Cyber-szok i niedowierzanie

To emocje, których wiele razy doznałam przez ostatnich kilka tygodni. Szok, bo kolejne zdarzenia pokazują, jak cyberbezpieczeństwo, bezpieczeństwo informacji i ochrona danych osobowych są lekceważone i bagatelizowane. Niedowierzanie, że różne osoby i podmioty nadal bezrefleksyjnie podchodzą do swoich obowiązków i działań dotyczących cyberbezpieczeństwa, bezpieczeństwa informacji i ochrony danych osobowych.

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 funkcję 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 dotyczących bezpieczeństwa 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.

Podpadł mi kolejny bank. W listopadzie 2018 r. przestałam być klientką banku z Żubrem, tymczasem po ponad 5 latach, w marcu 2024 r., otrzymałam pismo na papierze z informacją o zmianach w regulaminie składania i rozpatrywania reklamacji klientów banku będących konsumentami. Od razu wysłałam krótki e-mail do Inspektora Ochrony Danych banku, w którym podałam powyższe fakty i zadałam proste pytanie – na jakiej podstawie bank nadal przetwarza moje dane osobowe? Podpisałam się imieniem i nazwiskiem oraz numerem (byłego) klienta.

Po ponad trzech tygodniach otrzymałam e-mail ze skanem pisma Biura Inspektora Ochrony Danych z informacją, że forma złożenia wniosku w formie skanu nie pozwala jednoznacznie zidentyfikować mojej osoby żądającej dostępu do danych, a tym samym kontynuować procedowanie wniosku. Proszono mnie o wizytę w oddziale banku bądź pismo na papierze opatrzone własnoręcznym podpisem i zawierające mój numer PESEL lub numer klienta banku. Oczywiście wszystko w trosce o bezpieczeństwo moich danych.

Odpisałam, że w e-mailu podałam mój numer klienta oraz że nie wysyłałam żadnych skanów i nie żądałam dostępu do moich danych. Zapowiedziałam także moją wizytę w siedzibie biura IOD na ul. Żubra w Warszawie. Z wizyty zrezygnowałam, poczekam na kolejne pismo. Będzie, bo bank ewidentnie do tej pory nie ogarnął swoich czynności przetwarzania danych osobowych.

Kolejne tłumaczenie

W marcu br. Parlament Europejski zatwierdził Akt o Sztucznej Inteligencji (Artificial Intelligence Act, w skrócie AI Act). Pomna zamieszania z polską wersją GDPR/RODO od razu pobrałam wersję angielską nowego rozporządzenia ze

strony https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html i wersję polską ze strony https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_PL.html, by je zestawić artykuł po artykule i zweryfikować tłumaczenie. Ku mojemu zdziwieniu i niedowierzaniu bardzo szybko znalazłam poważne błędy.

Miesiąc później odbyło się posiedzenie Podkomisji stałej do spraw sztucznej inteligencji i przejrzystości algorytmów Sejmu RP, w trakcie którego przedstawiciele Ministerstwa Cyfryzacji przekazali informację na temat „regulacji zawartych w akcie w sprawie sztucznej inteligencji (AI Act), przyjętym przez Parlament Europejski 13 marca 2024 r.". Skorzystałam z okazji i zapytałam, czy polska wersja aktu będzie weryfikowana oraz czy kiepskiego tłumaczenia dokonała sztuczna inteligencja. W odpowiedzi usłyszałam, że pierwsza wersja Aktu była tłumaczona przez prawników lingwistów oraz że trwa weryfikacja przekładu przez prawników lingwistów. Zatem Ministerstwo Cyfryzacji będzie dysponowało własną polską wersją Aktu. Szkoda, że nie poinformowało o tym w swoim zaproszeniu do udziału w prekonsultacjach założeń wdrożenia AI Act w Polsce (https://www.gov.pl/web/cyfryzacja/wdrozenie-aktu-o-ai---prekonsultacje).

Sceptyków i niedowiarków informuję, że jednym z kardynalnych i niedopuszczalnych błędów popełnionych przy tłumaczeniu AI Act jest zrównanie pojęć „**governance**" i „**management**" za pomocą jednego polskiego odpowiednika „**zarządzanie**" (również w Corrigendum z 16 kwietnia 2024 r.). No cóż, szykuje się nam powtórka z rozrywki w postaci mylących komentarzy prawnych i zamieszania w stosowaniu rozporządzenia – o RODO do poprawki pisałam w numerze 1/2024 „Domeny".

> *Pozostaje pytanie: czy minister cyfryzacji zasiada w rządzie (government) czy w zarządzie (management) Rzeczpospolitej Polskiej?*

Kolejna infolinia

W poprzednim numerze „Domeny" analizowałam różne raporty dotyczące cyfryzacji i cyberbezpieczeństwa w Polsce. Miałam istotne zastrzeżenia dotyczące ich wiarygodności. Nie inaczej jest z raportem „Czas na cyfrową gospodarkę", opracowanym przez ponad czterdzieści organizacji oraz trzech byłych ministrów cyfryzacji pod egidą Fundacji Digital Poland (https://digitalpoland.org/publikacje/pobierz?id=80925fc7-6715-497d-a138-fecc2bf65df5). Raport wraz z rekomendacjami został zaprezentowany 7 marca 2024 r. na posiedzeniu Komisji Cyfryzacji Sejmu RP (https://www.sejm.gov.pl/Sejm10.nsf/biuletyn.xsp?skrnr=CNT-9).

Oprócz uwag, które wymieniłam w trakcie dyskusji w Sejmie, jedna istotna kwestia nie daje mi spokoju. Jest to **przerażający** pomysł zapewnienia doraźnej pomocy dla seniorów poprzez infolinię. Cytuję: *Dzięki profesjonalnej obsłudze seniorzy mogą bardziej świadomie i odważnie korzystać z urządzeń elektronicznych i aplikacji. Dodatkowo infolinia może dostarczać spersonalizowane porady i instrukcje dotyczące konkretnych zagadnień związanych z korzystaniem z komputera, smartfonów czy internetu w dogodnym dla seniorów czasie. Rozmowa z pracownikiem infolinii jest szczególnie ważnym aspektem dla seniorów przyzwyczajonych do kontaktu z człowiekiem*.

Pomysłodawcy ewidentnie nie zapoznali się z wynikami badania SW Research na zlecenie Banku Pocztowego, zrealizowanego w ramach programu „Cyberdojrzali. Bądź mądrzejszy od oszusta", opublikowanymi 26 października 2023 r. na stronie https://www.pocztowy.pl/komunikaty-bezpieczenstwa/news911.html. Badanie potwierdziło, że „to osoby w wieku 60+ zdecydowanie częściej mogą być ofiarami przestępców po drugiej stronie telefonu, maila czy komunikatora internetowego".

Skoro seniorzy nadal ufają osobom, z którymi rozmawiają przez telefon, nic nie stoi na przeszkodzie, by do znanych metod „na wnuczka", „na policjanta" czy „na tanią wycieczkę sakralną" doszła metoda „na infolinię". Tym bardziej, że są już „pewne oddolne inicjatywy", o których poinformowała w trakcie prezentacji jedna z autorek raportu. Otóż powołana 14 listopada ub.r. Koalicja Cyfrowi Seniorzy *oferuje seniorom doraźną pomoc, gdzie w wybranych godzinach mogą zadzwonić i zapytać o takie podstawowe kwestie na przykład jak obsłużyć komputer, jak skorzystać ze smartfona, jak pobrać sobie aplikacje*. I zapewne jak logować się do Internetowego Konta Pacjenta czy do konta bankowego. Szkoda, że na stronie https://cyfrowiseniorzy.pl zabrakło informacji, kto jest operatorem infolinii Koalicji i ponosi za nią odpowiedzialność. Może Fundacja Digital Poland wymieniona jako administrator danych osobowych w Polityce prywatności? Tyle, że tam nie ma słowa o infolinii (zrobiłam zrzut strony dla potomności).

Kolejne komisje

Może seniorzy są mniej sprawni w korzystaniu z komputera, smartfonu czy internetu, za to pani asystentka byłego wiceministra spraw zagranicznych nie miała problemów w korzystaniu z komunikatorów. Możemy się o tym dowiedzieć z jej zeznań złożonych 11 marca 2024 r. przed Komisją Śledczą do zbadania legalności, prawidłowości oraz celowości działań, a także występowania nadużyć, zaniedbań i zaniechań w zakresie legalizacji pobytu cudzoziemców na terytorium Rzeczypospolitej Polskiej w okresie od 12 listopada 2019 r. do 20 listopada 2023 r. (znaną jako komisja ds. wiz). Pani asystentka używała domyślnie WhatsAppa i Signala ze znikającymi wiadomościami do odbierania różnych list na telefonie służbowym i przesyłała je dalej sms-em do depar-

tamentów MSZ, bo *kopiowanie na skrzynkę, która jest na telefonie zabezpieczona, jest trudne i musiałabym użyć prywatnego maila, a nie chciałam tego robić*.

Na pytanie o szkolenie z RODO pani asystentka odpowiedziała, że miała. Na pytanie o szkolenie z zakresu bezpieczeństwa w MSZ pani asystentka odpowiedziała, że *jakieś na pewno*. Na pytanie o wykształcenie podała, że skończyła bezpieczeństwo międzynarodowe i politologię na Akademii Sztuki Wojennej i Uniwersytecie Warszawskim. Toteż z niedowierzaniem słuchałam, jak pani asystentka tłumaczyła członkom Komisji, jakby byli dziećmi, że ustawienie znikających wiadomości zapewnia większe bezpieczeństwo w używanych przez nią komunikatorach. Czyżby tego uczyli na uczelniach, na których studiowała?

Jeszcze większego szoku doznałam, słuchając na żywo transmisji zeznań złożonych 17 kwietnia 2024 r. przed Komisją Śledczą do zbadania legalności, prawidłowości oraz celowości działań podjętych w celu przygotowania i przeprowadzenia wyborów Prezydenta Rzeczypospolitej Polskiej w 2020 r. w formie głosowania korespondencyjnego (https://www.sejm.gov.pl/Sejm10.nsf/PosKomZrealizowane.xsp?komisja=SKGK#19) – znaną jako komisja ds. wyborów kopertowych. Tego dnia świadkami odpowiadającymi na pytania członków Komisji byli panowie Marek Zagórski, były minister cyfryzacji i były pełnomocnik rządu ds. cyberbezpieczeństwa, oraz Jan Nowak, były prezes Urzędu Ochrony Danych Osobowych. Każdy z panów przez ponad dwie i pół godziny wyjaśniał swój punkt widzenia na przekazanie Poczcie Polskiej bazy PESEL z danymi wszystkich Polaków i gminnych spisów wyborców. Obaj panowie mieli całkowite zaufanie do Poczty Polskiej i weryfikacji bezpieczeństwa naszych danych osobowych nie uznali za konieczną. O ocenie skutków dla ochrony danych (art. 35 RODO) nawet nie wspomnieli. Panowie byli spokojni, bo nigdy nie słyszeli, aby doszło do jakichkolwiek problemów z przetwarzaniem danych osobowych przez Pocztę Polską. Mówili to bez jakiegokolwiek wstydu i zażenowania.

Z ich zeznań nie dowiedziałam się, czy Poczta Polska usunęła ze swoich serwerów przekazaną bazę PESEL i przesłane spisy wyborców. Usłyszałam jedynie, że zapewniano obu panów o zniszczeniu nośnika. Liczę, że wyjaśnienie, co Poczta Polska ostatecznie zrobiła z naszymi danymi, znajdę w raporcie końcowym Komisji.

Kolejne diagnozy

Dzień wcześniej na konferencji SECURE 2024, zorganizowanej po raz 27. przez NASK, zaprezentowano wyniki programów zwiększających poziom cyberbezpieczeństwa w samorządach. Podsumowanie dotyczyło przede wszystkim **Diagnozy Cyberbezpieczeństwa** wykonanej w ramach projektu Cyfrowa Gmina, prowadzonego w latach 2022–2023 przez Centrum Projektów Polska Cyfrowa. Celem projektu było wsparcie rozwoju cyfrowego instytucji samorządowych oraz zwiększenie cyberbezpieczeństwa (https://www.gov.pl/web/cppc/cyfrowa-gmina4). W ramach analizy stanu cyberbezpieczeństwa JST (jednostek samorządu terytorialnego) każdy grantobiorca miał obowiązek przeprowadzić diagnozę własnego cyberbezpieczeństwa zgodnie z formularzem przygotowanym przez NASK.

Aby wykazać poprawę, w prezentacji NASK-u zestawiano wyniki Diagnozy z wynikami kontroli NIK dotyczącej „Zarządzania bezpieczeństwem informacji w jednostkach samorządu terytorialnego" z 2018 r. (https://www.nik.gov.pl/aktualnosci/zeby-elektronicznie-znaczylo-bezpiecznie.html).

Ja sięgnęłam do wyników najnowszych kontroli NIK:

- **Zapewnienie ochrony i prawidłowego przetwarzania danych, w tym danych osobowych gromadzonych w formie elektronicznej przez jednostki samorządu terytorialnego oraz podległe jednostki organizacyjne na stronach internetowych, poczcie elektronicznej oraz w związku z odbywającymi się sesjami organów uchwałodawczych w województwie podlaskim – raport opublikowany 22.02.2024 r.**
- **Zapewnienie bezpieczeństwa teleinformatycznego przez jednostki samorządu terytorialnego województwa zachodniopomorskiego – raport opublikowany 03.04.2024 r.**
- **Zarządzanie oprogramowaniem komputerowym przez administrację publiczną – raport opublikowany 29.04.2024 r.**

Ustalenia NIK-u są przygnębiające. Wykazały brak poprawy. Zacytuję kluczowe zdania z komunikatów prasowych NIK: *podstawowe elementy systemu ochrony danych osobowych w jednostkach samorządowych były nieskuteczne*, *samorządy nie były w stanie zapewnić skutecznej ochrony przed potencjalnymi atakami cyberprzestępców* oraz *urzędy dokonywały nie zawsze uzasadnionych zakupów oprogramowania, często od niezweryfikowanych dostawców, nie monitorowały jego stanu i aktualizacji ani też legalności wykorzystania*.

Ponieważ ustalenia kontroli zapewnienia ochrony i prawidłowego przetwarzania danych na Podlasiu nie napawały optymizmem, NIK postanowiła rozszerzyć postępowanie kontrolne w zakresie komunikacji urzędu i podległych mu jednostek z obywatelem za pomocą poczty elektronicznej na wszystkie samorządy w kraju oraz dokonać rozpoznania w innych sferach działalności publicznej. 26.02.2024 r. Delegatura NIK w Białymstoku wystosowała pismo do wójtów, burmistrzów, prezydentów, starostów i marszałków w całej Polsce z prośbą o *podjęcie aktywności w ramach swojej jednostki oraz jednostek podległych w ramach sprawowanego nadzoru, poprzez zweryfikowanie jakich adresów e-mailowych używa urząd/starostwo,*

jednostka podległa i ich pracownicy, czy nie jest to aby adres e-mailowy w publicznym serwisie komercyjnym, bez zawartej umowy powierzenia przetwarzania danych. Wobec tych, którzy nie podejmą z własnej inicjatywy działań naprawczych, Najwyższa Izba Kontroli zadecyduje, czy podjąć czynności kontrolne samodzielnie czy też zawiadomić Prezesa Urzędu Ochrony Danych Osobowych z prośbą o taką kontrolę.

> *Jak zaznaczono w piśmie, problem dotyczyć może kilkunastu tysięcy jednostek publicznych, w tym m.in. 43% szkół publicznych różnego szczebla, 32% gminnych i powiatowych jednostek opieki zdrowotnej, 28% ośrodków pomocy społecznej i 26% powiatowych centrów pomocy rodzinie oraz wielu innych podmiotów.*

Kolejny raport

W podsumowaniu Diagnozy Cyberbezpieczeństwa zawarto dwa szokujące wnioski. Otóż według NASK, mały urząd JST nigdy nie będzie w stanie spełnić wymagań ustawowych – KRI, uoKSC i RODO – w zakresie bezpieczeństwa informacji, zaś w przypadku średniego urzędu JST jest to mało prawdopodobne. Sprawdziłam – prawie wszystkie jednostki samorządowe objęte kontrolami NIK, których wyniki opublikowano w 2024 r., były beneficjentami programu Cyfrowa Gmina. Zatem wnioski NASK-u wydają się słuszne, zaś udział tych urzędów w projekcie „**Cyberbezpieczny Samorząd**" nie ma sensu. Skoro i tak nie dadzą rady spełnić wymagań cyberbezpieczeństwa albo dadzą radę z małym prawdopodobieństwem, to po co im przyznawać kolejne granty?

> *Kluczowe jest słowo „minimalne", czyli bez popisów, szpanowania, fajerwerków i wodotrysków oraz z wykluczeniem z prac informatyka, którzy nie wie, co to jest topologia sieci. Ważna jest trwałość przyjętych rozwiązań oraz dyscyplina wszystkich zainteresowanych.*

W przypadku kontroli NIK na Podlasiu włodarze skontrolowanych samorządów bardzo szybko podjęli działania naprawcze i jeszcze w trakcie kontroli zaprzestano korzystania z publicznych serwisów do komunikacji elektronicznej lub zaplanowano takie działanie w ciągu kilku tygodni. Z własnego doświadczenia też wiem, że da się spełnić minimalne wymagania w małej jednostce samorządowej.

Zajrzałam do raportu Pełnomocnika Rządu ds. Cyberbezpieczeństwa za 2023 r., zaprezentowanego publicznie 11 kwietnia 2024 r. (https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni), by zapoznać się z konkretnymi propozycjami dla małych i średnich JST. Dowiedziałam się, że:

- CSIRT NASK dostrzega w szczególności potrzebę podniesienia poziomu odporności i wzmocnienia jednostek samorządu terytorialnego (JST) w obszarze przeciwdziałania cyberzagrożeniom; w tym kontekście ważny jest udział NASK-PIB – jako partnera merytorycznego – w realizacji projektu grantowego „Cyberbezpieczny Samorząd";
- w październiku 2023 r. rozpoczęto realizację projektu utworzenia Centrum Cyberbezpieczeństwa NASK (CCN), obejmującego utworzenie specjalistycznego Krajowego Centrum Wsparcia Security dla JST (KCWS);
- w 2023 r. NASK-PIB przygotował publikację pt. „Cyberbezpieczny Samorząd – poradnik" (negatywną ocenę poradnika zawarłam w moim artykule w nr 3/2023 „Domeny").

Trochę skromnie jak na bieżące potrzeby samorządów i wiodącą rolę NASK w zapewnieniu cywilnego cyberbezpieczeństwa. W raporcie całkowicie przemilczano wszystkie dotychczasowe raporty NIK dotyczące cyberbezpieczeństwa, bezpieczeństwa informacji i ochrony danych osobowych i nie odniesiono się do zawartych w nich rekomendacji. Świadomie czy przez przypadek?

Kolejne talenty

Czy kolejne tygodnie i miesiące przyniosą kolejne zaskoczenia? Z pewnością. Właśnie słucham transmisji z posiedzenia jednej z komisji śledczych. Zeznaje pani dyrektor, która w 2019 r. znalazła się w gronie „TOP20 CyberSecurity Women in Poland". Spytano ją, dlaczego w latach 2018–2023 niektórzy jej współpracownicy korzystali także z prywatnych adresów e-mail do korespondencji służbowej, w tym w przypadku jej zastępcy-wolontariusza z adresu e-mail w domenie zagranicznej uczelni. Odpowiedziała, że było to uzgadniane z departamentem bezpieczeństwa urzędu. Nie dociekała, bo na pewno działo się to *z uzasadnionych powodów*. I na tym zakończę. Jestem w zbyt dużym szoku.

Post scriptum

Szok: Ministerstwo Cyfryzacji zdążyło z nowym Rozporządzeniem o KRI (https://www.dziennikustaw.gov.pl/DU/2024/773). Niedowierzanie: Ministerstwo zapomniało nas o tym poinformować na swojej stronie i w swoich mediach społecznościowych.

Wszystkie informacje zawarte w artykule są podane według stanu na 7 maja 2024 r.