Twoje dane – Twoja sprawa

To tytuł kampanii edukacyjnej organizowanej od wielu lat przez Urząd Ochrony Danych Osobowych (UODO). Jak wynika z badania na temat ochrony danych osobowych, przygotowanego przez operatora serwisu chronPESEL.pl, powinniśmy powtarzać to hasło jak mantrę. Raport opracowany na podstawie ankiety przedstawia aktualny stan wiedzy Polaków na temat tego, czym są dane osobowe i jak je chronić. Wyniki badania omawiano podczas webinarium zorganizowanego 29 czerwca 2023 roku.

W dyskusji wzięli udział: Jakub Groszkowski, zastępca prezesa UODO; Jacek Młotkiewicz, dyrektor Departamentu Kontroli i Naruszeń UODO; Wiesław Paluszyński, prezes Polskiego Towarzystwa Informatycznego, przewodniczący Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo; Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl oraz dr Maciej Andrzejewski, członek Rady Naukowej Instytutu Prawa Ochrony Danych Osobowych. Debatę poprowadził Adam Sanocki, rzecznik prasowy UODO, a wyniki – będące przyczynkiem do dyskusji – przedstawił Andrzej Kulik, rzecznik prasowy Krajowego Rejestru Długów (operatora systemu chronPESEL.pl).

W tegorocznej edycji badania postanowiono po raz pierwszy sprawdzić, czy wiemy, jakie informacje należą do danych osobowych, czyli to wszystko, co pozwala nas zidentyfikować.

Czy wiemy, co powinniśmy chronić?

Respondenci wskazywali najczęściej na PESEL, imię i nazwisko, adres zamieszkania, numer dowodu tożsamości. Tylko niecałe 50 proc. badanych wymieniło także dane biometryczne, takie jak wizerunek czy odciski palców, a jeszcze mniej osób (poniżej 30 proc.) uznało za dane osobowe informacje o stanie zdrowia, adres IP czy dane o lokalizacji. Tymczasem już w 2013 r.[1] badacze stwierdzili, że do identyfikacji 95 proc. ludzi wystarczą tylko cztery zestawy współrzędnych ich lokalizacji. Badanie pokazuje więc, że większość osób definiuje dane osobowe dość wąsko, nie zdając sobie sprawy, że cyfryzacja bardzo poszerzyła kategorię informacji pozwalających nas zidentyfikować.

1 Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, Vincent D. Blondel (2013). Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports (3)*, https://www.nature.com/articles/srep01376

Świadomość decydentów i ustawodawców dotycząca ochrony danych czasem nie nadąża nawet za tą powszechną. W przeciwieństwie do obywateli, władza nie zawsze pamięta np. o szczególnej ochronie numeru PESEL. Prezes PTI Wieslaw Paluszyński wskazał mechanizmy wymagane przez prawo, które jednocześnie ujawniają PESEL. Można je znaleźć na przykład w Krajowym Rejestrze Sądowym, przy nazwiskach osób składających sprawozdania finansowe. W certyfikacie podpisu kwalifikowanego musi – zgodnie z obowiązującym prawem – znaleźć się także PESEL. W 2009 r., podczas prac nad nowelizacją ustawy o podpisie elektronicznym, UODO był przeciwny takiemu rozwiązaniu, jednak prawodawcy nie wzięli pod uwagę opinii ekspertów.

W przypadku biometryki teoretycznie regulacje powinny zapewnić nam bezpieczeństwo. Nie wolno przechowywać bowiem pełnych danych, np. oryginału biometrycznego w postaci zdjęcia czy odcisków palców. Używany jest zamiast tego pewien skrót, przetworzony algorytmem kryptograficznym. W związku z tym wypłynięcie takiego wzorca nie powinno umożliwiać identyfikacji poszczególnych osób, bowiem do poznania pełnych danych potrzebna jest znajomość algorytmu, który stworzył skrót. W tym wypadku zagrożeniem są jednak kwestie organizacyjne, niesprecyzowane w przepisach. Bardzo istotne jest to, w jaki sposób dane są przesyłane, jak je się tymczasowo składuje i jaka jest procedura niszczenia oryginałów biometrycznych w momencie wytworzenia wzorca. Powinniśmy domagać się jasnych odpowiedzi na te pytania. Biometryka rodzi bowiem szczególne zagrożenie – w przypadku wycieku pełnych danych jest to sytuacja właściwie nieodwracalna. Nikt nie zmieni układu swoich linii papilarnych, układu naczyń krwionośnych na dłoni czy wyglądu źrenicy.

(Chyba) wiemy, jak chronić dane osobowe

Jak oceniają swoją wiedzę na temat ochrony danych zwykli obywatele? Podobnie jak w poprzednich edycjach badania, także tym razem Polacy wykazali daleko posunięty optymizm. Aż 89 proc. osób twierdziło, że wie, jak chronić dane osobowe; tyle samo deklarowało, że jest w stanie zidentyfikować próbę wyłudzenia, np. poprzez fałszywy email, sms. Jest tylko jedno „ale" – zaledwie kilkanaście procent respondentów jest absolutnie pewnych swojej wiedzy i umiejętności…

To, że w obszarze edukacji jest jeszcze wiele do zrobienia – pokazują także statystyki dotyczące utraty kontroli nad danymi przez osoby indywidualne. Aż 12 proc. respondentów przyznało, że padło ofiarą skutecznego wyłudzenia danych osobowych, a 6 proc. osób zostało zaatakowanych przez hakerów, którzy wykradli dane z urządzeń osobistych. Dalsze 20 proc. badanych nie jest pewnych, czy ich dane nie zostały bezprawnie ujawnione. Warto pamiętać, że nawet jeśli przestępcy nie znajdą na naszym komputerze danych wysoko wrażliwych, to dzięki zgromadzonym informacjom oraz metodom socjotechnicznym mogą skłonić nas do ujawnienia bardziej istotnych danych.

> *Z ankiety wynika, że nie doceniamy wpływu naszych zaniedbań i ich związku z możliwym ryzykiem utraty danych.*

Niespecjalnie troszczymy się o zabezpieczenie naszych urządzeń i usług cyfrowych, zapominając, że stały się one centrum naszego życia. Zaniedbania w osobistej cyberhigienie obejmują m.in. niestosowanie się do zaleceń i procedur bezpieczeństwa. 26 proc. respondentów przyznaje się, że używa tego samego hasła do kilku serwisów. Jego wykradzenie z jednej firmy naraża nas więc na utratę kontroli wielu zasobów.

Zabezpieczenie techniczne własnego sprzętu także szwankuje – 15 proc. badanych nie stosuje żadnego programu antywirusowego na komputerach, a ponad ¼ respondentów nie instaluje go na telefonach komórkowych, które obecnie przejęły właściwie wszystkie funkcje maszyn stacjonarnych. Wiadomo także, że większość tych, którzy mają antywirusy korzysta z wersji bezpłatnych, nieaktualizowanych na bieżąco przez dostawców.

Paradoksalnie wyniki ankiety wskazują, że jednocześnie 42 proc. osób deklaruje korzystanie z płatnych programów chroniących przed konsekwencjami utraty danych osobowych (np. ChronPESEL.pl). Nie wiadomo właściwie, czy interpretować to optymistycznie – jako dowód odpowiedniej zapobiegliwości, czy uznać za przyznanie się do braku kompetencji i ogromnej niepewności co do bezpieczeństwa własnych danych. Wygląda jednak na to, że jesteśmy bardziej skłonni zainwestować w niwelowanie skutków potencjalnego wycieku, niż przeznaczyć środki na zapobieganie takim zdarzeniom.

Mądry Polak po szkodzie?

Podobne podejście ma wiele firm, o czym mówił Jacek Młotkiewicz, dyrektor Departamentu Kontroli i Naruszeń UODO. Przeprowadzone inspekcje wskazują, że w wielu z przedsiębiorstwach do momentu ataku nie stosowano odpowiednich zabezpieczeń technicznych i procedur. Lista zaniedbań obejmuje często korzystanie z systemów przestarzałych, które utraciły już wsparcie producenta, nieaktualizowanie bazy programu antywirusowego, używanie urządzeń z nieaktualizowanym firmware lub źle skonfigurowanych. Brakuje także odpowiednich procedur i solidnej dokumentacji, np. analizy ryzyka.

Zwykle w firmach atak prowadzi do poprawy zabezpieczeń. Czy jednak użytkownicy indywidualni wiedzą, co zrobić

w przypadku naruszenia ich danych osobowych? 75 proc. badanych przyznało, że nie wie, kto powinien zająć się neutralizacją skutków wycieku danych osobowych. Respondenci wyposażeni w listę z możliwością wielokrotnego wyboru najczęściej wskazywali, że na wyciek danych powinny zareagować służby ścigania (policja, prokuratura); na kolejnym miejscu wymieniano firmę/instytucję, która jest administratorem bazy danych lub tę, której dane powierzono oraz Urząd Ochrony Danych Osobowych. Najmniej respondentów (37,8 proc.) przyznało, że osoba, której dane wyciekły, także powinna podjąć stosowne działania.

Jeśli dane utraciliśmy sami – nie zachowując odpowiedniej czujności lub zabezpieczeń technicznych – powinniśmy bezwzględnie zgłosić tę sprawę na policję. Trzeba zmienić wszystkie dotychczasowe hasła, często konieczne jest zastrzeżenie dowodu i karty płatniczej. Jednym z zaleceń wymienianych przez ekspertów jest także zachowanie ostrożności w kontaktach z innymi – zarówno w relacjach bezpośrednich, jak i tych prowadzonych poprzez email, telefon czy sms.

Jeśli dane wyciekły z podmiotów trzecich, takie firmy i instytucje mają obowiązek nie tylko zidentyfikować źródło problemu i poprawić zabezpieczenia, lecz także muszą poinformować zainteresowane osoby o naruszeniu, potencjalnych skutkach i środkach zaradczych, jaka każda z nich powinna podjąć. I w takim wypadku osoba, której dane zostały naruszone, także musi się zaangażować, nie może uznać, że „inni zrobią to za nią". Trzeba w takiej sytuacji zrealizować jak najwięcej zalecanych działań, bo leży to w naszym własnym interesie i często tylko my możemy je wykonać (np. wystąpić o nowy dowód osobisty).

Czarny scenariusz

Zabezpieczenia i środki zaradcze naprawdę warto wdrożyć – jeśli uświadomimy sobie, jakie mogą być koszty i konsekwencje utraty kontroli nad naszymi danymi. Jest bardzo prawdopodobne, że przestępcy na nasze dane zaciągną znaczne zobowiązania finansowe w bankach i firmach pożyczkowych. Mogą także wyłudzać środki pośrednio – na firmę założoną z użyciem wykradzionych danych osobowych. W takim przypadku wcześniejsze zgłoszenie utraty danych na policji pomoże nam bardzo, kiedy dojdzie do kontaktu z wierzycielem lub wynajętą przez niego firmą windykacyjną.

Rośnie świadomość społeczna, że wykradzione dane mogą także posłużyć do manipulacji naszymi znajomymi i rodziną lub do szantażowania osoby bezpośrednio poszkodowanej. Większość badanych zdaje sobie również sprawę z tego, że dane osobowe są towarem i mogą zostać odsprzedane innym przestępcom czy organizacjom.

Nie tylko jednak kryminaliści korzystają z naszych danych w sposób nieetyczny. Korporacje pozyskują te dane w sposób legalny, ale zwykle nie jesteśmy tego nieświadomi, bo nie czytamy długich i skomplikowanych dokumentów, jak regulaminy czy polityki prywatności. Prezes Wiesław Paluszyński przypomniał, że gromadzone w ten sposób dane są często wykorzystywane w celu wywierania wpływu na politykę i nasze zachowania konsumenckie. Dzięki profilowaniu odbiorców i dopasowywaniu przekazu do ich charakteru, wywierany wpływ staje się niezwykle skuteczny. Widać to było na przykładzie kampanii Donalda Trumpa i zwolenników Brexitu. Mechanizmy opierające się na mikrotargetowaniu wykorzystywane są także przez firmy do sterowania naszymi zachowaniami konsumenckimi i zwiększania sprzedaży (więcej na temat projektowania zachowań w poprzednim wydaniu „Domeny", w wywiadzie z dr. Miłoszem Babeckim).

Dlaczego, świadomi potencjalnych zagrożeń, tak niewiele uwagi i środków poświęcamy na ochronę prywatności? Dane są nienamacalne, w większości dryfują gdzieś w przestrzeni cyfrowej i chyba dlatego wydają się tak mało istotne. Jeśli ktoś ukradnie nam portfel z plikiem banknotów albo włamie się do mieszkania, uznajemy to za sytuację bardzo traumatyczną. Pora, żeby widmo utraty kontroli nad danymi wydało nam się nawet groźniejsze niż jednorazowa strata pieniędzy lub dóbr materialnych. Utrata danych stawia nas bowiem w sytuacji zagrożenia na długie lata.

Paulina Giersz