



wnp • economic trends

raport

Cyberodporność. Wersja polska



Szanowni Państwo,

cyberbezpieczeństwo odgrywa coraz ważniejszą rolę w wielu dziedzinach; decyduje o bezpieczeństwie i odporności struktur państwa, o jakości naszego życia, konkurencyjności gospodarek. Co ważne: debata o cyberbezpieczeństwie przestała być rozmową wyłącznie o technologiach i systemach IT. Jej miejsce jest dziś na salonach wielkiej polityki, w strategicznych panelach wielkich korporacji i w biurach małych firm, na uczelniach, w urzędach i szpitalach, a także wśród tych, którzy na co dzień korzystają z technologii w cybersferze – czyli... nas wszystkich.

Jako ludzie mediów i dialogu - wydawcy i organizatorzy publicznej debaty o gospodarce - wiemy, jak istotne dla demokracji, dla rozwoju, dla wolności słowa jest cyberbezpieczeństwo i odporność na cyfrową agresję, na tworzone z użyciem technologii kłamstwo i programowane oszustwo. Potrzeba skutecznej walki z tymi narastającymi zagrożeniami staje się jednym z głównych wyzwań współczesności.

Technologia to niezbędne narzędzie cyfrowej samoobrony. Ale jej skuteczność zależy od ludzi – ich wiedzy, wyobraźni i odpowiedzialności, umiejętności współdziałania. A ten kluczowy dla cyfrowego bezpieczeństwa „ludzki czynnik” wymaga dialogu różnych środowisk, zaufania opartego na normach i procedurach, woli dzielenia się doświadczeniem z różnych dziedzin.

Raport, który prezentujemy, to plon pracy publicystów portalu WNP i redakcji WNP Economic Trends: całościowa i aktualna analiza stanu rzeczy, systemu, potrzeb, barier – pożytkująca wiarygodne źródła, wiedzę ekspertów, dająca głos biznesowi i administracji. Wykorzystaliśmy w nim także uwagi, opinie i rekomendacyjne wskazania formułowane w czasie czerwcowego CYBERSEC EXPO & FORUM. Publikacja i wydarzenie tworzą całość – to nasz wkład w dialog służący wspólnemu bezpieczeństwu w cyfrowym świecie.

WOJCIECH KUŚPIAK,
PREZES GRUPY PTWP,

INICJATOR EUROPEJSKIEGO KONGRESU GOSPODARCZEGO

Spis treści

ROZDZIAŁ 1.

Cyberagresorzy i cyberbrońcy. Coraz zacieklejsze starcie

Przestrzeń cyfrowa to dziś jeden z kluczowych obszarów rywalizacji gospodarczej, politycznej i technologicznej 4

ROZDZIAŁ 2.

Imperatyw państwa, szansa dla rynku

Złożona i intensywna odpowiedź państwa na rosnącą skalę cyberzagrożeń to konieczność. Kluczowa będzie realizacja 12

ROZDZIAŁ 3.

Kluczowy punkt. Cyberbezpieczeństwo w strategii przedsiębiorstw

Dbłość o cyberbezpieczeństwo stała się integralną częścią zarządzania strategicznego 21

ROZDZIAŁ 4.

Gospodarka i firmy. Cyfrowe ryzyko, realne straty

Budowanie cyberodporności – firm, sektorów, infrastruktury – to nie sprint, lecz maraton 30

ROZDZIAŁ 5.

Do zadań cyfrowych. Niewidzialni wojownicy

Polska zbudowała jeden z najbardziej zaawansowanych komponentów cyberobrony w NATO 40

ROZDZIAŁ 6.

Zagrożeni pacjenci. Cyberataki w ochronie zdrowia

Od prawidłowego funkcjonowania sektora ochrony zdrowia – zależy zdrowie i życie obywateli 45

•

Po CYBERSEC EXPO & FORUM.

Bezpieczeństwo zależy od nas 50

•

Wnioski i rekomendacje 51

Cyberagresorzy i cyberbrońcy. Coraz zacieklejsze starcie

Przestrzeń cyfrowa to dziś jeden z kluczowych obszarów rywalizacji gospodarczej, politycznej i technologicznej. Widać wyraźną eskalację w liczbie cyberprzestępczych ataków, ich złożoności i skali skutków.

Czego dowiesz się z tego rozdziału?

- W jakim tempie rośnie skala cyberprzestępstw – na globie i w Polsce?
- Jakie kategorie przestępstw, nielegalnych technik i narzędzi dominują i co nas czeka na tym polu w przyszłości?
- Hakerzy – amatorzy i zawodowcy. W jaki sposób przejawia się profesjonalizacja w świecie zorganizowanej cyberagresji?
- Co można rzec o rozwoju polskiego systemu cyberobrony – i czy powinno nas to uspokajać?
- Państwa w roli cybernajeźdźców. Czy w Polsce jesteśmy bezpieczni?

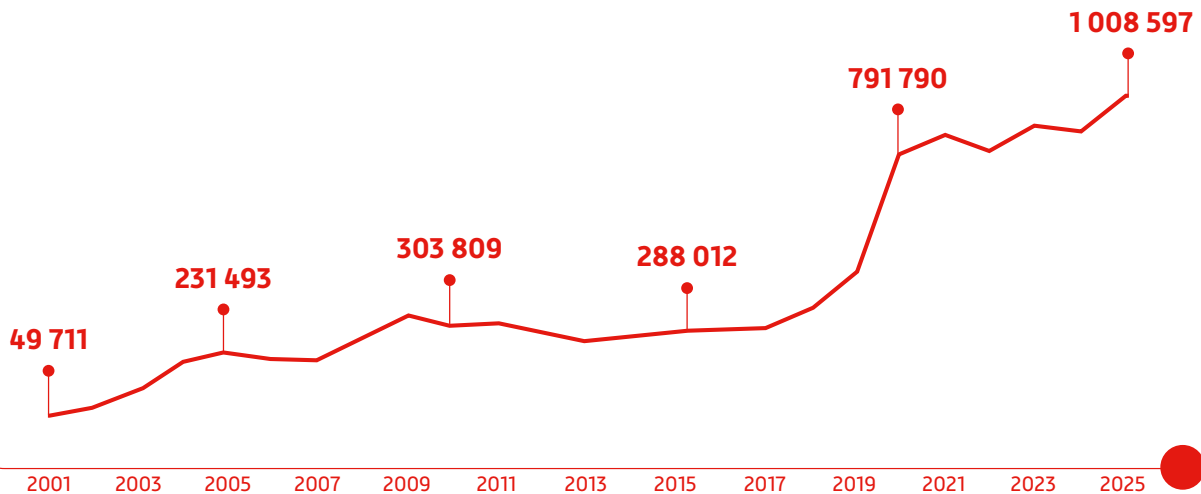
Współczesne modele działania cyberprzestępców opierają się na wysokim poziomie organizacji, sieciach współpracy oraz wykorzystaniu zaawansowanych narzędzi, w tym sztucznej inteligencji (AI).

Środowisko podwyższonego ryzyka wymaga nie tylko reaktywnego podejścia, ale przede wszystkim strategicznego rozumienia zagrożeń oraz skutecznego zarządzania ryzykiem. Cyberbezpieczeństwo zaczyna odgrywać strategiczną rolę w zapewnieniu ciągłości działania państw, instytucji publicznych, organizacji i firm.

Zarys globalnych zagrożeń

Z raportu FBI za 2025 rok wynika, że ośrodek Internet Crime Complaint Center (IC3) przyjmował średnio dziennie niemal 3 tys. zgłoszeń oszustw, a straty ofiar w zeszłym roku przekroczyły 20 mld dol. Najczęściej

USA. Liczba skarg złożonych w IC3.gov* w latach 2001-2025



*Internet Crime Complaint Center (FBI)

Źródło: Federalne Biuro Śledcze, Raport o przestępczości internetowej 2025

dochodziło do phishingu/spoofingu, oszustw inwestycyjnych (tu ofiary straciły ponad 8 mld dol.) i wycieków danych.

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA – European Network and Information Security Agency) w ostatnim raporcie (ENISA Threat Landscape 2025) podaje, że od 1 lipca 2024 r. do 30 czerwca 2025 r. zidentyfikowała 4875 incydentów. Najczęściej atakowane były administracja publiczna (38,2 proc. ataków), transport, infrastruktura i usługi cyfrowe, finanse i przemysł.

Dominowały ataki hakywistów: DDoS-y (atak typu rozproszona odmowa usługi) na strony internetowe organizacji w państwach członkowskich UE – ale tylko 2 proc. z tych incydentów prowadziło do zakłócenia w świadczeniu usług. Najpoważniejszym zagrożeniem są tu ataki ransomware (dzieło grup cyberprzestępczych) dla okupu – z pomocą złośliwego oprogramowania szyfrującego dane.

Dominującą techniką w sposobie inicjacji incydentu pozostawały taktiki oparte na inżynierii społecznej: w 60 proc. przypadków chodziło o phishing oraz wykorzystanie luk w zabezpieczeniach (21,3 proc.).

Najbardziej aktywna w UE była grupa No-Name057(16), odpowiedzialna za 60 proc. raportowanych incydentów (motywacje: głównie kwestie ideologiczne lub wydarzenia geopolityczne).

To właśnie sprawy ideologiczne motywowały hakywistów do ataków DDoS, a podbudki finansowe kierowały przede wszystkim cyberprzestępcami (13,4 proc. wszystkich incydentów). Kampanie cyberspiegostwa stanowiły 7,2 proc. przypadków.

Intensyfikacja w osaczeniu

Wicepremier i minister cyfryzacji Krzysztof Gawkowski wielokrotnie podkreślał, że Polska jest „najbardziej atakowanym krajem w Unii Europejskiej” oraz że na cyberbezpieczeństwo „wydajemy najwięcej w historii”. A w czasie tegorocznego XVIII Europejskiego Kongresu Gospodarczego wskazał na konieczność wsparcia dla samorządów, infrastruktury krytycznej, administracji oraz wzmocnienia kompetencji cyfrowych społeczeństwa.

Z raportu Pełnomocnika Rządu ds. Cyberbezpieczeństwa wynika, że CSIRT-y poziomu krajowego (CSIRT MON, CSIRT NASK, CSIRT GOV) w 2025 r. otrzymały 682 245 zgłoszeń i obsłużyły 272 941 realnych incydentów (wzrost o 144 proc. rdr). Najwięcej incydentów obsłużył CSIRT NASK – 260 783 (wzrost o 152 proc.), CSIRT MON – 7125 incydentów (przyrost o niemal 69 proc.), a CSIRT GOV – 5033 (plus 26,1 proc.).

Według raportu rocznego CERT Polska najpoważniejszą skalę incydentów z punktu widzenia Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego



Krzysztof Gawkowski wicepremier i minister cyfryzacji

– Świadomość dotycząca cyberbezpieczeństwa musi być rozbudowywana. Dzisiaj na cyfrowej wojnie – a Polska na takiej jest – nie ma cywilów. Każdy z nas, klikając w link, który dostanie, może być tym słabym ogniwem. Bądźmy czujni! (...) Odpowiedzialność za cyfrowy świat dotyczy również suwerenności technologicznej – bez niej nie ma dobrego, mocnego cyberbezpieczeństwa państwa. Ona musi się odbywać na poziomie strategicznym (z wypowiedzi na Europejskim Kongresie Gospodarczym, kwiecień 2026).

NASK stanowiły oszustwa komputerowe, jak np. phishing czy oszustwa inwestycyjne (aż 97 proc. całości). Dodatkowo na Listę Ostrzeżeń wpisano 250 tys. pozycji (przyrost o 166 proc. rdr), czyli dziennie identyfikowano średnio ok. 670 podejrzanych stron.

W ub.r. udaremniono też 140 mln prób wejścia na niebezpieczne strony, a 80 tys. SMS-ów uznano za szkodliwe (z puli 350 tys. wiadomości SMS przekazanych do analizy). CERT Polska opracował także 790 wzorców fałszywych wiadomości SMS-owych, wykorzystywanych w kampaniach smishingowych. Na tej podstawie zablokowano dostarczenie blisko 1,88 mln złośliwych wiadomości SMS (27 proc. więcej niż rok wcześniej).

Co stanowi z punktu widzenia Polski największe zagrożenie w cyberprzestrzeni? Według firmy ESET w I połowie 2025 r. nasz kraj był światowym liderem w liczbie wykrytych ataków ransomware (6 proc. globalnych incydentów); wyprzedziliśmy tu nawet USA. Inne obserwacje? Spadła wartość okupów płaconych grupom cyberprzestępczym, zwiększyła się też skala ich detekcji.

Eksperti Check Point Research w danych dla „Rzeczypospolitej” wskazali, że polski sektor administracji i instytucji publicznych mierzy się z niemal 3 tys. prób tygodniowo, sektor finansów – z 1795, a energetyczny i użyteczności publicznej – z ponad 1660. Jesteśmy w czołówce – obok Włoch i Hiszpanii. Nasz kraj pozostaje na celowniku takich grup cyberprzestępczych APT (ang. Advanced Persistent Threat – wysoce wyspecjalizowane zespoły cyberprzestępcze), jak APT44 (Sandworm), APT28 (Fancy Bear), APT29 (Cozy Bear).

Warto przypomnieć, że Polska była przedmiotem „szczególnego zainteresowania” cyberprzestępców, kiedy 29 grudnia ub.r. doszło do skoordynowanych ataków na sektor energetyczny. Specjaliści z CERT Polska informują, że staliśmy się wtedy celem jednego aktora (agresora) znanego jako „Static Tundra” (Cisco), „Berserk Bear” (CrowdStrike), „Ghost Blizzard” (Microsoft) oraz „Dragonfly” (Symantec).

Reperkusje cyberagresji

Z danych Centralnego Biura Zwalczania Cyberprzestępczości (CBZC) wynika, że tylko w 2025 r. przedstawiono zarzuty karne 1374



Źródło: Związek Banków Polskich oraz Biuro Informacji Kredytowej

podejrzanych, zatrzymano 1177 osób, a 417 tymczasowo aresztowano. Odzyskano też mienie o wartości 24,9 mln zł, zabezpieczono o wartości 80,8 mln zł; straty pokrzywdzonych sięgnęły 537 mln zł.

Cyberpolicja w ramach postępowań przygotowawczych miała najczęściej do czynienia z oszustwami internetowymi



Radosław Nielek

dyrektor NASK – Państwowego
Instytutu Badawczego

– Źródłem ryzyka staje się oprogramowanie, za którego podatność już po kilku latach nikt nie czuje się odpowiedzialny, nikt nie łąta luk, prowokując ryzyko. Ale to także kwestia uzależnienia od jednego dostawcy, który może skokowo podnieść cenę. (...) Moim marzeniem jest, byśmy byli w stanie stworzyć rozwiązanie, z którego będzie korzystać świat. To zrodziłoby wzajemną zależność, chroniącą na wypadek chęci wykluczenia nas czy pozbawienia dostępu do ważnych technologii.



Joanna Pawelek-Mendez

radca-minister ds. cyberbezpieczeństwa
w Departamencie Polityki
Bezpieczeństwa w Ministerstwie Spraw
Zagranicznych

– Zajmujemy się tym wymiarem cyberbezpieczeństwa, który odpowiada za polityczne nakładanie kosztów na tych, którzy w cyberprzestrzeni nas atakują, na naszych wrogów, oponentów. Pierwszym oficjalnym dokumentem, w którym pojawiła się nazwa cyberdyplomacja, jest Cyber Diplomacy Toolbox. To cyberdyplomatyczne instrumentarium, utworzone przez Unię Europejską, które służy temu, żeby właśnie nakładać koszty na oponentów i dbać o cyberbezpieczeństwo.



prof. Agnieszka Gryszczńska

członkini rady programowej
CYBERSEC Expo & Forum, dyrektor
Departamentu ds. Cyberprzestępczości
i Informatyzacji w Prokuraturze
Krajowej

– Mechanizm blokowania smishingowych SMS-ów realnie chroni najsłabszych. Część wiadomości w ogóle nie dociera do odbiorców, a jeśli dotrze, to dzięki wpisaniu złośliwej domeny na Listę Ostrzeżeń link prowadzi na planszę ostrzegawczą „Uwaga! Ta strona stanowi zagrożenie”, a nie na stronę przestępców. Zmieniłabym jednak dobrowolność stosowania tej listy na obowiązek dla wszystkich podmiotów dostarczających usługę dostępu do internetu.

(44 proc.), złośliwym oprogramowaniem (20 proc., w tym ransomware, ataki DDoS czy malware); 3 proc. stanowiły fałszywe alarmy, a 8 proc. – inne sprawy.

Izabela Albrycht, dyrektorka Centrum Cyberbezpieczeństwa AGH i pełnomocniczka rektora tej uczelni ds. Kraków DIANA Accelerator w AGH, członkini Rady Programowej CYBERSEC Expo & Forum zwraca uwagę na rosnącą skalę kosztów cyberataków.

– W skali globalnej – według Cybersecurity Ventures – cyberprzestępczość ma łącznie (kraje, biznes i obywateli) kosztować już około 10,5 bln dol. rocznie. Euro-pol wskazuje, że cyberprzestępczość w UE, w tym oszustwa online, to dziś jeden z najbardziej dochodowych obszarów działalności przestępczej.

Ekspertka dodaje, że w Polsce (dane CBZC) w 2024 r. zabezpieczono ponad 226 mln zł z oszustw – a to jedynie część rzeczywistej skali strat. I sumuje: cyberataki są dziś narzędziem destabilizacji, ale też stale rozwijającym się „modelem biznesowym”.

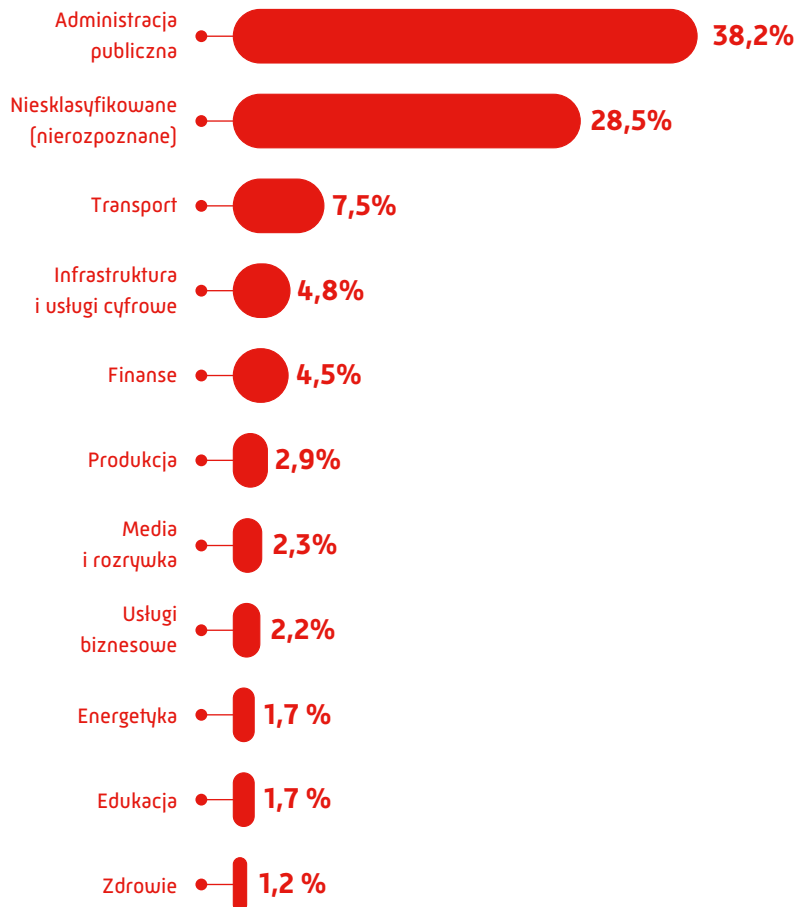
Krajobraz cyberzagrożeń jest złożony, dotyczy także m.in. prób kradzieży tożsamości i wyludzenia kredytów. Z raportu infoDOK Związku Banków Polskich za III kwartał 2025 r. wynika, że średnio co 36 minut ktoś próbował zaciągnąć zobowiązanie na cudze dane. W sumie w tym okresie odnotowano 3629 prób wyludzeń kredytów na łączną kwotę 78,3 mln zł. Średnia wartość jednej takiej próby sięgnęła 16,6 tys. zł, a największej 1,5 mln zł.

Cyberprzestępca. Wersja profesjonalna

Profesjonalizacja cyberprzestępczości sprawiła, że wiele grup w sieci funkcjonuje dziś jak firmy, a nawet wielkie korporacje. Opierają swe struktury na zarządzających, działach marketingu czy obsługi klienta – z konkretnymi zadaniami. To już globalny rynek o wysokiej marży, relatywnie wciąż niskim ryzyku wykrycia i coraz częściej w modelu „as-a-service” (cyberprzestępstwo jako usługa – np. Ransomware-as-a-Service).

W latach 2024-2025 celami cyberataków w Europie najczęściej były administracja publiczna, transport, infrastruktura i usługi cyfrowe, finanse i przemysł (dane: ENISA).

**Unia Europejska. Najczęściej atakowane sektory
(w proc. ogólnej puli zarejestrowanych cyberincydentów)**



Źródło: Raport ENISA Threat Landscape 2025

W cybergangach rekrutacja odbywa się jak firmach w branży IT: z procesami selekcji, testami kompetencji, a wynagrodzenia są oparte na prowizji od „przychodów”.

– Pracownicy są szkoleni z socjotechniki, rozmowy są nagrywane i odsłuchiwane, a osoby osiągające słabsze wyniki przechodzą dodatkowe szkolenia z psychomanipulacji prowadzone przez psychologa. Funkcjonują mechanizmy znane z dużych korporacji: ocena jakości pracy konsultantów, a nawet badania na wariografie – z pytaniami o kontakty z organami ścigania – podkreśla prof. Agnieszka Gryszczyńska, członkini rady programowej CYBERSEC Expo & Forum, dyrektor Departamentu ds. Cyberprzestępczości

i Informatyzacji w Prokuraturze Krajowej.

Maciej Broniarz, ekspert cyberbezpieczeństwa (także członek rady programowej CYBERSEC Expo & Forum) zajmujący się ratowaniem firm po ataku ransomware, jednoznacznie zaleca, by nie poddawać się szantażowi.

– Doradzamy, by nie płacić, bo odpowiedź jest jednoznaczna: te pieniądze idą np. na finansowanie putinowskiej maszyny wojennej. Grupy ransomware działają jak firmy: 24 godziny, 7 dni w tygodniu – za przyzwoleniem Rosji czy Białorusi.

Specjalista podkreśla, że wspomniane grupy długo tkwią w systemach organizacji i wyprowadzają dane na zewnątrz. A potem oferują np. dwa tygodnie na zapłatę



Izabela Albrzycht

dyrektorka Centrum Cyberbezpieczeństwa oraz pełnomocniczka rektora ds. Kraków DIANA Accelerator w AGH, członkini Rady Programowej CYBERSEC Expo & Forum

– Liczba i skala cyberataków pokazują, że stały się one powszechnym narzędziem wykorzystywanym w wojnie hybrydowej. (...) W świetle tych zagrożeń wielkiego znaczenia nabiera budowanie potencjału technologicznego, który może być pożytkowany do zwiększenia cyberodporności państwa, dlatego przedmiotem szczególnej troski i uwagi powinna być rosnąca liczba cyberataków na uczelnie, na których rozwijane są technologie dual-use, czyli z zastosowaniem zarówno cywilnym, jak i militarnym.



Borys Budka

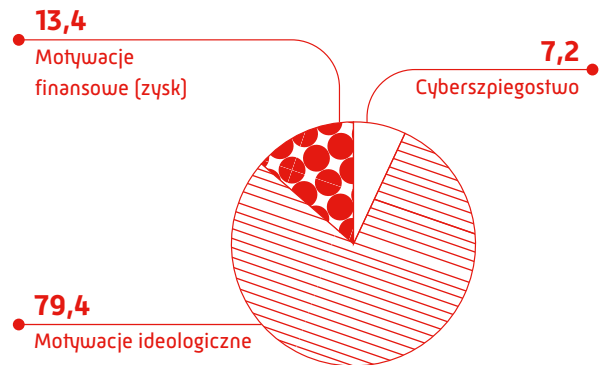
poseł do Parlamentu Europejskiego, przewodniczący Komisji Przemysłu, Badań Naukowych i Energii (ITRE)

– Wyzwaniem, także dla ludzi, którzy dbają o nasze cyberbezpieczeństwo, będzie komputer kwantowy, który w sekundę będzie mógł złamać cyfrowe zabezpieczenia. Musimy zaprojektować rozwiązania, które byłyby na to odpowiedzią i przeprogramować nasze myślenie o cyberbezpieczeństwie.

Unia Europejska. Najczęstsze początkowe wektory ataku (w proc. incydentów)



Unia Europejska. Motywacje/cele cyberataków (w proc. incydentów)



Źródło: Raport ENISA Threat Landscape 2025

okupu (groźba: zaszyfrowanie i ewentualny wyciek), gdyż inaczej dane trafią do internetu, co niesie za sobą konsekwencje prawne, biznesowe i wizerunkowe.

Jak opisuje Maciej Broniarz, ataki są powtarzalne: 99 proc. schematów to błąd ludzki, czyli phishing bez „uwierzytelnienia dwuskładnikowego”, zbyt wysokie uprawnienia członków zespołu (np. księgowej) czy profilowanie sekretariatów z dostępem do wszystkich plików i dokumentów w firmach.

– Mało organizacji filtruje ruch wychodzący i monitoruje sieć – logi pokazują anomalie, ale nikt na to nie patrzy – dodaje.

Nisko wiszące owoce

Istotnym „rynkiem” dla oszustów są także fałszywe inwestycje. Z danych CSIRT KNF wynika, że w 2025 r. spośród 41 751 zgłoszonych do zablokowania przez tę instytucję oszukańczych domen to właśnie fałszywe oferty szybkiego i łatwego zysku stanowiły ponad 96 proc.

Przestępczość kwitnie również za pośrednictwem platform społecznościowych. CSIRT KNF zgłosił do zablokowania 9751 oszukańczych reklam oraz 4358 profili, które specjalizowały się w publikowaniu fejkowych reklam (41,95 proc. więcej w porównaniu do ub. r.).

Wciąż plagą stanowi wykorzystanie wizerunku znanych osób do scamu w serwisach społecznościowych (politycy, celebryci czy dziennikarze); fałszywe treści mają też

„uwiarygadniać” dobrze znane firmy i instytucje, jak Orlen, ZUS, GPW czy projekty infrastrukturalne (np. Baltic Pipe).

Przegrupowanie i atuty obrońców

W Polsce system zwalczania cyberprzestępczości opiera się głównie na pracy Centralnego Biura Zwalczania Cyberprzestępczości (CBZC), które formalnie powstało 12 lipca 2022 r. Komendant Główny Policji gen. insp. Marek Boroń zapowiedział jednak istotne zmiany: powstanie Narodowe Biuro Śledcze Policji (z połączenia Centralnego Biura Śledczego Policji i CBZC).

NBS – poza kompetencjami obu biur – zajmie się także przestępstwami korupcyjnymi. W strukturach wyłonione zostanie też Biuro do Walki z Cyberprzestępczością, a rozbudowane – Biuro do Zwalczania Przestępczości Ekonomicznej. Reforma objęła również komendy wojewódzkie policji – od 1 marca 2026 r. rozpoczęły działanie wydziały do walki z przestępczością cyfrową.

– Zmiany w świecie przestępczym wymagają od policji dostosowania struktur i procedur, by jak najefektywniej i skuteczniej zapewnić bezpieczeństwo. Ostatnie dwa lata pokazały m.in. nowe zagrożenia (sabotaż, dywersje), z którymi nie mieliśmy do czynienia w 2021 r. A wzrost popularności przestępczości w sieci powoduje konieczność dostosowania struktur „cyber”, by społeczeństwo nie miało wątpliwości, że



Andy Garth

dyrektor ds. relacji z administracją publiczną w firmie ESET

– Dla Europy to kolejny przykład, jak bardzo jesteśmy zależni od amerykańskich technologii – w obszarach, które będą kluczowe dla przyszłości europejskiej gospodarki i rozwoju Europy (chodzi o decyzję administracji Donalda Trumpa, nakazującą firmie Anthropic ograniczenie zagrajnicznym użytkownikom dostępu do najnowszych modeli AI – dop. red.). Europa pozostaje zależna w każdym kluczowym sektorze technologicznym: w chmurze, w półprzewodnikach, w infrastrukturze, w oprogramowaniu. Sami pozwoliliśmy na takie uzależnienie. (...) Żyjemy w bardzo trudnych warunkach geopolitycznych. To zmusza nas do ponownej oceny tego, kim jesteśmy, kto jest naszym przyjacielem, kto jest naszym sojusznikiem i gdzie znajdują się nasze najważniejsze zależności.

funkcjonariusze z jednakową powagą podchodzą zarówno do ataków ransomware, jak i oszustw na portalach zakupowych – akcentuje komisarz Wioletta Szubska z Komendy Głównej Policji.

Na początku marca br. zmieniło się także kierownictwo cyberpolicji: dotychczasowy szef CBZC nadinsp. Adam Cieślak został odwołany ze stanowiska, a obowiązki komendanta powierzono mł. insp. Wojciechowi Olszowemu. Według zapowiedzi policja w nowej strukturze miałaby rozpocząć działania jeszcze w tym roku.

To nie koniec spodziewanych zmian. W Strategii Cyberbezpieczeństwa RP na lata 2025-2029 pojawiło się sporo propozycji nowelizacji przepisów, w tym w Kodeksie karnym. Chodzi m.in. o nowe regulacje, dotyczące umożliwienia organom ścigania szybszego dostępu do informacji stanowiących tajemnicę bankową, „urealnienie” przepisów o odpowiedzialności karnej za część cyberprzestępstw czy zaproponowanie rozwiązań „umożliwiających monitorowanie i ograniczanie wykorzystania sztucznej inteligencji do działań przestępczych” (terroryzm, automatyzacja ataków phishingowych, generowanie fałszywych treści, unikanie systemów wykrywania zagrożeń).

AI i cyberprzestępcy

Automatyzacja ataków, skalowalność ich działań oraz zdolność do tworzenia coraz lepszej jakości oszukańczych treści sprawiają, że zagrożenia ewoluują szybciej niż kiedykolwiek. To, co jeszcze nie tak dawno wymagało zespołu specjalistów, dziś może sprokurować jedna osoba wspierana przez model AI.

Szczególnie niebezpieczne są automatyzacja kampanii i wykorzystanie generatywnej AI w atakach socjotechnicznych (z elementami m.in. deepfake’ów wideo lub audio). Dzięki sztucznej inteligencji cyberprzestępcy mogą masowo tworzyć spersonalizowane wiadomości (phishing/smishing), które trudno odróżnić od autentycznej komunikacji, a także manipulować ofiarami z niespotykaną precyzją.

W ostatnim raporcie Pełnomocnika Rządu ds. Cyberbezpieczeństwa CSIRT MON wskazuje: „Wykorzystanie dużych modeli językowych do generowania spersonalizowanych treści phishingowych w języku

Incidenty obsługiwane przez CSIRT-y* poziomu krajowego (2025)		
	Incidenty	Zmiana proc. 2024/25
CSIRT MON	7125	69
CSIRT GOV	5033	26,1
CSIRT NASK	260 783	152
Łącznie	272 941	144

*[ang. Computer Security Incident Response Team – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego]

polskim osiągnęło poziom, gdzie nawet świadomi zagrożeń użytkownicy mają trudność z rozróżnieniem prawdziwej komunikacji od złośliwej”.

– Modele sztucznej inteligencji rozwinięły się już do tego stopnia, że przygotowanie ataku z wykorzystaniem zautomatyzowanego rozpoznania OSINT czy też analizy poczty e-mail wykradzonej z infrastruktury ofiary, jej kontrahentów lub współpracowników, daje naprawdę groźne i oczekiwane przez adversarza efekty. Ale właściwie wykorzystane AI staje się też potężnym narzędziem wsparcia obrony i analizy wrogich działań przeciwko chronionym systemom. Obecnie trwa analiza – z wykorzystaniem AI – tysięcy projektów informatycznych w kierunku poszukiwania podatności w ich kodzie – podkreśla Jarosław Wacko, współtwórca CSIRT MON, dziś główny specjalista w DKWOC i CSIRT MON.

I dodaje, że na szczęście dla obrońców wiele opracowań wskazuje, iż AI ma więcej do zaoferowania w defensywie niż działaniach ofensywnych.

– Dystans ten powinien rosnąć. Nie można jednak zapominać, że jednocześnie AI znacznie obniża „próg wejścia” dla początkujących cyberprzestępców, a przecież nie wszystkie systemy będą bronione z wykorzystaniem AI – chociażby te mniejszych podmiotów lub w zastosowaniach typowo domowych – zaznacza Wacko. – Tu zagrożenia mogą rosnąć lawinowo. Ostateczny wynik będzie zależał od kreatywności każdej ze stron – blue (Blue Team zabezpiecza i odpiera ataki w czasie rzeczywistym – przyp. red) i red (Red Team

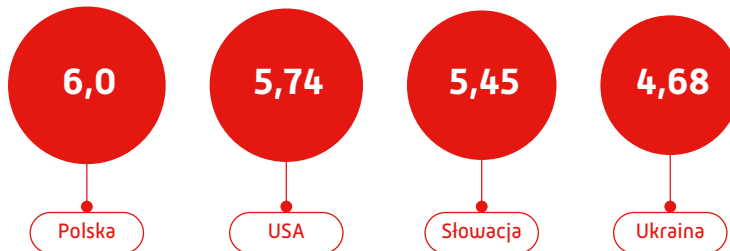


Karol Paciorek

kierownik CSIRT KNF

– Określenie „nisko wiszące owoce” bardzo dobrze oddaje rzeczywistość, zwłaszcza w kontekście fałszywych inwestycji. Przestępcy robią tylko to, co im się opłaca. (...) Dla wielu grup to jest pełnoetatowa „praca” w modelu przypominającym korporację: przychodzą na zmianę, wykonują setki telefonów czy komunikatów, a ich wynagrodzenie zależy od liczby skutecznie oszukanych osób.

Polska najczęściej narażona na ataki ransomware*



*dane za I półrocze 2025 r.; liczba wykrytych ataków ransomware na globie = 100 proc.
Źródło: Dane ESET za I połowę 2025 r.

symuluje zaś działania cyberprzestępców – przyp. red.).

Trendem, który – zdaniem CSIRT MON – będzie się rozwijał, jest wykorzystanie technologii deepfake do kampanii, w których dojdzie do podszywania się pod menedżerów, urzędników czy zaufanych współpracowników. Przewiduje się także mnożenie wykorzystania AI w operacjach ofensywnych „państwowego” wroga.

Szef CSIRT KNF Karol Paciorek zwraca uwagę na jeszcze jeden aspekt: AI coraz częściej służy także do zakładania tzw. boomer trapów, czyli kont budowanych na obrazkach tworzonych przez AI (mają wzbudzać emocje, litość, zbierać lajki, później zaś zmieniają się w profile używane do scamu).

– Sztuczna inteligencja odgrywa coraz większą rolę w dziedzinie fałszywych inwestycji. Kiedyś łatwo było rozpoznać nieprofesjonalne, amatorskie reklamy – tzn. źle zrobione grafiki czy toporne wideo. Dziś dzięki AI próg „wejścia do biznesu” jest bardzo niski: można generować wysokiej jakości grafiki, wideo, a także podkładać głos w sposób zbliżony do perfekcji – precyzuje.

Eksperti Światowego Forum Ekonomicznego (WEF) w raporcie „Global Cybersecurity Outlook 2026” podkreślają, że 94 proc. badanych wskazało, iż sztuczna inteligencja będzie czynnikiem decydującym o zmianach w ich podejściu do cyberbezpieczeństwa w bieżącym roku. Według 64 proc. ankietowanych narzędzia AI są bezpieczne, lecz zarazem – w opinii 87 proc. respondentów – w ub.r. wzrosło ryzyko podatności związanej z AI. Ale...

– W dobie zaawansowanej automatyzacji i AI sercem cyberodporności niezmienne pozostaje człowiek – to on jest ostatecznym strategiem i decydem w cyfrowym teatrze działań. Technologie i procesy stanowią jedynie (choć niezbędne) instrumentarium, które bez odpowiedniej kultury bezpieczeństwa i „cyfrowego instynktu” personelu traci swoją skuteczność. Najsilniejsze organizacje to te, które potrafią przekuć doświadczenia z pierwszej linii cyberwalki w codzienne nawyki każdego pracownika, czyniąc z nich najbardziej responsywną i świadomą linię obrony – podkreśla płk rez. Łukasz Jędrzejczak, były zastępca dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni, a teraz Cyber & Defense Sector Director w Deloitte Central Europe.

Na niewypowiedzianej wojnie

Państwa-agresorzy w cyberprzestrzeni? Koordynowane ataki na infrastrukturę krytyczną, systemy administracji publicznej czy media, operacje wpływu, akty sabotażu czy kampanie dezinformacyjne stają się elementem wywierania presji w stosunkach międzynarodowych (poniżej progu wojny czy w ramach cyberoperacji w wojnie hybrydowej).

Szczególnie niebezpiecznym aspektem podobnych działań jest ich wpływ na stabilność gospodarczą. Cyberataki mogą zakłócać działanie całych sektorów gospodarki, destabilizować łańcuchy dostaw czy systemy finansowe, prowadząc do strat ekonomicznych i utraty zaufania obywateli

**Dariusz Standerski**

sekretarz stanu w Ministerstwie
Cyfryzacji

– Suwerenność Polski jest niemożliwa bez Europy. Łańcuchy dostaw technologii wykraczają poza granice państw. Potrzebujemy ich dywersyfikacji, a tę trzeba budować na poziomie unijnym. Suwerenność to kwestia zarządzania łańcuchami dostaw, usług i produkcji. Żadne pojedyncze zadanie tego nie załatwia.

**Michał Gramatyka**

sekretarz stanu w Ministerstwie
Cyfryzacji

– Bardzo ważna jest mentalność, to, jak my widzimy problem cyberbezpieczeństwa. Istotne jest wyciąganie wniosków, „odrobienie lekcji” z incydentów, które nas spotkały, by każdy atak wykorzystał do tego, żeby jutro czy pojutrze takie rzeczy nam się nie przydarzyły. To muszą robić m.in. samorządy.

do władz państwowych i lokalnych. Wraz z kampaniami dezinformacyjnymi tworzą atmosferę niepewności, a ta osłabia państwo „od środka”. Jak to wygląda w polskim przypadku?

– Ten cyberterroryzm ma określoną flagę. To flaga rosyjska – wskazuje wicepremier i minister cyfryzacji Krzysztof Gawkowski, dodając, że rosyjskie cyberataki na Polskę to najpoważniejsze akty wrogości w historii naszego kraju od II wojny światowej. – Wypowiadamy wojnę cyfrowym terrorystom, którzy uważają, że w Polsce można robić chaos, wprowadzać panikę i realizować zadania, które stoją w sprzeczności z polską racją stanu.

Ciekawe czasy. Niebezpieczne trendy

Prognozowanie kierunków rozwoju cyberprzestępczości staje się kluczowe dla budowy odporności państw, organizacji i społeczeństw.

Europol wśród trendów rozwojowych cyberprzestępczości, przyspieszanych przez coraz bardziej zaawansowane narzędzia oraz metody, wskazuje zwłaszcza zagrożenia hybrydowe potęgowane atakami ransomware, koalicjami hakerów oraz atakami DDoS, by podważyć zaufanie do struktur i systemów państwowych. Czekają nas także więcej syntetycznych treści CSAM (Child Sexual Abuse Material – materiały przedstawiające seksualne wykorzystywanie dzieci), oszustw napędzanych przez AI oraz cyberprzestępczości motywowanej finansowo (powiązanej z rynkiem kryptowalut).

„Nową kategorią zagrożeń są ataki wymierzone bezpośrednio w agentów AI – modele działające z dostępem do wewnętrznych danych lub systemów operacyjnych organizacji. Problemy pojawiają się na dwóch poziomach: agenci AI z nadmiernymi uprawnieniami oraz ataki na same systemy AI” – czytamy w raporcie CERT Orange Polska.

Inne najbardziej istotne trendy 2026 r.? Wykorzystywanie w oszustwach reklamowych technologii coraz lepszej jakości i jednocześnie coraz tańszej; konflikty o podłożu geopolitycznym, kształtujące aktywność w cyberprzestrzeni; ataki na łańcuchy dostaw; intensyfikacja ataków na środowiska chmurowe czy coraz częstsze atakowanie urzędów z systemem macOS.

– Przewiduję, że w najbliższym czasie zwiększy się liczba ataków typu ransomware, phishing czy też ataki na narzędzia chmurowe, które wszystkie są wzmacniane przez narzędzia uczenia maszynowego. Żyjemy w „ciekawych technologicznie” czasach. Dlatego ważne, aby cyberbezpieczeństwo miało dla nas najwyższy priorytet – podsumowuje Tomasz Chomicki, dyrektor ds. rozwoju biznesu w Samsung Electronics Polska. ●

Automatyzacja ataków, skalowalność ich działań oraz zdolność do tworzenia coraz lepszej jakości oszukańczych treści sprawiają, że zagrożenia ewoluują szybciej niż kiedykolwiek.

Konsekwencje cyberataków w Polsce za rok 2025 (dane CBZC zł)



Dane dotyczące ilości strat, mienia odzyskanego oraz mienia zabezpieczonego które zawiera w sobie wartość zabezpieczonych kryptowalut w 2025 roku

*straty ofiar ataków odnotowane przez CBZC

Postępowania przygotowawcze według kategorii cyberprzestępstw (Polska, 2025 r.)



Dane dotyczące kategorii prowadzonych postępowań przygotowawczych w 2025 roku. Do kategorii złośliwe oprogramowanie zaliczamy – ransomware, DDOS czy działania malware. Inne – handel narkotykami, farmaceutykami, fałszywymi dokumentami w darknetcie

Źródło: Centralne Biuro Zwalczania Cyberprzestępczości; dane za 2025 rok

Imperatyw państwa, szansa dla rynku

Złożona i wielowymiarowa odpowiedź państwa na gwałtownie rosnącą skalę cyberzagrożeń to konieczność, ale jak zwykle kluczowa będzie skuteczność w realizacji. Nowe mechanizmy zmieniają funkcjonowanie firm, zasady życia zbiorowego, świadomość społeczną. W cyfrowej wojnie nie ma cywilów.

Czego dowiesz się z tego rozdziału?

- Co stanowi naczelny cel i jakie są cele szczegółowe świeżej polskiej strategii cyberbezpieczeństwa?
- Czemu mają służyć i jakie kompetencje mają nowe instytucje cyberobronne?
- Na jakich branżach, dziedzinach życia i podmiotach państwo szczególnie koncentruje uwagę w polityce cyberbezpieczeństwa?
- W jakim stopniu nasz kraj stać na suwerenność w cyberobronie?
- Co się dzieje w bankowości – swoistej forpoczcie zmian?
- Jak jest skonstruowany system kar za niedopełnianie obowiązków w obronie przez cyberagresorami?

Cyberbezpieczeństwo jako polska racja stanu? Takie zestawienie nie dziwi w dobie rosnącej agresji w cyberprzestrzeni. Do zdecydowanego działania we wspólnej sprawie namawiał wicepremier i minister cyfryzacji Krzysztof Gawkowski, kiedy w marcu 2026 roku rząd przyjmował Strategię Cyberbezpieczeństwa RP na lata 2025-2029.

– Budujemy odporne cyfrowo państwo: rozwijamy krajowe technologie, wzmacniamy współpracę instytucji odpowiedzialnych za cyberbezpieczeństwo i skuteczniej zwalczamy cyberprzestępczość – oceniał optymistycznie wicepremier, nawiązując do głównego celu strategii.

A w dokumencie określono ten cel jako: „Podniesienie poziomu odporności krajowych podmiotów przez zwiększenie poziomu ochrony informacji oraz zwiększenie zdolności do wykrywania i reagowania na

zagrożenia, promowanie wiedzy i dobrych praktyk oraz podnoszenie kompetencji w zakresie cyberbezpieczeństwa w sektorze publicznym (w tym militarnym), prywatnym, a także wśród obywateli". Temu głównemu wektorowi towarzyszy 6 celów szczegółowych (patrz: ramka „cele szczegółowe...").

– Potrzebujemy jasnego planu działań, który wzmocni ochronę państwa, gospodarki i danych obywateli – uzasadniał potrzebę strategii Paweł Olszewski, wiceminister cyfryzacji.

Wspomniany dokument to odpowiedź na wzmożoną aktywność grup prowadzących nielegalne operacje w cyberprzestrzeni: hakytywistów, cyberprzestępców, działających wyłącznie dla zysku lub powiązanych z innymi państwami, oraz agentów nieprzyjacielskich krajów.

Te zagrożenia nie są bynajmniej abstrakcją. Codziennie uderzają w obywateli, przedsiębiorstwa i instytucje publiczne. Przejawy? Na przykład ataki ransomware na szpitale, spoofing (podszywanie się pod zaufane osoby, instytucje lub urzędy) skierowany w klientów banków czy kampanie dezinformacyjne sięjące panikę lub zakłócające procesy demokratyczne.

Wzmacnianie cyberodporności: nowe instytucje

– Mnożą się ataki na Polskę, na polską infrastrukturę, ale również na firmy, instytucje prywatne i zwykłych obywateli. Definitywnie skończył się czas, gdy życie w cyberprzestrzeni było beztrudne. Na cyfrowej wojnie, a Polska na takiej jest, nie ma cywilów – podkreślił Krzysztof Gawkowski podczas XVIII Europejskiego Kongresu Gospodarczego w Katowicach (EEC).

Przypomnijmy: Polska w 2024 r. znalazła się na II miejscu w Unii Europejskiej pod względem incydentów cyberbezpieczeństwa w firmach – za Finlandią (dane Eurostatu).

Przewidziana w strategii cyberbezpieczeństwa kontrofensywa obejmuje aż 169 zadań (kontynuacja wcześniejszych projektów i nowe propozycje). Wśród kluczowych inicjatyw uwagę zwraca koncepcja nowej architektury instytucjonalnej, która sankcjonuje m.in. istnienie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC), „namaszczać” je na centralną instytucję cyberbezpieczeństwa

w kraju, czyli „jedno okienko” dla spraw z tego obszaru.

Ponadto powstanie Krajowy Cyber Hub (National Cyber Hub – NCH), tj. platforma budowy świadomości o cyberzagrożeniach; docelowo wejdzie ona do europejskiej sieci wymiany informacji o incydentach (European Cybersecurity Alert System).

W strukturach Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK) powstanie z kolei Centrum Cyberbezpieczeństwa NASK (CCN). Znajdą się w nim specjalistyczne centra, ośrodki i laboratoria kluczowe dla wzmocnienia krajowego systemu cyberbezpieczeństwa (KSC). Autorzy strategii spodziewają się, że wzmocni to zdolności skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych państwa oraz podmiotów o kluczowym znaczeniu dla gospodarki.

Nowa jednostka z kompetencjami w rozpoznawaniu, przeciwdziałaniu i zwalczaniu cyberterrorizmu i cyberszpiegostwa powstanie też w strukturze Agencji Bezpieczeństwa Wewnętrznego. A z myślą o zarządzaniu kryzysowym planuje się stworzenie Systemu Bezpiecznej Łączności Państwowej (SBŁP) – do tego ostatniego projektu kolejne rządy zabierają się jednak od ponad 20 lat...

Strategia zakłada również włączenie wymogów cyberbezpieczeństwa do warunków zamówień publicznych, co zwiłokrotni popyt na usługi i produkty z tej dziedziny.

Jak ocenił w rozmowie z WNP dr inż. Andrzej Bartosiewicz, adiunkt Politechniki Krakowskiej i prezes fundacji CISO #Poland, opisywana strategia stanowi „solidny fundament” cyberodporności. Ale...

– Sukces tego planu zależy od tego, czy zaproponowane rozwiązania zostaną realnie zaadaptowane przez rynek i administrację, czy też pozostaną jedynie w sferze formalnych zapisów – zastrzegł.

Droga do technologicznej suwerenności

Duży nacisk twórcy strategii położyli na suwerenność technologiczną (4. cel szczegółowy), co oznacza rozwój krajowych technologii i certyfikację rozwiązań ICT (produkty i usługi związane z technologiami informacyjno-telekomunikacyjnymi).

„Tylko panując w pełni nad technologią w wymiarze sprzętowym i programowym,

Cele szczegółowe Strategii Cyberbezpieczeństwa RP na lata 2025–2029

1. Rozwój krajowego systemu cyberbezpieczeństwa.
2. Przeciwdziałanie i zwalczanie cyberprzestępczości oraz uzyskanie zdolności doprowadzenia pełnego spektrum działań w cyberprzestrzeni.
3. Podniesienie poziomu odporności systemów informacyjnych w sferze publicznej (w tym militarnej) oraz prywatnej.
4. Zwiększanie potencjału krajowej bazy technologiczno-przemysłowej oraz wzmocnienie suwerenności technologicznej Rzeczypospolitej Polskiej w dziedzinie cyberbezpieczeństwa.
5. Budowanie świadomości, wiedzy i kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa oraz obywateli i przedsiębiorców.
6. Wzmocnienie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.



Andrzej Bartosiewicz

założyciel i prezes zarządu Fundacji CISO #Poland

– Z punktu widzenia regulacyjnego kluczowe jest to, że odpowiedzialność formalna pozostaje po stronie zarządu i CIO – przeciwnie, wzmacnia ich rolę jako doradców i partnerów w podejmowaniu decyzji.

Incydynty obsługiwane przez CERT Polska w latach 2018–2025

Rok	Liczba incydentów
2025	260 783
2024	103 449
2023	80 267
2022	39 683
2021	29 483
2020	10 420
2019	6 484
2018	3 739

Źródło: „Krajobraz bezpieczeństwa polskiego internetu” – raport roczny 2025 z działalności CERT Polska, CERT Polska (NASK)

Incydynty obsługiwane przez CERT Polska w 2025 roku w podziale na kategorie

Kategoria zagrożenia	Liczba incydentów	Procent
Oszustwa komputerowe	253 238	97,1%
Złośliwe oprogramowanie	3 438	1,3%
Podatne usługi	1 732	0,7%
Obrażliwe 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%
Inne	18	0%
Gromadzenie informacji	15	0%
Razem	260 783	100,0%

Źródło: „Krajobraz bezpieczeństwa polskiego internetu” – raport roczny 2025 z działalności CERT Polska, CERT Polska (NASK)

można zapewnić bezpieczeństwo w warstwie infrastrukturalnej i aplikacyjnej systemów teleinformatycznych” – czytamy w rządowym dokumencie.

Poleganie na amerykańskich podmiotach, dominujących w szeroko pojętym europejskim sektorze technologicznym, pozostaje ryzykowne nie z powodu uzależnienia się od jednego dostawcy (vendor lock-in).

– Big techy podlegają legislacji amerykańskiej. Są zarejestrowane w Europie, mają nawet spółki w Polsce, lecz ich centra znajdują się w Stanach Zjednoczonych i obowiązuje je amerykański Cloud Act. A ten mówi, że jeżeli rząd amerykański czy amerykańskie służby federalne zażądamy informacji, to dana firma musi to udostępnić – wyjaśniał Grzegorz Soczewka, wiceprezes ds. sprzedaży CEE w OVHcloud. Podkreślił: globalni giganci podlegają amerykańskiemu przepisowi, nawet jeśli zbudowali centrum danych na terenie Unii.

Zrealizowanie celu strategii dotyczącego suwerenności nie będzie łatwe. Zdaniem

Piotra Zielaskiewicza, menedżera z firmy DAGMA Bezpieczeństwo IT, inne kraje Unii odważniej podchodzą do redukcji zależności od pozaeuropejskich dostawców.

– W Polsce nadal częściej rozmawiamy o potrzebie suwerenności cyfrowej, niż wdrażamy konkretne mechanizmy, wspierające lokalny ekosystem technologiczny czy premiujące rozwiązania europejskie w sektorze publicznym – uważa Zielaskiewicz.

Aleksander Kostuch, ekspert w dziedzinie zabezpieczeń sieci i systemów IT z francuskiej firmy Stormshield (rozwiązania do ochrony sieci teleinformatycznych), wskazuje dwa powody powolnej budowy suwerenności technologicznej: niewystarczającą świadomość potrzeby niezależnienia się od big techów oraz rozmaite przeciwdziałania tych gigantów.

– Osiągnięcie autonomii w stopniu, w jakim jest ona możliwa – z uwzględnieniem specyfiki łańcucha dostaw w dziedzinie cyberbezpieczeństwa – oznaczać musi potężne inwestycje. Kluczowe jest, aby wspierać

Polska w 2024 r. znalazła się na II miejscu w Unii Europejskiej pod względem incydentów cyberbezpieczeństwa w firmach – za Finlandią.

ten proces, wybierając europejskie technologie wszędzie tam, gdzie to możliwe – stwierdza Aleksander Kostuch.

Ale w refleksji i działaniach na rzecz niezależności uwzględnić trzeba globalne łańcuchy dostaw, międzynarodową wymianę informacji o zagrożeniach i interoperacyjności systemów bezpieczeństwa; suwerenność nie może oznaczać izolacji.

– Nadmierny protekcyjizm mógłby ograniczyć tempo innowacji i utrudnić współpracę operacyjną między sojusznikami NATO i UE – ostrzega realistycznie specjalista.

Wychodzimy z serwerowni

Długo cyberbezpieczeństwo traktowano jako domenę specjalistów IT. Wyjście „z serwerowni” stało się priorytetem regulatorów i prawodawców dopiero, gdy się okazało, że skuteczny atak hakerski może zatrzymać elektrownię, sparaliżować szpital albo odciąć od wody miasto.

Dziś jesteśmy świadkami fundamentalnej zmiany: bezpieczeństwo cyfrowe przestaje być opcją, a staje się obowiązkiem prawnym – z listą konkretnych wymogów, terminów i sankcji.

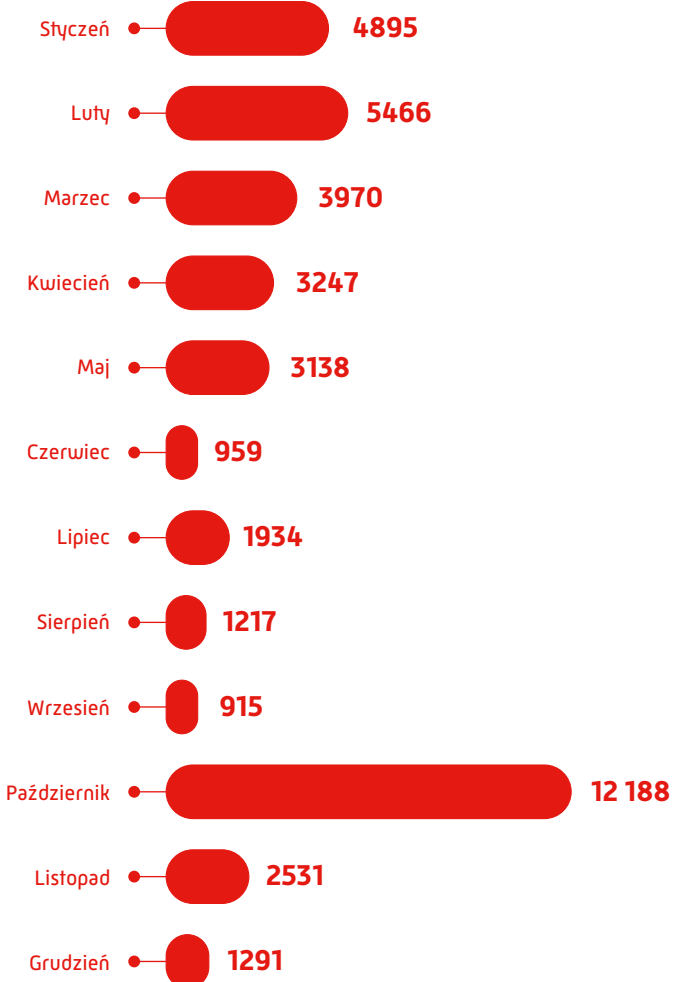
W Polsce „rewolucja 3 kwietnia” – wtedy weszła w życie nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC), wprowadzająca unijną dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa (NIS2) – objęła kilkadziesiąt tysięcy firm.

Wcześniej obowiązki cyberbezpieczeństwa wprowadzono w sektorze finansowym, stosując się do rozporządzenia UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA).

Zanim pojawiły się regulacje prawne, ochrona informacji opierała się na dobrowolnie stosowanych standardach. Najważniejszy? Norma ISO/IEC 27001, definiująca wymagania dla systemu zarządzania bezpieczeństwem informacji (SZBI). Organizacja, która ją wdraża, zobowiązuje się m.in. do systematycznego identyfikowania ryzyk i stosowania proporcjonalnych zabezpieczeń. Towarzyszy jej kilka norm uzupełniających: ISO 27035 (zarządzanie incydentami), ISO 22301 (ciągłość działania) oraz ISO 31000 (zarządzanie ryzykiem w szerszym kontekście biznesowym).

Problem, że dobrowolne obowiązki brały na siebie nieliczne przedsiębiorstwa;

Domeny zgłoszone do blokady przez CSIRT KNF [rok 2025]*



* zgłoszone do CSIRT NASK przez CSIRT KNF

Źródło: „Polski rynek finansowy w obliczu zagrożeń” – raport roczny cyberbezpieczeństwa 2025, CSIRT KNF

większość organizacji pozostawała poza systemem, co wykorzystywali atakujący.

Bankowość w szpicie

O tym, że odpowiednia regulacja to game changer bezpieczeństwa cyfrowego, przekonują zmiany w sektorze finansowym.

Rozporządzenie DORA jest stosowane w państwach członkowskich UE od 17 stycznia 2025 r. Cel? Zapewnić, że instytucje finansowe we Wspólnocie przetrwają cyberataki, nie przerywając świadczenia

usług. Nie wymagało ono transpozycji. Krajowa ustawa (weszła w życie 7 sierpnia 2025 r.) przede wszystkim reguluje kwestie nadzorcze i określa kary.

Przepisom DORA podlega w Polsce ok. 2,3 tys. podmiotów. Oprócz banków, domów maklerskich i innych instytucji finansowych to także kluczowi zewnętrznym dostawcy usług ICT (np. chmury obliczeniowej) dla tego sektora.

Rozporządzenie wskazuje obszary (filary), w których te podmioty muszą wykazać „realną gotowość”:

1. Zarządzanie ryzykiem ICT – tj. wdrożenie kompleksowej strategii identyfikacji, monitorowania i minimalizacji ryzyka technologicznego, z jasno wyznaczoną odpowiedzialnością organu zarządzającego.
2. Zarządzanie incydentami i ich raportowanie – obowiązek klasyfikacji i zgłaszania poważnych incydentów ICT do CSIRT KNF (tj. Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającemu w ramach Komisji Nadzoru Finansowego) w ściśle określonych terminach. Wstępne powiadomienie o poważnym incydencie należy zgłosić w ciągu 4 godzin, potem raport – w ciągu 72 godzin i raport końcowy – w ciągu miesiąca.
3. Sprawdzanie odporności cyfrowej – regularne testy systemów ICT, w tym dla największych podmiotów zaawansowane testy penetracyjne pod groźbą ataku (TLPT), przeprowadzane przez zewnętrznych audytorów co trzy lata.
4. Zarządzanie ryzykiem dostawców ICT – weryfikacja bezpieczeństwa wszystkich kluczowych dostawców technologii informacyjno-telekomunikacyjnych, klauzule umowne, zapewniające możliwość audytu i ciągłość usług, rejestr wszystkich umów z zewnętrznymi dostawcami ICT.
5. Wymiana informacji o zagrożeniach – podmioty objęte przepisami DORA zachęcane są do dobrowolnej wymiany informacji o cyberincydentach między sobą.

Za nieprzestrzeganie DORA instytucji finansowej grozi kara, która może przekroczyć 20 mln zł. W przypadku zewnętrznych dostawców ICT maksymalna „represja” to 5 mln euro.

W sprawozdaniu za 2025 rok CSIRT KNF stwierdza, że pierwsze miesiące

stosowania regulacji cyberbezpieczeństwa „uwidocznili rosnącą świadomość instytucji w zakresie konieczności niezwłocznego i kompletnego raportowania” incydentów. Dzięki temu „obrońcy” z tego sektora mają więcej danych i lepszy obraz sytuacji.

Ponadto wprowadzony przez DORA obowiązek przekazywania informacji o znaczących cyberzagrożeniach (potencjalnych aktywnościach cyberprzestępczych) „usprawnił przepływ informacji pomiędzy instytucjami rynku, umożliwił szybszą identyfikację nowych trendów i technik działania adversarzy oraz zwiększył zdolność do podejmowania działań prewencyjnych”.

Na wynikający z DORA obowiązek raportowania incydentów jako skuteczne narzędzie obrony zwraca uwagę kierownik CSIRT KNF Karol Paciorek.

– Oprócz formalnych raportów funkcjonuje też nasza platforma wymiany informacji, gdzie podmioty mogą na bieżąco opisywać swoje obserwacje i zagrożenia, a my możemy reagować oraz wspierać je w podnoszeniu świadomości i odporności – precyzuje.

Z raportu CSIRT KNF wynika, że w 2025 r. podmioty objęte DORA zgłosiły 274 poważne incydenty ICT. Prawie wszystkie dotyczyły awarii – w środowisku własnym instytucji (41 proc. zgłoszeń) oraz u zewnętrznych dostawców usług ICT (55 proc.).

Skuteczności nowych obowiązków cyberbezpieczeństwa dowodzi też raport krajowego CSIRT NASK (CERT Polska), w którym czytamy, że z prawie 261 tys. incydentów obsługiwanych w 2025 r. jako poważne – tj. mogące spowodować istotne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej – zaklasyfikowano 27. Większość z nich (14) dotyczyła sektora bankowości i infrastruktury rynków finansowych, 8 – ochrony zdrowia, a pozostałe 5 – transportu.

W porównaniu z rokiem 2024 liczba incydentów poważnych w kraju zmniejszyła się o 53 proc., ale w sektorze finansowym odnotowano większy spadek (68 proc.). W opinii ekspertów z CSIRT NASK wiąże się to z „wdrożeniem rozporządzenia DORA, które nakłada na podmioty finansowe obowiązek raportowania incydentów poważnych”.

Najczęściej spotykane cyberzagrożenia

36%

Ataki phishingowe

28%

Ataki na sieć wi-fi

19%

Ataki z użyciem trojanów

18%

Ataki na aplikacje

18%

Ataki DDoS

17%

Ataki na usługi cloud

17%

Spoofing tożsamości

16%

Ataki na urządzenia mobilne

14%

Ataki ransomware

Źródło: Raport ESET i DAGMA Bezpieczeństwo IT
– Cyberportret polskiego biznesu. Cyberbezpieczeństwo firm w obliczu nowych wyzwań.



– Budujemy odporne cyfrowo państwo: rozwijamy krajowe technologie, wzmacniamy współpracę instytucji odpowiedzialnych za cyberbezpieczeństwo i skuteczniej zwalczamy cyberprzestępczość
– zapewnił Krzysztof Gawkowski, wicepremier i minister cyfryzacji.

Cyfrowy rachunek sumienia

Dla wielu przedsiębiorstw w Polsce przystąpienie do cyberbezpieczeństwa dopiero się zaczyna. Do kwietnia w krajowym systemie cyberbezpieczeństwa (KSC) było niespełna 400 operatorów usług kluczowych i kilkadziesiąt dostawców usług cyfrowych.

Według nowych zasad (KSC 2.0), wprowadzających unijną dyrektywę NIS2, groźno to wzrosło do ok. 42 tys. firm i podmiotów publicznych, określanych jako kluczowe i ważne. W dawnym KSC było 9, teraz jest 18 sektorów gospodarki i administracji.

Większość organizacji z obowiązkami cyberbezpieczeństwa styka się zatem po raz pierwszy. Przede wszystkim muszą dokonać samooceny, czy podlegają nowym przepisom. Jeżeli tak, to do 3 października mają czas na wpisanie się do wykazu, a do 3 kwietnia 2027 r. – na wprowadzenie środków cyberbezpieczeństwa.

Ten trzeci krok będzie wymagał najwięcej pracy. Należy:

- wdrożyć system zarządzania bezpieczeństwem informacji (SZBI),
- wprowadzić procedury zarządzania ryzykiem i incydentami,

- przygotować dokumentację bezpieczeństwa,
- podłączyć się do systemu S46 i rozpocząć zgłaszanie incydentów.

Jak wyjaśniała WNP Agnieszka Wachowska, radczyni prawna, co-managing partner kancelarii Traple Konarski Podrecki i Wspólnicy, szacowanie ryzyka wystąpienia incydentu i zarządzanie nim będzie polegało na identyfikacji, jakie i skąd może przyjść zagrożenie – i wdrożeniu rozwiązań, które to zagrożenie zmięgują.

– Środkami zmniejszania ryzyka są m.in. regularne szkolenia dla zarządzających organizacją i osób mających wpływ na jej bezpieczeństwo – wskazała Agnieszka Wachowska.

Konieczny będzie też system zarządzania incydentami, które należy wykrywać i zgłaszać.

– Nowym obowiązkiem, któremu nie podlegają obecne podmioty KSC, będzie zapewnienie bezpieczeństwa łańcucha dostaw produktów, usług i procesów ICT. Trzeba będzie zweryfikować zarówno dostawcę, jak i jego produkt. To będzie duże wyzwanie dla organizacji – oceniła mec. Wachowska.



Andrzej Dulka

prezes Polskiej Izby Informatyki i Telekomunikacji

– W świecie rosnących zagrożeń cybernetycznych nie możemy już zakładać, że za nasze bezpieczeństwo odpowie państwo, regulator czy zagraniczny sojusznik. Odpowiedzialność spoczywa dziś również na producentach technologii i właścicielach firm. Oznacza to konieczność projektowania produktów bezpiecznych od samego początku, kontrolowania całego łańcucha dostaw oraz zapewnienia bezpieczeństwa przez cały cykl życia rozwiązania. Firmy, które jako pierwsze zbudują tu wiarogodność, zyskają przewagę konkurencyjną na rynku europejskim i globalnym.



Karol Skupień

prezes Krajowej Izby Komunikacji Ethernetowej

– Jako przedstawiciel biznesu i praktyk oceniam, że około 80 proc. firm, których dotyczy KSC, w ogóle nie ma świadomości tego faktu. Jeżeli zatem mówimy, że „połowa coś zrobiła”, to – moim zdaniem – to połowa z tych 20 proc. świadomych. Czyli około 10 proc. firm objętych regulacją coś robi, a reszta jest w lesie

Jak wskazywali eksperci w rozmowach z WNP, zapewnienie zgodności z NIS2 wymaga rewolucji w podmiotach objętych nowymi przepisami.

– Dostosowanie się do NIS2 wymaga zmiany sposobu zarządzania organizacją. Koszty tej operacji trudno wymierzyć – uważa Kinga Pawłowska-Nojszewska, radca prawny w Kancelarii Prawnej Media.

Pod szczególnym nadzorem

NIS2 dzieli objęte regulacją podmioty na dwie kategorie: te kluczowe podlegają surowszemu reżimowi i aktywniejszemu nadzorowi niż podmioty ważne.

Priorytetowo potraktowano sektory, które muszą spełniać najwyższe standardy cyberbezpieczeństwa, składające się na infrastrukturę krytyczną państwa – systemy i obiekty niezbędne do funkcjonowania gospodarki i życia obywateli. Ale nie tylko.

Sektorami kluczowymi są:

- energia (np. energia elektryczna, gaz, paliwa i ropa, ciepło);
- transport lotniczy, kolejowy, wodny i drogowy;
- finanse (bankowość i infrastruktura rynku finansowego, jak instytucje kredytowe, operatorzy systemów obrotu i partnerzy centralni);
- ochrona zdrowia, w tym podmioty świadczące opiekę zdrowotną, producenci podstawowych produktów farmaceutycznych i wyrobów medycznych o krytycznym znaczeniu oraz laboratoria referencyjne UE;
- woda pitna;
- ścieki;
- infrastruktura cyfrowa, w tym dostawcy usług centrów danych, usług przetwarzania w chmurze, publicznych sieci łączności elektronicznej i publicznie dostępnych usług łączności elektronicznej;
- zarządzanie usługami ICT;
- przestrzeń kosmiczna;
- wybrane podmioty publiczne.

Cyberataki na te sektory, rzecz jasna, mogą wyrządzić największe szkody.

– Zintegrowany, zmasowany atak, nie daj Bóg, na całą tę infrastrukturę w jednym momencie, groziłby paraliżem państwa. Nie możemy sobie na to pozwolić – mówi wiceminister cyfryzacji Paweł Olszewski.

Z kolei sektory ważne to:

- usługi pocztowe, w tym kurierskie;

- inwestycje energetyki jądrowej;
- gospodarka odpadami;
- produkcja, wytwarzanie i dystrybucja chemikaliów;
- produkcja, przetwarzanie i dystrybucja żywności;
- produkcja, w szczególności wyrobów medycznych, komputerowych, elektronicznych i optycznych, niektórych rodzajów sprzętu elektrycznego i maszyn, pojazdów silnikowych i innego sprzętu transportowego;
- dostawcy usług cyfrowych w zakresie internetowych platform handlowych, wyszukiwarek i sieci społecznościowych;
- badania naukowe;
- podmioty publiczne (regionalne): samorządowe jednostki budżetowe, samorządowe zakłady budżetowe, samorządowe instytucje kultury, spółki realizujące zadania użyteczności publicznej.

Czy podmioty działające w branżach objętych NIS2 są gotowe sprostać wyśrubowanemu obowiązkowi cyberbezpieczeństwa?

Z raportu „Incydenty pod kontrolą” z 2025 r., przygotowanego przez Media-recovery i Safesqr we współpracy z PMR Market Experts, wynika, że znakomita większość (91 proc.) polskich firm słyszała o dyrektywie i uznała, że dotyczy ich ona bezpośrednio lub pośrednio. Ale tylko 19 proc. w znacznym stopniu spełnia wymagania NIS2. Na przykład jedynie 5 proc. organizacji przygotowuje raporty po incydentach i prowadzi analizę ich przyczyn. Kluczowa bariera? Ograniczony budżet IT (wskazało na niego 77 proc. firm).

Dostawcy wysokiego ryzyka

Oszczędzanie na przygotowaniach może się jednak źle skończyć, bo za naruszenie obowiązków cyberbezpieczeństwa grożą surowe reperkusje.

– Maksymalne administracyjne kary pieniężne nakładane na podmioty kluczowe mogą sięgać 10 mln euro lub 2 proc. całkowitego rocznego globalnego obrotu firmy, a w przypadku podmiotów ważnych – do 7 mln euro lub 1,4 proc. obrotu – akcentuje Agnieszka Wachowska.

To nie koniec... Członkowie zarządów podmiotów kluczowych i ważnych mogą zostać ukarani grzywną w wysokości do trzykrotności miesięcznego wynagrodzenia, a wobec kierujących podmiotami

Nowy porządek w polskim cyberbezpieczeństwie

- 3 kwietnia weszła w życie nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC)
- 3 października mija termin rejestracji podmiotów ważnych i kluczowych
- do 3 kwietnia 2027 r. trzeba będzie mieć wdrożony system zarządzania bezpieczeństwem informacji (SZBI).



Agnieszka Jankowska

przewodnicząca Rady ds. Cyfryzacji przy Ministerstwie Cyfryzacji i dyrektor ds. korporacyjnych i public affairs w T-Mobile Polska

– Duże korporacje są przygotowywane na mierzenie się z cyberzagrożeniami. Musiały spełnić wymagania dyrektyw NIS1 oraz NIS2 i regulacji specyficznych dla poszczególnych sektorów. Największy problem to zejście do poziomu lokalnego – gmin, powiatów i mniejszych instytucji (np. w sektorze zdrowia) czy jednostek budżetowych podległych samorządom, które borykają się z podstawowymi problemami, jak finanse i utrzymanie specjalistów.



Jarosław Homa

pełnomocnik rektora
ds. cyberbezpieczeństwa,
wicedyrektor Centrum
Cyberbezpieczeństwa, Politechnika
Śląska

– CRA* to bardzo potrzebna regulacja. Rozwiązania, które po 11 grudnia 2027 r. będą dopuszczane do eksploatacji będą musiały być bezpieczne. (...) Porównam to do kupna zabawek: świadomi rodzice szukają znaku „CE”, bo oznacza, że zabawka została przebadana i dziecko nie zrobi sobie krzywdy.

kluczowymi wchodzi w grę decyzja czasowo zakazująca pełnienia funkcji kierowniczych.

– Dodatkowo brak należytej staranności może skutkować odpowiedzialnością cywilną. W określonych przypadkach, zwłaszcza przy rażącym i umyślnym uchybieniu obowiązkom wynikającym z KSC, możliwa jest również odpowiedzialność karna osób zarządzających, jeżeli zostanie wykazane, że ich zaniechanie było szkodliwe dla spółki – ostrzega prawniczka.

Znowelizowana ustawa o KSC przewiduje też okresowe kary pieniężne. Jak tłumaczyła WNP Kinga Pawłowska-Nojszewska, dyrektywa ich nie wymaga, ale dopuszcza. Będą nakładane za niezastosowanie się do nakazu organu cyberbezpieczeństwa i wyniosą od 500 zł do 100 tys. zł za każdy dzień opóźnienia.

Czysto polskim dodatkiem stała się zaś gigantyczna kara – do 100 mln zł – grożąca podmiotowi, który naruszy przepisy, powodując bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego, życia i zdrowia ludzi albo zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług.



Kinga Pawłowska-Nojszewska

radca prawny w Kancelarii Prawnej
MEDIA

– Cały czas jesteśmy skupieni na NIS2 i KSC. Dopóki polski rząd nie zajmie się wdrażaniem CRA*, czyli wyznaczeniem konkretnych organów odpowiedzialnych, dopóty zainteresowanie tym aktem wśród polskich przedsiębiorców może być mniejsze. Tylko naprawdę duże podmioty zaczęły się już w ogóle zastanawiać nad CRA...

W procesie legislacyjnym krytykowano to rozwiązanie jako „nadregulację”. Ministerstwo Cyfryzacji uzasadniało jednak, że każde naruszenie przepisów, spełniające przesłanki nałożenia 100 mln zł kary, „może wiązać się z poważnymi konsekwencjami dla państwa i jego obywateli, a tym samym powinno być obarczone odpowiednio wysoką sankcją, która będzie spełniać funkcję zarówno prewencyjną, jak i represyjną”.

Ta najwyższa kara już może być stosowana. Wszystkie pozostałe będą nakładane dopiero od kwietnia 2028 r.

W przeddzień wejścia w życie nowelizacji KSC kierownictwo resortu cyfryzacji zapewniało na spotkaniu z dziennikarzami, że celem ustawy nie jest karanie firm.

– Państwo ma wymuszać decyzyjność, a kara ma być ostatecznością. Przynajmniej tak jest myślenie Ministerstwa Cyfryzacji – wyjaśnił wicepremier Krzysztof Gawkowski.

A Paweł Olszewski zaznaczył, że KSC to nie system opresyjny, lecz system, który ma zapewnić bezpieczeństwo państwa. Marcin Wysocki, wicedyrektor departamentu cyberbezpieczeństwa w Ministerstwie Cyfryzacji, poinformował zaś, że przed nowelizacją ustawy o KSC można było nakładać



Krzysztof Silicki

dyrektor ds. Strategicznego Rozwoju
Cyberbezpieczeństwa, NASK, Rada
Zarządzająca i Rada Wykonawcza ENISA

– Nie każdy wymóg CRA* oznacza wielkie koszty. Przykład? Producenci IoT (...) wypuszczają produkt podłączony do internetu, który ma domyślne hasło: admin albo 1,2,3,4,5. Potem odbiorca to włącza, urządzenie samo łączy się z najbliższym wi-fi i nikt tego nie zmienia. Ile kosztuje producenta wprowadzenie procedury, która wymaga zmiany hasła przy pierwszym uruchomieniu? Śmiem twierdzić, że nie aż tak dużo.

Strategia Cyberbezpieczeństwa RP zakłada włączenie wymogów cyberbezpieczeństwa do warunków zamówień publicznych, co wielokrotnie popyt na usługi i produkty z tej dziedziny.

**Cyber Resilience Act zobowiązuje producentów do zapewnienia, by ich produkty na rynku UE były bezpieczne i pozbawione znanych podatności; sygnalizować to będzie znak „CE”.*

kary do 1 mln zł, ale od 2018 r. najwyższa kara wyniosła 50 tys. zł.

Najgłośniejszą krytykowaną nadregulacją i zarazem najbardziej kontrowersyjnym elementem nowych zasad cyberbezpieczeństwa są jednakże przepisy dotyczące dostawcy wysokiego ryzyka (DWR). Nie wynikają one z NIS2, lecz stanowią wdrożenie unijnych narzędzi oceny ryzyka dostawców sprzętu do sieci telekomunikacyjnych (znanych jako Toolbox 5G). Krytycy wytykali autorom nowelizacji, że w ten sposób środki bezpieczeństwa przewidziane tylko dla operatorów sieci komórkowych 5G rozszerzyli na 18 sektorów objętych NIS2.

Prawo wskazywania DWR nowelizacja przyznaje ministrowi cyfryzacji. Podstawą tych decyzji będą zarówno kryteria techniczne, jak i nietechniczne. Przewidziano też konsultacje z prokuraturą, stroną społeczną i kolegium ds. cyberbezpieczeństwa.

W konsekwencji wszystkie podmioty KSC będą musiały w ciągu od 4 do 7 lat wymienić objęte taką decyzją produkty i usługi ICT. Nie przewidziano za to rekompensat.

Według Krajowej Izby Komunikacji Ethernetowej koszty wymiany dla objętych KSC firm telekomunikacyjnych w skali 5 lat mogą wynieść 14,4 mld zł (netto). Do obliczeń przyjęto jednak najczarniejszy scenariusz: założenie, że wymianie może podlegać cały sprzęt i oprogramowanie od dostawców spoza UE i NATO.

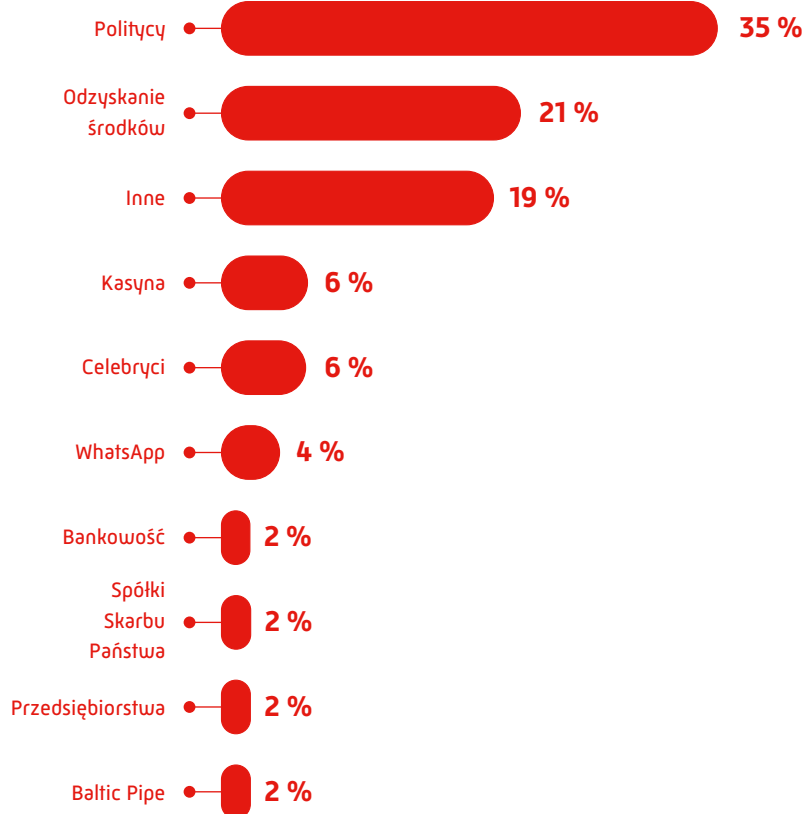
W grudniu 2024 r. Ogólnopolska Federacja Przedsiębiorców i Pracodawców Przedsiębiorcy.pl średni koszt takiej operacji dla firmy z branży gospodarowania odpadami szacowała na prawie 1 mln zł w ciągu 6 lat. Jak podawał Portalkomunalny.pl, mogło to dotyczyć blisko 9 tys. podmiotów. Dla innych sektorów brak podobnych estymacji.

Miliardy na cyberobronę

Prezentując w kwietniu sprawozdanie pełnomocnika rządu ds. cyberbezpieczeństwa za 2025 rok, wicepremier Gawkowski podkreślał, że rekordowa jest nie tylko liczba cyberzagrożeń, ale i publiczne wydatki na cyberbezpieczeństwo (w tym roku przekroczy 5 mld zł).

Wydatków na ten cel nie unikną też przedsiębiorstwa. Wspomniany raport „Incydenty pod kontrolą” wskazuje, że

Fałszywe wizerunki wykorzystywane w reklamach (rok 2025)



Źródło: „Polski rynek finansowy w obliczu zagrożeń” – raport roczny cyberbezpieczeństwa 2025, CSIRT KNF

89 proc. firm planuje inwestycje w IT związane z dostosowaniem do NIS2.

Jak duże środki będą potrzebne, by zapewnić zgodność z przepisami? EY w raporcie „Nowe obowiązki w cyberbezpieczeństwie – ryzyko nadregulacji” podawała w 2024 r., że inwestycja w system IT może kosztować od kilkudziesięciu tysięcy złotych (małe firmy) do milionów złotych (duże korporacje). A to niejeden koszt, bo trzeba też będzie np. przeprowadzić szkolenia pracowników.

Z drugiej strony obowiązek wdrożenia środków bezpieczeństwa cyfrowego przez kilkadziesiąt tysięcy podmiotów to wielka szansa dla rynku usług cyberbezpieczeństwa. Także firmy niewchodzące w skład KSC mogą stać się elementem tego łańcucha odpowiedzialności, gdy

kontrahenci-podmioty KSC zażądają od nich spełnienia określonych standardów bezpieczeństwa.

Do zrobienia będzie wiele: od wdrożenia systemów zarządzania bezpieczeństwem informacji, przez cykliczne audyty i usługi Security Operations Center (SOC), po szkolenia pracowników.

Już w 2025 r. wartość polskiego rynku cyberbezpieczeństwa wzrosła o 1/4, do ok. 3,5 mld zł (z 2,7 mld zł w 2024 r.) – szacowała firma PMR Market Experts by Hume’s. Z jej badania wynika, że dla prawie 2/3 przedsiębiorstw cyberbezpieczeństwo pozostaje kluczowym obszarem wydatków na IT. Według PMR w najbliższych latach ten rynek wciąż będzie szybko rósł, napędzany rosnącą liczbą zagrożeń, regulacjami oraz migracją firm do chmury.

Kluczowy punkt. Cyberbezpieczeństwo w strategii przedsiębiorstw

Cyfrizacja – uwzględniając lawinowo rosnącą liczbę incydentów w sieci – coraz wyraźniej kształtuje środowisko permanentnego ryzyka. Także biznesowego. Implikacja? Dbałość o cyberbezpieczeństwo stała się integralną częścią zarządzania strategicznego.

Czego dowiesz się z rozdziału?

- W jaki sposób cyberryzyko ewoluowało: z problemu technicznego do kategorii ryzyk strategicznych?
- Jak cyberincydenty przekładają się na wycenę rynkową firm, ich reputację oraz zaufanie interesariuszy, jak wpływają na ciągłość działania organizacji?
- Na czym w firmach polega strategiczne podejście do cyberobrony?
- Dlaczego traktowanie wydatków na cyberobronność jako klasycznego kosztu jest kardynalnym błędem?
- Jakie są dziś możliwości (i skutki) zawierania umów ubezpieczeniowych chroniących przed cyfrowym ryzykiem?

W ostatnich latach widać istotną zmianę w podejściu zarządów do cyberbezpieczeństwa: coraz częściej postrzegane jest ono jako ryzyko strategiczne, a nie wyłącznie operacyjne. Rosnąca liczba i coraz bardziej złożony charakter incydentów sprawiają, że zagrożenia związane z cyfrizacją procesów wpływają na wszystkie obszary działalności przedsiębiorstw.

Cyberzagrożenia mają zarazem wymiar systemowy, oddziałując nie tylko na pojedyncze organizacje, ale często na całe sektory gospodarki. W efekcie zarządzanie cyberryzykiem staje się integralnym elementem strategii przedsiębiorstw, które chcą być gotowe na nadchodzące wyzwania.

Eksperti cyberbezpieczeństwa przestrzegają, że pytanie, które powinna zadawać kadra zarządzająca, nie brzmi: „Czy moja firma zostanie zaatakowana?”, a raczej

„Kiedy moja firma padnie ofiarą cyberprzestępców?”.

Tegoroczna nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC) zmobilizuje menedżerów do zmian, ale i w praktyce nałoży na nich realną odpowiedzialność za zarządzanie cyfrowe, w tym konieczność szybkiego nadrobienia zaległości.

Powiązani i podatni: systemowe cyberryzyko

Ewa Piłat, Chief Information Security Officer w IATA (International Air Transport Association) i członkini Rady Programowej CYBERSEC Expo & Forum, przestrzega, że cyberryzyko coraz częściej ma charakter systemowy. Gospodarka opiera się bowiem na powiązanych ze sobą firmach, łańcuchach dostaw i usługach cyfrowych (o wpływie cyberbezpieczeństwa na łańcuchy dostaw bardziej „operacyjnie” i szczegółowo – z przykładami – piszemy w rozdziale IV).

– W praktyce problem jednej firmy może bardzo szybko przełożyć się na całą branżę, w tym na zwykłych konsumentów. Dobrym przykładem jest atak na United Natural Foods (UNFI) z ub.r. Firma ta jest jednym z największych dystrybutorów żywności w USA i obsługuje m.in. sieci sklepów. Po ataku ransomware doszło do poważnych zakłóceń całego łańcucha dostaw, co przełożyło się na niedostępność produktów w sklepach. Przykład UNFI pokazuje, że jedno naruszenie może mieć konsekwencje wykraczające daleko poza samą firmę – wpływając na rynek, partnerów i klientów jednocześnie – wskazuje.

Na fakt, że cyberzagrożenia plus brak spójnych procedur cyberbezpieczeństwa w firmach i instytucjach stanowią nierzadko realne ryzyko także dla całej gospodarki (oba nasilające się ryzyka implikują bezwzględną konieczność strategii i rozwiązań systemowych na poziomie państwa, gospodarki właśnie, ale i przedsiębiorstw), zwraca też uwagę Tomasz Pietrzyk, dyrektor techniczny w Palo Alto Networks w Europie Środkowo-Wschodniej.

– Brak odpowiednio wdrożonego i utrzymywanego przez organizacje systemu bezpieczeństwa wpływa na ten obraz, ponieważ większość incydentów nie wynika z zaawansowanych technik ataku, ale

z podstawowych, możliwych do uniknięcia luk bezpieczeństwa – zwraca uwagę ekspert.

I dodaje, że z danych zespołu badawczego Unit 42 w Palo Alto Networks wynika, że 87 proc. incydentów dotyczyło kilku „powierzchni ataku” (m.in. chmury, systemów lokalnych, SaaS i warstwy tożsamości): naruszenia rzadko mają charakter izolowany i szybko rozprzestrzeniają się w środowisku IT. W ok. 90 proc. przypadków kluczową rolę odgrywały tzw. preventable gaps, czyli możliwe do uniknięcia braki w zabezpieczeniach (jak błędy w konfiguracji, niewystarczająca kontrola dostępu, słabe procesy operacyjne).

– Oznacza to, że atakujący często nie musi przełamywać zabezpieczeń, lecz wykorzystuje braki w procedurach i organizacji pracy systemów IT. W efekcie pojedyncze niedociągnięcia przekładają się na incydenty bezpieczeństwa i zakłócenia, wykraczające często poza jedną organizację, wpływając na łańcuchy dostaw i stabilność kluczowych usług gospodarki – ocenia Tomasz Pietrzyk.

Prof. Dariusz Szostek, prof. WPiA UŚ, dyrektor Międzyuczelnianego Centrum Cyber Science, sędzia Trybunału Konstytucyjnego, członek Rady Programowej CYBERSEC EXPO & Forum, podkreśla, że infrastruktura krytyczna może zostać zniszczona i w sposób konwencjonalny, i poprzez ataki cyfrowe.

– Co za różnica – jeżeli chodzi o efekty – czy woda w wodociągu zostanie zatruta bądź zanieczyszczona konwencjonalnie, czy poprzez cyfrowe przesterowanie w procesie jej uzdatniania, czego próby obserwowaliśmy kilkakrotnie w zeszłym roku w Polsce? Czy też unieruchomienie elektrowni... W państwach rozwiniętych, gdzie gospodarka opiera się na dostępie do energii, nowoczesnej logistyce, produkcji i gdzie wykorzystywane są coraz bardziej skomplikowane algorytmy, kluczowe staje się cyberbezpieczeństwo, ale także uzależnienie technologiczne od innych państw. Coraz większe znaczenie ma autonomia i samodzielność cyfrowa państwa, co w Europie wreszcie zostało dostrzeżone – podsumowuje.

Cyberbrona jako koszt i inwestycja

W wielu organizacjach cyberbezpieczeństwo wciąż postrzegane jest jako koszt, a nie inwestycja. To skutkuje traktowaniem zabezpieczeń cyfrowych jak kolejnej pozycji

Ryzyko, niepokój – i co dalej?

- Ponad połowa małych firm w Polsce* nie przeprowadziła szkolenia pracowników dotyczącego cyberbezpieczeństwa.
- 78 proc. dużych organizacji i 18 proc. małych ma plan postępowania w razie incydentu.
- 30 proc. ankietowanych specjalistów ze wskazanych organizacji ryzyko cyberataku na swoją firmę oceniło jako „bardzo niskie”, a 41 proc. jako „raczej niskie”.

**Badanie na zlecenie Mastercard*

[10.2025 r. – 01.2026 r.; 300 osób odpowiedzialnych za cyberbezpieczeństwo w MŚP i dużych firmach w Polsce]



Krzysztof Dyl

wiceprezes Urzędu Komunikacji Elektronicznej

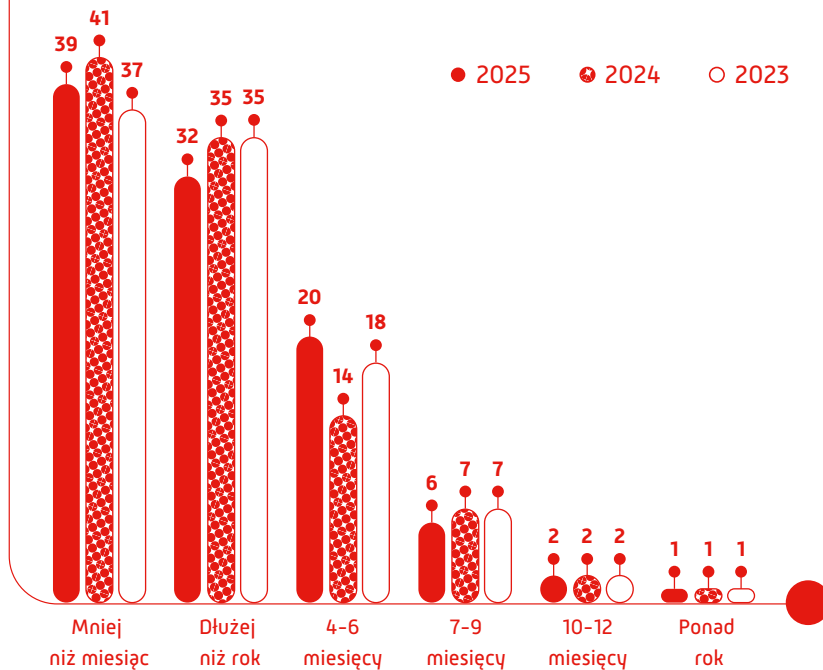
– Awaria sieci to nie tylko brak internetu w telefonie, ale paraliż usług, z których korzystamy bez zastanowienia. Nie wypłacimy pieniędzy z bankomatu, nie zapłacimy kartą w sklepie. Prawdopodobnie za parę dni część produktów nie pojawi się po prostu w sklepach. Dlatego odporność nie może być budowana osobno w każdym sektorze. Energetyka, telekomunikacja, bankowość, handel i administracja działają jak system naczyń połączonych. Regulacja oczywiście jest niezbędna, ale ona sama w sobie nie rozwiąże żadnego naszego problemu. Ćwiczenia, współpraca to są te elementy, na które ja bym położył największy nacisk.

Polska 2025. Ocena dojrzałości poszczególnych obszarów zabezpieczeń w organizacji



Źródło: Raport KPMG, Cyberodporność w erze zmian. Barometr Cyberbezpieczeństwa 2026 [dane za 2025 rok, publikacja marzec 2026]

Świat. Czas w organizacjach potrzebny na powrót do stanu sprzed cyberataku (w proc.)



Źródło: Raport Fortinet 2026 Global Cybersecurity Skills Gap (badanie: grudzień 2025, publikacja kwiecień 2026)

w budżecie IT, którą należy maksymalnie „odchudzić”. Na takie podejście kadry menedżerskiej rzutuje utrudnienie w wykazaniu „klasycznego” ROI (ang. Return on Investment – zwrot z inwestycji): wartość działań w cyberbezpieczeństwie najczęściej ujawnia się poprzez to, czego udaje się uniknąć: incydentów, kar regulacyjnych, procesów sądowych czy utraty reputacji.

W efekcie zarządy oraz departamenty ds. finansów często koncentrują się na minimalizacji wydatków, zamiast na strategicznym zarządzaniu ryzykiem i budowaniu odporności biznesu. Paradoks? Krótkoterminowe oszczędności często prowokują wielokrotnie wyższe koszty po poważnym incydencie – bezpośrednie (zatrzymanie produkcji/działalności operacyjnej, wypłaty odszkodowań, obsługa kryzysu organizacyjnie i wizerunkowo), jak i pośrednie (utrata zaufania klientów, spadek wartości firmy).

Dlatego coraz więcej ekspertów podkreśla konieczność zmiany perspektywy – na rzecz rozumienia bezpieczeństwa cyfrowego jako kluczowej inwestycji w ciągłość działania, przewagę konkurencyjną i długoterminowy wzrost organizacji.

Krzysztof Silicki, dyrektor ds. strategicznego rozwoju cyberbezpieczeństwa w NA-SK-PIB i członek rady programowej CYBERSEC Expo & Forum, podkreśla, że problem cyfrowych zagrożeń jest częścią ryzyka biznesowego, z którym ma do czynienia każda organizacja (nie tylko komercyjna).

– Nie zawsze jest to dobrze rozumiane. Często nakłady na cyberbezpieczeństwo traktowane są w podmiotach gospodarczych wyłącznie jako koszt. Zgadzam się, że niedostatki w cyberbezpieczeństwie w podmiotach z kluczowych czy ważnych sektorów stanowią systemowe ryzyko dla całej gospodarki. Dlatego nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa, implementując dyrektywę NIS 2, rozszerza zakres sektorów zobowiązanych do wdrażania bezpieczeństwa z wykorzystaniem analizy ryzyka, którą należy w przedsiębiorstwach prowadzić w sposób ciągły – akcentuje Silicki.

A zatem: cyberbezpieczeństwo jest zjawiskiem horyzontalnym; te same zagrożenia dotyczą większości sektorów, więc nie mówimy tu o silosowości – podkreśla Silicki. Każdy sektor może oczywiście dodatkowo zdefiniować zagadnienia specyficzne



Filip Kubiński

szef zespołu ds. bezpieczeństwa w Polsce w Accenture

– Takie sektory jak energetyka, finanse i telekomunikacja od dawna mają świadomość cyberzagrożeń i przygotowując się na walki z nimi, nie bawowały na regulacjach, tylko właśnie na ryzyku i zagrożeniach.

Pytanie, które powinna zadawać kadra zarządzająca, nie brzmi: „Czy moja firma zostanie zaatakowana?”, a raczej „Kiedy moja firma padnie ofiarą cyberprzestępców?”.



mł. insp. Wojciech Olszowy

komendant Centralnego Biura Zwalczania Cyberprzestępczości

– Jeśli chodzi o biuro do walki z cyberprzestępczością i wyzwania, które w tej chwili przed nami stoją, to jest parę płaszczyzn, na które należy zwrócić uwagę: sytuacja geopolityczna, szybkość rozwoju nowych technologii i transgraniczny charakter popełnianych czynów.

dla siebie, w tym np. musi powołać sektorowe CSIRT-y.

Od 2028 r. stale rozbudowywany system KSC działa horyzontalnie: podmioty z różnych sektorów mają takie same obowiązki w spełnianiu wymogów cyberbezpieczeństwa i reagowaniu na cyberincydenty. W niektórych sektorach, jak bankowość, rynki finansowe czy energia, powstają regulacje sektorowe, działające kompatybilnie z regulacjami horyzontalnymi.

Cel: zachować wartość przedsiębiorstwa

Incydenty cyberbezpieczeństwa mają bezpośredni i mierzalny wpływ na wartość przedsiębiorstwa. Reakcje rynku kapitałowego mogą prowadzić m.in. do zmiany kursów akcji. Jako się rzekło, naruszenie bezpieczeństwa danych wpływa też negatywnie na reputację organizacji i poziom zaufania interesariuszy i – rzecz jasna – stabilność pracy przedsiębiorstwa.

Wymowna ilustracja? Atak NotPetya w 2017 r. sparaliżował globalne operacje logistycznego giganta – firmy Maersk. Efektem była przerwa w działalności, zakłócenie łańcucha dostaw i konieczność odtworzenia systemów, co – według szacunków – miało kosztować firmę 250-300 mln dol.

– Dobrym przykładem jest historia Jaguar Land Rovera z września ub.r., gdzie w wyniku cyberataku firma była zmuszona całkowicie zatrzymać produkcję na kilka tygodni, a pracownicy zostali odesłani do domów. Zakłócenia objęły nie tylko samą firmę, ale też tysiące dostawców i partnerów biznesowych. Przypadek Jaguar Land Rovera pokazuje, jak rozpoznawalna marka może bardzo szybko stracić wiarygodność, jeśli nie jest w stanie zapewnić ciągłości działania i ochrony swoich systemów – wskazuje Ewa Piłat.

Marietta Gieroń, prezes zarządu Instytutu Kościuszki, przewodnicząca Rady Nadzorczej Polskiego Klastra Cyberbezpieczeństwa #CyberMadeInPoland i członkini rady programowej CYBERSEC Expo & Forum, potwierdza, że cyberbezpieczeństwo ma bezpośredni wpływ na wiarygodność firmy i poziom zaufania rynku, ale – według niej – nie oddziałuje jednak aż tak silnie, by wpływać np. na decyzje zakupowe klientów.

– Skuteczny atak, wyciek danych czy źle zarządzana komunikacja kryzysowa mogą

bardzo szybko przełożyć się na straty finansowe i wizerunkowe. Przykłady firm, takich jak Morele.net, ALAB czy Marriott, pokazują jednak, że – mimo dużego zainteresowania medialnego – konsumenci rzadko masowo rezygnują z usług firm po incydencie bezpieczeństwa; najczęściej reagują doraźnie, zmieniając hasła czy monitorując swoje dane – opowiada.

I dorzuca: w praktyce nadal często wygrywa wygoda, przyzwyczajenie lub brak alternatyw, dlatego kluczowe pozostaje budowanie świadomości społecznej i edukacja cyfrowa. Rynek coraz częściej ocenia przedsiębiorstwa oraz organizacje nie przez pryzmat tego, czy zostały zaatakowane, ale czy potrafią odpowiedzialnie zarządzać ryzykiem i reagować w sytuacji kryzysowej.

Zdaniem Gieroń, dopiero gdy konsumenci zaczną masowo i świadomie wybierać firmy, które realnie dbają o bezpieczeństwo danych i transparentnie zarządzają ryzykiem, to wtedy na rynku pojawi się prawdziwa presja, wymuszająca traktowanie cyberbezpieczeństwa jako strategicznego priorytetu biznesowego.

Zarządzanie ciągłością działania

Kluczowego znaczenia nabiera dziś integracja planów ciągłości działania z mechanizmami reakcji na incydenty oraz odbudowy systemów.

– Większość (organizacji – przyp. red.) ma procedury bezpieczeństwa informacji dzięki RODO; ok. 50 proc. ma procedury kryzysowe, ale bardzo mało organizacji przestrzega własnych procedur. Są też pozytywne przypadki: w 2024 r. w momencie incydentu jedna z dużych firm IT uruchomiła procedury i pracowała zgodnie z nimi przez cały czas – aż do przywrócenia pełnej sprawności organizacji. Zwykle jednak procedury są w... zaszyfrowanym SharePoincie – zdradza ekspert cyberbezpieczeństwa i członek rady programowej CYBERSEC Expo & Forum Maciej Broniarz.

Kluczowe jest zdefiniowanie krytycznych procesów IT, identyfikacja krytycznych zasobów, określenie stopnia zależności od dostawców oraz przygotowanie realnych scenariuszy działania w trybie awaryjnym, które pozwalają utrzymać kluczowe usługi nawet w czasie incydentu bezpieczeństwa.



Marcin Dudek

kierownik CERT Polska

– Jako CERT krajowy analizujemy incydent technicznie, pokazujemy, do jakich znanych wcześniej kampanii pasują obserwowane fakty i wskazujemy, jakie błędy popełniono, że taki atak był możliwy. Kto za tym stoi i dlaczego uderzył w tym momencie, to już jest rola służb.



Tomasz Chomicki

**dyrektor ds. rozwoju biznesu
w Samsung Electronics Polska**

– Właściciele firm lub osoby nimi zarządzające powinny zadbać o to, aby zasady cyberbezpieczeństwa zostały trwale wpisane w strategię organizacji. Skala działań cyberprzestępców jest dziś bezprecedensowa, dlatego cyberbezpieczeństwo musi być głównym filarem priorytetów każdej firmy.

*Krótkoterminowe
oszczędności w wydatkach
na cyberbezpieczeństwo
często prowokują wielokrotnie
wyższe koszty po poważnym
incydencie.*

Równie istotne jest regularne testowanie odporności w warunkach zbliżonych do rzeczywistych zdarzeń, segmentacja środowisk i stosowanie zasady ograniczonego zaufania „zero-trust” oraz poprawa zdolności do szybkiego wykrycia i powstrzymania ataku, zanim wpłynie on na kluczowe procesy biznesowe. W praktyce oznacza to przejście od samej „gotowości cybernetycznej” do budowania cyberodporności, czyli zdolności organizacji do ciągłości działania nawet w warunkach częściowej niedostępności systemów.

Krzysztof Silicki przypomina o jeszcze jednym aspekcie: scenariusze ryzyka to element nowoczesnego podejścia do zarządzania ryzykiem w szerszym ujęciu.

– Niezależnie od tego, czy jesteśmy małą organizacją bez wielkich zasobów do zajmowania się cyberbezpieczeństwem, czy też dużym podmiotem, który ma w pełni wdrożone normy bezpieczeństwa ISO, powinniśmy wyobrazić sobie scenariusze zagrożeń, które mogą być bolesne w skutkach, jeśli ryzyko się zmaterializuje. Te większe podmioty, mając wdrożony System Zarządzania Bezpieczeństwem Informacji, nie powinny się koncentrować wyłącznie na formalnym spełnieniu wymogów i tzw. compliance, lecz opracowywać właśnie scenariusze ryzyka, które będą dotyczyć konkretnie ich działalności, likwidować tzw. killchainy, analizować bezpieczeństwo łańcucha dostaw i ćwiczyć metody postępowania w przypadku wystąpienia sytuacji kryzysowych – stwierdza.

Tyle że życie uczy, że można formalnie spełniać normy, a i tak zostać zaskoczonym przez cyberincydenty...

– Mniejsze podmioty tym bardziej powinny „zainwestować” w scenariusze ryzyka, bo trudniej mikro- czy małym firmom przeznaczyć większe kwoty na cyberbezpieczeństwo, zbudować SOC czy CERT. Praca nad konkretnymi scenariuszami, które mogą najbardziej uderzyć w biznes podmiotu, po to, by się jak najlepiej zabezpieczyć, wydaje się dobrym podejściem przy zarządzaniu ryzykiem – wskazuje ekspert.

Budowa cyberodporności wymaga oczywiście kompleksowego podejścia, obejmującego nie tylko technologie, systemy i procesy organizacyjne, ale rozwój kompetencji pracowników. Nowoczesne rozwiązania



Artur Jóźefiak

wiceprezes Accenture w Polsce, szef Centrum Usług Cyberbezpieczeństwa dla Europy

– Cyberbezpieczeństwo wpływa na wartość organizacji na trzy sposoby: bezpośrednimi kosztami i przerwaniem ciągłości działania, zaufaniem oraz kosztem utraconego wzrostu. (...) Z badania Accenture „Cyber-Resilient CEO” wynika, że najbardziej odporne organizacje ponoszą koszty naruszeń od dwóch do trzech razy niższe niż konkurenci i jednocześnie osiągają lepsze wyniki biznesowe. Dlatego wartość dobrego stanu cyberbezpieczeństwa najlepiej mierzyć nie kosztem wdrożeń, lecz porównaniem ze scenariuszem skutecznego ataku, a tego, jak pokazuje WEF, nie można już dziś traktować jako mało prawdopodobnego.



prof. Dariusz Szostek

Wydział Prawa i Administracji Uniwersytetu Śląskiego, członek Rady Programowej CYBERSEC EXPO & Forum

– Powstała gospodarka cyfrowa, oparta na technologii funkcjonującej w przestrzeni cyfrowej, ale jednocześnie technologia cyfrowa mocno „zeszła” do tradycyjnej gospodarki, opartej na przemyśle, produkcji, handlu, nowoczesnej logistyce, a nawet rolnictwie. Współczesna gospodarka wymaga energii, ale także profesjonalnych systemów informatycznych, wspierających przedsiębiorstwa. Cyberbezpieczeństwo – obok energii – staje się kluczowym elementem mającym wpływ na gospodarkę państwa. (...) Jesteśmy w stanie „cyfrowej wojny” i nie bójmy się używać tego sformułowania.



Marietta Gieron

prezes zarządu, Instytut Kościuszki

– Pieniądze na inwestycje w cyberbezpieczeństwo są. Natomiast kluczem jest umieć wydać je efektywnie, a to wymaga świadomości. Sukcesu nie powinniśmy mierzyć tym, ile środków publicznych uda nam się pozyskać, tylko tym, jak uda nam się wyskalować biznes – zarówno na rynku polskim, jak i na zagranicznym.

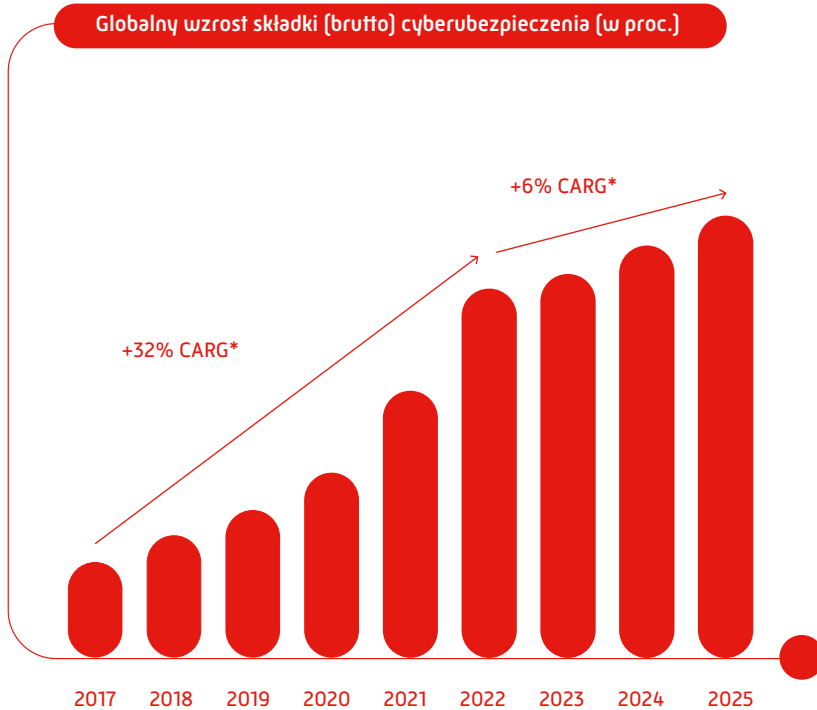


Zuzanna Wieczorek

prezes zarządu Techniska Polska Przemysłowe Systemy Transmisji Danych

– Koncepcja cyberobrony (w przemyśle - dop. red.) nie może być oparta na łataniu podatności na czas, bo to jest nierealne w dużej skali. Trzeba określić priorytety, skupić się na procesie, na tym, co jest krytyczne dla funkcjonowania firmy i to wbudować w ramy cyberbezpieczeństwa. Jeśli będziemy próbować zająć się wszystkim, to będzie paraliżujące.

Globalny wzrost składki (brutto) cyberbezpieczeństwa (w proc.)



*Skumulowany roczny wskaźnik wzrostu
Źródło: Swiss Re Cyber Data Lake, Market Reports

techniczne, jak systemy wykrywania zagrożeń czy zarządzania tożsamością stanowią istotny element ochrony, ale nigdy nie będą wystarczające, jeśli zawiedzie tzw. czynnik ludzki.

– Nawet najbardziej zaawansowane systemy i procedury nie zapewnią bezpieczeństwa bez dobrze przygotowanych specjalistów, świadomych zagrożeń i odpowiedzialnych za codzienne decyzje. Dlatego szkolenia, kultura bezpieczeństwa i kompetencje pracowników są równie istotne jak nowoczesna infrastruktura IT, spójne procesy oraz automatyzacja ochrony. To właśnie ich synergiczne połączenie decyduje dziś o realnej cyberodporności instytucji – ocenia rektor Politechniki Śląskiej prof. dr. hab. inż. Marek Pawełczyk (rolą „czynnika ludzkiego” obszerniej zajmujemy się w rozdziale IV).

Cyfrowa asekuracja – ekosystem usług

Cyberpolis powinny stanowić ważne uzupełnienie strategii zarządzania ryzykiem firm i organizacji, a wymagania stawiane

przez ubezpieczycieli wpływają na podnoszenie standardów bezpieczeństwa w organizacjach.

Na rozwój rynku „cyberasekuracji” istotny wpływ miały szeroko opisywane w mediach incydenty, w tym wspomniany już atak NotPetya (szacunkowo: globalnie straty na poziomie ok. 10 mld dol.). Notabene: amerykański gigant spożywczy Mondelez, który mierzył się ze skutkami NotPetya, pozwał szwajcarską firmę ubezpieczeniową Zurich Insurance za odmowę wypłaty odszkodowania (ostatecznie obie strony doszły do porozumienia).

Z kolei potentat farmaceutyczny Merck & Co (posiadał polisę „all risk”) szacował, że wspomniany atak kosztował go 1,4 mld dol. Kontrargumentem ubezpieczyciela było twierdzenie, że NotPetya rozpoczęła wojnę rosyjsko-ukraińską, zatem w tym przypadku ma zastosowanie klauzula wyłączenia obejmująca działania wojenne (z czym nie zgodziły się sądy niższej instancji)... I w tym razem strony zawarły w końcu porozumienie.



Piotr W. Zawadzki

ekspert w Dziale Zarządzania
Strategicznego, Narodowe Centrum
Badań i Rozwoju

– Z jednej strony chcemy, żeby państwo się nie wtrącało, żeby jego rola była minimalna. Ale też zdajemy się iść w stronę państwa opiekuńczego, które „przytuli” przedsiębiorcę, poradzi mu, zapewni pieniądze i wskaże kierunki działania. Musimy wypracować model. Powinniśmy firmom pomóc, ułatwić, zmienić przepisy, ale nie wyręczać w tym, co jest ich zadaniem w zakresie pozyskiwania dofinansowania.



Marianna Sidoroff

dyrektorka, Departament Gospodarki
Cyfrowej, Ministerstwo Rozwoju
i Technologii

– Zamówienia publiczne mogą być kołem zamachowym do tego, żeby nasze polskie firmy się rozwijały w zakresie cyber. Z jednej strony mamy wątek spółek Skarbu Państwa i wprowadzenia komponentu krajowego, a z drugiej strony jest jasno określona polityka zakupowa państwa, którą należy uzupełnić o kryteria suwerennościowe zakupu produktów i usług w postępowaniach IT.

Według szacunków Munich Re globalny rynek ubezpieczeń cybernetycznych wyniósł w 2025 r. prawie 15 mld dol.; do 2030 r. globalny wolumen składek wzrośnie do ok. 28 mld dol. To oznaczałoby średni roczny przyrost 15 proc. w latach 2020–2030.

– Rynek ubezpieczeń cyber w Polsce pozostaje relatywnie niewielki w porównaniu do tych bardziej dojrzałych – zachodnich, lecz jego dynamika wzrostu należy do najwyższych w sektorze ubezpieczeń majątkowych – wskazuje Sylwia Stańczyk, specjalistka ds. ubezpieczeń klientów strategicznych, TUW PZUW.

Jak dodaje, wartość tego rynku w naszym kraju można dziś oceniać na kilkaset milionów złotych rocznie – przy utrzymaniu stabilnego, dwucyfrowego tempa wzrostu, szacowanego na kilkanaście procent rok do roku.

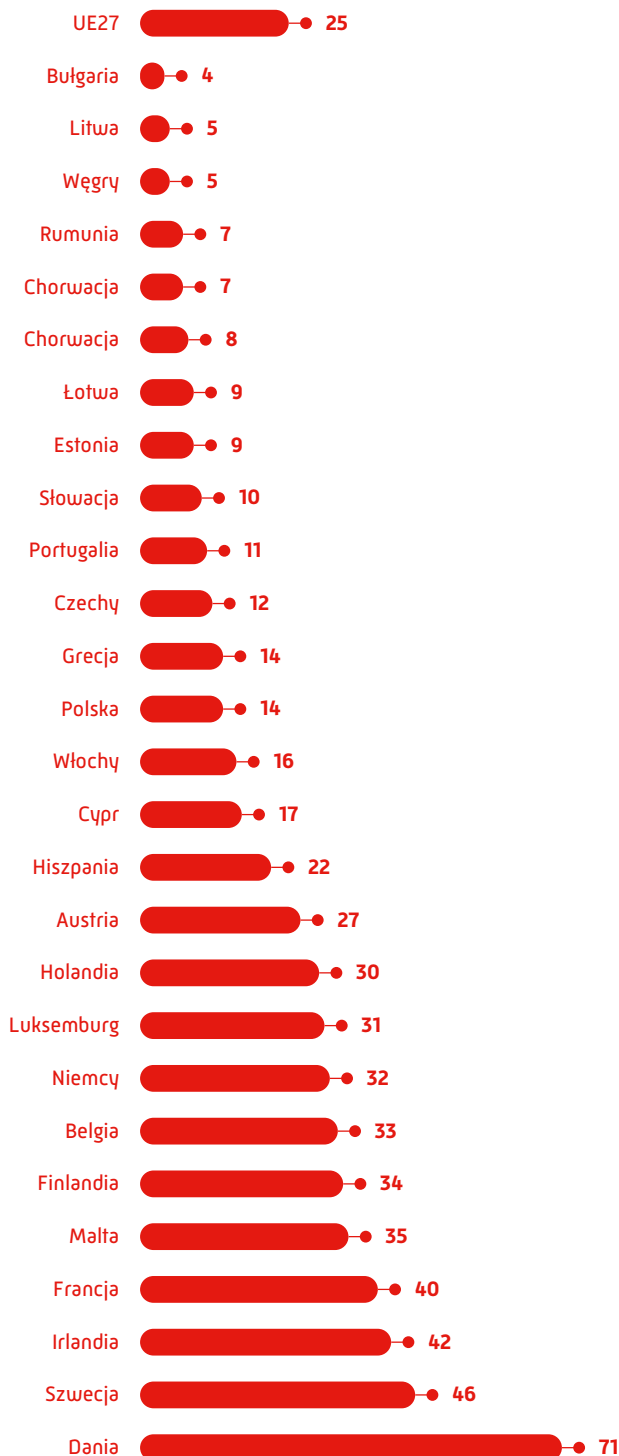
– W pierwszej fazie rozwoju – do ok. 2018 r. – rynek miał charakter marginalny i ograniczał się do największych podmiotów, głównie z sektora finansowego i międzynarodowych korporacji. Kolejne lata przyniosły wyraźne przyspieszenie, napędzane przez wdrożenie RODO, rosnącą skalę ataków ransomware oraz przyspieszoną cyfryzację po okresie pandemii – objaśnia.

Motywacja zawierania ubezpieczeniowych umów coraz silniej opiera się na świadomym i systemowym zarządzaniu ryzykiem; w najbliższych latach dodatkowym, istotnym impulsem rozwojowym będą regulacje takie jak dyrektywa NIS 2 oraz rozporządzenie DORA, które znacząco podnoszą wymagania w odporności cyfrowej organizacji i w praktyce wzmacniają rolę ubezpieczeń cyber jako integralnego elementu systemu zarządzania ryzykiem.

Według Sylwii Stańczyk współczesna oferta ubezpieczeń cyber wyraźnie wykracza już poza „klasyczne rozumienie polisy jako instrumentu wypłaty odszkodowania”. Coraz częściej przybiera formułę kompleksowego ekosystemu usług, który obejmuje zarówno komponenty finansowe, jak i operacyjne oraz doradcze wsparcie w zarządzaniu incydemem.

– Rynek ubezpieczeń cyber w Polsce znajduje się w punkcie zwrotnym. Z jednej strony dynamicznie rośnie, z drugiej – dojrzewa – ocenia Stańczyk.

Przedsiębiorstwa w krajach UE deklaruujące posiadanie ubezpieczenia przeciwko incydom cybernetycznym (w proc.)



Źródło: Raport VeloBanku „Ekonomiczne skutki cyberataków” [publikacja sierpień 2025]. Opracowanie VeloBank na bazie Eurostat

Kultura bezpieczeństwa. Przesłanki dla zarządów

– Na pytanie, czy zarządy dbają o cyberbezpieczeństwo i uwzględniają je w procesach zarządzania ryzykiem, można odpowiedzieć jednocześnie pozytywnie i negatywnie. Pozytywnie, bo podejście zarządów ewoluuje we właściwym kierunku, a stoją za tym regulacje takie jak NIS2 i nowelizacja ustawy o KSC, dotkliwe konsekwencje incydentów (jak choćby w przypadku Jaguar Land Rovera) oraz rosnąca świadomość niestabilności wynikającej z geopolityki i nowych technologii. A negatywnie, bo tempo tej zmiany jest nieadekwatne do tempa ewolucji zagrożeń, zwłaszcza dziś, gdy nowe modele AI wyraźnie zaburzają status quo w cyberbezpieczeństwie – mówi Artur Józefiak, wiceprezes Accenture w Polsce, szef Centrum Usług Cyberbezpieczeństwa dla Europy.

I dodaje, że przez ostatnie 20 lat ok. 95 proc. wydatków na cyber kierowano na prewencję: zabezpieczanie, wykrywanie i reagowanie, czyli unikanie szkód. Tymczasem wykorzystanie AI przez atakujących radykalnie zwiększa szybkość i skalę ataków, więc konieczne staje się budowanie dodatkowego rodzaju odporności, opartego na szybkim odtwarzaniu zdolności cyfrowych uszkodzonych wskutek skutecznego ataku.

– I właśnie zrozumienia tego na poziomie zarządów dziś zdecydowanie brakuje – uważa Józefiak.

Podsumowując: skuteczna strategia przedsiębiorstw przestała być jedynie kwestią technologicznych zabezpieczeń, a stała się fundamentem odporności organizacyjnej i warunkiem biznesowego sukcesu.

Krzepiące, że organizacje, świadome ryzyk, coraz powszechniej rozumieją, że strategiczne podejście do cyberobrony wymaga zintegrowania cyberbezpieczeństwa z celami biznesowymi, angażowania w ten proces wszystkich interesariuszy oraz budowania kultury bezpieczeństwa – i to na każdym poziomie działalności. ●



Łukasz Jędrzejczak

Cyber & Defense Sector Director, Deloitte Central Europe, były szef CSIRT MON, były zastępca Dowódcy Wojsk Obrony Cyberprzestrzeni ds. Cyberbezpieczeństwa

– Skuteczna strategia musi dziś wykraczać poza mury własnej organizacji, obejmując rygorystyczną kontrolę łańcucha dostaw oraz głęboką integrację z krajowym i międzynarodowym ekosystemem cyberbezpieczeństwa. W obliczu narastających zagrożeń hybrydowych kluczowe jest przejście od pasywnej ochrony do aktywnego budowania rezylencji, gdzie sztuczna inteligencja służy jako tarcza wzmacniająca ludzką percepcję, a nie ją zastępująca.



Grzegorz Wawryniuk

dyrektor Biura Produktu i Marketingu w EXATEL

– Bez infrastruktury telekomunikacyjnej, transmisji danych i bezpiecznej komunikacji, najlepiej kontrolowanej przez państwo, nie możemy mówić o cyberbezpieczeństwie i odporności kraju. To one spinają systemy administracji, energetyki, bankowości, logistyki i zarządzania kryzysowego. Jeśli przestaje działać komunikacja, państwo traci zdolność koordynacji.



Robert Posłajko

dyrektor marketingu i rozwoju w Axence Polska

– Strategia cyberochrony? Większość organizacji zaczyna od technologii, a powinna od podstaw: wiedzy, co chroni i kto za to odpowiada. Bez rzetelnej inwentaryzacji zasobów i przypisania odpowiedzialności nie ma mowy o realnej ciągłości działania. Dziś największym niedopatrzeniem nie są braki w systemach, tylko brak „backupu ludzi” – kompetencji, dostępów i decyzyjności w sytuacji kryzysowej. NIS2 jasno pokazuje, że odporność firmy to nie tylko infrastruktura, tylko zdolność organizacji do działania pod presją i szybkiego odtworzenia procesów.



prof. Jan Kozak

dyrektor, Sieć Badawcza Łukasiewicz – Instytut Sztucznej Inteligencji i Cyberbezpieczeństwa, Łukasiewicz – AI

– U nas nie mamy, niestety, certyfikacji urzędów, możemy je kupować skąd chcemy, z dowolnego państwa. Nie chcę stygmatyzować któregoś z kraju, bo to zarówno może być Zachód jak i Wschód. (...) Dyskutujemy o regulacjach dotyczących AI, ale rzadziej rozmawiamy o tym, jakie dane mogą być zbierane przez sam sprzęt.

Gospodarka i firmy. Cyfrowe ryzyko, realne straty

Zagrożenie cyfrowe nie jest abstrakcją ani symulacją, lecz realnym czynnikiem ryzyka rynkowego. Cyberbezpieczeństwo stało się warunkiem koniecznym działania współczesnej gospodarki. Jednak budowanie cyberodporności – firm, sektorów, infrastruktury – to nie sprint, lecz maraton. I to taki, w którym linia mety ciągle się oddala.

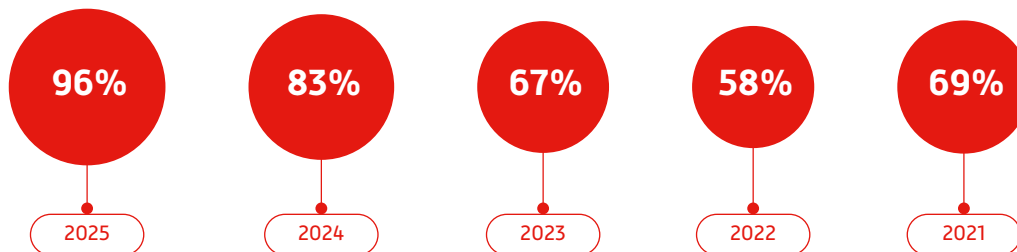
Czego dowiesz się z tego rozdziału

- Czy katastroficzne scenariusze unieruchomionej i zdezorganizowanej gospodarki mają odbicie w rzeczywistości?
- Jak cyberagresja wpływa na zaufanie między inwestorami, firmami i kontrahentami?
- Czym się objawia kaskadowość cyberataków? Jakie są tego skutki?
- Jaki jest związek między cyberbezpieczeństwem a gospodarczo-technologiczną suwerennością Europy?
- Jakich rozmiarów są kompetencyjne luki (liczba specjalistów) w cyberochronie u nas i gdzie indziej?

W grudniu 2025 r. analitycy Saxo Banku pierwszy raz uwzględnili Polskę w swoich eksperymentach, które nie są tradycyjnymi prognozami, lecz mają sprostować do myślenia. W zestawie „szokujących prognoz” (outrageous predictions) na rok 2026 znalazł się cyberatak na polską infrastrukturę energetyczną.

„Wczesną zimą złośliwy kod przenika do przemysłowych systemów sterowania, zmuszając operatorów do użycia awaryjnego odłączenia sieci, gdy ta przestaje reagować na polecenia” – opowiadał Aleksander Mrózek, VIP relationship manager z Saxo Banku, w serwisie internetowym firmy. – „Kraj się zatrzymuje. Fabryki, sektor finansowy i transport pogrążają się w ciemności”.

Polska. Przedsiębiorstwa, które zarejestrowały co najmniej jeden incydent bezpieczeństwa (w proc. ankietowanych firm)



Źródło: Raport KPMG Cyberodporność w erze zmian. Barometr Cyberbezpieczeństwa 2026 (dane za 2025 rok, publikacja marzec 2026)

Uwaga, to nie są ćwiczenia...

Gospodarka zamiera. Oprócz energetyki stają kopalnie, bankowość elektroniczna, giełda i przemysł ciężki. Zalamuje się transport, pustoszeją sklepowe magazyny.

Hipotetyczny blackout miałby trwać 72 godz. Straty gospodarcze przekroczyłyby pułap 80 mld zł. Notowania spółek energetycznych i wydobywczych spadłyby o 40-60 proc., a banków – o 15-25 proc.

Niedługo po publikacji tej rzeczywistości szokującej prognozy, 29 grudnia 2025 r., doszło do skoordynowanych cyberataków na polską elektrociepłownię zaopatrującą prawie 0,5 mln odbiorców, spółkę z sektora produkcyjnego oraz co najmniej 30 rozproszonych farm wiatrowych i fotowoltaicznych. Opinia publiczna dowiedziała się o tym 13 stycznia.

Blackoutu i jego ponurych konsekwencji na szczęście uniknęliśmy, bo ten gigatańc został odparty. Lekcja? Bardzo czytelna: zagrożenia cyfrowe to nie abstrakcja ani symulacja, lecz realny czynnik ryzyka rynkowego. Czy tego chcemy czy nie, cyberbezpieczeństwo stało się warunkiem koniecznym działania współczesnej gospodarki.

Bolesny cios w zaufanie

Gospodarka rynkowa opiera się na zaufaniu: między inwestorami, firmami, kontrahentami etc. Udany cyberatak może ten fundament ukruszyć w sposób trudny do naprawienia.

Z badania IBM wynika, że pełną sprawność po naruszeniu bezpieczeństwa danych odzyskało zaledwie 12 proc. organizacji.

Większości z nich (78 proc.) zajęło to ponad 100 dni, przy czym 35 proc. potrzebowało na to więcej niż 150 dni. Zaledwie 3 proc. podmiotów zdołało się podnieść po wycieku danych w czasie krótszym niż 50 dni (IBM Cost of a Data Breach Report 2024).

W opracowaniu przyjęto, że odzyskanie sprawności – oprócz przywrócenia normalnej działalności biznesowej w obszarach dotkniętych naruszeniem – obejmuje też m.in. odbudowę zaufania klientów i pracowników.

– Materializacja ryzyka związanego z technologiami informacyjnymi (ICT) może spowodować, że podmiot biznesowy zniknie z rynku. Przykładowo: skuteczny atak ransomware może sparaliżować organizację, spowodować utratę zaufania klientów – podkreśla Krzysztof Dąbrowski, dyrektor zarządzający Pionu Bezpieczeństwa Komisji Nadzoru Finansowego, w czasie Europejskiego Kongresu Gospodarczego w Katowicach (EEC) w kwietniu 2026 r.

Bankowość jest branżą, w której zaufanie odgrywa szczególnie istotną rolę. Jak stwierdził Krzysztof Dąbrowski, przepisy dotyczące odporności cyfrowej – przede wszystkim DORA i NIS2 – służą wzmocnieniu zaufania do objętych nimi firm i instytucji.

– Te regulacje kładą duży nacisk na odpowiedzialne uwzględnienie w zarządzaniu organizacją ryzyka w obszarze cyberbezpieczeństwa. To nie jest wymysł regulatorów, tylko próba nadążenia za rzeczywistością – zaznaczył.

– Z uwagi na rosnącą liczbę cyberataków, wycieków danych oraz nieuprawnionego

Coraz bardziej rozproszony polski system elektroenergetyczny, oparty na dziesiątkach tysięcy niezależnych instalacji, zwiększa podatność na cyberagresję, mnożąc cyfrowe punkty wejścia dla atakujących.



Dawid Zięcina

Technical Department Director,
DAGMA Bezpieczeństwo

– Największym wyzwaniem w tej chwili jest człowiek i to nie dotyczy tylko operatorów usług kluczowych. Osiem na dziesięć incydentów jest spowodowanych czynnikiem ludzkim. Wiele organizacji traktuje testy bezpieczeństwa jak obowiązek formalny. Tymczasem prawdziwą wartość daje dopiero sprawdzenie organizacji w warunkach zbliżonych do kryzysu. Taki cyberpoligon dla każdej firmy warto przeprowadzić i zobać, jak wtedy nasze mechanizmy w sposób praktyczny działają.

dostępu do nich firmy czują presję na intensyfikację aktywności w cyberbezpieczeństwie. Wszelkie incydenty w tym obszarze to nie tylko ryzyko kar pieniężnych, ale przede wszystkim utraty zaufania klientów i dobrego wizerunku – potwierdza, ale i przestrzega Michał Rykiert, chief technologist evangelist obszaru EMEA w firmie WEBCON, cytowany w niedawnym raporcie „Jak wzmocnić potencjał polskich firm. Biznes wobec presji demograficznej i globalnej konkurencji” autorstwa ING Banku Śląskiego i WNP Economic Trends.

A rzeczywistość stale przyspiesza. Jak poinformował na EEC dyrektor NASK-u Radosław Nielek, CSIRT NASK otrzymał w 2025 r. prawie 660 tys. zgłoszeń (tj. informacji o potencjalnym zagrożeniu w przestrzeni cyfrowej) i zarejestrował ponad 260 tys. incydentów (tj. potwierdzonych zdarzeń naruszających cyberbezpieczeństwo). Wzrost wobec roku 2024 wyniósł odpowiednio 10 proc. i 160 proc.

– Dziś dane nie są już tylko zasobem – są punktem ciężkości całego systemu. To na nich opiera się funkcjonowanie państwa, biznesu i nowych technologii, więc naturalne jest, że stają się też głównym celem ataków – akcentuje Radosław Nielek.

W tej sytuacji bezpieczeństwo danych staje się aktywnym każdej organizacji.

– Jeśli nie zabezpieczymy tego fundamentu, żadna rozmowa o rozwoju nie będzie miała realnego znaczenia – wskazuje dyrektor NASK-u.

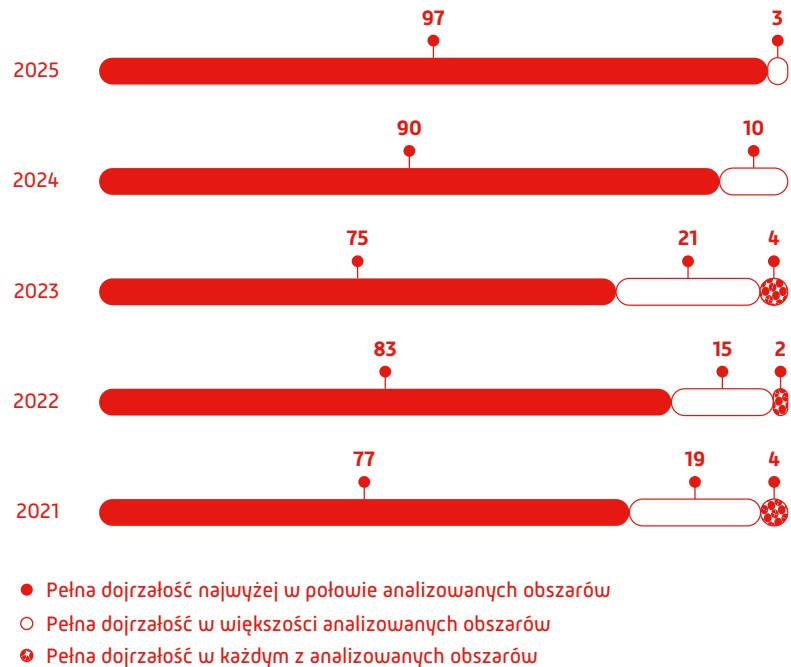
Kaskada niefortunnnych zdarzeń

Naruszenie bezpieczeństwa w kluczowym węźle infrastruktury może uruchomić efekt domina. To nie musi być nawet rozmyślny atak, wystarczy usterka lub zaniedbanie.

W lipcu 2024 r. błąd w aktualizacji oprogramowania firmy CrowdStrike Falcon spowodował awarię około 8,5 mln komputerów z systemem Windows na całym świecie: „niebieski ekran śmierci” (BSOD) zapętlili je w procesie restartowania.

Dotknięte błędem urządzenia nie stanowiły nawet 1 proc. komputerów z tym systemem operacyjnym, ale to wystarczyło, by uziemić samoloty, sparaliżować systemy obsługi pasażerów, uniemożliwić dostęp do dokumentacji medycznej, przerwać działanie bankomatów i giełd. Wszelkie przez plik konfiguracyjny jednej firmy!

Polska. Dojrzałość firm w zakresie cyberbezpieczeństwa



Źródło: Raport KPMG Cyberodporność w erze zmian. Barometr Cyberbezpieczeństwa 2026 (dane za 2025 rok, publikacja marzec 2026)

Niebezpieczeństwo reakcji kaskadowej dodatkowo podnosi poprzeczkę ryzyka w cyberprzestrzeni, gdzie wszystkie sektory są ze sobą powiązane.

– Odporność państwa to jest nie tylko siła armii, ale przede wszystkim odporność każdego pojedynczego sektora i umiejętność współpracy pomiędzy nimi. Finanse nie działają w próżni, zależą od energetyki, od telekomunikacji. Każdy inny sektor też współzależny od pozostałych – mówi Krzysztof Dąbrowski.

Ważnym aspektem tej współzależności są łańcuchy dostaw. Dlatego ich bezpieczeństwo należy do podstawowych wymogów regulacyjnych dotyczących cyberprzestrzeni.

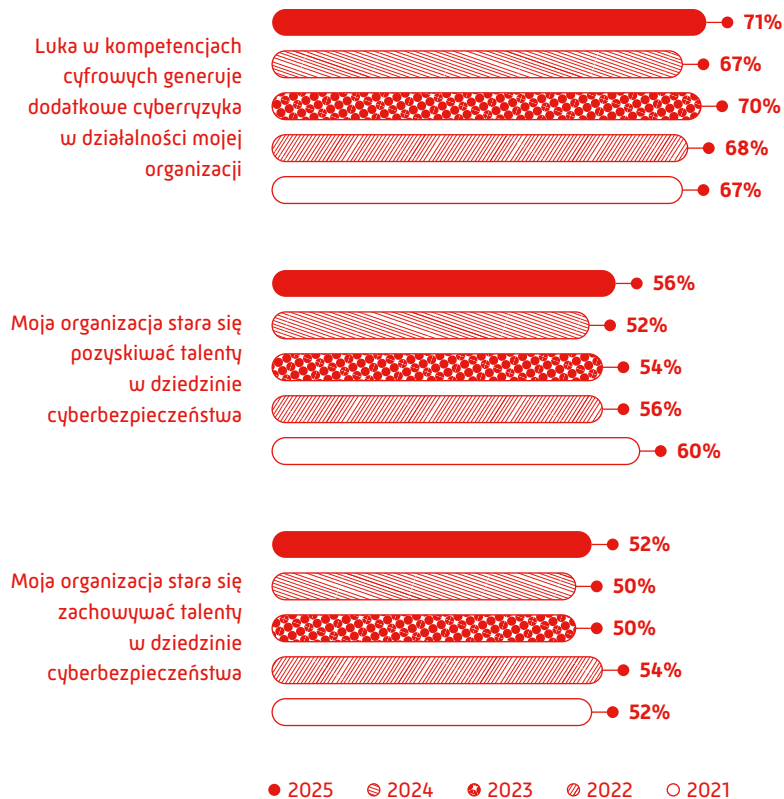
Jednym z trendów zdiagnozowanych przez podmioty krajowego systemu cyberbezpieczeństwa (KSC) w 2025 r. były właśnie uderzenia w łańcuchy dostaw (Supply Chain Attacks). Jak czytamy w sprawozdaniu Pełnomocnika Rządu do spraw Cyberbezpieczeństwa za zeszły rok: „dostrzegając rosnące koszty i trudności w atakowaniu dobrze chronionych



Mirosław Wróblewski
prezes Urzędu Ochrony Danych
Osobowych

– Wiele organizacji nadal próbuje ukrywać incydenty (z dziedziny cyberbezpieczeństwa – przyp. red). Zamiatanie problemów pod dywan nie działa. Informacje i tak prędzej czy później wychodzą na jaw, a konsekwencje bywają wtedy znacznie poważniejsze.

Wyzwania związane z brakiem (niedoborem) specjalistów od cyberbezpieczeństwa w organizacjach



Źródło: Raport Fortinet 2026 Global Cybersecurity Skills Gap [badanie: grudzień 2025, publikacja: kwiecień 2026]

podmiotów kluczowych, adversaries coraz częściej obierali za cel ich słabiej zabezpieczonych kontraktorów i dostawców usług zewnętrznych (IT/OT)”.
Łatwą „drogą wejścia” do dużych, lepiej bronionych organizacji, instytucji rządowych czy operatorów infrastruktury krytycznej może być np. serwisant urządzeń brzegowych, integrator usług cyfrowych lub firma kurierska. Wystarczy jedno słabe ogniwo w łańcuchu dostaw.

„Małe organizacje mogą posiadać znacząco mniej zasobów na ochronę cyberbezpieczeństwa, ograniczony dedykowany personel bezpieczeństwa informatycznego, przestarzałe oprogramowanie i sprzęt, nieadekwatne procedury tworzenia kopii zapasowych i niewystarczające szkolenia z zakresu świadomości bezpieczeństwa w porównaniu do dużych przedsiębiorstw czy instytucji rządowych” – stwierdził

CSIRT MON w sprawozdaniu za 2025 rok. Wykorzystywani w ten sposób dostawcy niekoniecznie nawet muszą zdawać sobie sprawę ze skali własnego negatywnego wpływu na funkcjonowanie ich klientów.

To wymusza zwiększoną czujność po stronie operatorów infrastruktury krytycznej i innych podmiotów KSC.

– Musimy audytować dostawców, a nie oczekiwać deklaracji zgodności z normami. To, że coś jest zgodne z normą, nie znaczy, że faktycznie nie ma podatności – podkreślał na EEC Krzysztof Drozdowski, członek zarządu i dyrektor ds. transformacji cyfrowej w spółce PKP Polskie Linie Kolejowe.

A jak z cyberbezpieczeństwem radzą sobie inne polskie firmy? Kilka przykładów.

– W przypadku biznesu Orlenu mówimy także o infrastrukturze krytycznej i fundamentalne znaczenie ma tu podejście



Mariusz Kujawski

prezes ComCERT (Grupa Asseco)

– W dzisiejszym świecie suwerenność technologiczna nie zawsze oznacza pełną kontrolę nad każdym elementem. Są produkty, których sami nie wytworzymy i których nie będziemy w stanie w pełni kontrolować. Dlatego suwerenność musi opierać się także na zaufaniu, dywersyfikacji i modelu multi-vendor (sposób działania firmy, w którym nie koncentruje się ona na jednym dostawcy technologii, usług lub produktów, tylko korzysta z kilku dostawców równolegle – przyp. red.).



Agnieszka Okońska

wiceprezeska PSE

– Robimy wszystko, co w naszej mocy, żeby być dobrze przygotowanym (mowa o cyberatakach – przyp. red.), ale byłabym daleka od tego, żeby zapewniać, że jesteśmy dobrze przygotowani do wszystkiego. Chyba nikt nie odważy się tego powiedzieć w dzisiejszym czasie... Na bieżąco reagujemy, na bieżąco doskonalimy nasze systemy i procedury, ale po drugiej stronie atakujący też cały czas się edukują i stają się coraz lepsi w tym, co robią.

do bezpieczeństwa. Bezpieczeństwo jest warunkiem koniecznym. Nasze zespoły cyberbezpieczeństwa uczestniczą niemal w każdym projekcie czy inicjatywie. (...) Każda technologia musi przejść rygorystyczną weryfikację bezpieczeństwa – podkreśla Magdalena Rempuszevska, dyrektor Biura Transformacji Cyfrowej i AI w Orlenie.

– W naszej firmie przez ostatnie 2-3 lata podjęliśmy w tej dziedzinie (cyberbezpieczeństwo – przyp. red.) wiele starań. Wprowadziliśmy nowe systemy bezpieczeństwa, intensywnie szkolimy też ludzi. Już kilka lat temu przeprowadziliśmy pierwszy audyt cyfrowego bezpieczeństwa firmy. Ale my jesteśmy dużą, giełdową spółką. W przypadku małych firm nie jest to natomiast takie łatwe ze względu na ograniczenia finansowe i kadrowe – ocenia Roch Jasiacek, dyrektor ds. IT w Grupie Kęty.

– Każde przedsiębiorstwo mówi, że podjęło „działania cyberobronne”. Ale praktyka wskazuje – zwłaszcza w sektorze MSP – że często mało skuteczne. Po prostu: gdy ktoś jeździ maluchem, to nie wygra morderczego, pełnego pułapek i niebezpieczeństw rajdu Paryż-Dakar. Dobrym rozwiązaniem ochronnym, niedostrzeganym jeszcze powszechnie w polskim biznesie, pozostaje np. chmura obliczeniowa – wskazuje Ireneusz Borowski, country manager Poland w Dassault Systèmes.

Tyłnymi drzwiami, przez boczną furtkę

Globalnym symbolem zagrożenia w łańcuchu dostaw stał się atak SolarWinds z 2020 r. Hakerzy umieścili złośliwy kod w aktualizacji legalnego oprogramowania do zarządzania sieciami. Tak zainfekowane oprogramowanie trafiło do 18 tys. organizacji na świecie, w tym do departamentów rządu USA. Nie włamano się do tych organizacji przez ich „główne cyfrowe drzwi”, lecz przez boczną furtkę – zaufanego dostawcę.

W analizie ryzyka, będącej częścią cytowanego sprawozdania pełnomocnika rządu ds. cyberbezpieczeństwa, stwierdzono m.in., że atakujący coraz częściej wykorzystują tę relację zaufania, uderzając w podmioty świadczące usługi dla administracji i operatorów infrastruktury krytycznej.

„Dodatkowym czynnikiem ryzyka jest rosnąca ekspozycja sektora energii na urządzenia pochodzące od dostawców spoza UE, przy ograniczonej możliwości weryfikacji ich bezpieczeństwa” – widnieje w przytoczonym sprawozdaniu pełnomocnika rządu.

O tym czynniku mówiła też Agnieszka Okońska, wiceprezeska Polskich Sieci Elektroenergetycznych.

– Do naszej elektroenergetyki, nie tylko polskiej, ale nawet europejskiej, wpuściliśmy przez wiele lat bardzo dużo urządzeń na różnym poziomie: dużych instalacji, mniejszych urządzeń, sterowników – co do których nie mamy pewności, czy nie zawierają jakichś backdoorów – podkreśliła. I dodała, że w PSE trwają prace nad sprawdzeniem poziomu bezpieczeństwa urządzeń, które już w sieci PSE działają.

Zagrożenie dotyczy wszystkich 18 sektorów objętych KSC, tj. podlegającym przepisom znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa. Przepisy te wprost nakładają na podmioty kluczowe i ważne obowiązki oceny bezpieczeństwa łańcucha dostaw ICT, co obejmuje weryfikację dostawców sprzętu, oprogramowania i usług cyfrowych pod kątem bezpieczeństwa. To zmiana „kulturowa”: dotychczas umowy z podwykonawcami koncentrowały się na cenie i dostępności.

Jeszcze większą rewolucję wzmacniającą bezpieczeństwo łańcucha dostaw jest wprowadzenie procedur oceny dostawców ICT w celu wykrycia i eliminacji rozwiązań od tzw. dostawców wysokiego ryzyka (DWR). W razie wydania przez ministra cyfryzacji decyzji o DWR, wszystkie podmioty KSC będą musiały wymienić objętą produktami i usługami ICT w ciągu 4-7 lat (zależnie od poziomu krytyczności sieci, w której się znajdują).

Długa droga do suwerenności

Autorzy sprawozdania Pełnomocnika Rządu ds. Cyberbezpieczeństwa za ubiegły rok podkreślają również, że „rosnąca zależność organizacji od zewnętrznych dostawców” – w tym usług chmurowych, telekomunikacyjnych, innych usług big techów – „przenosi koncentrację ryzyka poza bezpośrednią kontrolę podmiotów KSC”.

Raport Draghiego o konkurencyjności Unii Europejskiej z 2024 r. wskazuje, że



Małgorzata Domagała

VP i dyrektorka ds. produktów i rozwiązań Mastercard Europe na Polskę, Czechy i Słowację

– To właśnie pracownicy są pierwszym punktem, murem obronnym, tudzież murem otwierającym się przed cyberprzestępcami. Człowiek to najsłabsze ogniwo, ponieważ może być zaatakowany, może być zmanipulowany, może podlegać emocjom, może podlegać stresowi. Wydaje się, że najprostsze, co można zrobić, to wyedukować pracowników.

Gospodarka rynkowa opiera się na zaufaniu: między inwestorami, firmami, kontrahentami etc. Udany cyberatak może ten fundament ukruszyć w sposób trudny do naprawienia.



Maciej Broniarz

cyber incident response expert

– Kwoty okupu maleją, ale liczba incydentów rośnie. Grupy ransomware działają masowo i dostosowują okup do wielkości firmy.

Stary Kontynent jest zależny od nieeuropejskich rozwiązań technologicznych aż w 80 proc. W polskiej rzeczywistości ta zależność jest jeszcze wyraźniejsza. Zgodnie z raportem Fundacji InStrat z końca 2025 r. warunki niemal wszystkich (99 proc.) zamówień publicznych realnie wykluczają oprogramowanie biurowe innych producentów niż Microsoft.

Na gruncie cyberbezpieczeństwa oznacza to m.in. koncentrację ryzyka: jeśli pojawi się krytyczna podatność w oprogramowaniu tej firmy, uderzy ona jednocześnie w niemal całą administrację publiczną. Odpowiedzią na tę diagnozę ma być koncepcja suwerenności technologicznej. Na razie jednak przebija się ona raczej tylko w przemówieniach przedstawicieli rządu.

Stanisław Krzyżanowski, strategy and new business director w CloudFerro, zauważa w rozmowie z WNP, że choć polski sektor publiczny jest zależny od dostawców amerykańskich w stopniu większym niż w innych krajach Unii, to podejmuje „bardzo nieśmiałe próby budowania dla nich alternatywy”. Na kontynencie liderem takiej „emancypacji” jest Francja.

– Polska administracja centralna i idąca za nią samorządowa zachowują się tak, jakby nie widziały w tym problemu – stwierdza Krzyżanowski.

O ile wykorzystywane w Polsce i Europie rozwiązania chmurowe pochodzą przede wszystkim od amerykańskich big techów, o tyle sieci telekomunikacyjne przez lata bazowały głównie na chińskim sprzęcie. Co do tej ostatniej zależności technologicznej UE podejmuje śmielsze kroki.

– Mamy rekomendację, aby zachęcić państwa członkowskie do wykluczenia Huawei i ZTE z grona dostawców dla europejskich operatorów telekomunikacyjnych – mówił w maju rzecznik prasowy Komisji Europejskiej Thomas Regnier. Niektóre państwa członkowskie zrobiły to już zresztą wcześniej.

– Suwerenność to w dzisiejszych czasach jeden z najważniejszych czynników, jakie powinny wpływać na decyzje w obszarze IT, szczególnie w dużych organizacjach. Musimy dziś jako Europa myśleć o suwerennych rozwiązaniach oraz zabezpieczeniu łańcucha dostaw – przekonuje

Grzegorz Soczewka, wiceprezes ds. sprzedaży CEE w OVHcloud.

Infrastruktura. Na froncie cyberwojny

Grudniowy atak na polską energetykę skupił uwagę na tym sektorze.

– Robimy wszystko, co w naszej mocy, żeby być dobrze przygotowanym, ale byłabym daleka od tego, żeby zapewniać, że jesteśmy dobrze przygotowani do wszystkiego – mówiła w kwietniu Agnieszka Okońska, wiceprezesa PSE.

– Chyba nikt nie odważy się tego powiedzieć w dzisiejszym czasie. Na bieżąco reagujemy, na bieżąco doskonalimy nasze systemy i procedury, ale po drugiej stronie atakujący też cały czas się edukują i stają się coraz lepsi w tym, co robią.

Dziś trudno wątpić, że infrastruktura krytyczna – m.in. energetyczna, transportowa i finansowa – jest pierwszą linią frontu cyberwojny.

Prezes PSE Grzegorz Onichimowski w styczniu zapewniał, że do blackoutu w opisywanej na początku tego tekstu sytuacji było daleko.

– System elektroenergetyczny, jako infrastruktura krytyczna, nie był zagrożony – wyjaśniał.

Marcin Dudek, szef CERT Polska, przestrzega jednak przed ogólnym bagatelizowaniem cyberzagrożeń w energetyce. Fakt, tym razem hakerzy nie doprowadzili do blackoutu. Elektrociepłownia (wchodzi w skład KSC) była dobrze przygotowana, bo jej systemy wykrywały podejrzaną zdarzenia już w marcu i kwietniu 2025 r.

– Nie oznacza to jednak, że taki scenariusz jest niemożliwy, bo gdyby udało się przejąć wystarczającą liczbę obiektów, efekty mogłyby być bardzo poważne – przestrzega Dudek.

To spektakularne wydarzenie uwypukliło też paradoks polskiej transformacji energetycznej. Budując system coraz bardziej rozproszony, oparty na dziesiątkach tysięcy niezależnych instalacji OZE, Polska zwiększa odporność na jednorazowe awarie fizyczne, ale zarazem mnoży cyfrowe punkty wejścia dla atakujących.

– Mówimy o setkach czy tysiącach instalacji: farmach wiatrowych, fotowoltaicznych – należących do setek małych spółek. Większość z nich nie podlega żadnym



Magdalena Korona

ekspertka ds. cyberbezpieczeństwa
w mBanku

– Bankom bardzo by pomogło, gdybyśmy mogli w celach bezpieczeństwa sięgnąć do rzeczywistej lokalizacji klienta. Prawo nam jednak na to nie pozwala. Klient musi się zgodzić, żebyśmy z powodów bezpieczeństwa sięgnęli po jego lokalizację – i często ma z tym kłopot. Tak że, chcąc go chronić, chcielibyśmy móc korzystać z dodatkowych danych, które moglibyśmy na przykład pobrać z przeglądarki czy z aplikacji (te same dane są dostarczane np. mediom społecznościowym i z tym klienci nie mają problemu).

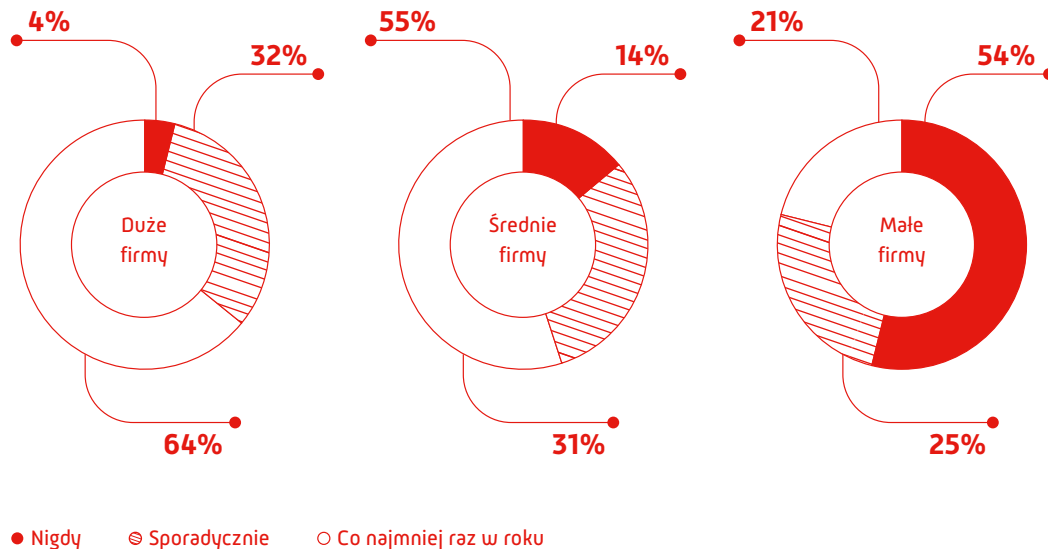


Ireneusz Jazownik

Chief Information Security Officer
w IBK Bank Polska

– Polski system bankowy jest bardzo ściśle związany z zewnętrznymi dostawcami technologii, co stanowi duże zagrożenie, biorąc pod uwagę to, że niewielki cyberatak może spowodować efekt domina w usługach chmurowych czy wśród dostawców telekomunikacyjnych.

Polska. Jak organizacje podchodzą do edukacji i szkoleń pracowników?



Źródło: Cyberbezpieczeństwo w polskich firmach (Minds & Roses dla Mastercard, październik 2025 r. – styczeń 2026 r., publikacja marzec 2026).

realnym obowiązkom w zakresie cyberbezpieczeństwa – podkreśla szef CERT Polska.

Mała farma wiatrowa, nieobjęta wymogami KSC, przeważnie ma niski poziom zabezpieczeń: nieaktualizowane urządzenia brzegowe, brak segmentacji sieci, domyślne hasła na urządzeniach sterujących.

– Każda taka farma osobno to „tylko” kilkanaście megawatów, więc w regulacjach wygląda na mały podmiot. Problem w tym, że gdy wiele takich źródeł zostanie wyłączonych jednocześnie, to ich wpływ na system może być bardzo znaczący – ostrzega Marcin Dudek.

Dywersja analogowa i cyfrowa

Polska kolej jest dość ciekawą częścią infrastruktury krytycznej, gdyż jej podatności mają charakter zarówno cyfrowy, jak i całkowicie analogowy.

Latem 2023 r. kilkanaście pociągów zatrzymało się na trasach w różnych regionach Polski. Nie spowodowało tego włamanie do żadnego systemu komputerowego. Sprawcy wykorzystali analogowy system Radio-Stop, wprowadzony pod koniec lat 80. XX w., który umożliwia zatrzymanie pociągu przez wciśnięcie przycisku alarmowego w radiotelefonie.

W styczniu 2025 r. internetowy system sprzedaży biletów PKP Intercity został zaatakowany metodą DDoS (Distributed Denial of Service): 100 mln prób wejścia do serwisu w ciągu jednej godziny mogło go rozłożyć na łopatki. System się temu oparł (na granicy wydolności), ale groźba paraliżu sprzedaży, chaosu informacyjnego i utraty zaufania pasażerów była całkiem realna.

Krzysztof Drozdowski z PKP PLK podczas EEC 2026 przyznał, że osoby czy grupy, którym zależy, by wprowadzić destabilizację, mogą wykorzystać jakąś podatność i zaatakować kolejowe systemy IT, częściowo „oślepiając” przewoźnika i paraliżując ruch pociągów.

– Na szczęście na kolei ten paraliż jest krótkotrwały, ponieważ mamy procedury czy to telefonicznego zapowiadania pociągów, czy to zabezpieczenia infrastruktury fizycznej – czyli rozjazdów kolejowych – na konkretny kierunek – zaznaczył.

Zapewnił też, że nawet gdyby skuteczny atak cybernetyczny „położył” większość kolejowych systemów, to kolej nie zostanie całkiem sparaliżowana: transport priorytetowy w takiej sytuacji będzie realizowany.



Iwona Prószyńska

kierownik zespołu ds. strategicznej komunikacji cyberbezpieczeństwa, NASK

– Z perspektywy obsługi incydentów widać wyraźnie, że CISO rozumie zarówno techniczny wymiar zdarzenia, jak i jego konsekwencje biznesowe. To często ta osoba, która wspiera transparentną komunikację w sytuacjach kryzysowych. Zarządy z kolei naturalnie dążą do ograniczania negatywnego przekazu, czasem próbując przedstawiać incydent jako awarię. To zrozumiałe z biznesowego punktu widzenia, ale w dłuższej perspektywie brak transparentności może prowadzić do większych strat wizerunkowych.

– Zazwyczaj mówimy tutaj o priorytetowym transporcie techniki wojskowej czy też o ewakuacji ludności. Kolej będzie gotowa, żeby taki transport realizować. Będzie to duża komplikacja, ale nie dojdzie do blackoutu. Trzeba będzie po prostu wykonać pewne działania i do tego jesteśmy przygotowani – zadeklarował Krzysztof Drozdowski.

Finansowe twierdze, fałszywe inwestycje

Największą pewność w zabezpieczeniach w infrastrukturze krytycznej przejawia sektor finansowy. Jak potwierdził Krzysztof Dąbrowski z KNF, ta branża pod względem cyberbezpieczeństwa plasuje się w krajowej czołówce.

– Efektem ubocznym tego, że duże podmioty finansowe, zwłaszcza banki, trudno skutecznie zaatakować, jest to, że cyberprzestępcy atakują głównie klientów. Tam – przy lepszej relacji nakładu do efektu – można uzyskać zwrot z „przestępczej inwestycji” – zaznacza.

Zamiast oblegać cyfrowe twierdze banków, cyberprzestępcy uciekają się zatem do „inżynierii społecznej”, phishingu i nęcenia ludzi fałszywymi inwestycjami. Rok 2025 był rekordowy pod względem liczby oszustw finansowych w polskim internecie.

– Świadomość użytkowników mediów społecznościowych jest wyższa, ale przestępcy dostosowali się i coraz częściej atakują te same ofiary ponownie, wykorzystując tzw. recovery scam – opowiada Karol Paciorek, kierownik CSIRT KNF.

Najpierw oszuści łowią ludzi na reklamy fałszywych inwestycji. Drugi raz naciągają ich, podszywając się pod kancelarie prawne czy firmy windykacyjne, specjalizujące się w odzyskiwaniu pieniędzy po oszustwach inwestycyjnych.

Nasz rozmówca dodaje, że fałszywe inwestycje są dla przestępców tym atrakcyjniejsze, że można je w całości przeprowadzić w ramach jednej platformy społecznościowej (np. na Facebooku).

– Nie trzeba już rejestrować domen ani kupować hostingu, co eliminuje ryzyko deanonimizacji poprzez dane rejestracyjne czy płatności za serwer – podkreśla Karol Paciorek.

Jego zdaniem możliwości i funkcjonalności samych platform społecznościowych

wręcz sprzyjają budowaniu takiej przestępczej infrastruktury.

Szef CSIRT KNF przyznał także, że walka z tym procederem jest bardzo trudna. Przestępcy coraz lepiej maskują fałszywe treści przed automatami wykrywającymi scam i przed doświadczonymi analitykami. Szybko też podnoszą się po każdej wpadce.

– To przypomina walkę z hydrą – odetniemy jedną głowę, pojawiają się trzy albo cztery nowe – porównuje Karol Paciorek.

Wakaty plus edukacyjna pustynia

– Na cyfrowej wojnie cywil łatwo zginie, jeżeli nie będzie miał świadomości. Każdy z nas, klikając w link, może być właśnie tym słabym ogniwem – ostrzegał wicepremier i minister cyfryzacji Krzysztof Gawkowski podczas EEC 2026.

Luka kompetencyjna pozostaje ogromnym wyzwaniem dla rozwoju cyberodporności. W Polsce brakuje zarówno zawodowych specjalistów, jak i podstawowej wiedzy o cyberbezpieczeństwie na co dzień.

Jeśli chodzi o zatrudnienie fachowców w tej dziedzinie, to globalna luka – według raportu Fortinet „2026 Global Cybersecurity Skills Gap” – może sięgać 4,8 mln specjalistów. Dla Polski brak aktualnych danych, ale podczas Forum Współpracy Edukacji i Biznesu EDUMIXER w październiku 2023 r. szacowano, że brakuje ponad 10 tys. specjalistów od cyberbezpieczeństwa.

Zgodnie z Cisco Cybersecurity Readiness Index 2025 ponad trzy czwarte (79 proc.) polskich firm wskazuje niedobór fachowców tego rodzaju jako główne wyzwanie, a przeszło połowa ma wakaty oceniane na ponad 10 proc. stanowisk związanych z bezpieczeństwem.

– Wiele firm nie ma po prostu możliwości zatrudnienia dedykowanego specjalisty od spraw bezpieczeństwa cybernetycznego i stąd wiedza o podstawowych elementach, które powinny być w ramach struktury IT dostarczane, jest trochę fragmentaryczna, a może i całkowicie nieobecna – ocenia Mateusz Majewski, IT&Digital Director w Grupie Saint-Gobain w Polsce.

Karol Paciorek w marcu 2026 r. mówił WNP, że znalezienie specjalisty od cyberbezpieczeństwa było trudne już trzy lata temu – „i jest bardzo trudne także dziś”.



Krzysztof Drozdowski

członek zarządu i dyrektor ds. transformacji cyfrowej w spółce PKP Polskie Linie Kolejowe

– Musimy audytować dostawców, a nie oczekiwać deklaracji zgodności z normami. To, że coś jest zgodne z normą, nie znaczy, że faktycznie nie ma podatności.

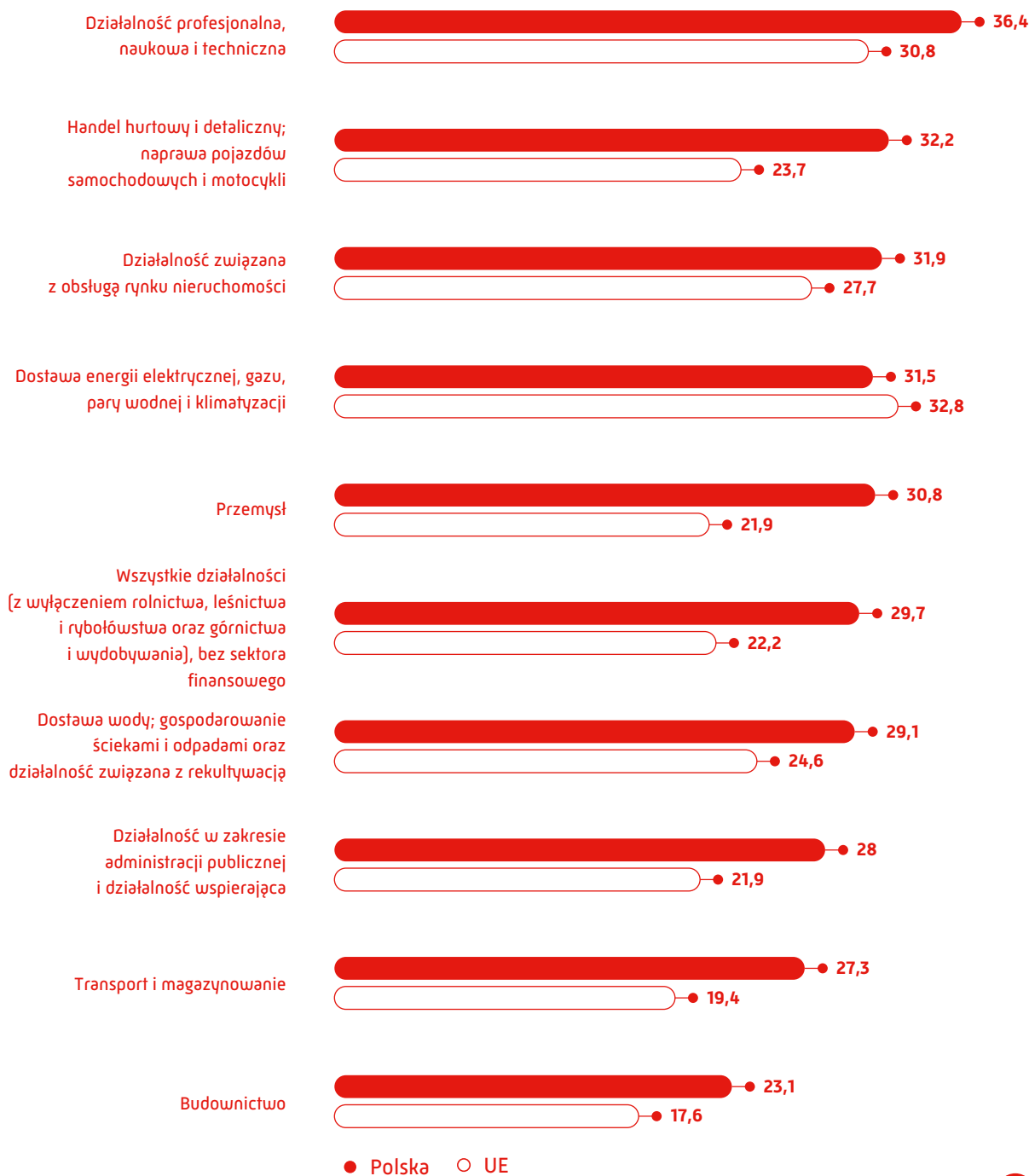


Joanna Klepacka

Key Account Manager, BTC

– Cyberodporność wymaga dziś połączenia technologii, procesów i świadomości pracowników. Coraz większe znaczenie mają ciągły monitoring, ochrona danych oraz przygotowanie do wymagań dyrektywy NIS2. Rozwiązania klasy DLP skutecznie ograniczają ryzyko wycieku informacji i wzmacniają bezpieczeństwo organizacji.

UE i Polska. Odsetek firm zgłaszających incydent cyberbezpieczeństwa - według branż (w proc.)



Źródło: Raport VeloBanku „Ekonomiczne skutki cyberataków” (publikacja sierpień 2025); opracowanie VeloBank na bazie Eurostat

Te kłopoty zaczynają już dotyczyć kilku-dziesięciu tysięcy podmiotów, które „przed chwilą” weszły w skład KSC.

Czy fachowców zacznie przybywać? Jaskółką jest zawód technika cyberbezpieczeństwa, który po wakacjach pojawi się w systemie edukacji branżowej. Ale jak się to kształcenie rozwinie, trudno przewidzieć... Barierą jest brak nauczycieli i sprzętu.

W szkolnictwie wyższym sytuacja jest natomiast lepsza niż kilka lat temu. Kierunek cyberbezpieczeństwo prowadzi już co najmniej 11 uczelni, w tym Politechnika Warszawska i AGH.

Paradoksalnie jednak nawet odczuwając brak specjalistów, firmy zaniedbują podstawową komunikację na temat cyberbezpieczeństwa. Na przykład jedynie 24 proc. dużych i poniżej jednej piątej małych i średnich (odpowiednio 19 proc. i 18 proc.) przedsiębiorstw poinformowało swoich pracowników o cyberataku i poinstruowało ich, co powinni zrobić w podobnej sytuacji w przyszłości (dane z badania cyberbezpieczeństwa w polskich firmach przeprowadzonego przez agencję Minds & Roses na zlecenie Mastercard w okresie od października 2025 r. do stycznia 2026 r.).

Profilaktyka od szkolnej ławy

Przytoczone badanie wskazuje też, że 54 proc. firm nigdy nie przeprowadziło szkolenia pracowników z cyberbezpieczeństwa. W grupie dużych organizacji proporcje są lepsze: 64 proc. z nich robi cyberszkolenia co najmniej raz w roku.

– To są porażające wyniki, jeżeli weźmiemy pod uwagę, że to właśnie pracownicy są tym pierwszym punktem, murem obronnym, tudzież murem otwierającym się przed cyberprzestępcami – podkreśliła, prezentując te wyniki, Małgorzata Domagała, VP i dyrektorka ds. produktów i rozwiązań Mastercard Europe na Polskę, Czechy i Słowację. – Człowiek to najsłabsze ogniwo, ponieważ może być zaatakowany, może być zmanipulowany, może podlegać emocjom, stresowi. Wydaje się, że najprostsze, co można zrobić, to wyedukować pracowników.

– W Amice podchodzimy do problemu bardzo poważnie, czego dowodem są regularne inwestycje w cyberbezpieczeństwo. Pamiętamy także o aspekcie, o którym wiele firm zapomina – obok systemów ochrony równie ważna jest edukacja pracowników.

Nasz system szkoleń jest skonstruowany tak, że przechodzi je każdy, łącznie z członkami zarządu – opowiada Paweł Biel, wiceprezes zarządu firmy Amica.

W edukacyjnej profilaktyce dotyczącej szeroko rozumianego cyberbezpieczeństwa państwo może odgrywać szczególną rolę i to w dwóch aspektach.

– O ile państwo polskie powołało jednostki do walki z atakami hakerskimi, o tyle powszechnie nie ma odczucia, ba, nawet wiedzy o tym, że ktoś nas chroni. (...) Tak jak kiedyś mówiliśmy o profilaktyce mycia zębów, tak dziś musimy mówić o profilaktyce cyfrowej – jak zabezpieczyć się przed cyberatakami, co zrobić w razie incydentu, jaka jest rola państwa i jakie wsparcie jest dostępne dla firm – precyzuje Artur Pollak, prezes zarządu APA Group.

– Rozwiązań powodujących znaczne podniesienie poziomu cyberobrony jest mnóstwo. Państwo powinno tu o wiele silniej, skuteczniej edukować: mocno je promować, zachęcać do cyberbezpieczeństwa. I to do profilaktyki, a nie do dominującego dziś motoru podnoszenia cyberodporności, czyli nauki na – niekiedy dotkliwych – własnych błędach – mówi Ireneusz Borowski, country manager Poland w Dassault Systèmes.

Równie oczywistym – i powszechnym – rozwiązaniem wydaje się włączenie podstaw cyberbezpieczeństwa do edukacji szkolnej. Ale i tu posuwamy się do przodu drobnymi krokami. Na razie ta kwestia pojawia się w podstawach programowych tylko pomocniczo, wpleciona w „edukację dla bezpieczeństwa” w liceach.

Mamy zatem jeszcze dużo do zrobienia. Budowanie cyberodporności to nie sprint, lecz maraton. I to taki, w którym linia mety ciągle się oddala. ●



Krzysztof Dąbrowski

dyrektor zarządzający Pionu
Bezpieczeństwa Komisji Nadzoru
Finansowego

– DORA i NIS2 – te regulacje kładą duży nacisk na odpowiednie uwzględnienie w zarządzaniu organizacją ryzyka w obszarze cyberbezpieczeństwa. To nie jest wymysł regulatorów, tylko próba nadążenia za rzeczywistością.



Joanna Karczevska

audytor SI, ekspert
ds. cyberbezpieczeństwa i ochrony
danych osobowych

– Największym zagrożeniem związanym z wykorzystaniem sztucznej inteligencji nie jest sam algorytm, lecz niewiedza jego użytkowników. W wielu organizacjach pracownicy korzystają z narzędzi AI bez świadomości konsekwencji związanych z przekazywaniem danych, ochroną informacji czy odpowiedzialnością za podejmowane decyzje. To właśnie luka kompetencyjna staje się dziś jednym z najpoważniejszych źródeł ryzyka.

Do zadań cyfrowych. Niewidzialni wojownicy

Cyberprzestrzeń – NATO traktuje ją na równi z lądem, morzem, powietrzem i przestrzenią kosmiczną. Polska – w odpowiedzi na eskalację ataków, ale też profilaktycznie – zbudowała jeden z najbardziej zaawansowanych komponentów cyberobrony w Sojuszu.

Czego dowiesz się z tego rozdziału?

- Jak polskie wojsko jest przygotowane do zwalczania cyberagresji? Co z kadrami?
- Jaka jest skala cyberataków wymierzonych w struktury i systemy państwa. Kto i w jaki sposób nas atakuje?
- Jakie wewnętrzne i zewnętrzne sojusze zawiera nasza cyberarmia w celu skutecznej neutralizacji zagrożeń?
- Wojska Obrony Terytorialnej a cyberbezpieczeństwo – czego się tu możemy spodziewać?

Ataki na infrastrukturę krytyczną, wykradanie danych, dezinformacja i zakłócanie systemów dowodzenia przeciwnika stanowią dziś standardowy zestaw narzędzi wojskowych. Te procedury mogą sparaliżować funkcjonowanie państwa.

– Myślę, że Polska jako członek NATO jest mniej narażona na atak w ujęciu konwencjonalnym niż na wojnę w cyberprzestrzeni – uważa Władysław Kosiniak-Kamysz, wicepremier i minister obrony narodowej.

Decyzja Sojuszu Północnoatlantyckiego z 2016 r. potwierdzająca, że cyberprzestrzeń też jest domeną operacyjną, pociągnęła za sobą konieczność utworzenia osobnych jednostek zajmujących się cyberbezpieczeństwem.

Na początku lutego 2022 r. – na podstawie Ustawy o obronie Ojczyzny i na fundamencie Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni – powstały

Wojska Obrony Cyberprzestrzeni (WOC). Pierwszym dowódcą został gen. dyw. Karol Molenda.

W strukturze cyberwojsk (zadania: bezpieczeństwo teleinformatyczne resortu obrony, rozwój technologii kryptologicznych, budowa systemów IT oraz badania i projekty rozwojowe) znajdują się jednostki taktyczne, Jednostka Wsparcia Działań w Cyberprzestrzeni oraz zespoły analityczne i kryptologiczne. Tu też działa CSIRT MON – zespół reagowania na incydenty, który stale monitoruje sieci resortu.

Cyberoperacje: czas pokoju, czas konfliktu

– Nikt nam wojny nie wypowiedział, ale w moim przekonaniu, jeśli chodzi o działania w cyberprzestrzeni, powinniśmy raczej mówić o stanach rywalizacji, konfliktu, a nawet wojny. WOC działają w trybie ciągłym, a każdy incydent jest analizowany pod kątem taktyk, technik i procedur przeciwnika – zapewniał w rozmowie z WNP gen. dyw. Karol Molenda, były dowódca WOC, architekt polskich cyberwojsk.

W czasie pokoju nasza cyberarmia systematycznie monitoruje sieci, reaguje na incydenty, wspiera instytucje cywilne i prowadzi działania kontrwywiadowcze. A w czasie konfliktu może prowadzić operacje ofensywne.

– Największy wysiłek ukierunkowany jest na obronę przed działaniami przeciwnika w przestrzeni cyfrowej, a gdyby politycy zadecydowali, że nie powinniśmy tylko się bronić w cyberprzestrzeni, w pełni realny jest również atak na infrastrukturę przeciwnika. Mamy do tego niezbędne kompetencje, narzędzia i możliwości – twierdził stanowczo gen. Molenda.

Owe „działania ofensywne” w praktyce oznaczają zakłócanie systemów przeciwnika, przejmowanie infrastruktury teleinformatycznej, prowadzenie operacji informacyjnych, wsparcie działań kinetycznych poprzez cyberatak, ale też, rzecz jasna, ochronę własnych systemów dowodzenia i łączności.

W marcu 2026 r. gen. Molenda został – decyzją Komitetu Wojskowego NATO – zastępcą szefa sztabu ds. planowania (Assistant Chief of Staff Requirements) w natowskim Dowództwie Sojuszników ds. Transformacji (HQ SACT) w Norfolk,

w stanie Wirginia (odpowiada za wzmocnianie cyfrowych zdolności Sojuszu). Na stanowisku Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC) zastąpił go gen. bryg. Mariusz Chmielewski.

Wybór polskiego generała do jednego z dwóch najważniejszych dowództw strategicznych NATO to bezpośrednie potwierdzenie, że kompetencje budowane przez Wojsko Polskie w dziedzinie transformacji cyfrowej (w tym dokonania samego nominata) są oceniane w Pakcie Północnoatlantyckim bardzo wysoko.

W kontakcie z przeciwnikiem. Skutecznie

Codziennie 6,5 tys. żołnierzy cyberwojska wykonuje gigantyczną pracę na rzecz naszego bezpieczeństwa. Każdy incydent analizuje się pod kątem taktyk, technik i procedur przeciwnika.

Do największych wyzwań należy przeciwdziałanie tzw. grupom APT (Advanced Persistent Threats), sponsorowanym przez państwa i atakującym infrastrukturę. Jeden z takich zespołów, zwany APT28, działa w strukturach rosyjskiego wywiadu wojskowego (GRU). WOC monitoruje dziś blisko 20 podobnych grup.

– Nie przygotowujemy się na wojnę, jak inne jednostki liniowe. My tę wojnę mamy na co dzień, bo nasi operatorzy codziennie wchodzi w interakcje z przeciwnikiem. Nie ma czasu na długie odprawy, narady i planowanie... Niekiedy decyzję trzeba podjąć w kilka minut. Nic, z czym nie bylibyśmy w stanie sobie poradzić, nie zostało odnotowane – podkreśla z dumą gen. Molenda.

O tym, pod jaką presją pracują żołnierze WOC, świadczy chociażby fakt, że – jak mówił wicepremier Kosiniak-Kamysz – w samej sieci wojskowej dochodzi do setek tysięcy incydentów. W 2025 r. tych potwierdzonych i poważnych zdarzyło się ponad 7 tys.

Również w 2026 r. utrzymuje się wysoka aktywność grup powiązanych z Rosją i Białorusią (w tym próby włamań, skanowania i ataki phishingowe).

Wśród najpoważniejszych znalazł się atak na infrastrukturę energetyczną w święta (Boże Narodzenie/Nowy Rok), który mógł pozbawić prądu wielu mieszkańców południowej Polski. Ale nie doszło do przerw w zasilaniu – atak został zneutralizowany.



Władysław Kosiniak-Kamysz
wicepremier i minister obrony
narodowej

– Polska jako członek NATO jest mniej narażona na atak w ujęciu konwencjonalnym niż na wojnę w cyberprzestrzeni.



gen. Karol Molenda
zastępca szefa sztabu ds. planowania
w natowskim Dowództwie
Sojuszników ds. Transformacji
(HQ SACT)

– Nie zbudujemy cyberobrony bez sektora prywatnego. To tam powstają technologie, które adaptujemy do działań wojskowych.

CSIRT MON. Incydenty według kategorii

Kategoria incydentu	Liczba (rok 2025)	Liczba (rok poprzedni)	Zmiana r/r (%)
Oszustwa komputerowe	131	171	-24%
Złośliwe oprogramowanie	354	555	-36,8%
Dostępność usług	17	20	-15%
Próby włamań	522	257	+101,6%
Bezpieczeństwo informacji	5885	2962	+97,7%
Inne	216	255	-14,9%

Źródło: Sprawozdanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa za 2025 rok

Ostatnio gros działań w cyberprzestrzeni zauważalnie przenosi się z infrastruktury na „przestrzeń kognitywną”: dezinformację i operacje wpływu.

Cyberobrona w wersji lokalnej

Wojska Obrony Cyberprzestrzeni to trzon cyfrowego komponentu Sił Zbrojnych RP. Nie jedyny. Coraz większą rolę odgrywa ją również Wojska Obrony Terytorialnej (WOT). Stają się formacją „będącą blisko” lokalnych systemów teleinformatycznych, gotową wspierać administrację, samorządy i infrastrukturę krytyczną w sytuacjach cyberkryzysowych.

Cyberkomponent WOT to jeden z najbardziej dynamicznie rozwijających się elementów terytorialnej służby wojskowej. W 2019 r. w Wojskach Obrony Terytorialnej rozpoczęło się tworzenie pierwszego zespołu do cyberwalki. W 2020 r. w eksperckim Zespole Działań Cyberprzestrzennych (ZDC WOT) pracowało już ok. 100 specjalistów – żołnierzy pełniących terytorialną służbę wojskową. Jednostka ta, zlokalizowana przy Dowództwie WOT w Zegrzu, stała się fundamentem programu CyberWOT. Planuje się podobne struktury we wszystkich Brygadach OT – jako ważny element systemu odporności państwa, szczególnie na poziomie lokalnym i regionalnym.

– WOT ma być formacją odporną, elastyczną i zdolną do działania tam, gdzie państwo najbardziej tego potrzebuje. Dziś

jednym z tych miejsc jest cyberprzestrzeń – mówił gen. Wiesław Kukuła, gdy był dowódcą Wojsk Obrony Terytorialnej.

WOT jako całość nie prowadzi operacji ofensywnych (to domena WOC), ale jego rola pozostaje kluczowa w reagowaniu na incydenty i we wsparciu lokalnych instytucji. Terytorialsi pomagają w analizie incydentów, przywracaniu właściwego działania systemów po atakach, testach bezpieczeństwa, budowaniu procedur reagowania.

Gdy szkoła, urząd gminy czy szpital stają się ofiarą cyberataku, to właśnie WOT może być pierwszą wojskową formacją na miejscu. Terytorialsi na bieżąco współpracują z operatorami infrastruktury energetycznej, wodociągowej, transportowej i telekomunikacyjnej.

W czasie konfliktu zbrojnego CyberWOT pełniłby rolę wsparcia dla WOC (zabezpieczenie lokalnych systemów łączności i administracji, ochrona zaplecza logistycznego, przeciwdziałanie sabotażowi cyfrowemu).

W 2025 r. w cyberkomponencie WOT służyło ponad 600 żołnierzy z kompetencjami IT. W 2025 i 2026 r. zespoły CyberWOT interweniowały kilkadziesiąt razy w samorządach i instytucjach publicznych po poważnych incydentach.

MON podkreśla: CyberWOT to zasób, którego nie da się zbudować wyłącznie w strukturach etatowych.



plk Jarosław Wacko

główny specjalista Dowództwa
Komponentu Wojsk Obrony
Cyberprzestrzeni

– Program Cyber Legion, który od prawie roku wdrażamy dosyć intensywnie, spotkał się z bardzo ciekawym i ciepłym przyjęciem. Myślę, że z tego powodu, że jest skrojony w ten sposób, by nie wydzierać nikomu specjalistów, a dawać szansę współpracy – z obopólną korzyścią.



Adam Dzwonkowski

Defense & Intelligence Technology
Lead w Microsoft

– Cyber Legion jest łącznikiem między wojskiem, a ludźmi, którzy nie zawsze chcą zakładać mundur, lecz chcą służyć swymi kompetencjami. Pewne cechy, które w wojsku można nabyć ze względu na to, że to służba, a nie praca, są potem bardzo korzystne w sektorze przemysłowym.

Legion, czyli dual-use dla cyberobronności

Ciekawym przykładem współpracy państwa, wojska i sektora prywatnego – i powodem do dumy cyberwojsk – jest Cyber LEGION. To nowa inicjatywa polegająca na zachęceniu cywilnych specjalistów – informatyków z różnych branż przemysłu, banków, służby zdrowia czy sektora energetycznego – by włączyli się w działalność na rzecz bezpieczeństwa państwa. Niekoniecznie w mundurach, lecz w ramach tzw. aktywnej rezerwy.

To swoisty przykład dual-use: praca na co dzień w firmie, a w niektórych sytuacjach – dla wojska. Program uruchomiono w maju 2025 r. i przez trzy miesiące zgłosiło się tysiąc wysokiej klasy informatycznych specjalistów. Minister zdecydował o utworzeniu kompanii kadrowej Cyber LEGIONU.

– Nie zbudujemy cyberobrony bez sektora prywatnego. To tam powstają technologie, które adaptujemy do działań wojskowych – zapewniał gen. Molenda.

Szczególnym przykładem takiego współdziałania w ochronie cyberprzestrzeni i infrastruktury państwa stała się operacja Niezłomny Żółw, prowadzona od 2023 r. i koordynowana przez WOC. W ramach tej operacji rozpoznano ok. 600 tys. ataków, prób skanowania i sondowania treści.

W ramach wspomnianej akcji współdziałają trzy krajowe zespoły reagowania na incydenty komputerowe (CSIRT): tworzą trzon państwowego systemu cyberbezpieczeństwa. Każdy z nich odpowiada za inny obszar administracji i infrastruktury.

Przypomnijmy: CSIRT MON (Computer Security Incident Response Team), czyli Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego Ministerstwa Obrony Narodowej, prowadzony przez Wojska Obrony Cyberprzestrzeni, pozostaje najbardziej „bojowym” zespołem CSIRT w Polsce.

Kolejnym jest CSIRT GOV (Computer Security Incident Response Team GOV) – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego GOV, który prowadzi Agencja Bezpieczeństwa Wewnętrznego (ABW). Odpowiada on za bezpieczeństwo systemów administracji rządowej, ochronę instytucji państwowych oraz przeciwdziałanie cyberatakami o charakterze szpiegowskim i sabotażowym. To CSIRT odpowiedzialny za „cywilną” część państwa.

Trzecim zespołem jest CSIRT NASK (Computer Security Incident Response Team NASK) – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego NASK („dowodzi” nim ten państwowy instytut badawczy). Odpowiada on m.in. za bezpieczeństwo operatorów usług kluczowych (energetyka, transport, zdrowie, finanse), ochronę sektora prywatnego i publicznego (poza MON i GOV) oraz monitorowanie zagrożeń w sieci krajowej. To CSIRT o najszerszym zasięgu, obejmujący większość infrastruktury krytycznej.

W ramach operacji Niezłomny Żółw te trzy człony naszej cyberobrony wspólnie analizują incydenty, wymieniają się informacjami o zagrożeniach, koordynują reakcję na ataki czy też opracowują wspólne ćwiczenia i procedury.

Wojsko, nawet najlepiej wyposażone, nie jest jednak w stanie samodzielnie nadążyć za tempem rozwoju technologii, które napędzają sektor prywatny i środowisko akademickie. Dlatego WOC, WOT i oczywiście MON od kilku lat budują trójkąt współpracy.

– W ramach operacji Niezłomny Żółw nastąpiło otwarcie na podmioty zarówno publiczne, jak i prywatne, które są strategiczne dla państwa polskiego. Mamy podpisane ponad 20 umów z różnymi jednostkami – podkreślał wicepremier Kosiniak-Kamysz.

To nie wszystko. MON podpisało umowy z kilkudziesięcioma uczelniami – m.in. z Politechniką Warszawską, Wrocławską i Poznańską, Wojskową Akademią Techniczną, Akademią Górniczo-Hutniczą, Uniwersyteciem Warszawskim czy też Uniwersyteciem Jagiellońskim.

W stronę najlepszej cyberobrony

Resort obrony podkreśla, że współpraca z uczelniami to inwestycja w ludzi. W 2023 r. powstała Akademia CYBER.MIL (łączy szkolenia wojskowe i akademickie, w tym praktyczne). Szkolą się tam operatorzy wykrywania, reakcji i obrony przed cyberatakami (SOC – Security Operations Center), analitycy, fachowcy od kryptologii oraz cyberoperacji ofensywnych i defensywnych.

Polscy specjaliści z wojska, sektora prywatnego i uczelni regularnie uczestniczą w ćwiczeniach – takich jak Cyber-EXE (organizowanych przez CSIRT NASK razem z CSIRT GOV i CSIRT MON), Cyber Polygon



gen. bryg. rez. Włodzimierz Nowak
ekspert w dziedzinie cyberbezpieczeństwa

– Firma przychodzi do MON z dobrym rozwiązaniem, a potem padają podstawowe pytania: gdzie powstaje produkt, kto go rozwija, czy deweloperzy pracują w firmie, czy za granicą, jakiej są narodowości, kto ma dostęp do danych i kodów źródłowych. I nagle okazuje się, że na tych pozornie prostych kwestiach zaczynają się poważne problemy.



Tomasz Florczak
prezes ChallengeRocket

– Kiedy coś odstrasza? Kiedy wiąże się z konsekwencjami. I może to jest jeden z elementów, którego troszkę brakuje. Może Polska powinna bardziej naciskać, by w ramach struktur NATO nie było to tylko odpieranie ataków – ja wiem, że to jest sojusz obronny – lecz także pewnego rodzaju budowanie kosztu dla agresora. I tego kosztu dyplomatycznego, i również realnego.

czy Cyber Mil-Hack i Cyber Tarcza (dzieło WOT).

Bierzemy też udział w najbardziej zaawansowanych ćwiczeniach cyberobrony na świecie – Locked Shields (pod auspicjami międzynarodowego centrum NATO w Tallinnie), polegających na realistycznej obronie państwa przed złożonym cyberatakami przez 48 godzin non stop.

Wspomniane ćwiczenia, a także opinie naszych partnerów z USA i Europy potwierdzają, że Polska należy do globalnych liderów cyberobrony w NATO. Jeden z dowodów? W 2025 r. drużyna żołnierzy WOC, ekspertów z NASK i studentów zajęła II miejsce w Europie właśnie w Locked Shields.

– Na międzynarodowych spotkaniach dowódców często jestem proszony o prezentację naszego modelu. Wiele krajów dopiero tworzy struktury cyberobrony i przygląda się Polsce jako wzorcowi – opowiadał gen. Molenda.

Wojska Obrony Cyberprzestrzeni cechuje bogata współpraca i wymiana doświadczeń – m.in. z USA, NATO, UE; tu nasi fachowcy współpracują m.in. z U.S. Cyber Command – dowództwem cybernetycznym Sił Zbrojnych Stanów Zjednoczonych, odpowiedzialnym za operacje w cyberprzestrzeni i ochronę sieci wojskowych USA.

WOC współdziała również z Cooperative Cyber Defence Centre of Excellence, centrum eksperckim NATO, które – oprócz cyberobrony – zajmuje się badaniami, szkoleniami i ćwiczeniami oraz z Europejską Agencją ds. Cyberbezpieczeństwa (ENISA) – agencją UE, której zadaniem jest wzmacnianie cyberbezpieczeństwa we Wspólnocie.

Niedawno WOC nawiązały współpracę ze Szwajcarią, niezwykle zaawansowaną w cyberobronie, w tym w ochronie infrastruktury krytycznej. Partnerstwo obejmuje wymianę informacji o zagrożeniach, wspólne szkolenia specjalistów i udział polskich żołnierzy w programach ćwiczeń i testów odporności systemów.

Po co to wszystko? To oczywiste: dzisiaj możliwości skutecznych działań w cyberprzestrzeni powodują, że kraj bez własnych zdolności w tej domenie pozostaje bezbronny wobec tych zagrożeń, niewymagających kosztownych czołgów czy samolotów.

CSIRT MON: zarejestrowane incydenty (2023–2025)

Rok	2023	2024	2025	wzrost w proc. 2024/25
Liczba incydentów	5841	4220	7125	68,9
Średnia dzienna	bd.	12	22	66

Źródło: Sprawozdanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa za 2025 rok



plk Jan Kelner

działek Wydziału Elektroniki WAT

– W zakresie technologii, które wykorzystuje od lat, wojsko dokładnie wie, czego oczekuje. Natomiast rozwiązania z cyberbezpieczeństwa, AI czy technologii dronowych są stosunkowo młode z punktu widzenia wdrażania ich do sprzętu wojskowego. Tu wojsko nie ma jeszcze doświadczeń, które pozwalałyby jednoznacznie wskazać oczekiwania, dlatego szuka kierunków rozwoju.



Tomasz Zdzikot

wiceprzewodniczący Rady ds. Bezpieczeństwa i Obronności przy prezydencie RP

– Powinniśmy szerzej oferować nasze kompetencje specjalistyczne całemu Sojuszowi (NATO – dop. red.). Wydaje się, że jest kilka pól zastosowań, w których Polska powinna widzieć sama siebie w roli lidera NATO. Nie powinniśmy godzić się na to, że dzisiaj za lidera cyfrowych kompetencji w NATO uchodzić próbuje Estonia (z całą sympatią do Estonii). (...) To dla nas wyzwanie, byśmy zaczęli siebie sami postrzegać i prezentować jako liderów technologicznych, liderów cyberbezpieczeństwa i cyberzdolności.

Zagrożeńi pacjenci. Cyberataki w ochronie zdrowia

Od prawidłowego i niezakłóconego funkcjonowania sektora ochrony zdrowia – części infrastruktury krytycznej państwa – zależy zdrowie i życie obywateli. A dane pacjentów gromadzone przez podmioty medyczne mogą stanowić źródło korzyści materialnych dla tych, którzy nielegalnie wejdą w ich posiadanie.

Czego dowiesz się z tego rozdziału?

- Dlaczego sektor ochrony zdrowia jest jednym z głównych celów cyberataków?
- Jakie typy ataków najczęściej paraliżują szpitale i placówki medyczne?
- Jak wygląda typowy scenariusz ataku ransomware?
- Dlaczego cyberatak na szpital może bezpośrednio zagrozić życiu pacjentów?
- Jakie błędy i zaniedbania najczęściej osłabiają bezpieczeństwo placówek medycznych?
- Jakie regulacje, procedury i technologie mogą zwiększyć odporność systemu ochrony zdrowia?

Nie przypadkiem z opublikowanego we wrześniu 2025 r. przez Komisję Europejską (KE) raportu „Targeted consultation on the Action Plan on the cybersecurity of hospitals and healthcare providers” wynika, że system ochrony zdrowia jest jednym z głównych celów ataków cyberprzestępców.

Trudny do ochrony, atrakcyjny dla przestępców

Jeremi Olechnowicz, kierownik Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego w Centrum e-Zdrowia (CSIRT CeZ), wyjaśnia, że sektor zdrowia łączy w sobie kilka czynników atrakcyjnych dla cyberprzestępców.

– Przetwarza bardzo wrażliwe dane, w tym osobowe, które mogą służyć do wyłudzeń. Ze względu na oczywisty priorytet, jakim jest ratowanie zdrowia i życia

pacjentów, sektor musi działać w trybie ciągłym (często bez możliwości przestoju), a jednocześnie bywa technologicznie różnicowany i trudny do zabezpieczenia. Presja na szybkie przywrócenie działania sprawia, że jest postrzegany (przez przestępców – przyp. red.) jako bardziej skłonny do ulegania szantażowi – mówi Jeremi Olechnowicz.

Liczba cyberataków na polski sektor zdrowia rośnie skokowo. W 2022 r. odnotowano 251 incydentów, w 2023 r. było ich 405, w 2024 r. – 1028, a w ub.r. – 1441. Należy się spodziewać, że bilans 2026 r. będzie jeszcze bardziej alarmujący.

Tymczasem ze wspomnianego opracowania KE wynika, że zaledwie 13 proc. ankietowanych (w przeważającej większości pracownicy sektora ochrony zdrowia) oceniło systemy cyberbezpieczeństwa w swoich krajowych systemach ochrony zdrowia jako bardzo zaawansowane (1 proc.) albo zaawansowane (12 proc.). Najwięcej (41 proc.) stwierdziło, że poziom dojrzałości systemu bezpieczeństwa jest średni.

Na to samo pytanie – tyle że w odniesieniu do własnej organizacji – odpowiadano znacznie bardziej optymistycznie. Opcję „bardzo zaawansowany” albo „zaawansowany” wybrało 36 proc. ankietowanych, a „średni” – 38 proc.

Źródeł deficytów ankietowani upatrują przede wszystkim w niewystarczającym finansowaniu, braku specjalistów ds. cyberbezpieczeństwa w placówkach medycznych i szkoleń dla personelu, który pozostaje nieświadomy różnorodności cyfrowych zagrożeń.

Podczas tegorocznego Kongresu Wyzwań Zdrowotnych podkreślano globalny wymiar cyberbezpieczeństwa. Nuta optymizmu? Systemy ochronne są już oparte na siatce powiązań wykraczających poza granice konkretnego państwa.

– Jeżeli szpital w Nowym Jorku zostanie zaatakowany, to szpital powiatowy np. w Przeworsku będzie o tym poinformowany. Narzędzia w nim wykorzystywane będą już w stanie przed tego typu atakiem ten szpital obronić. Cyberbezpieczeństwo to nie jest sprawa pojedynczego świadczonodawcy – wskazuje Tomasz Jaworski, dyrektor ds. cyberbezpieczeństwa w sektorze zdrowia w Palo Alto Networks.



Dane warte miliardy

Postępująca cyfryzacja to broń obosieczna. Zalety spopularyzowanej w pandemii telemedycyny są oczywiste. Podobnie jak przewagi EDM (Elektroniczna Dokumentacja Medyczna) nad tradycyjnymi kartami pacjenta: system ten, w przeciwieństwie do wewnętrznych baz konkretnej placówki, umożliwia transfer danych pacjenta między podmiotami. Dostęp do niego zapewnia również Internetowe Konto Pacjenta (IKP).

Elektronizacja danych niesie jednak z sobą ryzyko ich wycieku.

– Dla przestępców największą wartość mają kompleksowe dane pacjentów (medyczne + osobowe), które mogą być wykorzystywane do szantażu lub sprzedaży. Równie istotny jest dostęp do infrastruktury – bo pozwala sparaliżować działalność placówki i wymusić okup. W praktyce atakujący dążą do maksymalizacji wpływu, łącząc oba te elementy – mówi Jeremi Olechnowicz.

Placówka medyczna – ofiara ataku – zmagą się z jego skutkami przez wiele tygodni. Niepewność towarzyszy m.in. ponownemu uruchamianiu systemu.

– Nie wiemy, których kopii zapasowych możemy użyć, aby uniknąć ponownego incydentu... Istnieje ryzyko, że cyberprzestępcy ukryli „coś” w zakamarkach naszego



Małgorzata Wywrot

Project Managerka, NIL IN – Sieć Lekarzy Innowatorów, Naczelna Izba Lekarska, Szkoła Zdrowia Publicznego CMKP

– Naczelna Izba Lekarska organizuje szkolenia – z punktami edukacyjnymi. Średnio raz w miesiącu jest szkolenie dotyczące cyberbezpieczeństwa. Ile osób uczestniczy? Zazwyczaj pięćdziesiąt, sześćdziesiąt na pięćset (możliwych)... (...) To nie cieszy się dużym zainteresowaniem. Lekarze robią to po godzinach pracy. Może w godzinach pracy byłoby lepiej?

systemu. Jeśli go odbudujemy i uruchomimy ponownie, może się okazać, że za tydzień czy dwa wszystko znów przestanie działać – tak o skutkach ataku na szpital MSWiA w Krakowie mówił „Rzeczpospolitej” jego dyrektor Michał Zabojszcz. Straty szacował w milionach złotych...

Autorzy globalnego raportu IBM z 2025 r. „Cost of a Data Breach” średni koszt naruszenia danych w sektorze ochrony zdrowia obliczyli na 7,42 mln dol. – to dane ze Stanów Zjednoczonych, Indii, Wielkiej Brytanii, Niemiec, Japonii, Francji, Australii, Kanady, Korei Płd, Włoch, Afryki Płd, także z Beneluksu, krajów Bliskiego Wschodu, ASEAN i LATAM (państwa na południe od USA, gdzie językami urzędowymi są hiszpański i portugalski). Równie wysoko wycenianych strat nie przyniosły analogiczne ataki w sektorze finansowym, energetycznym, przemysłowym ani żadnym innym.

Największą różnicą między cyberatakiem na bank czy urząd i na placówkę medyczną jest oczywiście ryzyko bezpośredniego wpływu na zdrowie i życie pacjentów.

– W ochronie zdrowia niedostępność systemów może wstrzymać diagnostykę czy leczenie, dlatego reakcja musi być natychmiastowa, a działania obejmują często przejście na tryb awaryjny, np. dokumentację papierową – stwierdza kierownik CSIRT CeZ. To zaś prowokuje opóźnienia i koszty.

Arsenał przestępczych narzędzi

Do najczęstszych, a zarazem najbardziej dotkliwych dla pracy szpitali typów ataków należy ransomware. Przypomnijmy (w uproszczeniu): przestępca włamuje się do systemu, zdobywa dostęp do plików, zaszyfrowuje je i uniemożliwia dostęp, grożąc użytkownikowi zniszczeniem danych, gdy ten odmówi zapłaty okupu. Wirusy, za pomocą których przestępca przejmuje kontrolę nad urządzeniem, są rozpoznawane m.in. za pomocą maili z podejrzаныmi linkami.

CSIRT CeZ wskazuje, że w przypadku podejrzenia ataku ransomware kluczowe jest pierwsze 60 minut. Należy wówczas wyizolować komputer z sieci (LAN/Wi-Fi), ale nie odłączać go od zasilania ani nie restartować (grozi to utratą dowodów ataku); zabezpieczyć dowody (zdjęcia np. żądań okupu, zrzuty ekranu); zabezpieczyć kopie zapasowe (tzw. backup); zwołać sztab

Placówka medyczna, która padła ofiarą ataku, zмага się z jego skutkami przez wiele tygodni. Niepewność towarzyszy m.in. ponownemu uruchamianiu systemu.

kryzysowy (kierownik podmiotu, ASI, IOD, IOSI, dyrektor medyczny, rzecznik) oraz zgłosić incydent do CSIRT CeZ. I w żadnym razie nie należy spełniać żądań przestępców ani się z nimi komunikować.

Placówki medyczne mogą też paść ofiarą phishingu (podsyłanie się pod zaufaną instytucję celem wyłudzenia wrażliwych danych osobowych np. pacjentów). „Szczególną ostrożność należy zachować przy załącznikach. Falszywe pliki często mają podwójne rozszerzenia – np. faktura.pdf.exe – co może umknąć uwadze w natłoku obowiązków. Nawet zwykłe obrazy mogą zawierać złośliwy kod, jeśli pochodzą z nieznanego źródła” – ostrzega CSIRT CeZ.

– Tradycyjne kody SMS czy powiadomienia push są podatne na ataki typu MFA Fatigue (zameczanie użytkownika monitami). Dla kont o najwyższych uprawnieniach (administratorzy systemów, kadra zarządzająca) rekomendowane jest wdrożenie kluczy sprzętowych zgodnych ze standardem FIDO2 – zaleca Łukasz Jędrzejczak, dyrektor ds. sektora cyberbezpieczeństwa z Deloitte Central Europe.

Osobną – i w przypadku szpitali najbardziej niebezpieczną kategorię – stanowią ataki na urządzenia wspierające leczenie pacjentów. Wojciech Głazewski, szef Check Point na Polskę, ostrzega przed następstwami.

– Mogą opóźnić procedury medyczne, powodować zatory w izbach przyjęć oraz zakłócać usługi, co w skrajnych przypadkach może mieć bezpośredni wpływ na życie pacjentów – wylicza.

Strefa Internet of Medical Things (IoMT), czyli m.in. tomografy, rezonanse, kardiomonitoring, urządzenia pracujące na starszych, niewspieranych systemach operacyjnych – jak radzi Jędrzejczak – nigdy nie powinny mieć bezpośredniego dostępu do internetu ani do ogólnej sieci IT.

Przestarzałe systemy, skromne budżety

Opublikowane we wrześniu 2025 r. wyniki analiz prowadzonych w szpitalach przez CSIRT CeZ ujawniają, że nie są one



Tomasz Maciejewski
wiceminister zdrowia

– Na pewno będziemy musieli wspólnie z Ministerstwem Cyfryzacji pochylić się nad zabezpieczeniem puli pieniędzy na finansowanie cyberbezpieczeństwa w placówkach ochrony zdrowia.



Sebastian Szymanek
prezes Grupy Polpharma

– W cyberbezpieczeństwie realizujemy strategię „defense in depth”. Systemy IT są audytowane, monitorowane, a także zapewniają architektonicznie brak punktów pojedynczej awarii. Takie podejście zapewnia, że ekosystem IT zapewnia wysoką dostępność rozwiązań biznesowych. Wprowadzamy politykę Zero Trust i segmentację sieci OT. W skali krajowej dostrzegamy potrzebę powołania wyspecjalizowanych zespołów reagowania (CSIRT) dedykowanych przemysłowi farmaceutycznemu.

przygotowane na cyberataki. Niespełna 9 proc. placówek nie ma podstawowych mechanizmów ochrony (antywirus albo firewall). Uwierzytelnianie wieloskładnikowe albo logowanie wieloetapowe (MFA) nadal nie jest powszechnym mechanizmem. Mniej więcej 60 proc. podmiotów w ogóle nie monitoruje pojawiających się podatności (słabych stron własnych systemów IT), a 1/3 nie wykonuje cyklicznych testów kopii systemowych i metod ich odzyskiwania.

– W dobie ewolucji zagrożeń ze strony zorganizowanych grup cyberprzestępczych oraz wymogów regulacyjnych dyrektywy NIS2 i ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) podmioty lecznicze muszą budować odporność operacyjną (cyber resilience) opartą na architekturze Zero Trust – przekonuje Łukasz Jędrzejczak. (Szczegółowy opis i techniczna specyfikacja czterech filarów cyberbezpieczeństwa – dostępna na stronie Deloitte).

Wieloletnie zaniedbania, przestarzały sprzęt i zawodne systemy teleinformatyczne nie są skutkiem złej woli dyrektorów placówek, lecz ograniczonych budżetów coraz mocniej zadłużonych szpitali. Pula, którą Narodowy Fundusz Zdrowia (NFZ) przeznacza na cyberbezpieczeństwo, jest niewystarczająca, a środki przypadające na konkretną placówkę – nieadekwatne do jej realnych potrzeb.

Remedium miał być specjalny fundusz w ramach Krajowego Planu Odbudowy (KPO), z którego skorzysta kilkaset szpitali. Ale nie wszystkie...

– W dalszym ciągu 300, w dużej mierze małych, szpitali, które mają jednego bądź dwóch informatyków, nie dostało ani grosza na cyberbezpieczeństwo. (...) Potrzebujemy drugiego KPO na cyfryzację, „znaczonych pieniędzy” na cyberbezpieczeństwo – po kilka, kilkanaście milionów złotych (w zależności od wielkości szpitala) – mówił podczas Kongresu Wyzwań Zdrowotnych dr Michał Zabojszcz, dyrektor Samodzielnego Publicznego Zakładu Opieki Zdrowotnej MSWiA w Krakowie (ta placówka padła ofiarą cyberataku 8 marca br.).

Resort zdrowia przekonuje, że w pierwotnej wersji KPO w ogóle nie przewidziano funduszy na poprawę cyberbezpieczeństwa w ochronie zdrowia, dlatego wygospodarowanie jakichkolwiek pieniędzy należy uznać za sukces.



Michał Zabojszcz

dyrektor szpitala MSWiA w Krakowie

– Istnieje ryzyko, że cyberprzestępcy ukryli „coś” w zakamarkach naszego systemu. Jeśli go odbudujemy i uruchomimy ponownie, może się okazać, że za tydzień czy dwa wszystko znów przestanie działać.



Jeremi Olechnowicz

kierownik Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego w Centrum e-Zdrowia

– Dla przestępców największą wartość mają kompleksowe dane pacjentów (medyczne + osobowe), które mogą być wykorzystywane do szantażu lub sprzedaży. Równie istotny jest dostęp do infrastruktury, gdyż pozwala sparaliżować działalność placówki i wymusić okup.



Anna Sibilska

dyrektorka Biura Bezpieczeństwa Informacji i Ciągłości Działania w Narodowym Funduszu Zdrowia

– Cyberbezpieczeństwa nie da się podzielić na kawałki tortu: ja mam taki to a taki udział w rynku, więc jestem mały i się nie liczę. Wszyscy musimy patrzeć na cyberbezpieczeństwo jak na jeden wielki ekosystem! Obecnie w systemie ochrony zdrowia mamy kilkadziesiąt rejestrów medycznych, do których raportowane są dane – w tym Narodowy Fundusz Zdrowia, dysponenta największej liczby tego typu informacji (wspólnie z Centrum e-Zdrowia)...



Janusz Cieszyński

poseł na sejm RP, minister cyfryzacji w 2023 r., podsekretarz stanu w Ministerstwie Zdrowia w latach 2018–2020

– Gdyby w wyniku cyberataku przestały działać placówki ochrony zdrowia, byłby to gigantyczny problem dla państwa. Trzeba patrzeć na zapewnienie ciągłości działania krytycznego systemu ochrony zdrowia, co wymaga dużych środków i czasu. (...) To nie tylko kwestia konkretnej placówki, ale całego łańcucha dostaw.

– Na pewno będziemy musieli, wspólnie z Ministerstwem Cyfryzacji, pochylić się nad tym tematem – stwierdził wiceminister zdrowia Tomasz Maciejewski podczas tegorocznego Europejskiego Kongresu Gospodarczego. Nie wykluczył uruchomienia nowej puli na wsparcie tych placówek, które nie dostały dotychczas pieniędzy.

Świadomość zagrożeń, czyli czynnik ludzki

– System bezpieczeństwa jest tak silny, jak silne jest najsłabsze ogniwo tego systemu. W związku z tym zaczynamy szkolenia od podstawowego poziomu, od podstawowego poziomu cyberhigieny – stwierdza dr Marek Migdał, dyrektor Instytutu „Pomnik-Centrum Zdrowia Dziecka”. – Jeżeli nie zmienimy nastawienia na tym najniższym poziomie, to wdrażanie firewalli, zaawansowanych systemów nic nie da. Bo czynnik ludzki zdestabilizuje wszystko.

Ale nawet najlepiej przeszkolony personel nie wystarczy.

– Czynnik ludzki nadal odgrywa istotną rolę... Oszustwa komputerowe, w tym phishing, są jedną z najczęstszych przyczyn incydentów. Jednocześnie nie można jednoznacznie wskazać jednego „najsłabszego ogniwa” – bezpieczeństwo zależy od całego systemu. Nowe techniki, w tym wykorzystujące AI, zwiększają skuteczność ataków i utrudniają ich rozpoznanie, dlatego kluczowe jest stałe podnoszenie świadomości personelu – zaznacza Jeremi Olechnowicz.

Regulacje i standardy

W kwietniu br. weszła w życie ustawa KSC, czyli przepisy implementujące unijną dyrektywę NIS2. Szpitale także mają rok na wdrożenie ustawowych obowiązków oraz dwa lata na pierwszy obowiązkowy audyt cyberbezpieczeństwa (kolejne trzeba będzie przeprowadzać co najmniej raz na 3 lata).

Resort cyfryzacji wydał zalecenia dla podmiotów podlegających pod KSC (Krajowy System Cyberbezpieczeństwa), ze szczególnym uwzględnieniem sektora ochrony zdrowia: duży nacisk położono w nich na zabezpieczenia zdalnego dostępu do systemów informatycznych. Placówkom medycznym zaleca się m.in. wdrożenie tzw. polityki Least Privilege, czyli

W przypadku szpitali najbardziej niebezpieczną kategorię cyberagresji stanowią ataki na urządzenia wspierające leczenie pacjentów. Mogą opóźnić procedury medyczne, co w skrajnych przypadkach może mieć bezpośredni wpływ na życie pacjentów.

w praktyce dopuszczenie tylko niezbędnego ruchu sieciowego do celów służbowych oraz wymuszenie uwierzytelniania wieloskładnikowego (MFA) dla wszystkich połączeń VPN i RDP (Remote Desktop Protocol – umożliwia pracę zdalną na innym komputerze z systemem Windows). Konieczne jest również zweryfikowanie odporności VPN na ataki typu brute force (np. ograniczenie liczby nieudanych logowań do konkretnej liczby prób).

Wśród zaleceń znalazł się również bezwzględny zakaz logowania się kontami z uprawnieniami administratora domeny na stacjach roboczych, wymóg ścisłego monitorowania połączeń dostawców i firm trzecich (uprawnienia należy przyznawać czasowo i tylko do niezbędnych zasobów) oraz polecenie codziennego przeglądu dzienników zdarzeń AV/EDR pod kątem alertów typu „malware detection” (złośliwe oprogramowanie). Resort cyfryzacji zaznacza, że „ignorowanie tych alertów jest najczęstszą przyczyną udanych ataków ransomware”.

Zaleca się także „monitorowanie logów z usług dostępnych publicznie (np. telemedycyna, portale pacjenta). Kluczowe jest wdrożenie mechanizmów wykrywania i blokowania ataków typu Brute Force oraz aktualizacja systemów (rekomendowane możliwości przeprowadzenia aktualizacji w 24 godziny od wykrycia krytycznej podatności) i odpowiednio maksymalna ich izolacja od systemów wewnętrznych na wypadek kompromitacji”. (Pełen tekst wytycznych dostępny jako komunikat Pełnomocnika Rządu ds. Cyberbezpieczeństwa – zalecenia dla sektora ochrony zdrowia i innych podmiotów KSC).



Rafał Litwiński

ekspert sektorowego CSIRT CeZ

– Ataki zaczynają się najczęściej phishingiem. W dość łatwy sposób (przez odpowiednią edukację i komunikację) można tu uśmierzyć problemy - nie będą się tak często pojawiały. (...) Każdy menedżer kierujący ośrodkiem typu szpital musi odbyć szkolenia z podstaw cyberbezpieczeństwa. Drugim krokiem jest szkolenie całego personelu, od którego bardzo często zaczynają się wspomniane problemy.



Bezpieczeństwo zależy od nas

We are the firewall – hasło przypominające o wspólnej odpowiedzialności przyświecało tegorocznej edycji CYBERSEC EXPO & FORUM 2026 – konferencji wszechstronnie podejmującej temat gotowości na największe wyzwania cyfrowego świata.

Ponad 20 dyskusji obejmujących pełne spektrum problemów, dylematów i wyzwań związanych z cyberbezpieczeństwem i odpornością na rosnącą falę cyfrowej agresji złożyło się na program CYBERSEC EXPO & FORUM 2026. Dwudniowe wydarzenie odbyło się 15 i 16 czerwca br. w Międzynarodowym Centrum Kongresowym w Katowicach.

Debaty z udziałem przedstawicieli administracji rządowej, ekspertów, przedsiębiorców i świata nauki dotyczyły standardów

bezpieczeństwa, modeli regulacyjnych i architektury cyfrowej. Przed wyzwaniami związanymi z cyberbezpieczeństwem stoją instytucje państwowe, organizacje, biznes, ale i zwykli obywatele, korzystający na co dzień z rozwiązań w cyfrowej przestrzeni.

Program wydarzenia wypełniły rozmowy o odporności w świecie rosnących zagrożeń, coraz bardziej złożonych relacji geopolitycznych oraz nowych technologii. Hasło towarzyszące konferencji „We are the firewall” przypominało, że

cyberbezpieczeństwo zaczyna się od technologii, ale zależy od ludzi i ich odpowiedzialnych decyzji.

– Cybersec, unikatowe w europejskiej skali wydarzenie z 10-letnim doświadczeniem, po raz pierwszy w tym roku jest organizowane przez PTWP. Zależy nam na tym, by było to miejsce spotkania branży, gdzie wspólnie tworzymy najlepsze warunki do otwartej, wszechstronnej debaty o cyberbezpieczeństwie w Europie Centralnej – stwierdził Wojciech Kuśpiak, prezes Grupy PTWP.

Cyberbezpieczeństwo to nie tylko technologia, to bezpieczeństwo państwa, gospodarki i społeczeństwa – ta konstatacja powracała jako motto w wielu debatach i rozmowach – tych o strategicznym zakresie i tych bardziej specjalistycznych, poświęconych cyfrowej odporności w energetyce, przemyśle, czy systemie ochrony zdrowia.

– Debata o cyberbezpieczeństwie przestała być rozmową wyłącznie o technologiach i systemach IT. Coraz częściej dotyczy odporności państwa, gospodarki i infrastruktury, od której zależy codziennie funkcjonowanie obywateli i firm – zwróciła uwagę Aleksandra Helbin, redaktor naczelna WNP. – Dlatego podczas CYBERSEC EXPO & FORUM 2026 połączyliśmy perspektywę administracji, biznesu i ekspertów, by rozmawiać o cyberodporności jako jednym z kluczowych warunków bezpieczeństwa i rozwoju nowoczesnego państwa.

W trakcie gali Cybersec Awards uhonorowano osoby i organizacje wyznaczające nowe standardy ochrony w cyfrowym świecie. Nagrody zostały przyznane w kategoriach: Innowacja Roku, Firma Roku, Lider w Cyberedukacji oraz Mistrz Cyberbezpieczeństwa.

CYBERSEC wchodzi w nową dekadę z nowymi możliwościami – od 2026 roku rozwijany w strukturach Grupy PTWP, zyskuje skalę, zaplecze organizacyjne oraz kompetencje, które pozwalają mu stać się największym i najważniejszym wydarzeniem poświęconym cyberbezpieczeństwu w Europie Środkowo-Wschodniej.



WIĘCEJ
O WYDARZENIU

Wnioski i rekomendacje

01

Strategie

- Liczba i skala cyberataków pokazują, że stały się one powszechnym narzędziem, wykorzystywanym w wojnie hybrydowej. Dlatego wielkiego znaczenia nabiera budowanie potencjału technologicznego, który może być wykorzystany do wzmocnienia cyberodporności państwa.
- Sukces Strategii Cyberbezpieczeństwa zależy od tego, czy zawarte w niej rozwiązania realnie zaadaptuje rynek i administracja, czy też pozostaną jedynie w sferze formalnych zapisów. Nadal częściej rozmawiamy o potrzebie suwerenności cyfrowej, niż wdramy konkretne mechanizmy, wspierające lokalny ekosystem technologiczny czy premiujące rozwiązania europejskie w sektorze publicznym
- Osiągnięcie autonomii w stopniu, w jakim jest możliwa – z uwzględnieniem specyfiki łańcucha dostaw w dziedzinie cyberbezpieczeństwa – oznacza potężne inwestycje. Trzeba wspierać ten proces, wybierając europejskie technologie wszędzie tam, gdzie to możliwe.
- W działaniach na rzecz niezależności uwzględnić należy jednak globalne łańcuchy dostaw i międzynarodową wymianę informacji o zagrożeniach oraz interoperacyjność systemów bezpieczeństwa. Suwerenność nie może oznaczać izolacji. Nadmierny protekcjonizm mógłby ograniczyć tempo innowacji i utrudnić współpracę operacyjną między sojusznikami (NATO, UE).
- Plany ciągłości działania, scenariusze incydentów i ścieżki komunikacji nie mogą tkwić w dokumentach, lecz muszą być systematycznie i realnie testowane.

- Strategiczna luka w cyberbezpieczeństwie nie wynika z ram prawnych czy niedostatku regulacji, lecz z braku koordynacji działań między sektorami i „silosami” cyberobronnej działalności. Potrzebujemy więcej audytów i presji ze strony administracji centralnej.
- Korporacje i inne rozbudowane organizacje są przygotowywane na mierzenie się z cyberzagrożeniami. Samorządy pozostają na bardzo różnych poziomach dojrzałości cyfrowej. Kłopotem jest na razie „zejście” z działaniami do poziomu lokalnego, gdzie jednostki administracyjne borykają się z takimi problemami jak finanse i utrzymanie specjalistów. W tym przypadku (dotyczy to także MSP) nieodzowna jest pomoc państwa (bo nie chodzi tylko o finanse).
- Uproszczenie systemu... Jeden incydent prowokuje wiele zawiadomień trafiających do różnych jednostek policji i prokuratury, co utrudnia skuteczne ściganie sprawców. Koordynacja na wstępnym etapie pozwoliłaby łączyć postępowania prowadzone o ten sam czyn, albo wobec tej samej grupy.

02

Regulacje

- Podnoszenie wymagań bezpieczeństwa nie musi oznaczać trudności w innowacyjności. Przeciwnie: wspólne standardy mogą przyspieszyć rozwój rynku poprzez uporządkowanie zasad współpracy i przyrost zaufania do produktów cyfrowych. Firmy, które odpowiednio wcześniej dostosują się do nowych wymogów, będą mogły

wykorzystać bezpieczeństwo jako element przewagi konkurencyjnej.

- Nowe regulacje będą stopniowo wpływać na łańcuchy dostaw, sposób wyboru partnerów technologicznych oraz strategię zakupowe przedsiębiorstw. Wzrośnie znaczenie transparentności, zaufania i możliwości weryfikacji bezpieczeństwa produktów. To proces, który wymaga czasu, ale jego skutki mogą trwale zmienić europejski rynek technologiczny.
- Zakres obowiązywania NIS2, regulacji przyjętej w 2022 r., nie kończy się na organizacjach bezpośrednio nią objętych, lecz dotyczy także podwykonawców, dostawców usług, producentów oprogramowania i wszystkich firm z łańcuchów dostaw. Ok. 20 tys. podmiotów wprost wchodzi do systemu, ale drugie tyle może zostać objęte tymi wymaganiami pośrednio. Eksperci wskazują, że czas nagli: powinniśmy być już na etapie szczegółowych wdrożeń, tymczasem dominują ogólne rozważania i przygotowania.
- Nowe przepisy przewidują możliwość wskazania określonych dostawców lub technologii jako zagrożenia dla bezpieczeństwa państwa. Zachodzi obawa, że organizacje mogłyby zostać zobowiązane do wymiany sprzętu lub usług, nawet jeśli rozwiązania technicznie działają poprawnie. Może dojść do sytuacji, w której bezpieczny sprzęt trzeba będzie usunąć wyłącznie dlatego, że został uznany za element ryzykownego łańcucha dostaw.
- Biznes obawia się, że nowe regulacje prawne (KSC i NIS2) mogą w praktyce prowadzić do sytuacji, gdy po cyberataku firmy i instytucje będą rozliczane przede wszystkim z tego, czy wdrożyły odpowiednie procedury zarządzania ryzykiem i środki ochrony; to, że są ofiarą ataku, zejdzie na plan dalszy.
- Konieczna jest nowelizacja przepisów dotyczących pozyskiwania elektronicznego materiału dowodowego, zwłaszcza danych telekomunikacyjnych i objętych tajemnicą bankową.

Większość cyberprzestępstw jest nastawiona na monetyzację – tylko dzięki zasadzie „follow the money” można dotrzeć do sprawców i odzyskać te środki.

03

Biznes/organizacje

- Strategiczne podejście do cyberobrony wymaga zintegrowania cyberbezpieczeństwa z celami biznesowymi, angażowania w ten proces wszystkich interesariuszy oraz budowania kultury bezpieczeństwa.
- Skuteczna strategia cyberobrony musi wykraczać poza mury własnej organizacji, obejmując rygorystyczną kontrolę łańcucha dostaw oraz głęboką integrację z krajowym i międzynarodowym ekosystemem cyberbezpieczeństwa.
- Suwerenność technologiczna musi jednak – tak czy inaczej – opierać się na zaufaniu, dywersyfikacji i modelu multi-vendor (firma nie skupia się tylko na jednym dostawcy). Chodzi o to, żeby w razie przerwania łańcucha dostaw utrzymać ciągłość kluczowych procesów.
- Zarządy firm często koncentrują się na minimalizacji wydatków na cyberbezpieczeństwo, zamiast na strategicznym zarządzaniu ryzykiem i budowaniu odporności biznesu. Krótkoterminowe oszczędności prowokują wtedy wielokrotnie wyższe koszty po poważnym incydencie: bezpośrednie (zatrzymanie produkcji/działalności operacyjnej, wypłaty odszkodowań, obsługa kryzysu organizacyjnie i wizerunkowo), jak i pośrednie (utrata zaufania klientów, spadek wartości firmy). Bezpieczeństwo cyfrowego należy traktować jako inwestycję w ciągłość działania, przewagę konkurencyjną i długoterminowy wzrost organizacji.



- Fundamentalne w organizacji pozostaje zdefiniowanie krytycznych procesów IT, identyfikacja zasobów krytycznych, określenie stopnia zależności od dostawców oraz przygotowanie realnych scenariuszy działania w trybie awaryjnym, pozwalających utrzymać kluczowe usługi nawet w czasie incydentu bezpieczeństwa.
- Nie należy tracić z oczu dość prozaicznych niebezpiecznych dróg. „Drogą wejścia” do dużych, lepiej bronionych organizacji, instytucji rządowych czy operatorów infrastruktury krytycznej może być np. serwisant urządzeń brzegowych, integrator usług cyfrowych lub firma kurierska. Konieczne jest audytowanie dostawców; deklaracja zgodności z normami to za mało.
- Cyberbezpieczeństwo w przemyśle to nie tylko kwestia techniczna, ale w dużej mierze organizacyjna i zarządcza. Wyzwania wynikają ze skali i złożoności ekosystemu przemysłowego, gdzie

wiele podmiotów współpracuje przez długi okres eksploatacji. Kluczowe jest – znów – świadome zarządzanie ryzykiem, moderowanie procesów oraz nadzór ze strony zarządów firm.

- Poziom cyberbezpieczeństwa przedsiębiorstw podniosłoby regularne ćwiczenia symulacyjne, angażujące całe organizacje (w tym zarządy) i pozwalające przygotować się na incydenty. Konieczne jest opracowanie scenariuszy reagowania i stosowanie podstawowych standardów cyberhigieny (w tym dwuskładnikowego uwierzytelnienia).
- Najwyższy rangą menedżer w organizacji odpowiedzialny za strategię cyberbezpieczeństwa i ochronę informacji (CISO – Information Security Officer) powinien rozumieć techniczny wymiar incydentu, ale i jego konsekwencje biznesowo-wizerunkowe oraz wspierać transparentną komunikację w sytuacjach kryzysowych. Zarządy bowiem nierzadko dążą do ograniczania

negatywnego przekazu, próbując przedstawiać incydent jako awarię.

- Wykorzystanie AI przez atakujących radykalnie zwiększa szybkość i skalę ataków, więc konieczne staje się budowanie dodatkowego rodzaju odporności, opartego na szybkim odtwarzaniu zdolności cyfrowych uszkodzonych wskutek skutecznego ataku.
- Druga strona medalu: AI skróciła czas znajdowania podatności i anomalii – od wykrycia do wykorzystania – z dni w sekundy. Szybko pracujące systemy po stronie obrony pozwolą wykorzystać te możliwości.
- Cyberpolis (ubezpieczenia) powinny stanowić ważne uzupełnienie strategii zarządzania ryzykiem firm i organizacji; a wymagania stawiane przez ubezpieczycieli wpływają na podnoszenie standardów bezpieczeństwa.

04

Edukacja

- W dobie zaawansowanej automatyzacji i AI sercem cyberodporności pozostaje człowiek – to on jest ostatecznym strategiem i decydem w cyfrowym teatrze działań. Technologie i procesy stanowią niezbędne instrumentarium, które jednak bez odpowiedniej kultury bezpieczeństwa, przygotowania/przeszkolenia i „cyfrowego instynktu” personelu traci swoją skuteczność.
- Poziom umiejętności krytycznego myślenia jest w polskim społeczeństwie en bloc niski, co jest poważnym zagrożeniem w dezinformacji posługującej się coraz bardziej zaawansowanymi narzędziami (deepfake). Potrzebny jest nowy model edukacji – nastawiony właśnie na zdolność krytycznego myślenia i weryfikacji informacji, kształtujący analityczne podejście do treści internetowych.

- Państwo powinno skuteczniej edukować, zachęcać do cyberbezpieczeństwa – przede wszystkim do profilaktyki, wspierać w tym organizacje i firmy, promować cyberhigienę i krytyczne podejście do treści już na etapie edukacji szkolnej.
- Cyber Resilience Act wprowadza odpowiedzialność tam, gdzie wcześniej jej brakowało – już na etapie projektowania i tworzenia produktów. Dla uczelni i sektora edukacji CRA oznacza konieczność zmiany sposobu kształcenia przyszłych inżynierów. Bezpieczeństwo musi stać się integralną częścią procesu tworzenia oprogramowania. Potrzebujemy specjalistów, którzy będą projektowali systemy zgodnie z zasadą security by design, a nie naprawiali błędy po wdrożeniu produktu.

05

Wojsko, infrastruktura, zdrowie

- Ataki na infrastrukturę krytyczną, wykradanie danych, dezinformacja i zakłócanie systemów dowodzenia przeciwnika stanowią dziś standardowy zestaw narzędzi wojskowych, które – użyte przez przeciwnika – mogą sparaliżować działanie państwa.
- Najskuteczniejsza obrona przed cyberatakami to taka, która odstrasza, czyli wiąże się z konsekwencjami dla napastnika. Polska powinna naciskać, by w NATO nie było to tylko odpieranie ataków, lecz „budowanie kosztu dla agresora”.
- Polskie firmy mają technologie, które mogą zainteresować wojsko, ale na polu dual-use sama innowacyjność nie wystarczy. Kluczowe są bezpieczeństwo łańcucha dostaw, „kontrola nad kodem” i komponentami

oraz zrozumienie wymagań regulacyjnych.

- Polskie siły zbrojne będą potrzebować coraz więcej fachowców IT, w tym od cyberbezpieczeństwa. Dlatego system retencji kadr i retencji doświadczenia między wojskiem a sektorem cywilnym musi się zmienić. Przepływ fachowców musi być sprawny i efektywny, także w pomocy byłym mundurowym w przejściu na rynek cywilny.
- Przepisy bezpieczeństwa nie nadążają za zmieniającą się infrastrukturą mediów, w której coraz więcej zależy od dostawców technologii, serwisu, oprogramowania i komunikacji między urządzeniami. W cyberochronie infrastruktury krytycznej chodzi o przejście od ochrony konkretnych obiektów do realnego zapewnienia ciągłości usług kluczowych – przede wszystkim dostaw energii, wody i ciepła – niezależnie od tego, kto i gdzie utrzymuje dany element systemu.
- Brak w zamówieniach publicznych wymagań dotyczących jakości oprogramowania i testów bezpieczeństwa to poważny problem osłabiający ochronę systemów medycznych.
- Incydenty w służbie zdrowia mogą być częścią większego planu, np. destabilizacji politycznej i społecznej – wywołania chaosu informacyjnego. Cyberatak skutkujący przerwą w działalności placówek ochrony zdrowia byłby problemem całego państwa. Dlatego nadzernym celem winno być zapewnienie ciągłości działania systemu ochrony zdrowia w warunkach krytycznych.

Wnioski i rekomendacje stanowią wybór – w syntetycznej formie – wątków, uwag i postulatów, które pojawiły się w dyskusji podczas CYBERSEC EXPO & FORUM [15-16 czerwca 2026 r. w Katowicach] – spotkanie zorganizowanego przez Grupę PTWP.

wnp • economic trends



CYBERSEC EXPO & FORUM 2026 (15-16 czerwca br., Międzynarodowe Centrum Kongresowe w Katowicach), zorganizowane przez Grupę PTWP. Uważnie rejestrowaliśmy wypowiedzi w konferencyjnych dyskusjach – wybrane zamieściliśmy w niniejszej publikacji. Obserwacje i wnioski z katowickiej debaty znalazły też swoje odbicie we Wniosekach i rekomendacjach.

Autorzy tekstów w raporcie
„Cyberodporność. Wersja polska”

**Nikoła Bochyńska (rozdział I i III), Elżbieta Rutkowska (rozdział II i IV),
Włodzimierz Kaleta (rozdział V), Adam Pantak (rozdział VI)**

WYDAWCA:
PTWP SA, pl. Sławika i Antalla 1,
40-163 Katowice

PREZES ZARZĄDU:
Wojciech Kuśpik

REDAKTOR NACZELNA WNP:
Aleksandra Helbin

**OPRACOWANIE REKOMENDACJI,
REDAKCJA, PRZYGOTOWANIE
TECHNICZNE:**
Oskar Filipowicz, Jacek Ziarno (WNP
Economic Trends)

SKŁAD/OPRACOWANIE GRAFICZNE:
Katarzyna Karpińska

KOREKTA:
Justyna Wojdała, Tomasz Rabsztyn

FOTOEDYCJA:
Michał Oleksy

ZDJĘCIA:
archiwum PTWP, materiały prasowe
firm, Shutterstock, Adobe Stock

**wnp • economic
trends**