Niebezpieczny cyber-absurding

Swego czasu wysyłaliśmy w sieci tzw. pingi. Obecnie w cyberbezpieczeństwie panuje moda na inne ingi, czyli na nadawanie różnym cyberzjawiskom nazw kończących się na ing. Powstają z tego pojęcia często zupełnie niezrozumiałe dla nas i nieraz śmiesznie wymawiane, szczególnie przy ich polskiej deklinacji.

Skoro ingi stały się tak popularne, to chcę zaproponować kolejne.

Śmieszing – wstawianie śmiesznych zapisów do ustaw i innych przepisów

Wielokrotnie pisałam o zaskakujących zapisach dotyczących bezpieczeństwa informacji i ochrony danych osobowych wstawianych do różnych ustaw i rozporządzeń. Tym razem chcę skomentować projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej. W ramach konsultacji publicznych Polskie Towarzystwo Informatyczne zaproponowało użycie pojęcia „szalbierstwo" z odpowiednimi przymiotnikami jako polskiego odpowiednika vishingu, spoofingu, phishingu, smishingu i pharmingu (napisał o tym Wacław Iszkowski w numerze 3/2022 „Domeny"). Sięgnęłam do tabeli zgłoszonych uwag i znalazłam odniesienie KPRM-u „Uwaga nieuwzględniona" oraz kuriozalne uzasadnienie o następującej treści: „Określenie „szalbierczy" potwierdza bogactwo języka polskiego. Nie da się jednak nie zauważyć, iż jest to archaizm. Wyraz ten jest rzadko używany w codziennych dyskursach. Z tego powo-

Joanna Karczewska
One of Europe's Top Cyber Women

du proponuje się pozostawienie pojęcia „smishing", które jest powszechnie znane i wykorzystywane."

Uśmiałam się do łez i zatrwożyłam. Przypomnę, że już w 1562 r. Mikołaj Rej z Nagłowic upominał: „A niechaj narodowie wżdy postronni znają, iż Polacy nie gęsi, iż swój język mają". Sprawdziłam w Ocenie skutków regulacji, którzy urzędnicy równo 460 lat później zapomnieli o słowach ojca języka polskiego. Może wymienionym w dokumencie osobom imponują pojęcia angielskojęzyczne określające kolejne rodzaje oszustw internetowych. Niewątpliwie są takie ładne, amerykańskie. Jednak, jak wykazują badania, które już cytowałam w moim poprzednim artykule („Domena" nr 3/2022), 1/3 Polaków boi się utraty danych na skutek wycieku z bazy serwisu lub aplikacji, w której ma konto, a blisko 43 proc. Polaków jako najgroźniejszych wskazało oszustów wyłudzających dane – niezależnie od nazwy rodzaju oszustwa czy wycieku, z jakim będą mieli do czynienia.

Wyśmieszing - wyśmiewanie użytkowników IT

Na każdej konferencji o cyberbezpieczeństwie pojawia się co najmniej jeden mówca, który opowiada o audycie IT wyśmiewając audytowanych. Prelegentami są wygadani mężczyźni w wieku 30-50 lat o bardzo wysokim mniemaniu o własnej wiedzy i kompetencjach. Na uczestnikach świeżakach robią wrażenie. Ja ich słucham z konsternacją, wręcz przerażeniem.

Dla przykładu, ostatnio jeden chwalił się, jak w ramach testu świadomości użytkowników rozsypał w siedzibie klienta 20 pendrive'ów ze spreparowanym plikiem i monitorował zdalnie, ile osób będzie próbowało plik otworzyć. Słuchając go przypomniałam sobie konferencję sprzed pandemii, w trakcie której inny prelegent opowiadał o podobnym teście. Gdy go odpytałam o wynik końcowy, okazało się, że był dla niego zaskakujący. Bowiem test wywołał tak duże zamieszanie i negatywne odczucia w badanej firmie, że prezes finalnie odmówił zapłaty. Z kolei na innej konferencji prelegent pokazał „zanonimizowane" dokumenty klienta i „śmieszną" fotkę serwerowni. Nie wytrzymałam i od razu zwróciłam mu uwagę, że jest to niedopuszczalne. Audytorowi nie wolno pokazywać jakichkolwiek materiałów dotyczących klienta, nawet za jego zgodę.

Skąd w prelegentach tak wysokie mniemanie o sobie i taka pogarda dla użytkowników IT? Nie wiem. Kto ich upoważnił do publicznego wyśmiewania klientów i demonstrowania własnego poczucia wyższości? Nie wiem. Jako certyfikowany audytor z ponad 40-letnim doświadczenie zawodowym zalecam umiar i pokorę. Nie jesteście celebrytami na ściance. Swoim wyśmiewaniem użytkowników technologii informatycznych nadwyrężacie zaufanie do wszystkich audytorów, czego nie akceptuję.

Audyszing – wymuszanie kiepskich audytów

Skoro mowa o audytach IT, od lat w swoich wynikach kontroli bezpieczeństwa informacji i ochrony danych osobowych w jednostkach sektora finansów publicznych Najwyższa Izba Kontroli wykazuje brak corocznych audytów bezpieczeństwa wymaganych przez rozporządzenie o KRI. Ostatnio sytuacja się zmieniła i zapanowała wręcz moda na audyty bezpieczeństwa, z niewiadomych przyczyn nazywane diagnozami.

O Diagnozie Cyberbezpieczeństwa JST wymaganej w ramach programu Cyfrowa Gmina wspomniałam w moim artykule w „Biuletynie PTI" nr 4/2021. Jak wynika z prezentacji przedstawiciela NASK-u na konferencji Miasta w Internecie w czerwcu br.:

- na podstawie przesłanych danych będą prowadzone badania ankietowe, które pozwolą zdiagnozować kluczowe problemy w zakresie cyberbezpieczeństwa dotyczące gmin;

- ankiety zawierają „bardzo interesujące informacje statystyczne i merytoryczne do zbudowania obrazu cyberbezpieczeństwa w przyszłości".

Żeby obraz był wiarygodny, dokumenty bazowe muszą być rzetelne. Zalecam weryfikację audytorów, którzy podpisują się pod diagnozami. Znam przypadek osoby, która przedstawiała fałszywy certyfikat CIA i zdążyła wykonać osiem diagnoz mając dostęp do wszystkich zabezpieczeń w badanych urzędach, zanim oszustwo zostało ujawnione i zgłoszone na policję.

Teraz przyszła kolej na program Cyfrowy Powiat z tym samym wymogiem przeprowadzenia diagnozy cyberbezpieczeństwa zgodnie z tym samym zakresem oraz formularzem informacji. Formularz nadal zawiera skromną listę 32 lakonicznych wymagań zgodności z KRI/UoKSC i jeszcze skromniejszą, wręcz ascetyczną skalę ich oceny:

0 – brak informacji o spełnieniu wymagania,
1 – zbieżność oświadczeń osób audytowanych,
2 – informacja udokumentowana.

Ewidentnie jego autorzy nie szukali natchnienia i wzorów w innych dokumentach dotyczących badania stanu cyberbezpieczeństwa, takich jak szablony sprawozdań z audytu zgodności z UoKSC czy ankiety z audytu wewnętrznego zleconego w zakresie zarządzania bezpieczeństwem systemów teleinformatycznych w wybranych urzędach administracji rządowej. Na razie cierpliwie czekam na zakończenie obu programów i podsumowanie skuteczności podjętych działań w zakresie poprawy cyberbezpieczeństwa w JST.

Dużo ambitniejsza jest ankieta przygotowana przez Narodowy Fundusz Zdrowia w ramach finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów

teleinformatycznych świadczeniodawców, czyli podmiotów leczniczych wymienionych w Zarządzeniu nr 68/2022/BBIICD Prezesa NFZ z dnia 20 maja 2022 r. (wraz z późniejszą zmianą). W przypadku sektora zdrowia podmioty muszą najpierw wypełnić ankietę badającą poziom bezpieczeństwa zamieszczoną w Systemie Statystyki Ochrony Zdrowia a później wykazać za pomocą zamówionego audytu bezpieczeństwa, że doszło lub nie do zwiększenia poziomu bezpieczeństwa systemów teleinformatycznych wykorzystywanych do udzielania świadczeń opieki zdrowotnej. Ankieta liczy 126 szczegółowych pytań podzielonych na 9 grup. Skąd znam treść wewnętrznej ankiety? Otóż jeden podmiot opublikował wypełnioną przez siebie ankietę na stronie internetowej jako część dokumentacji zapytania ofertowego na przeprowadzenie audytu cyberbezpieczeństwa.

Cała akcja NFZ jest dość intrygująca. Po pierwsze jestem ciekawa, ile audytów wykaże brak zwiększenia poziomu bezpieczeństwa po zainstalowaniu zamówionego sprzętu i oprogramowania, co oznaczałoby brak rozliczenia środków wydanych przez podmioty lecznicze z Funduszu Przeciwdziałania COVID-19. Po drugie, przejrzałam kilkanaście ogłoszeń o zamówieniach publicznych w kontekście Zarządzenia NR 68/2022/BBIICD Prezesa NFZ i znalazłam nie jeden a kilka przypadków łączenia dostawy sprzętu i wykonania audytu w jednym zamówieniu i wyboru jednego wykonawcy.

Dokumenty przetargowe stanowią ciekawą lekturę. Dla przykładu, w kontekście moich wcześniejszych uwag o audytorach, przytoczę zastrzeżenie ze wzoru umowy Instytutu Medycyny Wsi w Lublinie:

„Podczas wykonywania czynności audytowych zabrania się Wykonawcy stosowania w szczególności podstępu i prowokacji, a w przypadku systemów teleinformatycznych działań niezgodnych z postanowieniami licencyjnymi audytowanych systemów."

Zaś olbrzymi szacunek należy się SZPZOZ im. Dzieci Warszawy w Dziekanowie Leśnym za następujący zapis w SWZ:

„Podmiot audytujący wykona audyty (Etap I i Etap II) realizując je w taki sposób, iż wszelkie prace będą przeprowadzone na miejscu u Zamawiającego, a wszelkie dane, na podstawie których będą opracowane wnioski pokontrolne, a także wszelkie inne dokumenty umożliwiające przeprowadzenie audytów pozostaną w miejscu ich wykonania. Nie dopuszcza się przetwarzania danych istotnych z punktu widzenia cyberbezpieczeństwa Szpitala poza jego siedzibą, a także ich kopiowania czy udostępniania w inny sposób."

Kanaring – proponowanie niesprawdzonych aplikacji

W trakcie konferencji i webinariów prelegenci lubią także przechwalać się swoją znajomością tajników cyberbezpieczeństwa. W tym celu pokazują i polecają nieznane programiki dostępne w sieci za darmo lub za niewielką opłatą.

Nie inaczej było w trakcie webinarium UODO na temat zabezpieczeń technicznych przetwarzanych danych osobowych (uodo.gov.pl/pl/138/2451). Jeden z prelegentów, superznawca Narodowych Standardów Cyberbezpieczeństwa, rekomendował m.in. serwis z kanarkiem (oryg. canary) w nazwie, gdzie „wystarczy wygenerować spreparowany plik np. Worda, Excela, czy też jakąś stronę www i wysłać taki link z nieznanego adresu e-mail i za każdym razem, gdy pracownik otworzy taki załącznik, otrzymają Państwo powiadomienie o tym fakcie". Polecane narzędzie ma pomóc w weryfikacji pracowników po szkoleniach z ochrony danych osobowych. Nie wiem, czy prelegent przeprowadził stosowną analizę ryzyka proponowanego narzędzia. Ja przeczytałam Privacy Policy producenta, firmy z siedzibą w Kapsztadzie w Południowej Afryce, i na razie nie skorzystam z jego usług.

Rekomendacja pracownika Urzędu jest trochę na bakier z wypowiedzią jego szefa, Dyrektora Departamentu Kontroli i Naruszeń UODO, przytoczoną w Newsletterze UODO dla IOD nr 10/2022:

„Jeśli zaś chodzi o wykorzystywane systemy informatyczne i urządzenia do przetwarzania danych osobowych, to nadal spotykamy się z sytuacjami używania przez administratorów systemów informatycznych, które utraciły już wsparcie producenta oraz urządzeń, na których nie ma możliwości aktualizacji oprogramowania firmware, co powoduje, że atakujący mogą stosunkowo łatwo przełamywać zabezpieczenia wykorzystując luki bezpieczeństwa istniejące w tych systemach."

Dodałabym ostrzeżenie przed używaniem niesprawdzonych programów i usług.

EduKanaring – stosowanie niesprawdzonych aplikacji w oświacie

Moje ostrzeżenie dotyczy przede wszystkim oświaty. Od lipca 2020 r. zwracam uwagę na zagrożenia związane z technologiami informacyjnymi i komunikacyjnymi, w skrócie TIK, stosowanymi do zdalnego nauczania. Polecam mój artykuł w nr 2-4/2020 „Biuletynu PTI" o znamiennym tytule „Oświata oddana walkowerem". Poruszyłam kwestię TIK-ów także na posiedzeniu Komisji Cyfryzacji Sejmu RP w dniu 28.09.2022 r., korzystając z obecności przedstawiciela Centrum Transformacji Cyfrowej Ministerstwa Edukacji i Nauki. Powiedziałam m.in. „Ktoś, kto zbierze dane, jak uczeń sobie radzi z obsługą programów, może naprawdę w przyszłości, za 10-15 lat, mieć idealny profil dzisiejszych dzieci – wtedy, za 15 lat, już dorosłych – i móc je wykorzystać". Niestety, w najnowszym Rozporządzeniu Ministra Edukacji i Nauki z dnia 2 września 2022 r.

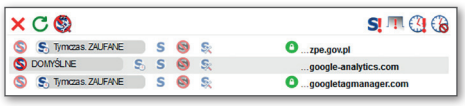
w sprawie organizowania i prowadzenia zajęć z wykorzystaniem metod i technik kształcenia na odległość nie wymieniono żadnych szczegółowych warunków dotyczących cyberbezpieczeństwa.

Sprawa jest naprawdę poważna. Jej kluczowe znaczenie wykazuje przygotowany przez organizację Human Rights Watch raport zatytułowany „**How Dare They Peep into My Private Life?' Children's Rights Violations by Governments that Endorsed Online Learning during the Covid-19 Pandemic**".

Raport jest dostępny na stronie https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments. Autorzy dokonali analizy technicznej i polityk dotyczących 164 TIK-ów (ang. EdTech), zatwierdzonych przez 49 państw. Zbadali 290 firm, które, jak ustalono, zbierają, przetwarzają lub otrzymują dane dzieci od marca 2021 r. Obecnie wzywają rządy do ustanowienia nowych praw ochrony danych dzieci w internecie. Przedstawili także rekomendacje dla:

- rządów,
- resortów edukacji,
- firm produkujących TIK-i,
- firm technologii reklamowych i innych otrzymujących dane z TIK-ów.

W przypadku Polski zbadano cztery produkty: Cisco Webex, Google Meet, Microsoft Teams oraz Epodreczniki.pl – obecnie Zintegrowana Platforma Edukacyjna. Pierwsze trzy produkty są stosowane w wielu państwach, Platforma jest tylko nasza.



Jej właściciel, Ministerstwo Edukacji i Nauki, potwierdza w Polityce prywatności, że przekazuje dane do firmy Google: „używamy cookies google-analytics.com, które służą do prowadzenia statystyk dla witryny zpe.gov.pl."

Najważniejsza jest pierwsza rekomendacja Human Rights Watch dla rządów i przytoczę ją w oryginale:

Facilitate urgent remedy for children whose data were collected during the pandemic and remain at risk of misuse and exploitation. To do so:

- Conduct data privacy audits of the EdTech endorsed for children's learning during the pandemic, remove those that fail these audits, and immediately notify and guide affected schools, teachers, parents, and children to prevent further collection and misuse of children's data.
- Require EdTech companies with failed data privacy audits to identify and immediately delete any children's data collected during the pandemic.
- Require AdTech companies to identify and immediately delete any children's data they received from EdTech companies during the pandemic.
- Prevent the further collection and processing of children's data by technology companies for the purposes of profiling, behavioral advertising, and other uses unrelated to the purpose of providing education.

Jest to niewątpliwie temat dla Rady Doradczej Rodziców powołanej przez NASK we wrześniu br.

Starszing – protekcjonalne traktowanie starszych użytkowników IT

Będąc emerytką z rozbawieniem obserwuję troskę o użytkowników IT w wieku 60+, których szczególnie politycy lubią nazywać nasi kochani lub nasi drodzy seniorzy. Jednocześnie mam nieodparte wrażenie protekcjonalnego traktowania. Może dlatego nie ma ze strony osób decyzyjnych chęci wykorzystania emerytowanych informatyków do cyfrowego uświadamiania osób 60+. Naszą gotowość kilkakrotnie zgłaszałam publicznie. Niestety, na razie bez odzewu. Za to Polska Policja angażuje swoich emerytów do prowadzenia szkoleń w celu ochrony seniorów przed wyłudzeniami i oszustwami.

Dobrym przykładem starszingu jest program Aktywni+ i jego priorytet nr 3 dotyczący m.in. zapewnienia bezpiecznego funkcjonowania osób starszych przy wykorzystywaniu współczesnych narzędzi cyfrowych (wspomniałam o nim w poprzednim artykule). Zgodnie z zarządzeniem nr 14 Ministra Rodziny i Polityki Społecznej z dnia 15 marca 2022 r. komisja konkursowa programu składa się z dyrektora i czterech pracowników Departamentu Polityki Senioralnej w MRiPS oraz dwóch przedstawicieli zgłoszo-

nych przez organizacje pozarządowe. W ramach dostępu do informacji publicznej dowiedziałam się, że byli nimi:

- mgr socjologii głoszona przez stowarzyszenie Zakład Doskonalenia Zawodowego w Warszawie,

- pracownik odpowiedzialny za wdrażanie strategii rozwojowej Fundacji Młode Kresy z Warszawy.

Niestety, nie otrzymałam informacji o ich kompetencjach w zakresie cyfryzacji, a tym bardziej cyberbezpieczeństwa, istotnych dla właściwej oceny składanych wniosków. A może nie są istotne, bo seniorzy ucieszą się z każdego darmowego kursu komputerowego?

W dniu 3 listopada br. odbyło się posiedzenie Komisji Polityki Seniorialnej Sejmu RP poświęcone dostępności edukacji cyfrowej osób starszych i ich cyberbezpieczeństwu. Dyskutowano m.in. o tym, czy organizowane cyfrowe kluby seniora można nazywać kafejkami internetowymi. Funkcjonujące swego czasu kafejki były najmniej bezpiecznym miejscem dostępu do internetu. Może warto uwzględnić wnioski z ich działalności dotyczące cyberbezpieczeństwa. Obejrzałam w internecie relacje ze szkoleń „Bezpieczny e-senior". Zastanawiam się, na czyim sprzęcie odbywają się zajęcia z zakładania i obsługi m.in. Internetowego Konta Pacjenta, profilu na PUE ZUS, e-konta bankowego czy skrzynki e-mail. Na zdjęciach widać identyczne tablety w rękach uczestników. Czy zajęcia są prowadzone na sprzęcie organizatorów? Przy wykorzystaniu darmowego wi-fi? Szkolenia odbywają się także w pracowniach komputerowych, np. biblioteki publicznej. Czy sprzęt jest odpowiednio skonfigurowany i zabezpieczony? Czy którykolwiek senior tego docieka?

Zupełnie inaczej ma się sprawa w projekcie „Cyfrowe Koła Gospodyń Wiejskich", na który Centrum Projektów Polska Cyfrowa przeznacza ponad 3,7 mln zł z Funduszy Europejskich. Jest przeznaczony dla członków Kół Gospodyń Wiejskich z terenów objętych pilotażem. Celem jest m.in. zmniejszenie wykluczenia cyfrowego i podniesienie kompetencji cyfrowych społeczeństwa, w szczególności osób w wieku 50+, 60+ z obszarów wiejskich oraz zachęcenie ich do korzystania z nowych technologii. Naukę ułatwią specjalne materiały szkoleniowe oraz tablety, które po zakończeniu szkolenia, uczestnicy otrzymają na własność.

Nudziaring – nużące wyświetlanie tzw. klauzul informacyjnych

Już ponad 4 lata jesteśmy nimi zanudzani. Do nich dochodzą polityki prywatności i polityki dotyczące cookies. Każde wejście na stronę internetową oznacza konieczność przynajmniej jednego kliknięcia, by z ekranu zniknęły komunikaty o ciasteczkach czy innym szpiegowaniu. Do prawie każdej służbowej wiadomości elektronicznej są doklejane lub załączane krótsze lub dłuższe komunikaty RODO. To samo dotyczy papierowych pism urzędowych. Jako audytor i osoba, której dane dotyczą, próbuję weryfikować zapisy klauzul i polityk ze stanem faktycznym i z przykrością stwierdzam, że nic dobrego z nich nie wynika.

Przykładem jest portal rządowy gov.pl, który u dołu ekranu wyświetla informację o ciasteczkach. Gdy klikniemy na „Zobacz politykę cookies", dowiemy się, że serwis stosuje m.in. cookies inspectlet.com, które służą do określenia sposobu używania strony przez użytkowników. Inspectlet jest firmą amerykańską z siedzibą w Santa Clara w Kalifornii. Jej „Privacy Policy" jest tylko w języku angielskim, a portal jest polski. Niestety, to na nas właściciel portalu zrzuca zadbanie o odpowiednie ustawienia naszych przeglądarek, by ograniczyć działanie ciasteczek.

Z kolei każde wejście na stronę systemu ePUAP oznacza konieczność kliknięcia „Zapoznałem się", by zniknęła klauzula informacyjna dotycząca przetwarzania danych osobowych. Ostatnio zastanawiam się, jaki ślad węglowy zostawiają wszystkie klauzule, komunikaty o ciasteczkach i inne okienka z pytaniem o zgodę. Może znajdzie się ośrodek naukowy, który go policzy.

Czy to koniec mojej listy cyber-absurdów? Absolutnie nie. Mam całą kolekcję a życie ciągle dostarcza nowe przykłady. Zatem zapraszam do lektury następnych wydań „Domeny", a tymczasem w Nowym Roku 2023 życzę wszystkim wytrwałości w walce o nasze cyberbezpieczeństwo.

Wszystkie informacje zawarte w artykule są podane według stanu na dzień 14 listopada 2022 r.