Cyber–raporty

Zgodnie ze standardami obowiązującymi audytorów systemów informatycznych certyfikowanych przez międzynarodową organizację ISACA, raport z audytu – by był wiarygodny – ma być sporządzony w sposób dokładny, jasny, zwięzły, obiektywny, konstruktywny i terminowy, zaś przedstawione ustalenia muszą być poparte dostatecznymi i odpowiednimi dowodami opartymi na uznanych kryteriach oceny.

Jestem certyfikowanym audytorem i pisząc moje artykuły również stosuję standardy raportowania. Od autorów raportów dotyczących w różnym stopniu cyberbezpieczeństwa oczekuję równej staranności w przedstawianiu swoich ustaleń i wynikających z nich rekomendacji.

Raport MIT

We wrześniu 2023 r. NASK pochwaliła się na swojej stronie szóstym miejscem Polski w rankingu „The Cyber Defense Index 2022/23" opublikowanym przez MIT Technology Review, dwumiesięczniku założonym w 1899 r., będącym własnością prestiżowej uczelni Massachusetts Institute of Technology (https://www.technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23/). W ocenie poziomu cyberbezpieczeństwa uwzględniono cztery kategorie: infrastruktura krytyczna, zasoby cyberbezpieczeństwa, zdolności organizacyjne oraz regulacje i otoczenie prawne w tym obszarze. Dane użyte w analizie pochodziły – jak zaznaczyli autorzy – z wielu publicznie dostępnych zasobów instytucji międzynarodowych i globalnych oraz ankiety przeprowadzonej wśród ponad tysiąca osób kadry kierowniczej odpowiedzialnych za cyberbezpieczeństwo w swoich organizacjach.

Ponieważ raporty NIK, które przywołałam w moim artykule w nr 4/2023 Domeny, oraz inne publicznie dostępne polskie opracowania nie wskazują na tak optymistyczny stan polskiego cyberbezpieczeństwa, napisałam do autorów raportu, by podali *primary and secondary sources of information about Poland's cybersecurity* wykorzystane w rankingu. Ku mojemu zaskoczeniu odmówili podania listy dokumentów źródłowych i innych danych, na podstawie których ocenili cyberbezpieczeństwo w Polsce. Uznałam raport za niewiarygodny i nie zamierzałam do niego wracać. Niestety, pozycja Polski w rankingu jest bezrefleksyjnie przytaczana w domenie publicznej, chociażby w audycji „Czy istnieją skuteczne metody ochrony naszych danych osobowych w sieci?" na portalu GEEKWEEK (https://geekweek.interia.pl/nauka-co-slychac/news-cyfrowy-swiat-nam-zagraza-warto-postawic-na-bezpieczenstwo,nId,7248689).

Raporty polskie

W związku z powołaniem nowego rządu, różne organizacje pozarządowe przygotowały swoje raporty poświęcone cyfryzacji, poruszające także kwestie cyberbezpieczeństwa. Jeden z nich był prezentowany 16 stycznia br. na posiedzeniu Komisji Cyfryzacji Sejmu RP (https://www.sejm.gov.pl/Sejm10.nsf/PosKomZrealizowane.xsp?komisja=CNT#5). Dokument o nazwie „Raport otwarcia w polityce cyfrowej" zawiera bardzo ogólne przemyślenia autorów dotyczące wybranych zagadnień cyfryzacji oraz ich rekomendacje na lata 2024–2027 (https://law4growth.com/raport-otwarcia-w-polityce-cyfryzacji/). W kwestii cyberbezpieczeństwa oprócz banalnych stwierdzeń typu „Zagrożenia cybernetyczne nie znają granic" czy „W XXI wieku inwestycje w cyberbezpieczeństwo są niezbędne" autorzy rekomendują transpozycję dyrektyw EKŁE i NIS2 oraz stworzenie Krajowego Centrum Przetwarzania Danych jako remedium na wszystkie cyber-zagrożenia. O ochronie danych osobowych nie wspominają zaś ani słowem. Autorzy nawet nie zanotowali, że zamiast przywołanego przez nich GIODO mamy obecnie UODO. W dokumencie nie znajdziemy też żadnej listy materiałów

źródłowych i referencyjnych. Toteż żadna z osób obecnych na posiedzeniu nie pochwaliła raportu. Wręcz przeciwnie, wielu uczestników, którzy zabrali głos, ocenili go bardzo krytycznie. Moja generalna uwaga była jedna: zanim autorzy napiszą kolejny raport o cyfryzacji i cyberbezpieczeństwie, niech popracują pół roku przy wdrożeniu i utrzymaniu średniej wielkości systemu informatycznego, najlepiej w jednostce samorządowej. Przekonają się na własnej skórze, jak praktyczne są ich zalecenia.

Drugi raport o nazwie „Państwo podmiotowej cyfryzacji. Diagnoza i kierunki niezbędnych działań" (https://www.batory.org.pl/publikacja/panstwo-podmiotowej-cyfryzacji--diagnoza-i-kierunki-niezbednych-dzialan/) został przedstawiony osobiście nowemu Ministrowi Cyfryzacji (https://www.gov.pl/web/cyfryzacja/koniec-pierwszej-serii-konsultacji-w-ministerstwie-cyfryzacji). Zawiera zestaw postulatów odnoszących się do cyfryzacji państwa, w tym „potrzeby poprawy zarządzania procesem cyfryzacji i wdrażania technologii". Jest w nim bardzo dużo o sztucznej inteligencji. Niestety ani razu nie pojawia się słowo „cyber" z jakimkolwiek rozwinięciem. Autorzy sygnalizują tylko potrzebę wprowadzenia mechanizmów zabezpieczających przed nieuprawnionym dostępem instytucji publicznych do danych obywateli i obywatelek. Są odwołania do innych dokumentów, ale tylko autorstwa zaprzyjaźnionych organizacji. Trzy razy użyto słowa „należy", z kolei słowa „powinien" z odmianami użyto 17 razy na zaledwie dziewięciu stronach publikacji. Mnie szczególnie zaintrygował zapis, że stworzenie organu ds. dostępu do danych dotyczących zdrowia przywróci zawiedzione zaufanie do państwa w obszarze ochrony zdrowia – wszystko przy zachowaniu wysokich standardów ochrony prywatności. Autorzy nie podają jednak, jakie to są standardy. Za to zaznaczają, że Urząd Ochrony Danych Osobowych obecnie nie jest w stanie sprostać nawet zadaniom wynikającym z RODO, a od 2024 r. powinien dodatkowo realizować zadania wynikające z DSA.

Obszaru ochrony zdrowia dotyczy trzeci raport „Dane medyczne w pracy lekarza – stan obecny & pożądane zmiany", przygotowany przez NIL IN – Sieć Lekarzy Innowatorów stworzoną przy Naczelnej Izbie Lekarskiej (https://nil.org.pl/uploaded_files/art_1707132900_raport-dane-medyczne--w-pracy-lekarza.pdf). Dokument prezentuje zagadnienia dotyczące regulacji prawnych w obszarze przetwarzania danych medycznych w Polsce. Tym razem jest wiele odwołań do innych opracowań, w tym raportów NIK. Jest też dużo o cyberbezpieczeństwie oraz statystyka, która podaje w wątpliwość ocenę polskiego cyberbezpieczeństwa wystawioną przez MIT, przynajmniej w sektorze zdrowia: „Pomimo szeregu wymogów związanych z ochroną danych medycznych, dostępne badania wskazują, że nie są one egzekwowane w zadowalającym stopniu. Jak wynika z analizy Centrum e-Zdrowia, w ponad połowie podmiotów zidentyfikowano potrzeby w zakresie cyberbezpieczeństwa (55,9%), przy czym najczęściej zgłaszały je szpitale (86,1%). Wskazywane potrzeby badanych placówek w zakresie cyberbezpieczeństwa to przede wszystkim odporność na cyberataki (68,9%), zwiększenie ochrony danych osobowych (65,9%) oraz poprawa stanu wiedzy o zagrożeniach informatycznych wśród pracowników/kierownictwa jednostki (59,4%)". Zastanawia rekomendacja zapisana w rozdziale 4. „Dane medyczne w pracy lekarza – jak być powinno?", w podrozdziale 4.4 Bezpieczeństwo: „Zasadniczy ciężar związany z zapewnieniem wysokiego poziomu ochrony danych powinien spoczywać na dostawcach sprzętu i oprogramowania, którzy są podmiotami wyspecjalizowanymi, znającymi bieżący stan wiedzy technicznej. Odpowiedzialność lekarza powinna ograniczać się do wyboru sprzętu i oprogramowania, którego dostawca zapewnia spełnianie takiego standardu. Lekarz powinien mieć w związku z tym dostęp do dokumentów, które pozwolą mu zweryfikować i łatwo ocenić dostawców oraz zakres ich odpowiedzialności."

Czyżby autorzy raportu, którzy są prawnikami, bazowali na stanowisku wyrażonym przez WSA w Warszawie w wyroku II SA/Wa 2259/21 z 19 kwietnia 2022 r. ? Dla przypomnienia: sąd w składzie trzyosobowym w uzasadnieniu wyroku uznał, że wybór usługi świadczonej przez profesjonalny podmiot, jakim jest pewna renomowana korporacja, z całą pewnością gwarantuje stosowanie przez ów podmiot przetwarzający odpowiednich środków organizacyjnych i technicznych ochrony danych osobowych wymaganych przez RODO (o sprawie napisałam w nr 1/2023 Domeny). Pozostaje pytanie, jakie dokumenty zostaną uznane – i przez kogo – za wystarczające do weryfikacji i łatwej oceny dostawców. Na razie tylko jedna korporacja amerykańska ma uznanie sądu.

Raporty RODO

W raporcie NIL IN-u zamieszczono tabelę z postulatami związanymi z wykorzystywaniem danych w pracy lekarza. Jako sposoby osiągnięcia postulatu „Dane przetwarzane przez lekarza powinny być bezpieczne", podano m.in.:

- zrealizowanie działań w obszarze bezpieczeństwa, takich jak te przewidziane w Programie rozwoju e-zdrowia w Polsce do 2027 r.;

- wypracowanie krajowej implementacji dyrektywy NIS2 w konsultacji ze środowiskiem medycznym, by nowe wymogi mogły być skutecznie wdrożone przez podmioty wykonujące działalność leczniczą;

- stosowanie kodeksu postępowania z art. 40 RODO.

Zgodnie z RODO kodeks postępowania wymaga wdrożenia odpowiednich mechanizmów monitorowania i egzekwowania zgodności z rozporządzeniem m.in. środków i procedur, o których mowa w art. 24 i 25, oraz środków zapewniających bezpieczeństwo przetwarzania, o których mowa w art. 32. Mechanizmy obejmują regularne przeprowadzanie audytów, których wynikiem jest stosowny raport.

Przejrzałam kodeksy przyjęte dla małych placówek medycznych i szpitali oraz kodeksy dla doradców podatkowych, firm badania opinii i rynku, centrów handlowych, biobanków i branży hotelarskiej złożone do zatwierdzenia. W kwestii środków technicznych i organizacyjnych zapewnienia odpowiedniego stopnia bezpieczeństwa danych osobowych:

- **kodeks postępowania dla sektora ochrony zdrowia dotyczący podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających, zwany kodeksem dla szpitali, odwołuje się do uznanych norm/standardów międzynarodowych, w tym norm PN-ISO/IEC z serii 27000 dotyczących systemów zarządzania bezpieczeństwem informacji (lista jest zawarta w załączniku nr 6);**
- **kodeks dla biobanków odwołuje się do Rozporządzenia o Krajowych Ramach Interoperacyjności i polskiej normy PN-ISO/IEC 27001 oraz przedstawia własne zalecenia techniczne;**
- **kodeks dla firm badania opinii i rynku obejmuje własny Program Kontroli Jakości Bezpieczeństwa Informacji;**
- **pozostałe kodeksy podają własne listy zabezpieczeń.**

Dlaczego audytorzy mają problem? Otóż zgodnie ze standardem audytu 1008 Kryteria, audytorzy są zobowiązani dla badanego przedmiotu sprawy wybierać kryteria oceny, które są obiektywne, kompletne, relewantne, wiarygodne, mierzalne, powszechnie uznawane oraz zrozumiałe przez lub dostępne dla wszystkich czytelników i użytkowników raportu. W sferze cyberbezpieczeństwa podstawowe zasady są uniwersalne i identyczne dla wszystkich branż i sektorów na całym świecie i są zawarte w powszechnie uznawanych standardach, normach i dobrych praktykach opracowanych przez wiodące organizacje zrzeszające specjalistów z całego świata. Audytorzy sięgną po nie w pierwszej kolejności. Dopiero w drugiej lub trzeciej wykorzystają kodeksowe programy czy listy, chyba że okażą się niekompletne bądź nieadekwatne.

Raport o laptopach

Od samego początku programu „Laptop dla ucznia" zwracałam szczególną uwagę na kwestię cyberbezpieczeństwa rozdawanych laptopów. Na posiedzeniu Komisji Cyfryzacji w dniu 14 grudnia 2022 r. podsekretarz stanu w KPRM Paweł Lewandowski zapowiadał, że laptopy będą przekonfigurowane przez dostawców sprzętu, „aby samorządy nie musiały jakoś szczególnie zaprzątać sobie głowy dodatkowym instalowaniem różnego softu czy konfigurowaniem dodatkowym tych komputerów". Zapytałam o zestaw oprogramowania, który będzie instalowany i czy obejmuje środki bezpieczeństwa/cyberbezpieczeństwa. Pan Lewandowski odpowiedział, że wykaz oprogramowania będzie w rozporządzeniu projektowanym przez Ministerstwo Edukacji i Nauki, zaś laptopy będą musiały „posiadać oprogramowanie, które będzie przynajmniej w sposób podstawowy chroniło przed zagrożeniami, jakie czekają na użytkownika Internetu".

Program antywirusowy nie znalazł się na liście oprogramowania instalowanego na pamięci masowej lub udostępnianego do nieodpłatnego pobrania przy rozpoczęciu użytkowania, zawartej w załączniku do Rozporządzenia Ministra Edukacji I Nauki z dnia 28 grudnia 2022 r. zmieniającego rozporządzenie w sprawie podstawowych warunków niezbędnych do realizacji przez szkoły i nauczycieli zadań dydaktycznych, wychowawczych i opiekuńczych oraz programów nauczania (Dz.U. z 2022 r. poz. 2811). Wpisano tylko wymóg techniczny wbudowanych mechanizmów bezpieczeństwa dostępu do danych. Ostatecznie Ministerstwo Cyfryzacji i Centrum Obsługi Administracji Rządowej, które prowadziło przetarg, zrezygnowali z wymogu instalowania jakiegokolwiek oprogramowania na zamówionych laptopach, by uniknąć zarzutów o wgrywanie przy okazji aplikacji szpiegującej.

Dzieci dostały fabrycznie nowy sprzęt z systemem operacyjnym MS Windows 11 Pro Edu i wygrawerowanym orzełkiem oraz portal www.laptopdlaucznia.gov.pl, prowadzony przez NASK-PIB, gdzie w Centrum informacji umieszczono Bazę wiedzy, obejmującą m.in. listę darmowego oprogramowania do wykorzystania na laptopach. O proponowanym programie pocztowym BlueMail napisałam w numerze 4/2023 Domeny.

Reszta listy nie obejmuje programu antywirusowego. Nie ma nawet informacji, czy jest potrzebny. Wprawdzie MS Windows 11 ma wbudowany moduł zabezpieczeń, jednak warto o nim poinformować beneficjentów programu i podpowiedzieć, jak skonfigurować różne opcje zabezpieczeń udostępnionych przez firmę Microsoft.

Jedyny poradnik „ABC Cyberbezpieczeństwa" do pobrania w sekcji „Edukacja" portalu zawiera ponad 150 alfabetycznie ułożonych haseł wraz z definicjami. Już widzę, jak dziesięciolatki i ich rodzice rzucają wszystko i biorą się za lekturę 105-stronicowego opracowania, zanim uruchomią swój nowy sprzęt. Nie rozumiem, dlaczego do każdego pudełka z laptopem nie włożono ulotki formatu A4 z podstawowymi zasadami cyberbezpieczeństwa. Mam całą kolekcję różnych materiałów o cyberbezpieczeństwie opracowanych dla dzieci przez NASK i inne podmioty za pieniądze publiczne (krajowe i unijne). Szczególny wysyp nastąpił w pandemii. Wystarczyło wybrać, dostosować, wydrukować i rozdać,

a wersję elektroniczną udostępnić na portalu. Wszystkie media powielałyby informację i samą ulotkę. Zasięgi byłyby niebotyczne. Cóż, zabrakło wyobraźni, myślenia i prawdziwej chęci uświadamiania o cyber–zagrożeniach.

Pojawiło się już pierwsze podsumowanie Programu „Laptop dla ucznia" (https://www.gov.pl/web/cyfryzacja/program-laptop-dla-ucznia-nie-mial-zabezpieczonego-finansowania). Jak podało Ministerstwo Cyfryzacji w komunikacie z 8 lutego 2024 r., problemy merytoryczne programu „Laptop dla ucznia" obejmują:

- **brak przygotowania systemowego do wykorzystywania urządzeń przez dzieci w szkole oraz w domu – brak strategii cyfryzacji edukacji przygotowanej przez poprzednie kierownictwo MEiN. Brak wytycznych dla nauczycieli i szkół, jak wykorzystywać komputery przez dzieci;**
- **brak przygotowania szkół do włączenia komputerów w działania edukacyjne – brak infrastruktury LAN, infrastruktury przyłączy elektrycznych, brak bezpiecznego systemu przechowywania laptopów, które stanowią własność rodziców;**
- **brak wsparcia uczniów w zakresie higieny cyfrowej.**

Informacja na temat realizacji programów „Laptop dla ucznia" oraz „Laptop dla nauczyciela" została także przedstawiona 22 lutego 2024 r. na burzliwym posiedzeniu wspólnym Komisji Edukacji i Komisji Cyfryzacji Sejmu RP.

Laptopy są własnością rodziców/opiekunów prawnych uczniów IV klas oraz nauczycieli. Korzystanie z prywatnego sprzętu do nauki zdalnej zostało już wypracowane w pandemii. Tym razem laptopy są przekazywane z ewidentnym założeniem, że będą noszone z domu do szkoły i ze szkoły do domu. W związku z tym konieczne jest wyjaśnienie m.in. następujących kwestii:

- Czy regulamin Ogólnopolskiej Sieci Edukacyjnej dopuszcza podłączanie do OSE prywatnych laptopów?
- Czy Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych szkoły dopuszcza podłączanie prywatnych laptopów do sieci szkolnej i jej zasobów?
- Czy opieka nad prywatnymi laptopami jest w zakresie obowiązków informatyka szkolnego wynikającym z jego/jej umowy o pracę, umowy o dzieło bądź umowy o świadczeniu usług?
- Co z ochroną danych osobowych na prywatnych laptopach uczniów i nauczycieli?

Przypomnę, że w samym Ministerstwie Edukacji wprowadzono ścisłe reguły pracy zdalnej:

- pracownikom na czas pracy zdalnej udostępniono laptopy służbowe; pracownicy mieli też możliwość zabrania stacjonarnych komputerów służbowych do domu; mogą również pracować w domu na laptopach prywatnych, po uprzednim skonfigurowaniu ich przez pracowników zespołu IT (odpowiedź na interpelację nr 3268);
- praca w miejscu zamieszkania może odbywać się wyłącznie z wykorzystaniem komputera (laptopa) służbowego oraz zgodnie z zasadami wynikającymi z obowiązującego Systemu Zarządzania Bezpieczeństwem Informacji w MEN (odpowiedź na interpelację nr 9654).

Szkoły zasługują na cyberbezpieczeństwo wzorowane na zasadach wprowadzonych w ministerstwie. Ministerstwo Cyfryzacji zapowiedziało w przywołanym komunikacie, że w przyszłym roku uczniowie otrzymają urządzenia mobilne, zaś rodzaj sprzętu, niezbędne oprogramowanie i zabezpieczenia będą przedmiotem analizy oraz dyskusji z partnerami społecznymi i rodzicami. Do dyskusji warto włączyć lokalnych administratorów sieci szkolnych i inspektorów ochrony danych placówek oświatowych.

Wielokrotnie pisałam o cyfrowym zaufaniu, czyli *digital trust*.

> *Zaufanie do cyfryzacji obejmuje także zaufanie do publikowanych raportów o cyfryzacji i o stanie cyberbezpieczeństwa.*

Ich wiarygodność jest istotna, skoro mają nam pomagać w podejmowaniu decyzji i inicjowaniu działań w celu zabezpieczenia naszych danych, zapewnienia naszej prywatności i właściwego korzystania z technologii informatycznych. Tym bardziej w dobie internetu pełnego dezinformacji i fake newsów.

Wszystkie informacje zawarte w artykule są podane według stanu na dzień 23 lutego 2024 r.

Joanna Karczewska