CYFROWA POLSKA

# Mapa drogowa polskiej cyberodporności

Warszawa, wrzesień 2025 r.

# Spis treści



# Michał Kanownik

Prezes Związku Cyfrowa Polska

Gdy świat mierzy się z napięciami geopolitycznymi i cyfrową rewolucją, cyberbezpieczeństwo przestaje być wyborem — staje się fundamentem stabilności i zaufania. Polska, odgrywając coraz istotniejszą rolę w kształtowaniu bezpieczeństwa, gospodarki i polityki cyfrowej w Europie Środkowo-Wschodniej, stoi dziś przed koniecznością systemowego wzmocnienia odporności na zagrożenia w cyberprzestrzeni — zarówno te wynikające z aktywności państw realizujących wrogą politykę cybernetyczną, jak i grup przestępczych oraz niekontrolowanych ryzyk technologicznych.

Jak trafnie zauważył laureat Nagrody Nobla z dziedziny ekonomii, Paul Romer: *„Technologia zmienia to, co jest możliwe. Polityka i społeczeństwo decydują o tym, co jest dozwolone”*. Ten cytat stanowi klucz do zrozumienia roli cyberbezpieczeństwa w kontekście nie tylko obrony, ale i tworzenia ram dla zrównoważonego rozwoju cyfrowej gospodarki i państwa.

Inwestycje w cyberbezpieczeństwo to dziś nie tylko kwestia techniczna, lecz strategiczny filar rozwoju gospodarczego. Budują zaufanie do cyfrowych usług, tworzą warunki do rozwoju nowoczesnych technologii i pozwalają firmom skutecznie ograniczać ryzyko strat – zarówno finansowych, jak i wizerunkowych. Dla obywateli oznacza to większą kontrolę nad własnymi danymi, ochronę prywatności i pewność, że podstawowe usługi publiczne — od zdrowia po administrację — funkcjonują stabilnie i bez zakłóceń. Z perspektywy administracji publicznej, silna infrastruktura cyberbezpieczeństwa to narzędzie sprawniejszego reagowania na sytuacje kryzysowe, skuteczniejszej ochrony zasobów krytycznych oraz utrzymania ciągłości działania instytucji w warunkach destabilizacji lub zagrożeń zewnętrznych. Dla świata nauki i biznesu to z kolei przestrzeń do synergii — wspólnego opracowywania zaawansowanych rozwiązań technologicznych, rozwoju nowoczesnych kompetencji oraz przekuwania wyników badań w realne innowacje z obszarów takich jak informatyka, kryptografia czy sztuczna inteligencja.

W obliczu globalnej polaryzacji, cyfrowych wojen zastępczych i intensyfikacji ataków na infrastrukturę państwową i prywatną, konieczne staje się wypracowanie spójnej, długofalowej strategii cyberodporności. Polska, dysponując kompetencjami eksperckimi, zapleczem akademickim i rosnącym sektorem technologicznym, ma potencjał, by nie tylko reagować, ale aktywnie kształtować europejskie standardy w zakresie cyberbezpieczeństwa.

Właśnie dlatego powstała ta publikacja — *głos firm i ekspertów, którzy nie tylko diagnozują aktualną sytuację, ale też wspólnie nakreślają mapę drogową dalszej cyfryzacji kraju.* Wskazujemy w niej mocne i słabe strony administracji, realne potrzeby biznesu oraz przeszkody, które hamują rozwój.

To nie jest raport tylko dla specjalistów. To kompas dla wszystkich, którym zależy na cyfrowej przyszłości Polski — od urzędników, przez liderów firm, po naukowców i organizacje społeczne. Pokazujemy, że prawdziwy postęp możliwy jest tylko wtedy, gdy administracja i biznes potrafią współpracować, dzielić się wiedzą i działać wspólnie na rzecz bezpieczniejszej, bardziej innowacyjnej i odporniejszej cyfrowo Polski.

# Wprowadzenie

Rok 2024 był kolejnym, w którym bezpieczeństwo cyfrowe znalazło się w centrum uwagi społeczeństw, państw, a także nauki i biznesu. Geopolityczna niestabilność, zwłaszcza w obliczu trwającej wojny w Ukrainie oraz rosnącej aktywności Federacji Rosyjskiej w sferze wojny informacyjnej, stawia Polskę – jako państwo frontowe NATO i UE – w epicentrum cyfrowej konfrontacji. Potwierdzają to słowa wicepremiera, ministra cyfryzacji - Krzysztofa Gawkowskiego, który w kwietniu 2025 powiedział, że **„Polska jest najczęściej atakowanym krajem w Europie przez rosyjskie kampanie dezinformacyjne i cyberataki”**. Ta deklaracja znajduje potwierdzenie zarówno w danych instytucji krajowych, jak i międzynarodowych analizach, których wyniki przedstawimy poniżej.

Jak wynika z raportu Experis „Prognozy CIO na 2025 rok: Kluczowe priorytety dla liderów technologii”, **globalne straty spowodowane cyberprzestępczością osiągnęły w 2024 roku wartość 9,5 biliona USD** - gdyby ta kwota odpowiadała produktowi krajowemu brutto jakiegoś państwa, byłaby to trzecia co do wielkości gospodarka świata, ustępująca jedynie Stanom Zjednoczonym i Chinom. Z kolei Cybersecurity Ventures przewiduje, że globalne koszty cyberprzestępczości będą rosły o 15 procent rocznie w ciągu najbliższych pięciu lat, osiągając 10,5 biliona dolarów rocznie.

Rozwój technologii, postępująca cyfryzacja procesów gospodarczych i społecznych oraz upowszechnienie sztucznej inteligencji, internetu rzeczy (IoT) i chmury obliczeniowej otwierają nowe możliwości – ale jednocześnie generują nowe wektory ataku. Obecnie **liczba użytkowników internetu w Polsce przekracza 36 milionów**, co oznacza, że niemal każdy obywatel staje się potencjalnym celem działań cyberprzestępczych, a każda instytucja – potencjalnym punktem wejścia dla bardziej złożonych operacji.



Z danych KPMG wynika, że **w 2024 roku tylko 17% polskich firm nie odnotowało żadnego incydentu cyberbezpieczeństwa** – to najniższy wynik w historii prowadzonych badań. Większość przedsiębiorstw doświadczyła ataków, co pokazuje skalę i intensywność wyzwań, z jakimi mierzy się sektor prywatny. Równolegle, dane NASK i CERT Polska wskazują, że **w 2024 roku odnotowywano średnio aż 300 incydentów dziennie**, co oznacza **wzrost o 29%** względem roku poprzedniego. **Liczba zgłoszeń zwiększyła się o 62%**, co świadczy nie tylko o wzmożonej aktywności zagrożeń, ale również o rosnącej świadomości potrzeby ich raportowania.

Niepokojące są także wnioski płynące z raportów Najwyższej Izby Kontroli i firmy EY. Pokazują one **niewystarczającą świadomość zagrożeń cyfrowych w administracji publicznej oraz wśród kadry zarządzającej w przedsiębiorstwach**, jak również ograniczoną gotowość wielu organizacji do skutecznego reagowania na incydenty. To alarmujący sygnał, który powinien stanowić impuls do systemowego działania.

Raport „Mapa drogowa polskiej cyberodporności” nie tylko diagnozuje aktualny stan zagrożeń i wyzwań, lecz także **wskazuje, co należy zrobić w pierwszej kolejności, aby podnieść odporność kraju na poziomie strategicznym, operacyjnym i technologicznym**. Przed nami ogrom pracy – ale także szansa na zbudowanie bardziej bezpiecznej, świadomej i odpornej cyfrowo Polski.

# 1. Skala cyberzagrożeń – świat i Europa

Współczesna architektura bezpieczeństwa cyfrowego ulega dynamicznym przemianom, na które bezpośredni wpływ mają napięcia geopolityczne oraz gwałtowny rozwój technologii. Zgodnie z raportem ENISA „Threat Landscape 2024", destabilizacja porządku międzynarodowego – szczególnie wynikająca z długotrwałej agresji Rosji na Ukrainę – wyraźnie intensyfikuje działania grup cyberprzestępczych oraz sponsorowanych przez państwa aktorów APT (Advanced Persistent Threats). Konflikty te stają się katalizatorem operacji w cyberprzestrzeni, służących zarówno celom szpiegowskim, sabotażowym, jak i propagandowym.

Na poziomie globalnym Federacja Rosyjska nie tylko kontynuuje ofensywę militarną, lecz prowadzi również złożone kampanie dezinformacyjne i cyberataki wymierzone w państwa wspierające Ukrainę. Coraz bardziej wyrafinowane formy manipulacji informacją mają na celu erozję zaufania społecznego, destabilizację instytucji demokratycznych oraz wywołanie chaosu politycznego. W Europie konflikty i kryzysy polityczne spowodowały wzrost liczby incydentów cybernetycznych, szczególnie w obszarach takich jak infrastruktura publiczna, sektory finansowe i transport. Wzrosła liczba ataków typu DDoS, które w wielu przypadkach nie powodują poważnych szkód, tylko zwiększają presję na systemy obronne. Zjawisko hacktywizmu również się pogłębia, napędzane zarówno przez tematy polityczne, jak i regionalne, takie jak wybory w UE, które stały się okazją do ofensywy informacyjnej. Z kolei w regionie Azji i Pacyfiku napięcia wokół Chin i Tajwanu prowadzą do intensyfikacji działań cyberszpiegowskich i sabotażowych. Grupy powiązane z państwami – zwłaszcza z Chinami i Koreą Północną – wykorzystują zaawansowane techniki, takie jak eksploatacja podatności typu zero-day, ataki na łańcuchy dostaw, a także strategię Living off the Land, umożliwiającą ukrywanie obecności w infrastrukturze ofiary.



Raport Grupy Zadaniowej NATO-UE ds. odporności infrastruktury krytycznej za 2024 rok wyraźnie wskazuje na wzrost incydentów cybernetycznych na poziomie około 35% w porównaniu z rokiem 2023, szczególnie w kluczowych obszarach, takich jak energetyka, transport oraz telekomunikacja, co potwierdza, że infrastruktura krytyczna pozostaje celem o najwyższym priorytecie dla aktorów zewnętrznych. Co istotne, ponad 60% tych ataków ma charakter wielowektorowy, łącząc różnorodne metody, takie jak ransomware, DDoS oraz kampanie dezinformacyjne. Taka strategia podnosi stopień trudności obrony i wymaga kompleksowego podejścia do zabezpieczeń, które wykracza poza tradycyjne mechanizmy obronne. Z raportu jasno wynika, że łańcuchy dostaw stanowią słaby punkt – około 45% udanych ataków wykorzystuje właśnie tę lukę, co podkreśla konieczność wzmożonej ochrony dostawców i integratorów technologicznych. Brak odpowiedniej kontroli w tym obszarze może prowadzić do poważnych konsekwencji dla całych systemów krytycznych. Niestety, pomimo rosnących zagrożeń, **ponad 70% państw członkowskich UE i NATO wskazuje na niedostateczny poziom koordynacji oraz wymiany informacji dotyczącej incydentów**. Ten deficyt współpracy stanowi poważne wyzwanie dla skutecznej reakcji i minimalizacji skutków ataków na infrastrukturę krytyczną. W odpowiedzi na te wyzwania, zauważalny jest wzrost inwestycji w zaawansowane technologie oparte na sztucznej inteligencji i uczeniu maszynowym – budżety państw członkowskich na obronę cybernetyczną w 2024 roku wzrosły o ponad 25% w tym obszarze. To strategiczne przesunięcie podkreśla rosnącą świadomość, że nowoczesne narzędzia analityczne są kluczowe dla efektywnego wykrywania i neutralizacji złożonych zagrożeń. W obliczu eskalujących ataków, tylko kompleksowe i skoordynowane działania mogą zapewnić bezpieczeństwo kluczowych systemów, od których zależy funkcjonowanie całych gospodarek i społeczeństw.

Z kolei, jak wskazuje najnowszy „Microsoft Digital Defense Report", najbardziej rozpowszechnionymi technikami stosowanymi obecnie przez cyberprzestępców jest inżynieria społeczna — w szczególności phishing — oraz naruszenie tożsamości i wykorzystywanie luk w zabezpieczeniach aplikacji publicznych lub niezałatanych systemów operacyjnych. **Gdy przestępcy przedostaną się do atakowanej sieci, zazwyczaj są w niej aktywni przez mniej niż 2 godziny, co oznacza, że zdążą z niej wyjść, zanim zostaną wykryci. Ostatnie 12 miesięcy to również 2,75-krotny wzrost liczby ataków ransomware. Co jednak ważne, nastąpił trzykrotny spadek liczby ataków z żądaniem okupu, które doszły do etapu zaszyfrowania danych.**

**Raport ENISA „Threat Landscape 2024" wśród kluczowych zagrożeń dla bezpieczeństwa cyfrowego w 2024 wskazał na:**

- **Ransomware** – zagrożenie o największym wpływie operacyjnym, coraz częściej wykorzystujące techniki podwójnego i potrójnego wymuszenia *(double/triple extortion)*.
- **Ataki sponsorowane przez państwa i grupy propaństwowe** – ukierunkowane na infrastrukturę krytyczną, administrację oraz systemy wyborcze.
- **Dezinformację** – szczególnie intensywną podczas kryzysów społeczno-politycznych i kampanii wyborczych.
- **Phishing i techniki socjotechniczne** – nadal dominujące wektory ataku, szczególnie wobec podmiotów sektora publicznego i MŚP.
- **Eksploatację podatności w oprogramowaniu i łańcuchach dostaw** – często wykorzystywaną do uzyskania dostępu do infrastruktury krytycznej.
- **Ataki DDoS** – coraz bardziej złożone i zautomatyzowane, często związane z wydarzeniami politycznymi.



Z danych zawartych w raporcie jednoznacznie wynika, że Unia Europejska mierzy się z bezprecedensową intensyfikacją zagrożeń w przestrzeni cyfrowej. **Wzrost liczby incydentów o 24% w skali roku, przy równoczesnym przetasowaniu dominujących typów ataków** (DDoS wyprzedza ransomware), wskazuje na zmianę taktyki przeciwnika – z celów czysto finansowych na działania zakłóceniowe i destabilizujące. W szczególności nasilają się kampanie ukierunkowane na infrastrukturę teleinformatyczną, procesy wyborcze i łańcuchy dostaw – elementy kluczowe dla funkcjonowania państw i odporności społeczeństw. Równolegle, stale rośnie skala wykrywanych podatności – blisko 20 tysięcy CVE w ciągu roku – co w połączeniu z ich wysokim stopniem krytyczności (ponad 30% klasyfikowanych jako wysokiego lub bardzo wysokiego ryzyka) stwarza ogromne wyzwanie operacyjne dla sektora publicznego i prywatnego. Dynamiczne środowisko zagrożeń wymaga nie tylko reakcji taktycznej, ale i strategicznego podejścia do zarządzania ryzykiem, które uwzględnia pełny cykl życia podatności oraz weryfikację bezpieczeństwa partnerów w łańcuchu dostaw.

Zauważalna jest również ewolucja metod ataku – coraz częściej wykorzystywane są techniki takie jak *Living Off The Land* (LOTL), ataki supply chain oraz narzędzia oparte na sztucznej inteligencji (m.in. do automatyzacji phishingu czy manipulacji narracją informacyjną). To wymusza konieczność integracji rozwiązań AI w systemach cyberobrony i inwestycji w zaawansowane mechanizmy detekcji oraz reagowania (EDR, SOAR, threat intelligence). Szczególnym wyzwaniem stają się ataki DDoS, których skala i automatyzacja stanowią realne zagrożenie dla ciągłości działania instytucji i przedsiębiorstw. W połączeniu z rosnącym wpływem hacktywizmu i kampanii informacyjnych, tworzy to środowisko cyberzagrożeń o wyraźnym podłożu politycznym i hybrydowym.

**Wnioski z raportu ENISA 2024 nie pozostawiają wątpliwości: odporność cyfrowa w UE wymaga dziś nie tylko modernizacji infrastruktury technicznej, ale także skokowej poprawy zdolności analitycznych, procedur zarządzania kryzysowego i współpracy transgranicznej.**

- **Wzrost liczby incydentów o 24%**
  - w okresie lipiec 2023–czerwiec 2024 zgłoszono ponad 11079 incydentów, czyli o ćwierć więcej niż w poprzednim raporcie (lipiec 2022–czerwiec 2023).
- **Przesunięcie struktury typów ataków – DDoS wyprzedza ransomware**.
  W 2024 r. ataki DDoS stanowiły 41% wszystkich zdarzeń (4120 incydentów), przewyższając ransomware (26%) i naruszenia danych (19 %) - wcześniej ransomware dominowało (34%), a DDoS stanowił 28%.
- **Wzrost skali ataków DDoS i incydentów zakłóceniowych.**
  Ataki zakłóceniowe (DDoS/hacktivizm) podwoiły się między IV kw. 2023 a I kw. 2024, częściowo za sprawą geopolitycznych napięć i zbliżających się wyborów.
- **Wzrost liczby luk i poważnych podatności.**
  W czasie raportowanego okresu zidentyfikowano 19754 podatności (CVE), z tego 9,3% jako krytyczne, a 1,8% jako wysokiego ryzyka, co stwarza ogromne wyzwanie dla obrony w UE.
- **Zaangażowanie nowych technik: AI, LOTL, supply chain.**
  W 2024 r. ENISA odnotowała wzrost wykorzystania Generative AI do phishingu i dezinformacji, techniki Living Off The Land do ukrywania ataków, oraz eskalację ataków na łańcuch dostaw – w porównaniu z wcześniejszym rokiem, gdy te zagrożenia pojawiały się, lecz w mniejszym wymiarze.

# 2. Skala cyberzagrożeń – Polska

W Polsce dynamika zagrożeń odzwierciedla globalne tendencje, jednak ze względu na strategiczne położenie i aktywne zaangażowanie w pomoc Ukrainie, nasz kraj znajduje się w szczególnie wrażliwej pozycji. **Z danych CERT Polska (NASK) wynika, że w 2024 roku rejestrowano średnio 300 incydentów dziennie, co oznacza wzrost o 29% w porównaniu z rokiem poprzednim.** Jednocześnie liczba zgłoszeń wzrosła o 62%, co może świadczyć o rosnącej świadomości zagrożeń, ale również o eskalacji działań wymierzonych w polską przestrzeń cyfrową. Co warte podkreślenia, aż 103 449 incydentów miało realny wpływ na bezpieczeństwo cyfrowe kraju, **a jeden z rekordowych ataków DDoS miał siłę 1,3 Tbps – co czyni go najpotężniejszym w historii polskiej sieci – i został skutecznie odparty dzięki współpracy operatorów i Centrów CERT. Z kolei incydentów** dotyczących infrastruktury telekomunikacyjnej, w tym ataków DDoS na operatorów, prób przełamań zabezpieczeń systemów zarządzania siecią oraz prób phishingu i socjotechniki wymierzonej w pracowników firm telekomunikacyjnych - odnotowano ponad **200**, a incydentów dotyczących systemów SCADA, systemów zarządzania energią oraz inteligentnych sieci energetycznych - 150. Takie zdarzenia pokazują, jak istotna jest odporność szeroko rozumianej infrastruktury telekomunikacyjnej i wdrażanie rozwiązań typu *scrubbing center* oraz redundancji.

Zgodnie z Barometrem Cyberbezpieczeństwa KPMG 2025, **83 % firm odnotowało co najmniej jeden incydent w 2024 r., co oznacza wzrost o 16 pkt proc. rok do roku**. Wzrost ten dotyczy firm wszystkich rozmiarów, choć szczególnie duże organizacje są najbardziej eksponowane. Warto zauważyć, że choć odsetek organizacji bez żadnego incydentu spadł do rekordowego minimum (17%), to liczba firm z ponad 30 atakami w roku wynosi już tylko 4% – to najniższy wynik w historii badania. Dominujące zagrożenia to phishing, złośliwe oprogramowanie oraz wycieki danych – w tym także incydenty z udziałem pracowników. Aż 56% firm obawia się, że rozwój technologii AI zwiększy ryzyko cyberataków, lecz równocześnie 68% organizacji nie wdrożyło jeszcze działań przygotowujących do wymogów AI Act, co pokazuje istotną lukę w adaptacji do nowych regulacji.

Również administracja publiczna pozostaje w kręgu zainteresowania cyberprzestępców i grup APT. **Tylko w styczniu 2024 roku CERT Polska odnotował 201 incydentów w podmiotach publicznych, z czego ponad połowa dotyczyła administracji centralnej i lokalnej - w tym przypadki ransomware, phishingu czy DDoS.** Ponadto informowano o incydentach podczas weekendu, gdy **tylko przez dwa dni odnotowano 704 zdarzenia — co daje średnio 352 zdarzenia dziennie. To ponad trzykrotnie więcej niż średnia dzienna na początku stycznia** (6–7 zdarzeń dziennie). Taka kumulacja wskazuje na starannie zaplanowaną taktykę atakujących – w celu opóźnienia reakcji i maksymalizacji efektu. Incydenty wykryte w weekend często dotyczyły phishingu, co sugeruje kampanie ukierunkowane na użytkowników mniej chronionych, takich jak urzędnicy pracujący zdalnie lub korzystający z prywatnych urządzeń.

Zagrożenia nie ominęły także indywidualnego użytkownika urządzeń końcowych. Warto tu zwrócić uwagę na to, że **na początku 2024 roku w Polsce aktywnie korzystało z internetu około 35,75 mln użytkowników, a dostęp do sieci miało niemal 96% gospodarstw domowych**. Przewagę uzyskał szerokopasmowy internet stacjonarny, z zasięgiem obejmującym 72% gospodarstw domowych, jednak kluczowym medium pozostaje internet mobilny, z którego korzysta ponad 88% populacji. **Z kolei liczba smartfonów użytkowanych w Polsce przekracza 30 milionów, co plasuje je jako główny punkt styku użytkownika z cyfrową rzeczywistością.** Ten fakt determinuje priorytety w ochronie cybernetycznej, ponieważ urządzenia mobilne stają się głównym celem ataków — zwłaszcza tych opartych o phishing, smishing oraz kampanie zaprojektowane z myślą o mobilnym UX.

Jak wskazują dane CERT Polska z 2024 roku, zagrożenia wobec użytkowników wciąż eskalują, a potwierdzają to liczby - **ponad 70 milionów prób dostępu do domen o potencjalnie złośliwym charakterze, co stanowi wzrost o 33% względem roku poprzedniego**. Liczba zgłoszonych incydentów przekroczyła 600 tysięcy, rosnąc o 62% rok do roku, co odzwierciedla zarówno wzrost aktywności przestępców, jak i skuteczniejszą detekcję oraz reakcję służb.

- **Między 2023 a 2024 rokiem nastąpił znaczący wzrost skali cyberzagrożeń w Polsce.** Liczba zgłoszeń do CERT Polska wzrosła o 62%, osiągając poziom ponad 600 000, co odzwierciedla zarówno większą aktywność cyberprzestępców, jak i rosnącą świadomość społeczną.
- **Potwierdzonych incydentów było o 29% więcej niż rok wcześniej** – łącznie 103 449. Najbardziej dynamiczny wzrost odnotowano w obszarze phishingu, który w 2024 roku stanowił aż 95% wszystkich incydentów, przy niemal czterokrotnym wzroście liczby zgłoszeń względem 2023.
- **Smishing (złośliwe SMS-y) również przybrał na sile – liczba zgłoszeń wzrosła o 60% r/r. Zablokowano też 1,5 mln niebezpiecznych wiadomości.**
- Szczególnie niepokojąca jest sytuacja w administracji publicznej, gdzie w 2024 roku zgłoszono ponad 1 900 incydentów, co stanowi wzrost o 58% w porównaniu do roku poprzedniego.
- W 2024 roku zablokowano ponad 70 mln prób dostępu do niebezpiecznych domen — to wzrost o 33% względem 2023 r.

# 3. Główne zagrożenia w Polsce

**Kluczowym wektorem ataku pozostaje phishing**, odpowiedzialny za około 95% wszystkich incydentów zgłaszanych do CERT Polska. **W samym 2024 roku zarejestrowano ponad 600 tysięcy zgłoszeń związanych z tą metodą ataku, z czego blisko 40 tysięcy dotyczyło prób wyłudzenia danych uwierzytelniających** (*credential phishing*). Ten rodzaj ataku nadal pozostaje wyjątkowo skuteczny dzięki wykorzystaniu socjotechniki oraz presji czasu — jak wskazuje raport „Verizon DBIR 2024", użytkownik potrzebuje średnio mniej niż 60 sekund, aby paść ofiarą phishingu.



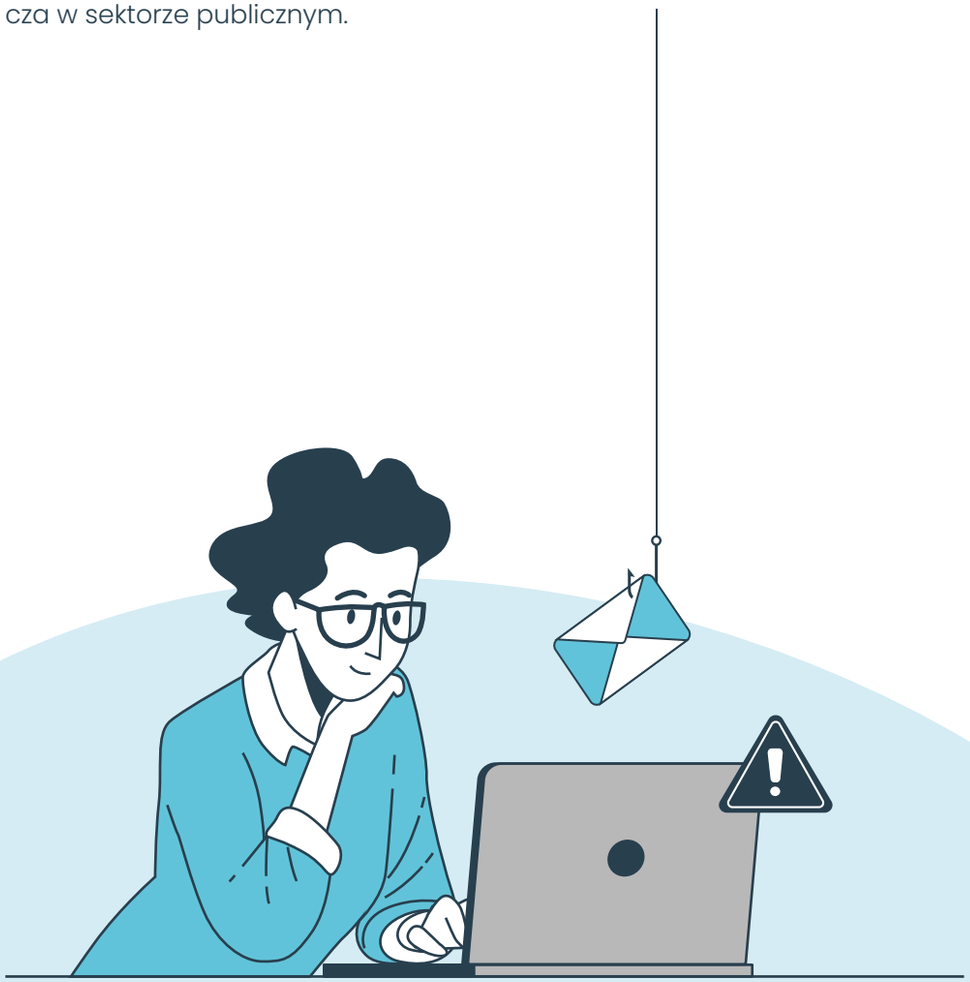
Wraz z rosnącą penetracją urządzeń mobilnych, które w Polsce obsługują ponad 30 milionów użytkowników, **rośnie również skala ataków smishingowych** — czyli phishingu realizowanego za pośrednictwem wiadomości SMS. **W 2024 roku liczba takich incydentów przekroczyła 355 tysięcy, co oznacza wzrost o 60% względem roku poprzedniego.** Liderzy rynku tacy jak Samsung czy Apple, wdrożyli zaawansowane mechanizmy blokujące smishing już na poziomie sieci, co znacząco ogranicza skuteczność tych ataków u ich źródła. Przykładem może być platforma CyberTarcza Orange, która w 2024 roku zablokowała 305 tysięcy domen phishingowych, chroniąc blisko 5 milionów użytkowników.

Kolejnym, coraz bardziej istotnym zagrożeniem jest **dezinformacja**, która w 2024 roku osiągnęła nowy poziom dzięki wykorzystaniu technologii sztucznej inteligencji, zwłaszcza deepfake'ów i generowanych automatycznie fake newsów. Raport „Dezinformacja oczami Polaków 2024" wskazuje, że **aż 84% badanych zetknęło się z fałszywymi informacjami, a 90% potwierdziło wiarygodność przynajmniej jednej z nich**, co pokazuje ogromny wpływ tego zjawiska na społeczne postrzeganie rzeczywistości. Szczególnie narażone są obszary polityki, zdrowia, energetyki oraz zmian klimatycznych, gdzie fałszywe narracje mogą prowadzić do osłabienia zaufania do instytucji i pogłębiania społecznych podziałów.

Nastąpił także **wzrost skali ataków ransomware** - to znaczący skok jasno wskazujący na eskalację zagrożenia w krótkim czasie. Według danych ESET Threat Report z II półrocza 2024, liczba ataków ransomware w Polsce **wzrosła aż o 37% względem I półrocza tego samego roku**. Druga połowa roku wyniosła Polskę na 7. pozycję na świecie pod względem liczby ataków ransomware (4% globalnych incydentów), podczas gdy w I półroczu 2024 plasowaliśmy się dopiero na 13. miejscu (2,3% światowego udziału). Ransomware szczególnie dotknął polskie instytucje publiczne i firmy z sektora transportowego – przykładem jest atak na Scania Polska, w wyniku którego zaszyfrowano dane zarówno firmy, jak i jej klientów.

# 4. Świadomość cyberzagrożeń w Polsce – luka między deklaracjami a praktyką

W 2024 roku diagnoza stanu świadomości i gotowości cyfrowej instytucji publicznych oraz sektora prywatnego w Polsce ujawnia wyraźne kontrasty między poziomem deklarowanych inwestycji w technologie cyfrowe, a realnym stanem przygotowania do reagowania na cyberzagrożenia. Choć rośnie zainteresowanie transformacją cyfrową, to poziom operacyjnej dojrzałości w zakresie cyberbezpieczeństwa nadal pozostaje niewystarczający – zwłaszcza w sektorze publicznym.





## Niedostateczna odporność instytucji publicznych

Kontrola przeprowadzona przez Najwyższą Izbę Kontroli w 24 jednostkach samorządu terytorialnego (17 gmin i 7 powiatów) wykazała aż 222 przypadki nieprawidłowości w zakresie cyberbezpieczeństwa. Choć 51 z nich udało się usunąć już w trakcie kontroli, aż 71% urzędów otrzymało ocenę negatywną w zakresie przygotowania do zapewnienia ciągłości działania systemów IT w warunkach kryzysowych (takich jak atak hakerski, awaria czy działania hybrydowe). Istotne uchybienia stwierdzono w 23 z 24 badanych jednostek – co stanowi poważny sygnał alarmowy w kontekście bezpieczeństwa usług publicznych.

NIK zwróciła również uwagę na brak uwzględniania wymagań dotyczących bezpieczeństwa informacji w procedurach zamówień publicznych. **W wielu przypadkach umowy z dostawcami usług IT nie zawierały zapisów dotyczących poufności,** co rodzi istotne ryzyko dla integralności systemów w przypadku incydentu cybernetycznego. Innym problemem był fakt, że wiele gmin korzystało z publicznych kont e-mail (np. Gmail/Outlook), co stwarza ryzyko wycieków danych wrażliwych. Skala problemu objęła tysiące skrzynek mailowych w całej administracji lokalnej. Zgodnie ze sprawozdaniem rządowym (Gov.pl), w 2024 roku **liczba zgłoszeń incydentów teleinformatycznych wzrosła o 60%**, a potwierdzonych przypadków - o 23% względem 2023 roku. **W sektorze publicznym wykryto 58% więcej incydentów.**

## Biznes inwestuje

Z drugiej strony sektor prywatny wykazuje coraz większe zrozumienie wagi cyfrowej transformacji i zarządzania ryzykiem technologicznym. Jak wynika z raportu EY „Cyfrowa Transformacja 2024", aż 84% przedsiębiorstw w Polsce traktuje cyfryzację jako priorytet strategiczny (wzrost z 38% w 2020 r.). Co istotne, **49% firm już wdrożyło działania z zakresu cyberbezpieczeństwa**, a w nadchodzących 12 miesiącach to właśnie ten obszar ma pochłonąć największe nakłady inwestycyjne – **44% firm wskazało bezpieczeństwo cyfrowe jako główny cel budżetowy, wyprzedzając szkolenia (36%) i usługi chmurowe (34%)**. To sprawia, że Polska plasuje się w europejskiej czołówce wzrostu wydatków na cyberbezpieczeństwo — według IDC, wydatki te rosną o ponad 15% rok do roku, co przekłada się na krajowy rynek wart ~2,5 mld zł w 2024 roku (2 mld zł w 2023 r.).

Uwagę zwraca również udział firm w praktycznych testach gotowości, takich jak ćwiczenia Cyber-EXE Polska 2024, w których udział wzięło 18 instytucji sektora finansowego. Scenariusze oparte na rzeczywistych metodach ataków ujawniły wysokie kompetencje techniczne uczestników w zakresie klasyfikacji, analizy i zgłaszania poważnych incydentów zgodnie z wymaganiami regulacyjnymi NIS2 i DORA. Jednocześnie zarekomendowano wprowadzenie bardziej złożonych scenariuszy w kolejnych edycjach, co wskazuje na chęć dalszego rozwoju i adaptacji do coraz bardziej zaawansowanych zagrożeń.

Rosnąca adopcja narzędzi i procesów IT świadczy o dojrzałości, choć braki kadrowe i budżetowe wciąż pozostają barierą dla firm - jak wskazuje raport KPMG „Barometr Cyberbezpieczeństwa", aż 57% firm wskazuje, że nie posiada wystarczających środków, a 53% doświadcza trudności z rekrutacją specjalistów. Jednak 84% firm deklaruje korzystanie z wsparcia zewnętrznego (outsourcing), często w obszarze szkoleń i reakcji na incydenty, zamiast próby budowania kompetencji jedynie wewnątrz organizacji.



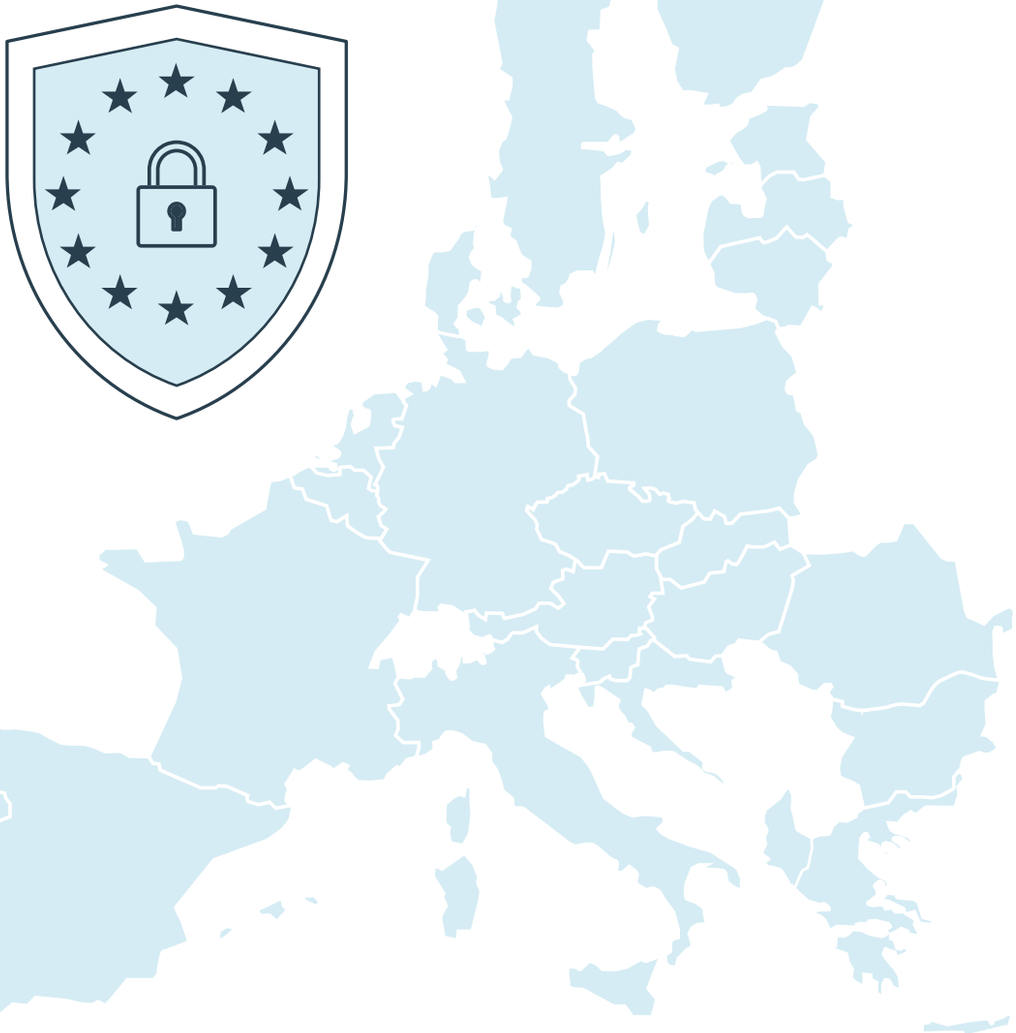
## Świadomość społeczna

Z badania CBOS „Korzystanie z internetu w 2024 roku" wynika, że 77% dorosłych Polaków korzysta z internetu, przy czym w grupie osób poniżej 45. roku życia dostęp do sieci jest niemal powszechny. Rosnąca liczba aktywności online – takich jak zakupy, bankowość elektroniczna, korzystanie z komunikatorów czy serwisów streamingowych – zwiększa powierzchnię ataku, na jaką narażeni są użytkownicy. Aż 83% internautów korzysta z bankowości elektronicznej, a ponad 50% dokonuje zakupów online w skali miesięcznej.

Mimo że badanie CBOS nie zawiera bezpośrednich danych o świadomości zagrożeń, poziom cyfrowej aktywności – szczególnie w kontekście phishingu, oszustw finansowych czy ataków socjotechnicznych – sugeruje, że użytkownicy często nie są w pełni świadomi zagrożeń, jakie niosą za sobą codzienne działania online. Problem pogłębiają różnice demograficzne – osoby starsze i z niższym wykształceniem pozostają znacznie bardziej podatne na manipulację, a jednocześnie rzadziej korzystają z narzędzi ochrony, takich jak uwierzytelnianie dwuskładnikowe czy aktualne oprogramowanie zabezpieczające.

# 5. Cybertarcza Unii Europejskiej

W odpowiedzi na narastające zagrożenia w cyberprzestrzeni oraz rosnące uzależnienie państw i gospodarek od infrastruktury cyfrowej, Unia Europejska przyjęła szereg aktów prawnych mających na celu budowę wspólnotowej „cybertarczy", takich jak między innymi:





## Dyrektywa NIS2

**(Network and Information Security Directive)**

Zastępuje poprzednią dyrektywę NIS1 z 2016 roku. Jej głównym celem jest podniesienie poziomu cyberbezpieczeństwa w Unii Europejskiej poprzez:

- rozszerzenie zakresu regulacji na 18 sektorów krytycznych, w tym energetykę, transport, opiekę zdrowotną, finanse, gospodarkę wodną, administrację publiczną i sektor kosmiczny;
- wprowadzenie jednolitych ram prawnych w zakresie zarządzania ryzykiem i reagowania na incydenty,
- zobowiązanie państw członkowskich do opracowania krajowych strategii cyberbezpieczeństwa oraz współpracy transgranicznej w zakresie egzekwowania przepisów.

Dyrektywa nakłada obowiązki na średnie i duże podmioty z sektorów krytycznych, m.in. w zakresie wdrażania środków zarządzania ryzykiem, raportowania istotnych incydentów cyberbezpieczeństwa, czy zapewnienia odpowiedzialności kierownictwa za niewypełnianie obowiązków.

## DORA

**(Digital Operational Resilience Act)**

Rozporządzenie obowiązujące od 17 stycznia 2025 r., ma na celu zapewnienie odporności sektora finansowego na zagrożenia cyfrowe. Obejmuje ono m.in.: jednolite standardy zarządzania ryzykiem ICT, obowiązki w zakresie raportowania incydentów i testowania odporności systemów oraz nadzór nad dostawcami usług ICT, w tym chmurowych. Wprowadza bezprecedensowy poziom ujednolicenia zasad w całej UE, obejmując zarówno instytucje finansowe, jak i kluczowych dostawców usług cyfrowych.

## Dyrektywa CER

**(Critical Entities Resilience) z 14 grudnia 2022 r.**

Zastępuje wcześniejszą dyrektywę 2008/114/WE, rozszerzając zakres ochrony podmiotów kluczowych dla funkcjonowania państw i społeczeństw UE. Zakres dyrektywy obejmuje 11 sektorów, m.in. energetykę, transport, bankowość, zdrowie, wodę pitną i ścieki, cyfrową infrastrukturę, oraz produkcję i dystrybucję żywności.

Podmioty objęte dyrektywą muszą prowadzić ocenę ryzyka, wdrażać środki techniczne i organizacyjne, opracowywać plany ciągłości działania i reagowania, szkolić personel i realizować ćwiczenia symulacyjne, a także zgłaszać poważne incydenty. Z kolei Komisja Europejska może także przeprowadzać misje doradcze dla podmiotów o znaczeniu europejskim.

## Cyber Resilience Act

**(CRA)**

To regulacja wprowadzająca obowiązki cyberbezpieczeństwa dla całego cyklu życia produktów cyfrowych. CRA obejmuje zarówno sprzęt, jak i oprogramowanie – od urządzeń IoT po aplikacje i systemy operacyjne. Zgodnie z nią, producenci muszą projektować produkty zgodnie z zasadą "security by design", zapewniać aktualizacje bezpieczeństwa, przeprowadzać ocenę zgodności i stosować oznakowanie CE, zgłaszać incydenty i podatności w ciągu 24 godzin. CRA ma zapewnić, że wszystkie produkty z elementami cyfrowymi spełniają minimalne normy bezpieczeństwa, zanim trafią na rynek UE.



## AI Act

To pierwsza kompleksowa regulacja dotycząca sztucznej inteligencji w UE. Klasyfikuje systemy AI według poziomu ryzyka - na przykład te z obszaru wysokiego ryzyka (zdrowie, finanse, zatrudnienie) muszą spełniać rygorystyczne wymagania w zakresie zarządzania ryzykiem, dokumentacji technicznej, nadzoru ludzkiego, oceny zgodności oraz transparentności działania. Dodatkowo, dostawcy i użytkownicy systemów AI są zobowiązani do zapewnienia, że systemy nie naruszają podstawowych praw obywateli – takich jak prywatność, równość czy prawo do wyjaśnienia decyzji podejmowanych automatycznie. AI Act przewiduje także zakaz stosowania systemów AI o niedopuszczalnym ryzyku, takich jak np. manipulacyjne techniki wpływające na zachowanie dzieci czy masowy nadzór biometryczny w czasie rzeczywistym (z pewnymi wyjątkami dla organów ścigania).

## EUCS

**(European Cybersecurity Certification Scheme for Cloud Services)**

To rozwijany przez ENISA schemat certyfikacji usług chmurowych w UE. Zakłada trzystopniowy system poziomów bezpieczeństwa (podstawowy, istotny, wysoki). Certyfikacja jest dobrowolna, lecz może stanowić istotny atut konkurencyjny na rynku. Schemat ma na celu zapewnienie spójnych standardów ochrony danych w całej Unii – szczególnie w sektorze publicznym i kluczowych gałęziach gospodarki. Początkowo projekt zawierał tzw. wymogi suwerennościowe (lokalizacja danych i jurysdykcja), jednak ze względu na sprzeciw branży i niektórych państw członkowskich zostały one złagodzone.

# 6. Polski system cyberodporności

System cyberodporności w Polsce znajduje się w fazie intensywnych reform. Kierunki zmian wyznacza dostosowanie do europejskich regulacji, wzmocnienie kompetencji instytucji publicznych oraz mobilizacja środków finansowych na rzecz zwiększenia odporności cyfrowej całego państwa – od szczebla centralnego po lokalny, od administracji po sektor prywatny i naukę.

Centralnym filarem tego systemu jest **Krajowy System Cyberbezpieczeństwa** (KSC), który został ustanowiony ustawą z 5 lipca 2018 r., implementującą pierwszą unijną dyrektywę NIS. Jego głównym celem jest zapewnienie ciągłości świadczenia usług kluczowych i cyfrowych poprzez podnoszenie poziomu bezpieczeństwa systemów teleinformatycznych. Obecnie trwają prace nad nowelizacją ustawy o KSC, których celem jest dostosowanie przepisów do wymagań dyrektywy NIS2. Projekt nowelizacji zakłada m.in. obowiązek wycofywania sprzętu lub oprogramowania uznanego za niebezpieczne, zwiększenie odpowiedzialności operatorów usług kluczowych i dostawców usług cyfrowych, obowiązkową analizę ryzyka uzależnioną od specyfiki działalności, nowe obowiązki raportowe oraz sankcje administracyjne.

W ramach KSC funkcjonują trzy krajowe zespoły reagowania na incydenty komputerowe (CSIRT), które pełnią kluczową rolę w wykrywaniu, analizie i neutralizacji incydentów bezpieczeństwa oraz we wzajemnej wymianie informacji o zagrożeniach. Są to:

- **CSIRT GOV**
  – koordynowany przez Agencję Bezpieczeństwa Wewnętrznego (ABW),
- **CSIRT MON**
  – działający w ramach Ministerstwa Obrony Narodowej,
- **CSIRT NASK**
  – obsługiwany przez NASK PIB.



Kolejnym filarem systemu jest certyfikacja cyberbezpieczeństwa. W 2025 roku Rada Ministrów przyjęła projekt ustawy o krajowym systemie certyfikacji, który wdraża przepisy rozporządzenia UE 2019/881 (Cybersecurity Act). Certyfikaty (krajowe i europejskie) będą mogły być wydawane dla produktów, usług i procesów ICT. Choć certyfikacja ma charakter dobrowolny, jej posiadanie potwierdza odporność na cyberzagrożenia, zwiększa zaufanie użytkowników i kontrahentów, ułatwia udział w przetargach publicznych oraz zwiększa konkurencyjność firm na rynku europejskim. System przewiduje nadzór Ministra Cyfryzacji i Polskiego Centrum Akredytacji oraz zaangażowanie sektora prywatnego i publicznego w procesy oceny zgodności.

Jednym z kluczowych źródeł finansowania krajowej cyberodporności jest Fundusz Cyberbezpieczeństwa, utworzony w 2021 r. jako państwowy fundusz celowy. Od lipca 2024 r. jego roczny budżet zwiększono do 250 mln zł. Fundusz przeznaczany jest m.in. na dodatki do wynagrodzeń dla specjalistów ds. cyberbezpieczeństwa w administracji publicznej, modernizację infrastruktury IT, zakup sprzętu i oprogramowania oraz na szkolenia i rozwój kompetencji cyfrowych pracowników sektora publicznego. Dzięki zwiększonemu budżetowi możliwe jest stabilizowanie zatrudnienia w strategicznych instytucjach państwa i zmniejszenie odpływu specjalistów do sektora prywatnego.

Z kolei samorządy, jako operatorzy usług publicznych, również zostały objęte wsparciem systemowym. Program „Cyberbezpieczny Samorząd" jest ogólnopolską inicjatywą realizowaną przez Centrum Projektów Polska Cyfrowa (CPPC) i NASK PIB, a finansowaną ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021–2027.

Program ma na celu m.in. aktualizację polityk bezpieczeństwa informacji (SZBI), wdrażanie zarządzania ryzykiem, audyty bezpieczeństwa i działania zwiększające odporność na ataki oraz rozwój kompetencji cyfrowych kadr JST. Do programu przystąpiło aż 90% uprawnionych jednostek samorządu, a całkowita wartość złożonych wniosków wyniosła ok. 1,5 mld zł.

Oprócz krajowych środków, podmioty publiczne i prywatne mogą sięgać po różne źródła finansowania działań z zakresu cyberbezpieczeństwa. Rozwój polskiego systemu cyberodporności jest możliwy dzięki takim źródłom finansowania jak np.:

## Dla jednostek administracji

- Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC)
  – m.in. programy Cyfrowa Gmina, Cyfrowa Szkoła, Cyberbezpieczny Samorząd,
- REACT-EU – środki na odbudowę po pandemii COVID-19 (z komponentem cyfrowym),
- KPO (Krajowy Plan Odbudowy)
  – inwestycje w transformację cyfrową i bezpieczeństwo usług publicznych,
- Fundusz Cyberbezpieczeństwa (środki krajowe).

## Dla biznesu

- Fundusze Horyzont Europa (Horizon Europe)
  – programy badawczo-innowacyjne z komponentem cyberbezpieczeństwa,
- Digital Europe Programme (DEP)
  – m.in. dotacje na rozwój kompetencji, infrastrukturę i testowanie nowych rozwiązań ICT,
- PARP i NCBR
  – krajowe konkursy dla firm na rozwój technologii bezpieczeństwa cyfrowego,
- Fundusz Cyberbezpieczeństwa
  – możliwy udział firm w zamówieniach publicznych związanych z projektami ICT i cyber.

## Dla nauki i sektora B+R

- Horyzont Europa (klastry 3 i 4 – bezpieczeństwo i technologie cyfrowe),
- Program INFOSTRATEG NCBR,
- EIT Digital – europejska sieć innowacji cyfrowych,
- DEP – pilotażowe projekty testowania AI i bezpieczeństwa IT.

# 7. Mapa drogowa Cyfrowej Polski dla wzmocnienia cyberbezpieczeństwa państwa

W obliczu rosnącej liczby incydentów oraz coraz bardziej wyrafinowanych zagrożeń cyfrowych, cyberbezpieczeństwo musi być dziś traktowane jako wspólny obowiązek – zarówno publiczny, jak i biznesowy. Ochrona zasobów cyfrowych nie może być postrzegana wyłącznie jako koszt czy kwestia techniczna. To jeden z filarów funkcjonowania nowoczesnego państwa, stabilności gospodarki oraz zaufania społecznego. Takie podejście wymaga współpracy wszystkich interesariuszy – administracji, sektora prywatnego, środowisk akademickich i obywateli. Nie istnieje rozwiązanie gwarantujące stuprocentową ochronę przed cyberatakami. Dlatego kluczowe jest przyjęcie strategii minimalizacji ryzyka – budowania wielowarstwowej ochrony, opracowania planów awaryjnych oraz wdrażania skutecznych procedur reagowania na incydenty. Cyberbezpieczeństwo nie polega na tworzeniu złudzenia nietykalności, lecz na świadomym i konsekwentnym zarządzaniu zagrożeniami oraz ograniczaniu ich skutków. Nie jest też produktem, lecz procesem – ciągłym, wymagającym konsekwencji, systematyczności i kultury organizacyjnej opartej na odpowiedzialności. Ochrona danych i systemów nie kończy się na wdrożeniu technologii – to cykl nieustannej oceny, aktualizacji, szkoleń oraz reagowania na nowe typy zagrożeń. Najsłabszym ogniwem w tym łańcuchu nadal pozostaje człowiek – dlatego inwestycje w edukację, zwiększanie świadomości użytkowników i rozwój kompetencji cyfrowych są równie ważne, jak wdrażanie nowoczesnych rozwiązań technologicznych.

Choć organizacje – zarówno publiczne, jak i prywatne – coraz skuteczniej implementują procedury związane z cyberbezpieczeństwem i zarządzaniem ryzykiem IT, szczególnej uwagi wymaga obszar ochrony urządzeń końcowych: smartfonów, laptopów, tabletów, komputerów stacjonarnych, drukarek i urządzeń wielofunkcyjnych. W dobie pracy zdalnej i hybrydowej ich bezpieczeństwo staje się jednym z kluczowych komponentów cyberodporności organizacji. Nie ma dziś instytucji czy firmy – szczególnie działających międzynarodowo – które byłyby wolne od ryzyka cyberataków. Dlatego jednym z najważniejszych priorytetów powinno być systemowe podnoszenie poziomu edukacji w zakresie cyberbezpieczeństwa – zarówno na poziomie ogólnokrajowym, jak i w ramach wewnętrznych struktur organizacyjnych.

W dalszej części Raportu przedstawiamy rekomendacje branżowe – postulaty, których wprowadzenie jest konieczne w odpowiedzi na wyzwania związane z obecnymi cyberzagrożeniami oraz zalecenia dla firm i pojedynczych użytkowników urządzeń końcowych opracowane na podstawie doświadczeń firm zrzeszonych w Związku Cyfrowa Polska. Równolegle z edukacją i technologią, niezbędna jest także ścisła współpraca między sektorem publicznym, a prywatnym na rzecz budowy odpornego systemu cyberbezpieczeństwa. Dostęp do innowacyjnych rozwiązań wypracowanych przez polski sektor ICT pozwala skutecznie odpowiadać na dynamicznie ewoluujące wyzwania, z jakimi mierzy się dziś polska gospodarka, administracja i społeczeństwo cyfrowe.

# 8. Rekomendacje branżowe

Postulaty branży technologicznej, w tym firm zrzeszonych w Związku Cyfrowa Polska, dotyczą nie tylko implementacji najnowszych wymogów unijnych, lecz także kompleksowego podejścia do budowy cyberodporności na wszystkich poziomach: od infrastruktury, przez technologie, po ludzi i procesy. Wspólne działania administracji, przedsiębiorstw i środowiska technologicznego są niezbędne, by skutecznie przeciwdziałać rosnącym zagrożeniom w cyberprzestrzeni i zapewnić bezpieczeństwo cyfrowej transformacji Polski.

Wśród najważniejszych rekomendacji znajduje się:

1. **Eliminacja niepewności regulacyjnej.** Obecna fragmentacja przepisów cyberbezpieczeństwa w poszczególnych państwach członkowskich UE powoduje znaczące komplikacje dla dostawców usług i producentów technologii. Harmonizacja przepisów, obejmująca takie regulacje jak Dyrektywa NIS2, oraz Rozporządzenie DORA (Digital Operational Resilience Act), jest niezbędna dla sprawnego funkcjonowania jednolitego rynku cyfrowego UE. Konieczność dostosowywania produktów i procesów do różnorodnych wymogów prawnych w poszczególnych krajach zwiększa koszty operacyjne, wydłuża czas wdrożeń i ogranicza możliwości ekspansji międzynarodowej firm. Dlatego tak ważne jest wprowadzenie spójnego, jednolitego systemu regulacji na poziomie UE, który zminimalizuje rozdrobnienie rynku, ułatwi działalność przedsiębiorstw oraz podniesie ogólny poziom bezpieczeństwa infrastruktury cyfrowej. Umożliwi to firmom działanie na całym terytorium Unii według jednolitych zasad, co zwiększy przewidywalność, ograniczy ryzyko niezgodności i wesprze innowacyjność. Szczególnie w obliczu rosnących, złożonych zagrożeń, takich jak ataki oparte na AI czy cyberkampanie o podłożu geopolitycznym, spójna i szeroka odporność cyfrowa państw członkowskich jest warunkiem skutecznej obrony.



2. **Usprawnienie procesu legislacyjnego i modernizacja ram regulacyjnych w obszarze cyberbezpieczeństwa i innowacji cyfrowych.** Przewlekłość procesów legislacyjnych, brak decyzyjności czy silne przywiązanie do nieaktualnych regulacji, znacząco ograniczają zdolność państwa i sektora prywatnego do skutecznego reagowania na nowe wyzwania i implementowania rozwiązań zapewniających bezpieczeństwo i konkurencyjność. Dlatego tak ważne jest wdrożenie bardziej elastycznego podejścia do tworzenia prawa oraz mechanizmów regulacyjnych, w tym rozwój procesów konsultacyjnych opartych na realnym partnerstwie z sektorem technologicznym. Szczególnie istotne jest zapewnienie ram prawnych, które umożliwią szybkie wdrażanie nowoczesnych rozwiązań, takich jak technologie chmurowe, AI czy automatyzacja zarządzania incydentami, bez konieczności czasochłonnych procedur uzgodnień i interpretacji przestarzałych norm. Z punktu widzenia cyberodporności państwa i instytucji, kluczowe jest również budowanie modelu współpracy opartego na wzajemnym zaufaniu, otwartości na dialog ekspercki oraz gotowości do testowania i skalowania innowacji w modelu „sandboxowym". Tylko dynamiczne i współbieżne z rynkiem działania legislacyjne pozwolą na skuteczne zabezpieczenie infrastruktury krytycznej, danych obywateli oraz ciągłości działania instytucji publicznych w realiach rosnącej presji geopolitycznej i technologicznej.

3. **Wdrożenie zasad Zero Trust oraz integracja sztucznej inteligencji w detekcji incydentów.** Model bezpieczeństwa Zero Trust zakłada, że żadna jednostka ani urządzenie nie jest z założenia zaufane, nawet w obrębie sieci wewnętrznej. Realizacja tego modelu wymaga zaawansowanego zarządzania tożsamością, stałej weryfikacji dostępu oraz segmentacji sieci. Równocześnie istotne jest wykorzystanie sztucznej inteligencji do automatycznej detekcji, analizy i monitoringu incydentów cybernetycznych, co pozwala na szybszą reakcję i ograniczenie ryzyka eskalacji zagrożeń.

4. **Rozbudowa infrastruktury krytycznej w sektorach bezpieczeństwa publicznego, obronności i transportu.** Zabezpieczenie systemów w obszarach takich jak obronność, bezpieczeństwo publiczne czy transport jest priorytetem, szczególnie wobec rosnącej liczby zaawansowanych cyberataków na te sektory. Dlatego ich systemy muszą być nie tylko wysoce odporne na ataki, ale również zdolne do szybkiego wykrywania i neutralizacji incydentów cybernetycznych. Konieczne jest pilne wdrożenie nowoczesnych technologii, które z jednej strony podniosą poziom bezpieczeństwa, a z drugiej pozwolą na efektywne zarządzanie ryzykiem i szybkie reagowanie na zagrożenia. Kluczowe jest między innymi uznanie technologii 5G jako strategicznej podstawy cyfryzacji oraz aktywny udział w rozwoju 6G, które umożliwią szybkie reagowanie i ograniczanie skutków incydentów. W kontekście zagrożeń płynących z rozwoju komputerów kwantowych, niezbędne jest już dziś wdrażanie sieci typu Quantum Safe. Dzięki silnej obecności lokalnej i gotowym technologiom Polska ma szansę być jednym z liderów przyszłej, bezpiecznej cyfrowo Europy.

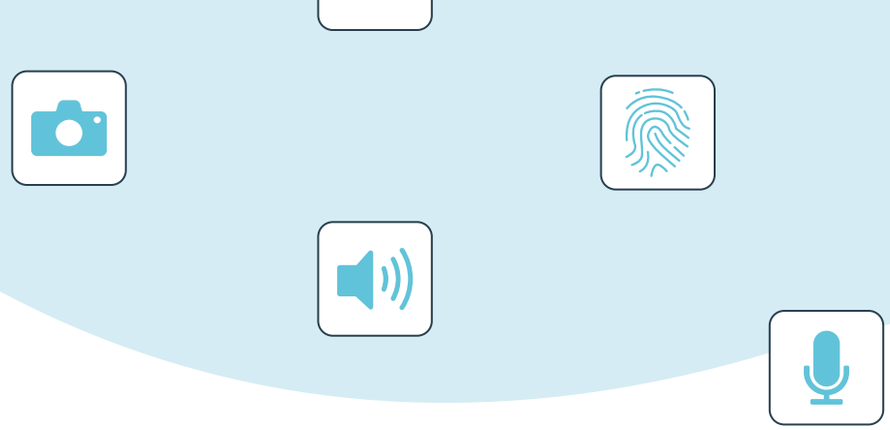
5. **Wprowadzenie dedykowanych uprawnień dostępu do sieci i systemów.** Specjalne mechanizmy zarządzania dostępem, takie jak role-based access control (RBAC) oraz polityki minimalnych uprawnień (least privilege), stanowią podstawę skutecznej ochrony przed nieautoryzowanym dostępem oraz zagrożeniami pochodzącymi z wnętrza organizacji. Wdrożenie nowoczesnych rozwiązań, w tym autoryzacji wieloskładnikowej (MFA) oraz ciągłej analizy zachowań użytkowników (User and Entity Behavior Analytics – UEBA), pozwala na szybkie wykrywanie anomalii i nieprawidłowości w dostępie do zasobów. Takie podejście minimalizuje ryzyko wycieków danych i sabotażu oraz wzmacnia ogólną odporność systemów na ataki wewnętrzne i zewnętrzne. Dodatkowo, dynamiczne zarządzanie uprawnieniami, oparte na kontekście użytkownika i sytuacji operacyjnej, umożliwia elastyczne i bezpieczne dostosowanie dostępu do zmieniających się wymagań bezpieczeństwa.



6. **Systematyczne szkolenia urzędników i pracowników w zakresie cyberbezpieczeństwa i zarządzania dostępem.** Najsłabszym ogniwem w ochronie systemów informatycznych pozostaje człowiek, dlatego tak ważne jest znaczące zwiększenie nakładów na edukację oraz podnoszenie kompetencji personelu zarówno w administracji publicznej, jak i w sektorze prywatnym oraz instytucjach. Regularne i obligatoryjne szkolenia z zakresu identyfikacji zagrożeń cybernetycznych, stosowania najlepszych praktyk w zarządzaniu dostępem do danych oraz skutecznego reagowania na incydenty stanowią fundament budowy odpornej i bezpiecznej organizacji. Ponadto, takie działania pozwalają na redukcję ryzyka błędów ludzkich, które często stanowią furtkę dla cyberataków. Inwestycja w rozwój świadomości oraz kształtowanie kultury bezpieczeństwa stanowi niezbędne uzupełnienie wdrożenia zaawansowanych technologii, umożliwiając ich efektywne wykorzystanie. Edukacja personelu powinna być ciągła i dostosowana do zmieniających się zagrożeń, co pozwala na utrzymanie wysokiego poziomu gotowości oraz odporności na nowe typy ataków.

7. **Implementacja zasady Secure by Design – bezpieczeństwo w fazie projektowania systemów i produktów.** Bezpieczeństwo powinno stanowić integralny i nieodłączny element całego procesu tworzenia systemów, aplikacji oraz produktów informatycznych już od samego początku, czyli na etapie ich projektowania (Secure by Design). Oznacza to, że wszystkie rozwiązania muszą być konstruowane z myślą o ochronie danych, minimalizacji potencjalnych zagrożeń oraz zapewnieniu łatwego i skutecznego utrzymania mechanizmów bezpieczeństwa przez cały cykl życia produktu. Takie podejście pozwala na wczesne wykrywanie i eliminację luk bezpieczeństwa, które w późniejszych fazach mogą prowadzić do kosztownych i skomplikowanych poprawek, a także narazić użytkowników na ryzyko utraty danych lub ataków cybernetycznych. Dodatkowo, wdrażanie Secure by Design zwiększa zaufanie klientów i użytkowników końcowych, co przekłada się na wyższą wartość rynkową i konkurencyjność produktów oraz usług. Wdrożenie tej zasady w regulacjach i standardach dotyczących tworzenia oprogramowania oraz infrastruktury ICT, powinno być obowiązkowe, aby bezpieczeństwo stało się fundamentem rozwoju cyfrowego.

# 9. Zalecenia dla firm oraz indywidualnych użytkowników urządzeń końcowych



## Rozwiązania poprawiające bezpieczeństwo urządzeń mobilnych

### Mobile Threat Defense (MTD)

Nowoczesne rozwiązania MTD oferują kompleksowy monitoring urządzeń mobilnych oraz zainstalowanych aplikacji, analizując, jakie dane są przesyłane, do kogo, oraz które sensory urządzenia (mikrofon, kamera, lokalizacja) są aktywne. Wykorzystują one zaawansowane mechanizmy, często oparte na sztucznej inteligencji i analizie behawioralnej, co pozwala na automatyczne wykrywanie nietypowych aktywności i potencjalnych zagrożeń. Dzięki temu możliwe jest szybkie reagowanie, blokowanie ryzykownych funkcji aplikacji lub całych aplikacji narażających dane na wyciek.

### Bezpieczne połączenie VPN oraz podejście Zero Trust

Szyfrowane kanały transmisji danych, takie jak VPN, nadal stanowią fundament bezpiecznego dostępu do zasobów firmowych i prywatnych z dowolnej sieci. Jednak wraz z rozwojem architektur sieciowych rośnie znaczenie podejścia Zero Trust Network Access (ZTNA), które eliminuje zaufanie do sieci wewnętrznych i wymaga ciągłej weryfikacji tożsamości użytkownika oraz urządzenia na każdym etapie połączenia.



### Bezpieczna komunikacja głosowa, tekstowa i video

Szyfrowanie end-to-end w komunikatorach stało się standardem dla ochrony poufności rozmów i wymiany danych. Coraz więcej aplikacji wykorzystuje unikalne, dynamiczne klucze szyfrujące oraz mechanizmy ochrony przed podsłuchem i manipulacją danymi, co wzmacnia zaufanie użytkowników do tych rozwiązań.

### Podpis biometryczny i kwalifikowany

Podpis elektroniczny, zarówno kwalifikowany, jak i biometryczny, jest dziś kluczowym narzędziem w cyfrowej weryfikacji tożsamości i autentyczności dokumentów. W kontekście nadchodzących regulacji eIDAS 2.0 w UE, rośnie rola takich rozwiązań, które łączą wygodę z wysokim poziomem bezpieczeństwa. Ważne jest, aby producenci sprzętu dostarczali certyfikacje dotyczące jakości i bezpieczeństwa matryc biometrycznych, co umożliwia rzetelną weryfikację podpisów.

# Higiena korzystania z urządzeń mobilnych pod względem bezpieczeństwa

### Zabezpieczenie dostępu do danych i uwierzytelnienie

Najbezpieczniejszą i najwygodniejszą metodą ochrony urządzenia jest biometria (odcisk palca, rozpoznawanie twarzy). Alternatywnie stosuje się silne hasła lub PIN-y, najlepiej długie i unikalne, zarządzane przez menedżery haseł. Warto także stosować regularne zmiany haseł i unikać ich powtarzania w różnych usługach.

### Weryfikacja wieloskładnikowa (MFA)

Dla dostępu do szczególnie wrażliwych danych oraz aplikacji zaleca się stosowanie uwierzytelniania wieloskładnikowego, łączącego coś, co użytkownik zna (hasło), posiada (token lub telefon) oraz czym jest (biometria). MFA znacznie utrudnia ataki typu phishing i przejęcie konta.

### Wi-Fi, Bluetooth i ochrona łączności

Wyłączanie Wi-Fi i Bluetooth, gdy nie są używane, to podstawowa zasada bezpieczeństwa. Należy unikać korzystania z niezabezpieczonych, publicznych sieci Wi-Fi bez dodatkowej ochrony, takiej jak VPN. Ataki polegające na wymuszaniu przejścia na niższe technologie transmisji (downgrade attacks) są realnym zagrożeniem, dlatego korzystanie z 5G i najnowszych standardów łączności znacząco podnosi poziom ochrony.

### Aplikacje

Instaluj aplikacje wyłącznie z oficjalnych sklepów (Google Play, Apple App Store). Kontroluj uprawnienia aplikacji i odinstalowuj te, które są nieużywane lub wykazują podejrzane zachowania (np. nadmierne zużycie transferu czy procesora).

### GPS i prywatność lokalizacji

Odbieraj uprawnienia do lokalizacji tym aplikacjom, które ich rzeczywiście potrzebują. Możliwość śledzenia lokalizacji to duże zagrożenie prywatności i bezpieczeństwa.

### Publiczne ładowarki i USB

Unikaj podłączania urządzeń do nieznanych publicznych ładowarek lub komputerów, które mogą być źródłem ataków typu juice jacking. Warto stosować specjalne kable blokujące transmisję danych (*USB data blockers*).

### Backup danych

Regularnie wykonuj kopie zapasowe najważniejszych danych w chmurze lub na zewnętrznych nośnikach. To zabezpieczenie przed skutkami awarii, kradzieży, zgubienia urządzenia czy ataku ransomware.

### Aktualizacje systemu i aplikacji

Utrzymuj system operacyjny oraz aplikacje w najnowszych wersjach, aby korzystać z załatania znanych luk bezpieczeństwa. Weryfikuj źródło aktualizacji, zwracając uwagę na podpisy cyfrowe, aby uniknąć ataków na łańcuch dostaw (*supply chain attacks*).



### Oryginalne oprogramowanie

Nie instaluj nieautoryzowanych wersji systemów ani nie rootuj urządzenia, gdyż takie praktyki narażają na instalację złośliwego oprogramowania i utratę gwarancji bezpieczeństwa.

### Wymiana urządzenia

Przed sprzedażą lub przekazaniem urządzenia wykonaj pełne wyczyszczenie danych i przywróć ustawienia fabryczne, aby chronić swoje prywatne informacje.

### Edukacja użytkowników

Bezpieczeństwo to proces ciągły – śledzenie aktualności, korzystanie z wiarygodnych źródeł takich jak Niebezpiecznik.pl, Zaufana Trzecia Strona czy Instytut Kościuszki, a także regularne szkolenia i symulacje phishingowe w organizacjach, znacząco podnoszą poziom cyberodporności.

### Strategia ochrony danych i polityka bezpieczeństwa w firmach

Firmy i instytucje publiczne powinny mieć jasno określone polityki korzystania z urządzeń mobilnych, w tym regulacje dotyczące urządzeń prywatnych pracowników (BYOD) i procedury zabezpieczania danych wrażliwych.

# Tomasz Chomicki

Dyrektor ds. rozwoju biznesu
w Samsung Electronics Polska

Cyberbezpieczeństwo to dziś jedno z kluczowych wyzwań nie tylko dla takich firm jak Samsung, ale także dla struktur państwowych i całego społeczeństwa. Polska, jako dynamicznie rozwijający się rynek cyfrowy, stoi przed ogromnym wyzwaniem zbudowania spójnego, odpornego na zagrożenia systemu. To zadanie wymaga współpracy i to na zupełnie nowym poziomie.

Ze środowiskiem naukowym staramy się dzielić wiedzą praktyczną, ponieważ to praktycy dziś najczęściej definiują kierunki rozwoju technologii bezpieczeństwa. Młodzi ludzie – studenci i doktoranci – powinni mieć dostęp do tej wiedzy w sposób przystępny, zrozumiały i inspirujący. Tylko w ten sposób zwiększymy świadomość zagrożeń i wykształcimy nowe pokolenie ekspertów, które będzie realnym wsparciem dla instytucji publicznych i prywatnych.

Współpraca z biznesem to z kolei szansa na budowanie praktycznych kompetencji: umiejętności tworzenia polityki bezpieczeństwa, stosowania silnych haseł, czy systematycznej aktualizacji urządzeń i oprogramowania. To działania podstawowe, a jednak często pomijane. Dlatego tak ważne jest, aby firmy aktywnie inwestowały w edukację swoich pracowników i klientów.

Szczególnie ważnym obszarem staje się dziś implementacja nowych technologii – zwłaszcza metod płatności mobilnych. Korzystając z telefonu czy smartwatcha, coraz częściej przekazujemy dane o swojej lokalizacji, zwyczajach zakupowych, a nawet dane medyczne czy finansowe. I tu kluczowe jest pytanie: kto jest producentem technologii, z której korzystamy? Jakie dane przekazujemy – i komu? Jeśli nie jesteśmy w stanie tego zweryfikować, narażamy się na bardzo poważne ryzyko. Informacja o tym, gdzie płacimy, komu, w jakiej kwocie, a nawet czy jesteśmy chorzy, to dane o wyjątkowo wysokiej wartości – zarówno dla legalnych, jak i nielegalnych podmiotów. Nieświadome udostępnianie ich nieautoryzowanym dostawcom to dziś jedna z najczęstszych walut na nielegalnym rynku danych. Dlatego tak ważne jest, aby korzystać wyłącznie z autoryzowanych, zweryfikowanych technologii – i edukować użytkowników, że prywatność to nie abstrakcja, tylko realna wartość.

Stąd też wielkie wspólne zadanie jakim jest podnoszenie świadomości o cyberzagrożeniach – od edukacji wczesnoszkolnej, przez młodzież, aż po seniorów. Kampanie społeczne muszą być dostosowane do specyfiki i potrzeb różnych grup odbiorców, aby przekaz był skuteczny i zrozumiały. To zadanie powinni angażować się wszyscy aktywni gracze na rynku cyfrowym – od firm technologicznych, przez instytucje publiczne, po organizacje pozarządowe, bo tylko wspólne działanie pozwoli nam budować prawdziwą cyberodporność.

# Katarzyna Chojecka

Head of Government Affairs
CEE w Cisco

Według danych Cisco zawartych w niedawno opublikowanym raporcie „Cybersecurity Readiness Index 2025”, zaledwie 3% organizacji w Polsce osiągnęło w pełni dojrzały poziom cybergotowości, co jest wynikiem zbliżonym do globalnej średniej (4%). To pokazuje, że pomimo rosnącej świadomości, realna odporność na cyberzagrożenia pozostaje niska.

W ciągu ostatniego roku ponad połowa polskich organizacji (52%) padła ofiarą cyberataków, a ich zdolność do obrony była ograniczona poprzez skomplikowane i niespójne systemy zabezpieczeń. W przyszłość respondenci również patrzą z niepokojem - 65% firm w Polsce spodziewa się w ciągu najbliższych 12-24 miesięcy zakłóceń w swojej działalności spowodowanych cyberatakami, co podkreśla pilną potrzebę wdrożenia uproszczonych strategii obronnych przeciwko zagrożeniom zewnętrznym.

Rozwój sztucznej inteligencji, choć oferuje nowe możliwości obrony, jednocześnie znacząco komplikuje krajobraz zagrożeń. Aż 86% polskich firm doświadczyło incydentów związanych z AI w ostatnim roku. Szczególnym wyzwaniem jest zjawisko Shadow AI. 26% pracowników w Polsce ma nieograniczony dostęp do publicznych narzędzi GenAI, a aż 63% organizacji nie jest pewnych, czy potrafi wykryć nieautoryzowane wdrożenia AI, co stwarza poważne luki bezpieczeństwa.



Dodatkowo, w modelu pracy hybrydowej 88% polskich organizacji doświadcza większych zagrożeń z powodu dostępu do firmowej sieci z niezarządzanych urządzeń. Do tego dochodzi chroniczny niedobór wykwalifikowanych specjalistów ds. cyberbezpieczeństwa, wskazywany przez 79% polskich respondentów. Aż 57% firm ma wakaty na ponad dziesięciu procentach stanowisk.

W obliczu tych wyzwań, polskie firmy muszą pilnie zredefiniować swoje strategie. Kluczowe jest inwestowanie w rozwiązania napędzane AI, uproszczenie środowisk bezpieczeństwa, zwiększenie świadomości pracowników oraz priorytetowe traktowanie AI w wykrywaniu i reagowaniu na zagrożenia. Tylko kompleksowe podejście, obejmujące również zarządzanie ryzykiem związanym z niezarządzanymi urządzeniami i Shadow AI, pozwoli zbudować cyberodporność niezbędną w erze AI.

Cisco, jako globalny lider w dziedzinie sieci i cyberbezpieczeństwa, pomaga klientom w realizacji ich strategii cyberodporności. Opiera się ona na ochronie tożsamości z uwierzytelnianiem bezhasłowym/wieloskładnikowym, weryfikacji dostępu zgodnie z zasadami Zero Trust, zapewnieniu odporności i gotowości sieci na erę sztucznej inteligencji oraz kompleksowym zabezpieczenie samej sztucznej inteligencji – zarówno technologii i modeli, jak i sposobu jej wykorzystania przez pracowników. Takie podejście pozwala na budowanie holistycznej i przyszłościowej obrony cyfrowej, odpowiadającej na współczesne wyzwania.

# Artur Miękina

Director of Sales And Business Development w Asseco Data Systems

Dostosowanie się do nowej regulacji NIS 2 to z jednej strony spore inwestycje infrastrukturalne czy osobowe, z drugiej zaś - unifikacja standardów w zakresie cyberbezpieczeństwa w UE. Ułatwi to współpracę między podmiotami transgranicznymi, ale bez wątpienia, zwiększy odporność cyfrową na cyberzagrożenia.

Warto w tym miejscu wskazać, że kwalifikowane usługi zaufania mogą stanowić ważny element pod kątem ich wykorzystania w zakresie uzyskania zgodności z NIS 2 przez podmioty z sektorów objętych dyrektywą. Na korzyści z outsourcingu zabezpieczeń wymaganych przez NIS 2 do kwalifikowanych dostawców usług zaufania wprost wskazuje fragment artykułu 24 tej regulacji: „...państwa członkowskie zachęcają podmioty kluczowe i ważne do korzystania z kwalifikowanych usług zaufania".

Przyjrzyjmy się zatem kilku elementom z NIS 2, w których kwalifikowane usługi zaufania mogą być pomocne.

- Ochrona integralności i autentyczności danych. Wymóg integralności danych mogą w znakomity sposób zaadresować kwalifikowane podpisy elektroniczne i pieczęci elektroniczne, których zastosowanie wprost zapewnia autentyczność (źródło pochodzenia) i integralność danych, co jest kluczowe w sektorach objętych NIS 2.



- Bezpieczne przysyłanie danych. Kwalifikowana usługa doręczania elektronicznego gwarantuje poufność i integralność przesyłanych danych, przez co wpisuje się w wymagania NIS 2 w zakresie bezpiecznej informacji wymienianej między poszczególnymi podmiotami.
- Zgodność z wymogami prawa. Kwalifikowane usługi zaufania są już zgodne z przepisami UE, co pozwala podmiotom objętym NIS 2 uniknąć konieczności opracowywania własnych rozwiązań.
- Interoperacyjność w UE. Interoperacyjne usługi zaufania wspierają wymianę danych między państwami i organizacjami w ramach UE, co jest kluczowe dla efektywnej koordynacji działań w przedsiębiorstwach realizujących działalność transgranicznie.

Podsumowując, kwalifikowane usługi zaufania stanowią solidny fundament funkcjonalny i technologiczny dla realizacji wielu wymogów NIS 2, a ich umiejętne zastosowanie minimalizuje ryzyko cyberzagrożeń i ułatwia podmiotom spełnienie obowiązków z niej wynikających. Dyrektywa stanowi istotny krok w kierunku zwiększenia poziomu cyberbezpieczeństwa w Unii Europejskiej, w tym w sektorze kwalifikowanych usług zaufania. Choć wiąże się z licznymi wyzwaniami, jej wdrożenie może przyczynić się do zwiększenia zaufania do usług cyfrowych oraz poprawy odporności na zagrożenia cybernetyczne.

# Tomasz Omelaniuk

Presales Technical Consultant /
Security SME w HP Inc Polska

Dokument „Mapa drogowa polskiej cyberodporności” jest niezwykle trafnym i aktualnym opracowaniem, które doskonale odzwierciedla wyzwania, z jakimi mierzymy się na co dzień w obszarze cyberbezpieczeństwa. Jako osoba zajmująca się również tematyką „cyber*”, mogę potwierdzić, że obserwacje przedstawione w dokumencie są zgodne z naszymi doświadczeniami zarówno na poziomie globalnym, jak i lokalnym.

Polska, podobnie jak wiele innych krajów, stoi w obliczu rosnącej liczby i złożoności cyberzagrożeń. Wzrost liczby incydentów, takich jak phishing czy ataki ransomware, jest zauważalny nie tylko w Polsce, ale również na całym świecie. W tym kontekście Polska nie jest wyjątkiem, a wręcz przeciwnie – stanowi ważny element globalnej układanki cyberbezpieczeństwa.

Dlatego też tak ważnym elementem naszej codzienności jest nie tylko świadomość potencjalnych zagrożeń, ale przede wszystkim korzystanie z urządzeń i rozwiązań, które pomogą nam zachować odpowiedni poziom naszej codziennej cyberhigieny. Które w przypadku napotkania zagrożenia, będą w stanie je wykryć, odpowiednio zareagować np. poprzez ich skuteczną izolację w bezpiecznym środowisku, a w przypadku uszkodzenia np. systemu operacyjnego, będą pozwalały na szybkie i łatwe jego przywrócenie, aby móc zachować ciągłość pracy naszej organizacji.



Jako firma HP, od wielu lat rozwijamy nasze urządzenia oraz rozwiązania ze szczególną uwagą skierowaną na kwestie bezpieczeństwa właśnie. Z generacji na generację nasze komputery, ale również całe pozostałe portfolio uzupełniane jest o kolejne właściwości oraz funkcje, pozwalające naszym użytkownikom pracować nie tylko wydajnie, ale przede wszystkim bezpiecznie w każdej chwili. Nieważne, czy aktualnie surfują po sieci bądź odpowiadają na maile, będąc w domu, kawiarni czy pociągu – pracując na sprzęcie HP mogą mieć pewność, że nasza technologia zrobi wszystko co tylko możliwe, aby ochronić ich dane, sprzęt oraz też samą organizację.

Niezwykle istotne w dokumencie jest również podkreślenie potrzeby harmonizacji przepisów dotyczących cyberbezpieczeństwa na poziomie UE oraz usprawnienia procesów legislacyjnych i modernizacji ram regulacyjnych. Wprowadzenie europejskich i lokalnych polskich regulacji, które uporządkują pewne obszary w zakresie cyberochrony od strony procesowej, jest niezbędne do skutecznego przeciwdziałania zagrożeniom. Takie podejście wymusza na firmach wdrożenie odpowiednich środków ochrony, co w dłuższej perspektywie przyczyni się do zwiększenia ogólnego poziomu bezpieczeństwa cyfrowego.

Warto również zwrócić uwagę na znaczenie współpracy między sektorem publicznym a prywatnym oraz na konieczność systematycznych szkoleń dla pracowników w zakresie cyberbezpieczeństwa. Tylko poprzez wspólne działania i ciągłe podnoszenie świadomości możemy skutecznie stawić czoła wyzwaniom, jakie niesie ze sobą dynamicznie rozwijający się krajobraz cyberzagrożeń.

Podsumowując, dokument ten jest cennym narzędziem, które może przyczynić się do wzmocnienia cyberodporności Polski i stanowi ważny krok w kierunku budowy bezpiecznego środowiska cyfrowego.

# Tomasz Olejnik

Dyrektor Sektora Publicznego
w Europie Środkowo-Wschodniej
w Amazon Web Services

Tempo cyfrowej transformacji w Polsce jest bezprecedensowe – nasze badania pokazują, że co dwie minuty kolejna polska firma zaczyna korzystać z AI. To imponujące tempo adopcji nowych technologii, które przekłada się na ponad 740 000 polskich przedsiębiorstw aktywnie wykorzystujących sztuczną inteligencję. Jako AWS, z perspektywy globalnego doświadczenia w zabezpieczaniu krytycznej infrastruktury cyfrowej, dostrzegamy zarówno ogromny potencjał, jak i wyzwania związane z tym gwałtownym wzrostem.

Nasze doświadczenia z Ukrainy, gdzie w krytycznym momencie pomogliśmy zabezpieczyć ponad 15 petabajtów kluczowych danych państwowych - od rejestrów rządowych po dokumentację bankową - pokazują, jak istotna jest budowa cyfrowej odporności na poziomie państwowym. Dla zobrazowania skali: gdybyśmy chcieli zapisać te dane na standardowych płytach DVD, stos sięgałby blisko połowy wysokości Mount Everestu. To doświadczenie nauczyło nas, że prawdziwa cyberodporność wymaga kompleksowego podejścia, łączącego nowoczesne technologie z głębokim zrozumieniem specyfiki zagrożeń.

W kontekście polskiego rynku, gdzie adopcja AI wzrosła o 56% w ciągu roku (najszybciej w UE), kluczowe staje się budowanie odpornej infrastruktury, inteligentne skalowanie zabezpieczeń oraz bezpieczna implementacja GenAI. Nasze środowiska chmurowe muszą gwarantować nieprzerwaną dostępność i bezpieczeństwo, dlatego wykorzystujemy zaawansowane narzędzia AI, które analizują do 200 bilionów zapytań dziennie w jednym tylko regionie AWS, identyfikując średnio 182 000 złośliwych witryn. To podejście przynosi wymierne efekty - 44% polskich firm już dostrzega znaczącą poprawę cyberbezpieczeństwa dzięki AI, a 23% notuje wzrost produktywności w obszarze IT i cyberbezpieczeństwa.

Patrząc w przyszłość, widzimy, że do 2025 roku globalne wydatki na generatywną AI przewyższą nakłady na tradycyjne zabezpieczenia. To fundamentalna zmiana paradygmatu, która wymaga nowego podejścia do architektury bezpieczeństwa. W AWS wierzymy, że kluczem do sukcesu jest zunifikowany system monitorowania zagrożeń, proaktywna analiza zabezpieczeń sieciowych oraz rozszerzona detekcja zagrożeń obejmująca środowiska kontenerowe, gdzie coraz częściej rozwijane są rozwiązania AI.

Rządowa inicjatywa zainwestowania 1 mld złotych w rozwój AI to ważny krok w dobrym kierunku. Jednak prawdziwy sukces będzie zależał od umiejętności połączenia innowacji z solidnymi fundamentami bezpieczeństwa. Nasze doświadczenia z zabezpieczania krytycznej infrastruktury w sytuacjach kryzysowych pokazują, że technologia chmurowa i AI nie są tylko narzędziami modernizacji - są fundamentem budowania prawdziwej cyfrowej odporności państwa. W AWS jesteśmy przekonani, że przyszłość należy do organizacji i krajów, które potrafią zrównoważyć szybkie tempo adopcji AI z rygorystycznym podejściem do cyberbezpieczeństwa, tworząc ekosystem innowacji oparty na zaufaniu i bezpieczeństwie.

# Jakub Desperak

Solution Sales Specialist
w Lenovo Poland

Jako że bezpieczeństwo infrastruktury IT nie może być traktowane jako element wtórny, nowoczesne urządzenia tworzone są zgodnie z zasadą „Secure by Design". Model ten zakłada uwzględnianie wymagań bezpieczeństwa już od najwcześniejszych faz projektowania systemów, aplikacji i infrastruktury.

Kluczowe elementy tego podejścia to przede wszystkim minimalizacja powierzchni ataku, wdrażanie kontroli dostępu w oparciu o hierarchię uprawnień, szyfrowanie danych oraz implementacja wbudowanych mechanizmów wykrywania i reagowania na incydenty bezpieczeństwa. Takie podejście pozwala na budowanie systemów i urządzeń odpornych na ataki już od początkowych etapów ich powstawania, z uwzględnieniem walidacji autentyczności i bezpieczeństwa indywidualnych komponentów.

Ponadto, cykliczne aktualizowanie firmware'u i systemu operacyjnego urządzeń jest podstawowym, lecz często zaniedbywanym elementem ochrony organizacji przed zagrożeniami. Firmware, jako najbardziej zaufana warstwa oprogramowania, zarządza krytycznymi funkcjami sprzętu, a jego podatności mogą być wykorzystywane do ataków typu firmware rootkit czy firmware-level malware. Systematyczne aktualizacje eliminują znane luki bezpieczeństwa opatrzone m.in. sygnaturami CVE, zwiększają odporność systemu na nowe formy zagrożeń oraz zapewniają zgodność z bieżącymi standardami ochrony danych. Zaleca się więc stosowanie polityki automatycznego aktualizowania oraz ścisłego monitorowania integralności oprogramowania układowego na wszystkich platformach sprzętowych.

Najważniejszym czynnikiem wpływającym na bezpieczeństwo organizacji jest jednak świadomość użytkowników końcowych. Cyberbezpieczeństwo powinno być postrzegane jako kompetencja podstawowa, rozwijana na wszystkich poziomach organizacji. W praktyce oznacza to organizację cyklicznych szkoleń z zakresu bezpieczeństwa informacji, promowanie zasad bezpiecznego korzystania z internetu i urządzeń mobilnych, kształtowanie postawy sceptycznego podejścia do nieznanych wiadomości, załączników i linków, wspieranie kultury odpowiedzialności za ochronę danych oraz prowadzenie cyklicznych audytów poziomu bezpieczeństwa w organizacji. Wzrost kompetencji użytkowników to inwestycja, która minimalizuje ryzyko skutecznych ataków socjotechnicznych, takich jak phishing, będących jednym z najczęstszych i najskuteczniejszych wektorów ataków.

# Adam Grodecki

Head of Professional Services
Optical Networks, Nokia

Bezpieczna infrastruktura cyfrowa jest dziś nie tylko warunkiem sprawnego funkcjonowania państwa i gospodarki, ale także fundamentem suwerenności technologicznej Europy. Nie wystarczy już mówić o szybkim Internecie czy nowoczesnych usługach – kluczowe jest to, jak i na czym budujemy łączność. Infrastruktura sieciowa musi być od początku projektowana jako zaufana, odporna na zagrożenia i zdolna do adaptacji w kontekście dynamicznie zmieniających się ryzyk – w tym także tych, które przyniesie era komputerów kwantowych.

W Polsce mamy ogromny potencjał, aby znaleźć się w centrum europejskiej mapy bezpieczeństwa cyfrowego. Dysponujemy wysoko wykwalifikowaną kadrą inżynierską, nowoczesnym zapleczem badawczo-rozwojowym oraz – co niezwykle ważne – praktycznym doświadczeniem we wdrażaniu rozwiązań dla najbardziej wymagających sektorów: energetyki, transportu, infrastruktury krytycznej czy administracji publicznej. Dla takich właśnie potrzeb Nokia już dostarcza, oraz przede wszystkim projektuje i rozwija najnowsze technologie w naszych centrach R&D we Wrocławiu, Bydgoszczy i Krakowie, które już dziś wspierają bezpieczeństwo sieci nie tylko w Polsce, ale też na całym świecie – od platform wiertniczych, przez systemy łączności portów i lotnisk, po sieci telewizyjne i wojskowe.



Nie możemy jednak popaść w samozadowolenie z już osiągniętych sukcesów. W obliczu rosnącej liczby cyberataków, a także zbliżającego się przełomu w dziedzinie obliczeń kwantowych, musimy myśleć o cyberbezpieczeństwie przyszłości właśnie teraz, mimo że komputery kwantowe dopiero się rozwijają. Będą one w stanie złamać obecnie stosowane systemy szyfrowania, jeśli tylko zostaną one dzisiaj podsłuchane i przechowane wystarczająco długo. Dlatego właśnie Nokia rozwija i wdraża rozwiązania Quantum Safe, które integrują klasyczne oraz postkwantowe metody ochrony danych, bazując m.in. na kryptografii o wysokiej entropii i dystrybucji kluczy z wykorzystaniem fizyki kwantowej. Co ważne, wiele z tych bardzo nowoczesnych rozwiązań jest możliwe do szybkiego wdrożenia w sieciach transportowych IP oraz optycznych w Polsce, także dzięki temu, że Nokia jest dostawcą większej liczby takich sieci w naszym kraju.

Naszym wspólnym celem – firm, administracji i środowisk akademickich – powinno być nie tylko nadążanie za innymi, ale wyznaczanie kierunków. Potrzebujemy sprawnej legislacji, stabilnego klimatu inwestycyjnego oraz wspierania lokalnych ekosystemów innowacji. Polska ma realną szansę stać się europejskim liderem w zakresie bezpiecznych technologii sieciowych. Nokia już dzisiaj współtworzy wiele platform współpracy i wymiany doświadczeń, jak Program Współpracy Cyber w Ministerstwie Cyfryzacji, czy działania w Cyfrowej Polsce, dlatego zapraszamy do współpracy i budowania przyszłości, która jest już dziś w zasięgu naszych rąk.

# Źródła:


Financial Times – „Poland 'most attacked' online by Russia, says minister" Alice Hancock and Raphael Minder
*https://www.ft.com/content/e0e1a016-e4e0-4628-a0ac-c4a6e9d15db6

NASK – Raport grupy zadaniowej NATO-UE ds. odporności infrastruktury krytycznej
*https://cyberpolicy.nask.pl/raport-grupy-zadaniowej-nato-ue-ds-odpornosci-infrastruktury-krytycznej/

KPMG – Blisko 60% firm uważa, że AI zwiększy ryzyko cyberataków (2025)
*https://kpmg.com/pl/pl/home/media/press-releases/2025/02/media-press-blisko-60-procent-firm-uwaza-ze-technologia-ai-zwiekszy-ryzyko-cyberatakow.html

KPMG – Barometr Cyberbezpieczeństwa 2024
*https://kpmg.com/pl/pl/home/insights/2024/02/barometr-cyberbezpieczenstwa-2024.html

NASK – Partnerstwo dla Cyberbezpieczeństwa: liderzy gospodarki i instytucje
*https://nask.pl/aktualnosci/partnerstwo-dla-cyberbezpieczenstwa-liderzy-gospodarki-i-kluczowe-instytucje

NASK – Raport CERT Polska 2024: 300 incydentów dziennie
*https://nask.pl/aktualnosci/300-incydentow-dziennie-premiera-raportu-cert-polska-za-2024-rok

NASK – Wicepremier Gawkowski podczas SECURE 2024: „Jesteśmy w zimnej cyberwojnie"
*https://archiwum.nask.pl/pl/aktualnosci/5378%2CWicepremier-Gawkowski-podczas-SECURE-2024-Jestesmy-w-zimnej-cyberwojnie-nie-tylk.html

Interia Biznes – Polska najbardziej atakowanym państwem UE
*https://biznes.interia.pl/gospodarka/news-polska-najbardziej-atakowanym-panstwem-ue-co-dzien-dochodzi-,nId,7957866

Legislacja.gov.pl – Projekt ustawy dot. cyberbezpieczeństwa
*https://legislacja.gov.pl/projekt/12384504

NASK – Plany na 2024/2025 (zmiany w statucie i regulaminach)
*https://archiwum.nask.pl/pl/aktualnosci/5415%2CPlany-NASK-na-2024-i-2025-rok-Zmiany-w-statucie-Instytutu-i-w-regulaminach.html

NASK – Centrum Cyberbezpieczeństwa NASK
*https://nask.pl/projekty/centrum-cyberbezpieczenstwa-nask

CERT Polska – Raport roczny 2024
*https://cert.pl/posts/2025/04/raport-roczny-2024/

CyberDefence24 – Statystyki NASK (200 tys. zgłoszeń, 86 tys. SMS phishingowych)
*https://cyberdefence24.pl/cyberbezpieczenstwo/200-tys-zgloszen-86-tys-sms-ow-phishingowych-mamy-statystyki-nask

mSerwis – 21 ciekawych statystyk phishingowych (2024)
*https://www.mserwis.pl/blog/21-ciekawych-statystyk-dotyczacych-phishingu-ktore-warto-znac-w-2024-roku/

SCdn Kielce – Raport „Dezinformacja oczami Polaków 2024"
*https://samorzad.gov.pl/web/scdn-kielce/dezinformacja-oczami-polakow-2024

Najwyższa Izba Kontroli – Cyberbezpieczeństwo w samorządach (2025)
*https://www.nik.gov.pl/aktualnosci/bezpieczenstwo/cyberbezpieczenstwo-w-samorzadach-2025.html

Bankier.pl – Cyberprzestępczość kosztuje więcej niż większość gospodarek
*https://www.bankier.pl/wiadomosc/Cyberprzestepczosc-kosztuje-wiecej-niz-wiekszosc-gospodarek-8925125.html

Microsoft – Digital Defense Report (Polska jednym z 3 najbardziej zagrożonych państw w Europie)
*https://news.microsoft.com/pl-pl/2024/11/22/microsoft-digital-defense-report-polska-jednym-z-trzech-najbardziej-zagrozonych-panstw-w-europie/

EY – Cyfrowa transformacja 2024 (AI, FY24)
*https://www.ey.com/pl_pl/newsroom/2024/06/ey_ip_cyfrowa_transformacja_2024-ai-fy24

EY – Cyfrowa transformacja polskich firm (2024)
*https://www.ey.com/pl_pl/newsroom/2024/07/ey-cyfrowa-transformacja-polskie-firmy

EY – Cyber-Exe Polska 2024 (strona)
*https://www.ey.com/pl_pl/insights/cybersecurity/cyber-exe-polska-2024

EY – Raport Cyber-Exe Polska 2024 (PDF)
*https://www.ey.com/content/dam/ey-unified-site/ey-com/pl-pl/insights/consulting/documents/ey-raport-cyber-exe-polska-2024.pdf

CBOS – Raport „Bezpieczeństwo i cyberzagrożenia" (2024)
*https://www.cbos.pl/SPISKOM.POL/2024/K_070_24.PDF

Komisja Europejska – Dyrektywa NIS2
*https://digital-strategy.ec.europa.eu/pl/policies/nis2-directive

Komisja Europejska – Apel o pełną transpozycję NIS2 (2024)
*https://digital-strategy.ec.europa.eu/pl/news/commission-calls-19-member-states-fully-transpose-nis2-directive

KNF – Rozporządzenie DORA
*https://www.knf.gov.pl/dla_rynku/dora

Infor.pl – Przewodnik: Rozporządzenie DORA
*https://www.infor.pl/prawo/nowosci-prawne/6899931,rozporzadzenie-dora-co-to-jest-i-kogo-dotyczy-przewodnik.html

Eur-Lex – Making critical entities more resilient (CER Directive)
*https://eur-lex.europa.eu/PL/legal-content/summary/making-critical-entities-more-resilient.html

Gov.pl – Akt o AI (rewolucja w regulacji)
*https://www.gov.pl/web/ai/rewolucja-w-regulacji-wchodzi-w-zycie-akt-o-ai

PFR Startup – AI Act: bezpieczeństwo i etyka w AI
*https://startup.pfr.pl/artykul/ai-act-bezpieczenstwo-i-etyka-w-ai-przewodnik-po-zasadach-bezpieczenstwa-i-etyki-w
PFR Startup – AI Act: nowe wyzwania i obowiązki dla startupów
*https://startup.pfr.pl/artykul/ai-act-nowe-wyzwania-i-obowiazki-dla-startupow-technologicznych

Komisja Europejska – Cyber Resilience Act
*https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

CyberResilienceAct.eu – Wyjaśnienie CRA
*https://www.cyberresilienceact.eu/the-cra-explained/

Komisja Europejska – Cyber Resilience Act (komunikat prasowy)
*https://ec.europa.eu/newsroom/cipr/items/713799/en

Reuters – UE rezygnuje z wymogu suwerenności w schemacie certyfikacji cyberbezpieczeństwa (2024)
*https://www.reuters.com/technology/eu-drops-sovereignty-requirements-cybersecurity-certification-scheme-document-2024-04-03/

Gov.pl – Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC)
*https://www.gov.pl/web/cyfryzacja/ustawa-o-krajowym-systemie-cyberbezpieczenstwa-weszla-w-zycie

PARP – Krajowy System Cyberbezpieczeństwa: zmiany i wpływ na rynek ICT
*https://www.parp.gov.pl/component/content/article/88231%3Akrajowy-system-cyberbezpieczenstwa-zmiany-w-funkcjonowaniu-i-ich-wplyw-na-rynek-ict-2

Prawo.pl – Nowe standardy KSC
*https://www.prawo.pl/biznes/krajowy-system-cyberbezpieczenstwa-nowe-standardy%2C531257.html

Gov.pl – Ramy prawne dla certyfikacji cyberbezpieczeństwa (projekt ustawy MC)
*https://www.gov.pl/web/cyfryzacja/ramy-prawne-dla-certyfikacji-cyberbezpieczenstwa---projekt-ustawy-ministerstwa-cyfryzacji

CyberDefence24 – System certyfikacji cyberbezpieczeństwa (projekt rządowy)
*https://cyberdefence24.pl/cyberbezpieczenstwo/system-certyfikacji-cyberbezpieczenstwa-rzad-przyjal-projekt

Gov.pl – Zasady ubiegania się o środki z Funduszu Cyberbezpieczeństwa
*https://www.gov.pl/web/baza-wiedzy/przypominamy-zasady-ubiegania-sie-o-srodki-z-funduszu-cyberbezpieczenstwa

Gov.pl – Więcej pieniędzy na Fundusz Cyberbezpieczeństwa
*https://www.gov.pl/web/cyfryzacja/wiecej-pieniedzy-na-fundusz-cyberbezpieczenstwa

Gov.pl – 350 mln zł na wzmocnienie cyberbezpieczeństwa administracji
*https://www.gov.pl/web/cyfryzacja/350-mln-zl-na-wzmocnienie-cyberbezpieczenstwa-administracji-rzadowej

Gov.pl – Program „Cyberbezpieczny Samorząd 2"
*https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad2

Gov.pl – Samorządy zwiększają swoją cyberodporność
*https://www.gov.pl/web/cyfryzacja/samorzady-zwiekszaja-swoja-cyberodpornosc

Gov.pl – 1,5 mld zł dla samorządów na cyberbezpieczeństwo
*https://www.gov.pl/web/cyfryzacja/15-mld-zl-dla-samorzadow-na-cyberbezpieczenstwo

Raport został przygotowany przez ekspertów **Związku Cyfrowa Polska**, z wiodącą rolą **Michała Kanownika** – Prezesa Zarządu Związku Cyfrowa Polska, z udziałem:
**Katarzyny Chojeckiej** - Head of Government Affairs CEE w Cisco;
**Tomasza Chomickiego** - Dyrektora ds. rozwoju biznesu w Samsung Electronics Polska;
**Artura Miękiny** - Director of Sales And Business Development w Asseco Data Systems;
**Tomasza Omelaniuka** - Presales Technical Consultant / Security SME w HP Inc Polska;
**Tomasza Olejnika** - Dyrektora Sektora Publicznego w Europie Środkowo-Wschodniej w Amazon Web Services;
**Jakuba Desperaka** - Solution Sales Specialist w Lenovo Polska;
**Adama Grodeckiego** – Head of Professional Services Optical Networks w Nokii.

www.cyfrowapolska.org