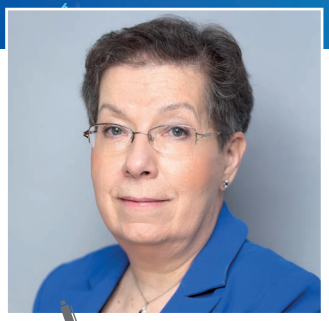
Cyber-stan

Mamy nowy rząd, w wielu resortach zapowiadane są audyty. Jako certyfikowany audytor systemów informatycznych zalecam zbadanie wielu obszarów dotyczących cywilnego cyberbezpieczeństwa.



Joanna Karczewska

absolwentka Wydziału Elektroniki PW z ponad 40-letnim doświadczeniem w informatyce. Jako certyfikowany audytor systemów informatycznych – CISA – specjalizuje się w audytach informatycznych w jednostkach sektora finansów publicznych. Pełni także rolę inspektora ochrony danych w placówkach oświatowych. Jako Expert Reviewer uczestniczyła w opracowaniu metodyk COBIT5 i COBIT 2019, ITAF 4th Edition oraz publikacji ISACA dotyczących Digital Trust Ecosystem Framework. Bierze udział w konsultacjach aktów prawnych dotyczącychbezpieczeństwa informacji, cyberbezpieczeństwa i ochrony danych osobowych, również na forum Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii Sejmu RP. Uznana w 2022 roku za jedną z Europe's Top Cyber Women. Ekspert Najwyższej Izby Kontroli.

Po wielu latach starań i ośmiu podejściach w dniu 22 października 2019 r. Rada Ministrów przyjęła Strategię Cyberbezpieczeństwa RP na lata 2019–2024.

Strategia na papierze

Przypomnę główny cel: *podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji*. Czy po czterech latach podnoszenia i zwiększania ktokolwiek widział jakąkolwiek informację o stopniu realizacji Strategii? Czy ktokolwiek wie, czy został osiągnięty którykolwiek z pięciu wyznaczonych celów szczegółowych? Jeżeli nie, to co udało się wprowadzić czy wdrożyć, a co jeszcze wymaga pracy?

Ponad rok temu, w dniu 6 lipca 2022 r. na posiedzeniu Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (CNT) Sejmu RP Janusz Cieszyński, sekretarz stanu w Kancelarii Prezesa Rady Ministrów i zarazem pełnomocnik rządu do spraw cyberbezpieczeństwa, przedstawił najważniejsze – według niego – informacje ministra cyfryzacji na temat realizacji Strategii. Skorzystałam z okazji i zadałam konkretne pytania dotyczące celów szczegółowych. Do dziś dnia nie otrzymałam pisemnej odpowiedzi, którą chciałam się podzielić z czytelnikami „Domeny".

Pisemne informacje przekazywane komisjom sejmowym przez ministrów i prezesów urzędów nie są udostępniane innym zainteresowanym oprócz posłów. Jeżeli szukamy informacji, to pozostaje nam mozolne przeglądanie sprawozdań z posiedzeń komisji oraz odpowiedzi na interpelacje i zapytania poselskie publikowane na stronie internetowej Sejmu.

W przypadku Komisji CNT są sprawozdania z posiedzeń:

- **z 9 marca 2023 r., na którym rozpatrzono informację na temat przygotowania państwa na płynące z zagranicy zagrożenia związane z cyberprzestępczością;**
- **z 12 lipca 2023 r., na którym rozpatrzono informację Najwyższej Izby Kontroli o wynikach kontroli „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości";**
- **z 16 sierpnia 2023 r., na którym rozpatrzono informacje ministra cyfryzacji dotyczące niedoboru wykwalifikowanej kadry z zakresu IT i cyberbezpieczeństwa, podnoszenia kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa oraz szczególnych zasad wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.**

W minionej kadencji Sejmu interpelacji dotyczących cyberbezpieczeństwa było sporo. Ostatnia o numerze 44299 z 9 października 2023 r. dotyczyła wykorzystania Funduszu Cyberbezpieczeństwa. Z zapytań najciekawsze jest z 16 sierpnia 2023 r. o realizację przez Pełnomocnika Rządu do spraw Cyberbezpieczeństwa zadań w obszarze zarządzania ryzykiem niewłaściwego użycia informacji chronionej przez najwyższe kierownictwa instytucji publicznych.

> *Dla zainteresowanych wymienione dokumenty wraz z odpowiedziami stanowią pierwszą wskazówkę, jaki może być faktyczny stan cywilnego cyberbezpieczeństwa RP oraz co wymaga poprawy lub zmiany, bowiem nawet lakoniczne lub hurraoptymistyczne odpowiedzi pozwalają dokonać oceny bieżącej sytuacji, także za pomocą analizy lingwistycznej.*

Tropem raportów NIK

Najwyższa Izba Kontroli przez ostatnie dziewięć lat przeprowadziła wiele kontroli. Pierwsza dotyczyła realizacji przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP i została przeprowadzona w 2014 r. (wyniki opublikowano w 2015 r.). W kolejnych latach były m.in. kontrole:

- zapewnienia bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych;
- zarządzania bezpieczeństwem informacji w jednostkach samorządu terytorialnego;
- wdrożenia przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych;
- wdrożenia przez administrację publiczną regulacji dotyczących ochrony danych osobowych po wejściu w życie RODO;
- bezpieczeństwa teleinformatycznego RP;
- bezpieczeństwa informacji w pracy na odległość i mobilnym przetwarzaniu danych.

Warto sięgnąć do wniosków pokontrolnych i sprawdzić, czy zostały wdrożone. Czy też, jak w przypadku wymienionej wcześniej kontroli zapobiegania i zwalczania skutków wybranych przestępstw internetowych, badana jednostka nie wdrożyła rekomendacji, bo w raporcie jest pewne *pomieszanie z poplątaniem*, a głównym efektem raportu jest *nieprawdziwe i zmanipulowane pokazanie rzeczywistości, przypisanie różnym organom kompetencji, których nie miały i pominięcie absolutnie całego kontekstu funkcjonowania internetu* – jak stwierdził Paweł Lewandowski, podsekretarz stanu w Ministerstwie Cyfryzacji, na posiedzeniu Komisji CNT 12 lipca 2023 r.

Ministerstwo Cyfryzacji w stanie hibernacji

Koordynatorem wdrażania Strategii Cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji. Zajrzałam na oficjalną stronę Ministerstwo Cyfryzacji > Co robimy > Cyberbezpieczeństwo na portalu gov.pl. Ostatnia modyfikacja miała miejsce 15.07.2020 o godz. 13:10. Podstrona > Strategia jest datowana 20.12.2019. Czyżby w cyberbezpieczeństwie RP nic się nie zmieniło od 3–4 lat?

Sprawdziłam także zakres obowiązków Departamentu Cyberbezpieczeństwa, którym kieruje dyrektor i trzech zastępców. Otóż zadania Departamentu to:

- koordynowanie prac związanych z: Krajowym Systemem Cyberbezpieczeństwa, Krajowym Systemem Certyfikacji Cyberbezpieczeństwa, Strategią Cyberbezpieczeństwa RP i Narodowymi Standardami Cyberbezpieczeństwa;
- przygotowanie i prowadzenie programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i budowania świadomości z zakresu cyberbezpieczeństwa;

- prowadzenie spraw związanych z nadzorem ministra nad Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym (NASK-PIB).

Na wspomnianym lipcowym posiedzeniu Komisji CNT okazało się, że *w pionie ministerstwa, który się zajmuje cyberbezpieczeństwem, są 63 osoby bardzo wysoko wykwalifikowane, które mają olbrzymie doświadczenie na rynku, w służbach i zajmują się tymi kwestiami w sposób bardzo systemowy*. Biorąc pod uwagę chociażby wcześniej wymienione dokumenty oraz moje artykuły, w których od trzech lat opisuję różne cyber-odklejki, cyber-absurdy i cyber-bambików, wykonywanie zadań Departamentu wymaga gruntownej weryfikacji.

Jak wykazała kontrola NIK dotycząca zapobiegania i zwalczania skutków wybranych przestępstw internetowych, *w KPRM zostały utworzone odrębne, rozbudowane struktury przeznaczone do obsługi kancelaryjno-biurowej Pełnomocnika (Biuro Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa), w której na koniec 2021 r. było zatrudnione 17 osób)*. Na stronie www.gov.pl/web/premier/pelnomocnik-rzadu-do-spraw-cyberbezpieczenstwa opublikowana jest tylko podstawa prawna powołania Pełnomocnika, zaś na portalu gov.pl znalazłam jedynie 3 komunikaty, 1 informację, 1 rekomendację i 1 oświadczenie obecnego jeszcze Pełnomocnika, opublikowane po jego powołaniu w czerwcu 2021 r. Dowiedziałam się także, że w Biurze jest nawet Wydział Promocji Polityki Cyfrowej (cokolwiek to znaczy). Pełnomocnik jest ustawowo zobowiązany do opracowania i przedłożenia sprawozdań Radzie Ministrów w terminie do 31 marca każdego roku za poprzedni rok kalendarzowy. Dla audytorów sprawozdania będą kolejnym tropem.

NASK nie bez skazy

NASK jest dziwnym podmiotem. Powstał w 1991 r. jako zespół na Uniwersytecie Warszawskim, późniejsze zmiany następowały aż do 2017 r., gdy został państwowym instytutem badawczym (PIB). Prowadzi „badania naukowe, prace rozwojowe", a jego misją jest „poszukiwanie i wdrażanie rozwiązań, służących rozwojowi sieci teleinformatycznych w Polsce oraz poprawie ich efektywności i bezpieczeństwa". Deklaracja pokrywa się z zapisami ustawy o instytutach badawczych (Dz.U. nr 498 z 2022 r. z późn. zm.), według której do podstawowej działalności każdego PIB należy:

– prowadzenie badań naukowych i prac rozwojowych – przystosowywanie wyników badań naukowych i prac rozwojowych do potrzeb praktyki,
– wdrażanie wyników badań naukowych i prac rozwojowych oraz
– wykonywanie zadań szczególnie ważnych dla planowania i realizacji polityki państwa w zakresie opracowywania i opiniowania standardów, a także monitoringu zjawisk i wydarzeń mogących stwarzać zagrożenie publiczne.

Jednocześnie, jak przyznają jego przedstawiciele, NASK prowadzi „działalność operacyjną na rzecz bezpieczeństwa polskiej cywilnej cyberprzestrzeni", bowiem od 2018 r. jako CSIRT jest kluczowym cywilnym elementem krajowego systemu cyberbezpieczeństwa. Zajmuje się też edukacją użytkowników internetu. Powstały dualizm działalności naukowej i operacyjnej wprowadza pewne pomieszanie z poplątaniem, szczególnie gdy mówimy o odpowiedzialności i rozliczalności.

NASK został ustawowo uznany za wiodący ośrodek wiedzy o cyberbezpieczeństwie. Zatem można oczekiwać od niego najwyższej dbałości i staranności zawodowej. Niestety, tak nie jest.

Oto kilka przykładów poważnych wpadek:

- rok 2019: kontrola NIK „Realizacja programu Ogólnopolskiej Sieci Edukacyjnej (OSE)" wykazała brak Polityki bezpieczeństwa dla sieci OSE, której budowa rozpoczęła się w 2017 r. Stosowne normy i standardy wyraźnie wskazują, że NASK powinien był opracować i wdrożyć Politykę nie później niż w dniu rozpoczęcia procesu korzystania z OSE przez szkoły. Nie zrobił tego przez dwa lata, chociaż w ramach OSE dostarcza szkołom bezpłatne usługi bezpieczeństwa teleinformatycznego, obejmujące ochronę przed szkodliwym oprogramowaniem oraz monitorowanie zagrożeń i bezpieczeństwa sieciowego;

- rok 2020: wyniki badania bezpieczeństwa stron internetowych placówek oświatowych, wykonanego przez NASK na zlecenie Ministerstwa Cyfryzacji, z nieznanych powodów nigdy nie trafiły do osób najbardziej zainteresowanych. Jeżeli badanie miało coś wnieść, to dyrektorzy wszystkich jednostek objętych badaniem powinni byli otrzymać indywidualne raporty, by móc podjąć stosowne działania kontrolne i naprawcze. Wielu nawet nie wiedziało o badaniu. NASK nie wyciągnął żadnych wniosków dotyczących procedur, o czym się przekonałam w tym roku, gdy badanie jest powtarzane bez ładu i składu;

- rok 2021: poważną wpadkę NASK-u dotyczącą formularza informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa JST, wymaganej w ramach programu „Cyfrowa Gmina", opisałam w numerze 4/2021 Biuletynu PTI. Na szczęście Centrum Projektów Polska Cyfrowa nie dopuściło do blamażu. Z kolei o zamieszaniu i kontrowersjach dotyczących przeprowadzenia samej diagnozy w jednostkach samorządu terytorialnego możemy przeczytać w artykule „Audyt za 1 zł" Katarzyny Żółkiewskiej-Malickiej w numerze 3/2023 „Domeny";

- rok 2022: wspomniana już kontrola NIK dotycząca zapobiegania i zwalczania skutków wybranych przestępstw internetowych wykazała brak wdrożenia przez NASK mechanizmów ewaluacji efektów prowadzonych działań edukacyjnych z zakresu cyberbezpieczeństwa, które umożliwiłyby zwiększenie skuteczności tych działań, w tym dopasowanie sposobów docierania z komunikatami do poszczególnych grup docelowych.

- rok 2023: w poprzednim numerze „Domeny" wykazałam błędy i niedoróbki w poradnikach przygotowanych przez NASK w ramach programów „Cyberbezpieczny Samorząd" i „Firma Bezpieczna Cyfrowo". Moje uwagi zostały odebrane przez zainteresowanych jako kąśliwości, bo przecież są to *specjaliści najlepsi w regionie, a może nawet w Europie*. Ponadto, jak mi tłumaczono, poradniki zostały zatwierdzone przez 30-osobową Radę Naukową NASK-u.

Należy zaznaczyć, że w 2022 r. NASK realizował, na zlecenie Ministerstwa Cyfryzacji, następujące projekty finansowane ze środków budżetu państwa (https://www.nask.pl/pl/projekty-dofinansowane/projekty-realizowane-ze):

- **działania prewencyjno-edukacyjne z zakresu cyberbezpieczeństwa dla kluczowych osób w państwie: dotacja celowa w wysokości 1 630 264,57 zł w 2022 r. (w 2021 r. dotacja celowa wyniosła 1 351 593,75 zł);**
- **działania prewencyjno-edukacyjne z zakresu cyberbezpieczeństwa dla przedstawicieli jednostek samorządu terytorialnego (JST) w województwie podlaskim: dotacja celowa w wysokości 2 080 077,00 zł w 2022 r.;**
- **działania prewencyjno-edukacyjne z zakresu cyberbezpieczeństwa dla pracowników Podstawowej Opieki Zdrowotnej (POZ) – pilotaż w powiecie pajęczańskim: dotacja celowa w wysokości 278 275,00 zł w 2022 r.**

Razem dotacje wyniosły prawie 4 mln złotych. W 2023 r. NASK-owi również przyznano dotacje celowe na:

- **działania prewencyjno-edukacyjne z zakresu cyberbezpieczeństwa w 2023 r. – podnoszenie odporności Rzeczypospolitej Polskiej na zagrożenia w przestrzeni cyfrowej w wysokości 8 950 244,50 zł;**
- **realizację kampanii informacyjno-edukacyjnych dotyczących edukacji społeczeństwa w obszarze cyberbezpieczeństwa i rozwoju społeczeństwa informacyjnego w wysokości 5 406 106,50 zł.**

Razem to ponad 15 mln złotych do rozliczenia i ewaluacji efektów ich wydatkowania.

Na stronie https://laptopdlaucznia.gov.pl w zakładce Centrum informacji > Darmowe oprogramowanie > Program do obsługi poczty elektronicznej oprócz znanego Thunderbirda rekomendowany jest program Blue-Mail amerykańskiej firmy Blix, Inc. z siedzibą w Jersey City, USA. Dlaczego właśnie ten produkt spośród wielu innych dostępnych na rynku? Jako audytor czekam na przedstawienie uzasadnienia wyboru oraz szczegółowej oceny skutków dla ochrony danych dla tego produktu – informacja zawarta na stronie https://bluemail.me/privacy nie wystarczy.

Może nadszedł czas na analizę i zmianę struktury NASK-u, by lepiej podkreślić jego rolę operacyjną w krajowym systemie cyberbezpieczeństwa i doprecyzować odpowiedzialność za podejmowane działania.

> *Czy Rada Naukowa zatwierdzała także listę darmowego oprogramowania proponowanego przez NASK czwartoklasistom, którym właśnie rozdano laptopy?*

Nie trzymamy ręki na pulsie

Sztuczna tzw. inteligencja wzbudza skrajne emocje. Jedni się zachwycają i liczą, że rozwiąże wiele problemów naszego świata. Inni straszą, że pozbawi nas pracy czy wręcz wykończy. Przypominam, że jeszcze 5 lat temu administratorzy systemów AI skarżyli się na brak dostatecznego wsadu danych. Potem nastała pandemia, która wymusiła nagminne i powszechne korzystanie z internetu. Przez dwa lata karmiliśmy bestie naszymi danymi bezrefleksyjnie i bez opamiętania. Wystawiliśmy bestiom także nasze dzieci, wprowadzając naprędce naukę zdalną. Już w 2020 r. alarmowałam o zagrożeniu na konferencji Security First oraz w moim artykule w numerze 2–4/2020 Biuletynu PTI – bez jakiegokolwiek zainteresowania i reakcji ze strony Ministerstwa Edukacji i Nauki.

Teraz musimy nauczyć się z bestiami żyć. W sukurs przychodzi Unia Europejska, przyjmując kolejne przepisy. Niestety, po RODO-wych doświadczeniach mam obawy, czy w Polsce poradzimy sobie z ich skutecznym wdrożeniem i stosowaniem. A problemów przybywa, co wykazała m.in. Podkomisja stała do spraw regulacji prawnych dotyczących algorytmów cyfrowych w trakcie swoich prac w minionej kadencji Sejmu RP.

Ku mojemu zdziwieniu Polska nie uczestniczyła w konferencji AI Safety Summit (www.aisafetysummit.gov.uk), która odbyła się na początku listopada w Bletchley Park z inicjatywy premiera Wielkiej Brytanii i z udziałem znaczących polityków i reprezentantów czołowych firm technologicznych z całego świata. W Deklaracji podpisanej przez rządy 29 państw czytamy m.in.: *There is potential*

*for **serious, even catastrophic, harm**, either deliberate or unintentional, stemming from the most significant capabilities of these AI models. Given the rapid and uncertain rate of change of AI, and in the context of the acceleration of investment in technology, we affirm that **deepening our understanding of these potential risks and of actions to address them is especially urgent**.* W związku z tym premier Rishi Sunak zapowiedział powołanie pierwszego na świecie AI Safety Institute, którego zadaniem będzie testowanie bezpieczeństwa kolejnych pojawiających się rodzajów sztucznej inteligencji.

Tymczasem w Polsce odchodzący minister edukacji i nauki powołuje Instytut Badań nad Renesansem i Barokiem przy Akademii Zamojskiej, który będzie prowadził badania naukowe w zakresie historii literatury polskiej i pedagogiki (https://akademiazamojska.edu.pl/pl/news/1163-instytut-badan-nad-renesansem-i-barokiem-powstal).

Samo MEiN od 8 listopada br. zachęcało do wypełnienia ankiety dotyczącej roli sztucznej inteligencji w edukacji (https://www.gov.pl/web/edukacja-i-nauka/rola-sztucznej-inteligencji-w-edukacji-z-perspektywy-dyrektorow-nauczycieli-i-uczniow-zapraszamy-do-wypelnienia-ankiety), by zebrać – **poniewczasie** – opinie na temat:

- roli sztucznej inteligencji (AI) w edukacji,
- **potencjalnych korzyści i zagrożeń**, które wiążą się z wykorzystywaniem narzędzi opartych na AI,
- wsparcia, którego oczekuje środowisko szkolne w tym obszarze.

Badanie jest skierowane do dyrektorów i nauczycieli oraz uczniów klas VI–VIII szkół podstawowych i szkół ponadpodstawowych. Najwyraźniej to oni zostali uznani przez ministra edukacji za najlepszych specjalistów od oceny zagrożeń ze strony sztucznej inteligencji w oświacie. Instytut Badań Edukacyjnych im tylko asystuje.

Czas na weryfikację przez audytorów procesu realizacji „Polityki dla rozwoju sztucznej inteligencji w Polsce od roku 2020" przyjętej 28 grudnia 2020 r. uchwałą nr 196 Rady Ministrów.

Cyber-kadry

Ostatnie posiedzenie Komisji CNT w mijającej kadencji Sejmu RP (16 sierpnia 2023 r.) poświęcone było problemom z kadrami dla cyberbezpieczeństwa. Podsekretarz stanu w MC Paweł Lewandowski przedstawił bardzo ogólną informację o podejmowanych działaniach szkoleniowych. Niestety, nie powiedział, jak jest mierzona skuteczność organizowanych szkoleń.

Na posiedzeniu dowiedzieliśmy się także o stanie wymienionych wcześniej indywidualnych szkoleń z zakresu cyberbezpieczeństwa organizowanych od 2021 r. dla najważniejszych osób w państwie – parlamentarzystów oraz kadry kierowniczej administracji centralnej i samorządowej. Okazało się, że na koniec kadencji mniej więcej 1/3 parlamentarzystów nadal nie przeszła szkolenia. Szkoda, że lista owych posłów nie jest publiczna.

Czy w nowej kadencji wszyscy parlamentarzyści potraktują własne cyberbezpieczeństwo poważnie? W czwartek 26 października br. nowo wybrani posłowie byli szkoleni z:

- ochrony informacji niejawnych przez przedstawicieli ABW,
- ochrony danych osobowych przez pracowników Kancelarii Sejmu,
- cyberbezpieczeństwa przez przedstawiciela NASK.

Chyba szkolenie nie było skuteczne, skoro na portalu X (dawny Twitter) jeden z nowych posłów już w pierwszym dniu pierwszego posiedzenia Sejmu kwestionował środki bezpieczeństwa informatycznego obowiązujące w Sejmie. Do myślenia daje także liczba odsłon owego wpisu (1,3 mln) i treść komentarzy pod nim, szczególnie pseudofachowców.

Temat cyberbezpieczeństwa prawie nie pojawiał się w debatach politycznych w minionej kampanii wyborczej do Sejmu i Senatu RP. Nieliczne wzmianki w programach poszczególnych partii znajdziemy w zestawieniu przygotowanym przez redaktorkę Nikolę Bochyńską z portalu CyberDefence24 na stronie https://cyberdefence24.pl/polityka-i-prawo/wybory-2023-co-w-cyberbezpieczenstwie-obiecywali-politycy. Nasz kolega Jarosław Deminet w numerze 2/2023 „Domeny" starannie uzasadnił konieczność likwidacji Ministerstwa Cyfryzacji, wiemy jednak z doniesień medialnych, że ministerstwo pozostanie. Należy zatem wspierać działania nowego ministra na rzecz naszego cyberbezpieczeństwa.

Wszystkie informacje zawarte w artykule są podane według stanu na dzień 15 listopada 2023 r.