Bezpieczeństwo i suwerenność cyfrowa – jak je dziś rozumieć i jak je budować?

DR KRZYSZTOF GAWKOWSKI
Wiceprezes Rady Ministrów, Minister Cyfryzacji, Pełnomocnik Rządu ds. Cyberbezpieczeństwa

Bezpieczeństwo – to słowo, które uspokaja. Suwerenność – to takie, które zobowiązuje. A przymiotnik „cyfrowy"? On potrafi zmienić znaczenie każdego z nich. Sprawia, że to, co znane, staje się inne. Nadaje dobrze znanym pojęciom nowy wymiar. I dlatego właśnie trzeba je na nowo zrozumieć. Dzięki dynamicznemu rozwojowi kompetencji w zakresie cyberbezpieczeństwa, inwestycjom w infrastrukturę cyfrową oraz aktywnej roli w strukturach NATO i Unii Europejskiej, rola Polski na cyberfroncie znacząco wzrasta. I właśnie dlatego dziś – bardziej niż kiedykolwiek – Polska musi być bastionem. Bastionem cyfrowym Zachodu.

Skala i charakter cyberzagrożeń

W 2024 roku zespoły CSIRT działające w ramach Krajowego Systemu Cyberbezpieczeństwa zarejestrowały łącznie ponad 111 tysięcy incydentów – o 23% więcej niż rok wcześniej. Sam CSIRT NASK odnotował 103 tysiące zdarzeń, co oznacza wzrost aż o 29%. Dominowały oszustwa komputerowe (ponad 97 tysięcy przypadków), wykrycie szkodliwego oprogramowania (ponad 1800 przypadków) oraz podatności usług (ponad 1600 przypadków). To dowód na dynamicznie rosnącą skalę zagrożeń i konieczność dalszego doskonalenia systemów ochrony.

Nasza cyfrowa twierdza jest stale pod ostrzałem cyberprzestępców – i musi być wzmacniana w każdej warstwie – doskonalić systemy teleinformatyczne.

Ataki nie są dziś jedynie masowe. Oprócz klasycznych kampanii phishingowych, coraz częściej mamy do czynienia z precyzyjnymi działaniami grup APT – struktur działających na zlecenie państw wrogo nastawionych wobec Polski. Ich celem jest nie tylko kradzież danych, ale także zakłócanie działania krytycznych systemów i przygotowywanie gruntu pod

> ***Cyberataki stają się coraz bardziej złożone i celowe – nasza cyfrowa twierdza musi być stale wzmacniana, bo dziś nieustannie jesteśmy pod obstrzałem, a wróg uderza w fundamenty naszej infrastruktury.***

ataki strategiczne. To działania wycelowane w fundamenty naszej infrastruktury – jak sabotażyści, którzy chcą skruszyć kamień węgielny bastionu.

Kto dziś jest na celowniku

Celem ataków są instytucje administracji publicznej i podmioty krytyczne w łańcuchach dostaw. To już nie tylko problem resortu obrony czy spraw wewnętrznych. Ministerstwo Cyfryzacji – którego pracami kieruję – wspólnie z zespołami CSIRT, służbami oraz Pełnomocnikiem Rządu ds. Cyberbezpieczeństwa – którego funkcję również pełnię – prowadzi działania osłonowe wobec szerokiego spektrum podmiotów. Każda gmina, każde przedsiębiorstwo wodociągowe, każdy powiat to cegła w murze polskiego bastionu – jeśli któraś wypadnie, cała konstrukcja traci odporność.

Wojna w Ukrainie istotnie zmieniła krajobraz zagrożeń – zarówno cyfrowych, jak i geopolitycznych. Polska, jako logistyczne zaplecze walczącego państwa, stała się jednym z kluczowych celów wrogich operacji cyfrowych. Uderzenia są wymierzone w infrastrukturę transportową i informatyczną. Rosnąca aktywność grup przestępczych i haktywistycznych, często działających przy wsparciu wrogich państw, potęguje presję. Dlatego nasz bastion musi mieć nie tylko solidne mury, ale i wartowników – gotowych na każdą zmianę kierunku natarcia.

Co robi państwo – regulacje, kompetencje, technologie

Odpowiedzią jest podejście systemowe: regulacje, technologia, kompetencje. Trwa proces wdrażania dyrektywy NIS2 poprzez nowelizację ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC). Inwestujemy w szkolenia, rozbudowujemy Fundusz Cyberbezpieczeństwa, tworzymy struktury zdolne do operacyjnego reagowania w czasie rzeczywistym – takie jak Połączone Centrum Operacyjne Cyberbezpieczeństwa.

> ***Każdy element państwa – od urzędu gminy po centralny system logistyczny – jest częścią cyfrowego bastionu. Jeśli choć jeden zawiedzie, cała konstrukcja traci odporność.***

Wdrażamy technologie, które mają kluczowe znaczenie dla bezpieczeństwa narodowego: CTI (*Cyber Threat Intelligence*), systemy bezpiecznej łączności, ochronę AntyDDoS dla instytucji strategicznych, w tym Sił Zbrojnych RP, oraz platformę zarządzania bezpieczeństwem S46. Nie tylko budujemy bastion – wzmacniamy także jego bramy, mury i wewnętrzną komunikację.

Programy sektorowe – „Cyberbezpieczny Samorząd", „Cyberbezpieczny Rząd" i „Cyberbezpieczne Wodociągi" – wspierają modernizację jednostek samorządowych, centralnych i branżowych. Obejmują rozwój infrastruktury IT oraz zwiększenie kompetencji zespołów technicznych w jednostkach publicznych. Bastion to nie twierdza jednego miasta – to sieć ufortyfikowanych punktów, które muszą współdziałać i wzajemnie się wspierać.

Szeroko zakrojone działania muszą być kontynuowane, bo prognozy jednoznacznie wskazują, że zagrożenia będą się pogłębiać.

Bezpieczeństwo cyfrowe nie zaczyna się na froncie – zaczyna się od regulacji, kompetencji i technologii, które tworzą niewidzialny, ale nieprzenikniony mur obronny.

Wzrośnie liczba ataków na łańcuchy dostaw, a także wykorzystywanie luk w urządzeniach brzegowych i systemach przemysłowych dostępnych z poziomu sieci. To wymaga nowych kompetencji, nowych zabezpieczeń, nowego myślenia. Bo współczesny przeciwnik nie szturmuje murów – on szuka nieszczelności w przewodach i zapomnianych wejść przez tylne drzwi.

AI jako broń, zaniedbania jako furtka dla ataków

Wciąż wielu operatorów infrastruktury krytycznej i jednostek administracji publicznej nie wdrożyło wieloskładnikowego uwierzytelniania (MFA). W dobie ataków sponsorowanych przez państwa to niedopuszczalne zaniedbanie – bo umożliwia przejęcie kontroli nad systemami o znaczeniu strategicznym. Brak tak podstawowego zabezpieczenia to jak pozostawienie otwartych drzwi w wartowni. A przecież w bastionie drzwi nie mogą same się uchylać.

Obserwujemy narastające zagrożenia wynikające z rozwoju generatywnej sztucznej inteligencji – które wcześniej były jedynie prognozowane. Generatywna AI jest coraz częściej wykorzystywana do tworzenia fałszywych wizerunków, głosów i treści. Przestępcy budują złożone kampanie oszustw, dezinformacji i wpływu psychologicznego. W cyfrowej twierdzy celem są także umysły jej mieszkańców.

W odpowiedzi budujemy systemy oparte na współpracy i wymianie informacji. Wzmacniamy Kolegium ds. Cyberbezpieczeństwa, rozbudowujemy operacyjne struktury zarządzania kryzysowego, integrujemy działania służb i instytucji – w tym CSIRT NASK, GOV, MON, CEZ, CBZC i CSIRT KNF. Regularne spotkania operacyjne Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC) pozwalają na błyskawiczną reakcję w sytuacjach kryzysowych. Bo tylko zgrana załoga potrafi obronić bastion przed szturmem i sabotażem jednocześnie.

Klucz: współpraca i szybka reakcja

Nie patrzymy tylko na dziś. Przyszłość to komputery kwantowe – mogące unieważnić obecne metody szyfrowania. Dlatego rozwijamy kryptografię postkwantową (PQC) i budujemy własne kompetencje w obszarze kwantowej transmisji danych. Mamy się czym pochwalić – w czerwcu, w Poznaniu, uruchomiliśmy pierwszy europejski komputer kwantowy. Dzięki temu projektowi Polska dołączyła do liderów rozwoju technologii kwantowych w Europie.

W cyfrowej wojnie wystarczy jedno zaniedbanie, by wróg wszedł na nasz teren bez walki. Przeciwnik nie szturmuje wyłącznie murów naszej twierdzy – szuka nieszczelności w przewodach i zapomnianych wejść przez tylne drzwi.

Ważne jest, aby działać w tym zakresie teraz – zanim będzie za późno. Nie można czekać, aż wróg wyważy bramę – trzeba ją wzmocnić, zanim postawi pierwszy taran.

Cyberbezpieczeństwo przyszłości zaczyna się dziś – bo tylko bastion zbudowany z kompetencji, technologii i przewidywania przetrwa atak, którego jeszcze nie widać.

Cyberbezpieczeństwo jutra: technologie kwantowe i inwestycje strategiczne

Budujemy Centrum Cyberbezpieczeństwa NASK – złożone m.in. z Krajowego Centrum Odzyskiwania Danych, Centrum Operacyjnego, Laboratorium AI, Laboratorium Fuzzingu oraz Ośrodka Certyfikacji i Modelowania. Projekt wart 310 mln zł zostanie zrealizowany do 2029 roku. To inwestycja w infrastrukturę, kompetencje i niezależność – kluczowa również dla wdrażania dyrektywy NIS2. To serce bastionu – centrum dowodzenia, które musi być odporne na każdą formę zagrożenia.

Realizujemy także cztery strategiczne przedsięwzięcia w ramach KPO – o łącznej wartości ponad 864 mln zł – w tym rozwój pięciu sektorowych zespołów CSIRT, modernizację 500 instytucji publicznych oraz budowę wojewódzkiej sieci ekspertów. Dzięki temu wzmacniamy system zarówno na poziomie lokalnym, jak i ogólnokrajowym. Bo każdy bastion potrzebuje nie tylko murów, lecz także obserwatorów, zwiadowców i ludzi od napraw.

Suwerenność cyfrowa kontra cyberkolonializm

O sile bastionu nie świadczą wyłącznie systemy obronne, lecz także suwerenność cyfrowa. To przed czym przestrzegałem w „Cyberkolonializmie" w 2018 roku[1] – urzeczywistnia się na naszych oczach. Nasze dane są paliwem globalnych koncernów, a my oddajemy kontrolę nad algorytmami, procesami i infrastrukturą. To tak, jakby pozwolić obcym dowodzić własną obroną – z uśmiechem na twarzy.

PLLuM – przykład suwerennej technologii

Dlatego stawiamy na własne rozwiązania technologiczne – jak PLLuM, polski duży model językowy stworzony przez naszych ekspertów, rozwijany z myślą o administracji, edukacji i innowacji. Udostępniliśmy go publicznie, by wspierał transformację cyfrową w zgodzie z polskim językiem, kulturą i potrzebami. Bo jeśli AI ma się do nas odzywać, niech mówi naszym głosem – z wnętrza naszej fortecy, a nie zza jej murów.

Polska dziś chroni nie tylko siebie – staje się architektem wspólnej cyfrowej europejskiej twierdzy.

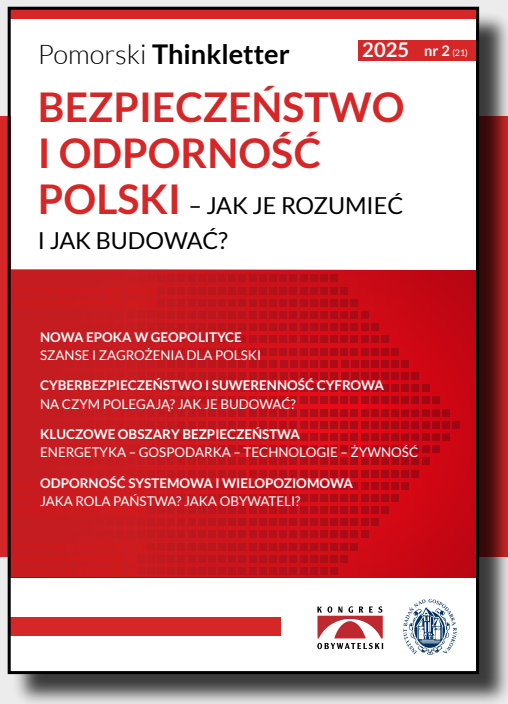
Polska w UE – lider cyfrowego bezpieczeństwa

Dziś bezpieczeństwo i suwerenność cyfrowa to nie wybór, lecz obowiązek. Podczas polskiej prezydencji w Radzie UE uczyniliśmy cyberbezpieczeństwo jednym z kluczowych priorytetów. Efektem naszych działań było przyjęcie unijnego Cyber Blueprint – wspólnych ram reagowania Unii na wielkoskalowe incydenty w cyberprzestrzeni. Polska odegrała tu rolę architekta cyfrowego bezpieczeństwa Europy. Pokazaliśmy, że nie tylko bronimy własnych murów, lecz budujemy wspólną, bezpieczną twierdzę europejską. Polska już dziś jest bastionem cyfrowym Zachodu. I nie ustąpi pod presją. ■

1 K. Gawkowski, *Cyberkolonializm. Poznaj świat cyfrowych przyjaciół i wrogów*, Gliwice 2018.

O AUTORZE

dr Krzysztof Gawkowski – Wiceprezes Rady Ministrów, Minister Cyfryzacji, Pełnomocnik Rządu ds. Cyberbezpieczeństwa. Doktor nauk humanistycznych, absolwent studiów podyplomowych z zakresu prawa pracy na Uniwersytecie Warszawskim. W latach 2002–2010 Radny Rady Miejskiej w Wołominie, 2010-2014 Radny Sejmiku Województwa Mazowieckiego. Od 2019 roku Poseł na Sejm RP z okręgu bydgoskiego, Członek Sejmowej Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii. W latach 2019-2023 Przewodniczący Klubu Parlamentarnego Lewicy, od 2021 roku Wiceprzewodniczący partii Nowa Lewica. Wykładowca akademicki, ekspert w zakresie cyberbezpieczeństwa państwa. W latach 2015-2020 Członek Komitetu Technicznego Polskiego Komitetu Normalizacyjnego. Autor licznych artykułów naukowych oraz publikacji monograficznych poświęconych nowym technologiom, cyfryzacji, sztucznej inteligencji i cyberbezpieczeństwu, w tym książki Cyberkolonializm. Poznaj świat cyfrowych przyjaciół i wrogów, wyróżnionej przez Polskie Towarzystwo Informatyczne.



POBIERZ CAŁĄ PUBLIKACJĘ

www.**kongresobywatelski**.pl