Cyber-SAP-anie

Czy znacie przebojową piosenkę popularnego nigeryjskiego artysty Adekunle Gold zatytułowaną RODO? Polecam – www.youtube.com/watch?v=cR-vup5r35g – bardzo melodyjna, od razu wpada w ucho. My zaś mamy zabawny skecz o RODO Kabaretu Moralnego Niepokoju (www.youtube.com/watch?v=XjVPTIHuMWQ) dostępny na kanale Polsatu.

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.

Jak wynika z badania z maja 2024 r., przeprowadzonego przez serwis ChronPESEL.pl i Krajowy Rejestr Długów pod patronatem Urzędu Ochrony Danych Osobowych (https://chronpesel.pl/aktualnosci/co-czwarty-polak-jest-gotow-udostepnic-dane-osobowe-za-dodatkowe-korzysci), **co czwarty Polak jest gotów udostępnić dane osobowe za dodatkowe korzyści.**

My rozdajemy

Okazuje się, że za atrakcyjną zniżkę czy darmowy produkt najczęściej jesteśmy gotowi podać adres e-mail (76,1 proc.), imię i nazwisko (64,7 proc.), numer telefonu (61,6 proc.), a co dziesiąty z nas – numer PESEL (9,4 proc.).

Niestety, nasze środowisko też jest zadziwiająco skłonne do takich praktyk.

- Uczestniczenie w webinarium KPMG o kodeksie postępowania dla szpitali na bazie art. 40 RODO (luty 2024 r.) wymagało podania wielu innych danych oprócz standardowych: imienia, nazwiska i adresu e-mail.

- W przypadku konferencji o ochronie danych osobowych w świetle aktu o sztucznej inteligencji i innych aktów wdrażających europejską strategię w zakresie danych, zorganizowanej w czerwcu 2024 r. na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego, udział wymagał rejestracji poprzez Google Forms.

- Wojska Obrony Cyberprzestrzeni uruchomiły w sierpniu 2024 r. swój quiz #CyberBezpieczny, przygotowany dla dzieci i młodzieży, na platformie Microsoft 365, korzystając z forms.office.com.

Wszystkich jednak przebiło Warszawskie Centrum Innowacji Edukacyjno-Społecznych i Szkoleń w Warszawie (WCIES) z okazji konferencji „RODO w edukacji", zorganizowanej we współpracy z UODO w październiku 2024 r. Otóż WCIES, które prowadziło zapisy, żądało podania numeru PESEL i miejsca urodzenia. Konferencja została odwołana po moim sygnale o problemie wysłanym do UODO, jednak kilkadziesiąt osób zdążyło się zapisać.

O niekontrolowanym rozdawnictwie danych osobowych naszych dzieci przez placówki oświatowe pisałam w artykule „Oświata oddana walkowerem", zamieszczonym w numerze 2-4/2020 biuletynu PTI. Do tematu wracałam kilkukrotnie, m.in. w artykułach w numerach 4/2022 i 1/2023 kwartalnika „Domena". Jednak dopiero latem 2024 r. Ministerstwo Edukacji Narodowej zainteresowało się przetwarzaniem danych dzieci w systemach dzienników elektronicznych prowadzonych przez firmy komercyjne. Nie wynikało to, o dziwo, z troski o dane. Larum podnieśli rodzice, bo firmy dostarczające systemy wprowadziły dodatkowe opłaty za część funkcjonalności e-dzienników. Wreszcie zaczęła się także dyskusja o ochronie wizerunku dzieci w sieci. W trakcie posiedzenia Komisji do spraw Dzieci i Młodzieży Sejmu RP (26.09.2024 r.) mowa była nawet o zakazie publikowania zdjęć dzieci na stronach internetowych szkół i przedszkoli oraz w ich mediach społecznościowych.

Pozostaje problem rodziców należących do grup klasowych i szkolnych w mediach społecznościowych. Co oznacza komunikacja rodziców poprzez komunikatory? Bezrefleksyjne dzielenie się szczegółami z życia uczniów i ich rodzin. Jeżeli sami nie doświadczacie Państwo emocji związanych z życiem klasowym waszych pociech, polecam artykuł z portalu Onet https://kobieta.onet.pl/wiadomosci/grupy-klasowe-to-koszmar-rodzicow-hej-co-jest-jutro-na-biologie/0x8wycs,.

Szczególną grupę rozdawaczy stanowią celebryci i politycy. Jedni i drudzy publikują w internecie wiele osobistych szczegółów, chwaląc się swoim życiem rodzinnym, zawodowym i towarzyskim. Niestety, internet nie zapomina, o czym przekonują się zainteresowani, gdy próbują usunąć opublikowane informacje. Ostatnio kilku „studentów" wypierało się dyplomu MBA wydanego przez Collegium Humanum. Dociekliwi dziennikarze znaleźli jednak stare wpisy. Prawo do bycia zapomnianym nie pomogło.

Wy korzystacie

W zeszłym roku znajomy chciał zmienić bank. Poszedł założyć rachunek w największym banku uniwersalnym w Polsce z ponad 100-letnią historią. Jakież było jego zdziwienie, gdy okazało się, że jego dane już tam są – ze starym adresem zamieszkania. Sam nigdy wcześniej nie korzystał z usług tego banku. Biorąc pod uwagę, że przed 1989 r. ów bank był jedyną powszechną kasą oszczędności, znajomy doszedł do wniosku, że bank pozyskał jego dane jeszcze za PRL-u i je zachomikował. Wystarczyło, że podał nowy adres i już mógł korzystać z usług banku.

Latem trzy razy dzwonili do mnie telemarketerzy proponując pakiety medyczne grupy Luxmed w promocyjnej cenie. Za pierwszym i drugim razem po prostu się rozłączyłam. Za trzecim razem zadałam standardowe pytanie, skąd mają moje dane. Tym razem operatorka tłumaczyła, że gdzieś udzieliłam zgody na ich wykorzystanie. Zaprzeczyłam i zaczęłam drążyć. Ostatecznie pani powiedziała, że trafię na ich czarną listę. Faktycznie, już więcej się nie odezwali. Luxmed nie jest pierwszą firmą, która zleca podwykonawcy szukanie klientów. Podobnie postąpił Krajowy Rejestr Długów Biura Informacji Gospodarczej S.A. Dziwi mnie tylko, że poważny podmiot medyczny przetwarzający dane wrażliwe i poważny podmiot finansowy nie dociekają, skąd firma reklamowa pozyskała dane osobowe do swojej bazy marketingowej.

Może nie powinnam się dziwić. Przejrzałam pytania stawiane w nowej, drugiej wersji Testu Dojrzałości Cyfrowej opracowanego w ramach programu Cyfrowa Wyprawka dla Firm przez Polski Fundusz Rozwoju S.A. i Fundację Digital Poland w celu

wsparcia organizacji w transformacji cyfrowej. Jest promocja wybranych produktów i usług cyfrowych znanych firm, szczególnie big-techów i entuzjastyczne namawianie do wdrożenia nowych technologii. Są także pytania dotyczące cyberbezpieczeństwa, chociaż zrezygnowano z pytania o regularne realizowanie audytów bezpieczeństwa teleinformatycznego przez zewnętrzny podmiot (było w pierwszym wydaniu Testu). Ścisłe odniesienia do wymogów RODO pojawiają się tylko raz:

- w teście dla mikro i małych firm w pytaniu „Zbieramy zgody marketingowe naszych klientów i jesteśmy je w stanie zidentyfikować i wycofać na życzenie klienta";
- w teście dla średnich i dużych firm w punkcie „Informujemy transparentnie i w zrozumiały sposób klientów o tym, po co i jak przetwarzamy ich dane".

Szczególnie spodobało mi się wycofanie zgody na życzenie klienta bez dodania, że oznacza to zaprzestanie samego przetwarzania. Co do transparentnego informowania w zrozumiały sposób wszyscy wiemy, jak to wygląda na co dzień.

Albo nie

W Warszawie są wprowadzane kolejne strefy parkowania. Tym razem padło na moje osiedle. Pobrałam stosowny wniosek o wydanie identyfikatora uprawniającego do wjazdu w strefę ze strony warszawa19115.pl, wypełniłam go i udałam się do urzędu dzielnicowego. Na miejscu dowiedziałam się, że potrzebny jest jeszcze dowód rejestracyjny mojego samochodu lub ... zdjęcie dowodu. Panie Burmistrzu Pragi-Południe! W dobie sztucznej inteligencji zdjęcie dowodu rejestracyjnego ma potwierdzać posiadanie dowodu rejestracyjnego? Spytałam panią w okienku, dlaczego nie może sprawdzić mojego pojazdu w systemie CEPiK, skoro są w nim wszystkie moje dane. Pani stwierdziła, że ona nie ma dostępu do systemu – w przeciwieństwie do koleżanek z sąsiednich stanowisk, które go mają, bo obsługują mieszkańców przychodzących rejestrować pojazdy. Za drugim podejściem okazałam dowód osobisty i dowód rejestracyjny w aplikacji mObywatel. Pani zajrzała do swojego systemu i stwierdziła, że mój identyfikator z 2015 r. jest nadal ważny i nowy nie jest potrzebny. Dwa razy niepotrzebnie odbyłam dłuższe spacery i straciłam czas. Panie Burmistrzu Pragi-Południe! Cyfryzacja naszej dzielnicy jest do poprawki.

Podobne zamieszanie zaliczyłam w ZUS-ie. Od 1 stycznia 2023 r. ZUS wydaje emerytom i rencistom legitymacje tylko w systemie mObywatel. Uzyskanie legitymacji plastikowej wymaga złożenia oddzielnego, dodatkowego wniosku ERL. Podobno wprowadzono nowe zasady, by plastikowe legitymacje nie zalegały w szufladach zainteresowanych. W ramach dostępu do informacji publicznej próbowałam dowiedzieć się, ilu emerytów i rencistów całkowicie zrezygnowało z legitymacji plastikowej w 2023 r. Departament Legislacyjno-Prawny ZUS odpisał mi, że:

> *realizacja Pani wniosku musiałaby zostać poprzedzona koniecznością przeprowadzenia szeregu czynności organizacyjnych oraz analitycznych na zbiorach danych według konkretnych założeń. Zakład nie posiada narzędzi w postaci systemów informatycznych, które pozwoliłyby w prosty sposób na automatyzację czynności wymaganych do wygenerowania danych oraz sporządzenie raportów według kryteriów wskazanych we wniosku. W celu ustalenia wnioskowanych informacji wymienionych we wniosku niezbędne byłoby zaangażowanie grupy pracowników w poszczególnych 43 terenowych jednostkach organizacyjnych ZUS, przeprowadzenie ręcznej kwerendy, która polegałaby w pierwszej kolejności na przeglądaniu, analizie i weryfikacji zarejestrowanych w poszczególnych Oddziałach wniosków ERL i wyodrębnienia z nich wyłącznie wniosków dotyczących wydania legitymacji emeryta-rencisty.*

Sprawdziłam. Wszystkie wnioski o emerytury/renty i legitymacje emeryta/rencisty są przetwarzane w potężnym systemie o nazwie Platforma Usług Elektronicznych ZUS, który kosztował miliardy złotych. Z kolei w trakcie seminarium „Przetwarzanie danych przez ZUS i płatników składek w związku z realizacją ustawowych obowiązków" (19.06.2024 r.) przedstawiciele działów kontroli ZUS chwalili się korzystaniem ze sztucznej inteligencji do realizacji zadań związanych z przeprowadzaniem kontroli płatników. Zatem ZUS ma dane i narzędzia. Jednak odmówił podania statystyk, o które zapytałam. Panie Prezesie ZUS-u, dlaczego?

Oni zbierają

W Ameryce Łacińskiej grupa aktywistek prowadziła badanie „masowego gromadzenia i przetwarzania danych przez rządy, firmy i nas samych w celu monitorowania miast, domów, kieszeni i ciał". Aktywistki Analizowały działania **CHUPADADOS**, czyli po angielsku datasucker, a po polsku zasysacza danych (https://chupadados.codingrights.org/en/intro/). Obrazowo opisały, jak zasysacze kontrolują, co robimy, śledzą, z kim się spotykamy i dzielą się naszymi prywatnymi danymi z obcymi podmiotami. Ostrzegają przed hurraoptymistycznym wdrażaniem pomysłów typu Big Data, Smart Cities czy Internet Rzeczy bez zgłębienia, jak te technologie działają i komu faktycznie służą.

Na problem zwracają uwagę także autorzy poradnika „ABC Cyberbezpieczeństwa", dostępnego na portalu Ogólnopolskiej Sieci Edukacyjnej (it-szkola.edu.pl) prowadzonym przez NASK: [...] *dzięki tzw. ciasteczkom (pliki cookies) serwery stron śledzą naszą aktywność w sieci. Wszystkie te informacje mogą trafić w niepowołane ręce i służyć m.in. do szpiegowania czy kradzieży tożsamości*. Tyle że przejście do portalu w celu pobrania poradnika wymaga zgody zarówno na podstawowe, jak i na funkcjonalne cookies. Jak zaznaczo-

no w polityce prywatności portalu OSE, niektóre pliki cookies są tworzone przez podmioty, z usług których korzysta NASK, w tym wymienione Google Inc., Facebook, Twitter i Youtube. W celu dopełnienia formalności dodano odnośniki do polityk wymienionych firm.

NASK ostrzega i jednocześnie sama karmi zasysaczy. Niestety, serwis GOV.pl również korzysta z usług i plików cookies big-techów.

Inni badają

W ramach kontroli „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości", przeprowadzonej w 2022 r., Najwyższa Izba Kontroli zleciła badanie sondażowe w celu ustalenia deklarowanego przez respondentów stanu wiedzy na temat aktualnych zagrożeń występujących w cyberprzestrzeni oraz zweryfikowanie działań podejmowanych przez obywateli i właściwe organy państwa w sytuacji faktycznego ataku przestępców komputerowych. Zadano m.in. pytanie: *Przez kogo, jaką instytucję był/a Pan(i) ostrzegany(a) o aktualnych zagrożeniach i trwających kampaniach oszustów komputerowych?* Okazało się, że najczęściej przez banki (42%) i rodzinę/znajomych (20%).

Dla przypomnienia: NIK oceniła jako nierzetelne i nieskuteczne prowadzone w badanym okresie działania mające na celu edukowanie i ostrzeganie obywateli na temat niebezpieczeństw grożących im ze strony sprawców przestępstw internetowych, w tym kradzieży tożsamości. W rezultacie indywidualni użytkownicy internetu byli w znacznej mierze pozbawieni aktualnych i pochodzących z oficjalnych źródeł państwowych informacji na temat zagrożeń ze strony przestępców komputerowych oraz rekomendowanych środków ochrony. W związku z tym NIK zwrócił się do Ministra Cyfryzacji i Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa we współpracy z Kierownictwem NASK-PIB z wnioskiem o stworzenie jednego, rozpoznawalnego, oficjalnego, państwowego serwisu, zawierającego łatwo dostępne informacje na temat zagrożeń cyberbezpieczeństwa, trwających kampanii, a także zaleceń i dobrych praktyk z zakresu „cyberhigieny".

Ustalenia NIK potwierdzają badania z trzech ostatnich lat zamówione przez inne podmioty:

- „Polaków Portfel Własny – Bezpieczni na e-zakupach 2022" Santander Consumer Banku z lutego 2022 r. z pytaniem *Skąd czerpiemy wiedzę o zagrożeniach w sieci?*;
- „Świadomość Polek i Polaków z zakresu cyberbezpieczeństwa" dla Google z października 2022 r. z pytaniem *Skąd czerpiemy wiedzę o cyberbezpieczeństwie?*;
- „InfoSenior 2023 r." Warszawskiego Instytutu Bankowości ze stycznia 2023 r. z pytaniem *Skąd najczęściej czerpie Pan(i) informację na temat cyberbezpieczeństwa?*;
- „Czy czujesz się bezpiecznie w Internecie?" Banku Pekao S.A.z czerwca 2023 r. z pytaniem *Skąd czerpiemy wiedzę na temat bezpieczeństwa w sieci?*;
- „Bezpieczeństwo cyfrowe Polaków" firmy SMSAPI ze stycznia 2024 r. z pytaniem *Zaznacz wszystkie źródła, z których zdobywasz wiedzę na temat aktualnych zagrożeń bezpieczeństwa w sieci;*
- „Polacy w sieci: wiedza, nawyki i obawy" w ramach PAYBACK Opinion Poll z czerwca 2024 r. z pytaniem *Skąd Pan/i czerpie wiedzę na temat bezpieczeństwa w sieci?*;
- „Technologia w służbie społeczeństwu – cybersecurity" Fundacji Digital Poland z października 2024 r. z pytaniem *Gdzie lub jak uczestniczono w kampaniach?* w ramach tematu „Uczestniczenie w kampanii zwiększającej świadomość i wiedzę na temat cyberbezpieczeństwa".

Wynika z nich jednoznacznie, że Polacy nadal sami szukają w sieci wiedzy o cyberbezpieczeństwie bądź pytają rodzinę i znajomych zamiast korzystać ze źródeł rządowych (Policja, NASK czy Ministerstwo Cyfryzacji) – w przeciwieństwie do Brytyjczyków, którzy mają znakomity portal https://www.ncsc.gov.uk.

SAP-my

Komunikat o wynikach kontroli kradzieży tożsamości Najwyższa Izba Kontroli zatytułowała „Obywatelu, przed cyberatakiem broń się sam". Ponad dwa lata później nadal jesteśmy zdani na siebie. Zatem bądźmy:

- **S**ceptyczni – do wszelkich cyfrowych komunikatów i treści
- **A**sertywni – śmiało odmawiajmy telemarketerom i hakerom
- **P**okorni – pamiętajmy, że nie ma i nigdy nie będzie 100-proc. cyberbezpieczeństwa.

Wszystkie informacje zawarte w artykule są podane według stanu na dzień 15 października 2024 r.