educationestonia.org/innovation/digital-competence
13. ENISA, ENISA Strategy, dostęp online: www.enisa.europa.eu/sites/default/files/2024-10/enisa-strategy-leaflet-pl.pdf
14. ENISA, European Cybersecurity Skills Framework Role Profiles, European Union Agency for Cybersecurity, 2022, dostęp online: www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles
15. EU Kids Online, EU Kids Online 2020: Survey Results from 19 Countries, 2020. www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf
16. European Crime Prevention Network, The cyber defence field of study at Põltsamaa Coeducational Gymnasium. www.eucpn.org/document/the-cyber-defence-field-of-study-at-poltsamaa-coeducational-gymnasium
17. Government Accountability Office, Critical Infrastructure Protection: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity, GAO-23-105480, Washington 2022. www.gao.gov/products/gao-23-105480
18. Komisja Europejska, The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final, EUR-Lex.
19. Krajowe Centrum Kompetencji Cyberbezpieczeństwa, Krajobraz cyberprzestrzeni. Sprawozdanie o stanie cyberbezpieczeństwa Polski za rok 2025, gov.pl.

www.gov.pl/web/baza-wiedzy/krajobraz-cyberprzestrzeni-sprawozdanie-o-stanie-cyberbezpieczenstwa-polski-za-rok-2025
20. Krajowe Centrum Kompetencji Cyberbezpieczeństwa, Nowe możliwości rozwoju kompetencji w obszarze cyberbezpieczeństwa, gov.pl. www.gov.pl/web/cyber-nccpl/nowe-mozliwosci-rozwoju-kompetencji-w-obszarze-cyberbezpieczenstwa
21. Ministerstwo Edukacji Narodowej, Urząd Ochrony Danych Osobowych, Ochrona danych osobowych w szkole. Poradnik UODO i MEN. www.gov.pl/web/edukacja/ochrona-danych-osobowych-w-szkole--poradnik-uodo-i-men
22. National Cyber Security Centre, Cyber Security Training for School Staff, NCSC, United Kingdom. www.ncsc.gov.uk/information/cyber-security-training-schools
23. National Institute of Standards and Technology, Workforce Framework for Cybersecurity (NICE Framework), NIST Special Publication 800-181 Revision 1, 2020. https://csrc.nist.gov/pubs/sp/800/181/r1/final
24. Norwegian Data Protection Authority, Datatilsynet, dostęp online: www.datatilsynet.no/en/
25. Parlament Europejski i Rada Unii Europejskiej, Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, NIS2, EUR-Lex.
26. Parlament Europejski i Rada Unii Europejskiej, 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. https://sip.lex.pl/akty-prawne/dzienniki-UE/dyrektywa-2016-1148-w-sprawie-srodkow-na-rzecz-wysokiego-wspolnego-68659478/art-4
27. Parlament Europejski i Rada Unii Europejskiej, Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych, tzw. akt o cyberbezpieczeństwie, EUR-Lex.
28. Parlament Europejski i Rada Unii Europejskiej, Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., ogólne rozporządzenie o ochronie danych, RODO/GDPR, EUR-Lex.
29. Parlament Europejski i Rada Unii Europejskiej, Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych, Digital Services Act, DSA, EUR-Lex.
30. Parlament Europejski i Rada Unii Europejskiej, Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 w sprawie horyzontalnych wymagań cyberbezpieczeństwa dla produktów z elementami cyfrowymi, Cyber Resilience Act, CRA, EUR-Lex, dostęp online: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
31. Parlament Europejski i Rada Unii Europejskiej, Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji, AI Act, EUR-Lex. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
32. Republic of Estonia Information System Authority, Estonian schools should prioritise cybersecurity. www.ria.ee/en/estonian-schools-should-prioritise-cybersecurity
33. Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2024 poz. 773. https://api.sejm.gov.pl/eli/acts/DU/2024/773/text.pdf
34. SiteGuardian, Benchmark cyberbezpieczeństwa: edukacja. https://siteguardian.io/pl/benchmark/education
35. System-3, Cyberbezpieczeństwo w systemie edukacji – wyzwania i rozwiązania. https://system-3.com.pl/blog/cyberbezpieczenstwo-w-systemie-edukacji---wyzwania-i-rozwiazania

36. The Guardian, Estonia phone bans in schools / AI and education, 2025. www.theguardian.com/education/2025/may/26/estonia-phone-bans-in-schools-ai-artificial-intelligence
37. Tomczyk Ł., Srokowski Ł., Kompetencje w zakresie bezpieczeństwa cyfrowego w polskiej szkole, projekt Cyfrowobezpieczni.pl, 2016. www.researchgate.net/profile/Lukasz-Tomczyk-4/publication/313060967_Kompetencje_w_zakresie_bezpieczenstwa_cyfrowego_w_polskiej_szkole/links/588f2929aca272fa50e19671/Kompetencje-w-zakresie-bezpieczenstwa-cyfrowego-w-polskiej-szkole.pdf
38. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/ochrona-danych-osobowych-18722262
39. Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe. https://lexlege.pl/prawo-oswiatowe
40. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. https://eli.gov.pl/eli/DU/2005/565/ogl
41. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. https://eli.gov.pl/api/acts/DU/2018/1560/text/T/D20181560L.pdf
42. Vuorikari R., Kluzer S., Punie Y., DigComp 2.2: The Digital Competence Framework for Citizens, Joint Research Centre / European Commission, 2022. www.digcomp.pl/wp-content/uploads/2023/03/DigComp2.2_TEXT_pl_.pdf
43. Zintegrowana Platforma Edukacyjna, Materiały dotyczące cyberbezpieczeństwa. https://zpe.gov.pl/pobierz/R1J8N6FP8LLHS

https://securitybeztabu.pl/cyberataki-na-sektor-edukacji-rosna-o-63-rocznie-szkoly-i-uczelnie-pod-coraz-wieksza-presja/#Rekomendacje