Brytyjczycy nie ufają technologii opartej na danych

Zespół Ada Lovelace Institute przeanalizował dostępne publikacje dotyczące oczekiwań ludzi wobec wykorzystania ich danych. Wbrew lansowanej od lat tezie branży internetowej użytkownicy i użytkowniczki rozwiązań cyfrowych wcale nie pogodzili się z nieograniczonym eksploatowaniem informacji na swój temat.

Brytyjscy odbiorcy są zwolennikami innowacji opartych na danych, ale uważają, że powinny one być etyczne, odpowiedzialne i służyć dobru wspólnemu. Istnieją też liczne dowody na to, że Brytyjczycy i Brytyjki popierają pomysł lepszego uregulowania wykorzystania technologii opartych na danych. Oczekują też jaśniejszej informacji o tym, jak są wykorzystywane ich dane i jak wpływa to na prawa i wolności użytkowników. Potrzebne są jednak dalsze badania, żeby doprecyzować, jakie dokładnie wymagania mają wobec przepisów, a także co dokładnie rozumieją pod pojęciem wspólnego dobra.

Społeczeństwo opiera się stosowaniu wykorzystujących dane systemów, jeśli nie ma do nich zaufania. Raport Ada Lovelace Institute podpowiada, że nie należy ignorować niepokoju ludzi wobec wykorzystania ich danych, tłumacząc go brakiem wiedzy czy zrozumienia. Problemu nie rozwiąże samo oczekiwanie, że użytkownicy i użytkowniczki staną się bardziej ufni wobec technologii. Liczne publikacje wskazują, że kluczem do budowania zaufania jest regulacja. Dopiero przepisy zaprojektowane tak, by chronić ludzi przed nieprzejrzystą i niesprawiedliwą technologią, dadzą poczucie bezpieczeństwa.

Badania dotyczą Wielkiej Brytanii. A co polskie społeczeństwo sądzi o technologiach opartych na danych?

Irlandia Północna zawiesza system paszportów szczepionkowych po incydencie wycieku danych

Departament Zdrowia Irlandii Północnej (DoH) tymczasowo wstrzymał swoją internetową usługę certyfikacji szczepionek przeciw COVID-19 po incydencie związanym z ujawnieniem danych, podkreślając ryzyko powierzenia danych dotyczących zdrowia rządowi.

Według DoH niektórym użytkownikom usługi COVIDCert NI przedstawiono w pewnych okolicznościach dane innych użytkowników. Stwierdzono, że ograniczona liczba użytkowników była potencjalnie narażona na dane innych użytkowników.

COVIDCert umożliwia w pełni zaszczepionym osobom z Irlandii Północnej uzyskanie cyfrowego zaświadczenia potwierdzającego status szczepienia przeciw COVID-19. Jest to system odrębny od przepustki COVID *National Health Service* (NHS) stosowanej w Anglii i Walii oraz podobnej usługi w stylu paszportu szczepień stosowanej przez *Public Health Scotland*.

Witryna COVIDCert i aplikacja mobilna nie działają

Usługa Irlandii Północnej jest dostępna za pośrednictwem strony internetowej covidcertni.nidirect.gov.uk lub aplikacji mobilnej dla użytkowników systemów Android i iOS. Zarówno witryna COVIDCert, jak i punkty końcowe aplikacji mobilnej nie działały podczas testów przeprowadzanych przez *BleepingComputer*, witrynę zajmującą się nowościami technologicznymi.

„Nasze usługi nie są obecnie dostępne. Pracujemy nad jak najszybszym przywróceniem wszystkich usług. Sprawdź ponownie wkrótce" – czytamy w jednym z komunikatów o błędach generowanych przez usługę na swojej stronie internetowej.

W międzyczasie komunikat „zasób… usunięto" jest wyświetlany użytkownikom aplikacji mobilnej, którzy próbują się zalogować.

DoH natychmiast zgłosił problem do *Biura Komisarza ds. Informacji* w Wielkiej Brytanii (ICO). „DoH bardzo poważnie traktuje prywatność danych obywateli i nawiązano kontakt z ICO w ramach należytej staranności w zakresie ochrony danych obywateli", powiedział departament w ogłoszeniu opublikowanym we wtorek, 27 lipca.

„Podjęto również natychmiastowe działanie w celu tymczasowego usunięcia części usługi zarządzającej tożsamością".

Lista stron, na które incydent nie miał wpływu

DoH opublikowała również listę stron, na które incydent nie miał wpływu, w tym wnioskodawców, którzy już posiadają certyfikat (ich aplikacje lub papierowe kopie nadal działają); wnioskodawców, którzy złożyli wniosek za pośrednictwem portalu internetowego o plik PDF do pobrania, którzy jeszcze go nie otrzymali (ich plik PDF zostanie dostarczony); oraz wnioskodawcy, którzy złożyli wniosek za

pomocą aplikacji COVIDCert NI o wydanie certyfikatu elektronicznego, którzy go jeszcze nie otrzymali (otrzymają plik PDF jako etap pośredni).

Incydent nie będzie miał wpływu na niektóre osoby, które już złożyły wniosek o certyfikat cyfrowy lub oczekują na weryfikację tożsamości. Mogą nadal normalnie korzystać z usług po przywróceniu operacji.

Wnioskodawcy, którzy złożyli wniosek o wydanie certyfikatu elektronicznego, ale zamiast tego otrzymali kopię PDF, będą mogli się zalogować i pobrać wersję elektroniczną po rozwiązaniu problemu. Wnioskodawcy, którzy obecnie przechodzą weryfikację tożsamości w przepływie pracy NIDirect, mogą kontynuować. Po pomyślnym zweryfikowaniu będą musieli się wstrzymać, aż problem zostanie rozwiązany.

Niektórzy użytkownicy mogą nie być w stanie zalogować się przez swoje konto NIDirect, ponieważ zostali zablokowani z powodu problemów technicznych.

Liczba naruszeń danych w służbie zdrowia rośnie z roku na rok

Incydent z danymi miał miejsce w czasie, gdy wśród społeczeństwa jest wiele kontroli i obaw dotyczących paszportów szczepionkowych przeciwko COVID-19. Naruszenia danych w służbie zdrowia rosną wykładniczo z roku na rok i nie wydaje się, aby w najbliższym czasie spowolniły.

Ważne jest, aby specjaliści IT z opieki zdrowotnej podejmowali kroki w celu zabezpieczenia swoich systemów, niezależnie od tego, czy oznacza to ochronę przed zewnętrznymi zagrożeniami stwarzanymi przez hakerów i cyberprzestępców, czy zabezpieczenie wewnętrznych zagrożeń wynikających z nadużyć dostępu ze strony użytkowników wewnętrznych.

Dane dotyczące opieki zdrowotnej są cenne na czarnym rynku, ponieważ często zawierają wszystkie informacje

umożliwiające identyfikację danej osoby, a nie pojedynczą informację, która może zostać znaleziona w przypadku naruszenia finansowego.

Rekord danych medycznych jest wart na czarnym rynku do 250 USD

Według raportu Trustwave, rekord danych medycznych może być wyceniany na 250 USDna czarnym rynku, w porównaniu do 5,40 USD za kolejny rekord o najwyższej wartości – karty płatnicze.

Większość z tych naruszeń można przypisać przestępcom wewnętrznym i hakerom, którzy uzyskują dostęp za pośrednictwem zewnętrznych dostawców. Instytut Ponemon ustalił, że koszty związane z naprawą naruszenia szacuje się na 740 000 USD. Jeśli osoba trzecia spowoduje naruszenie danych, koszt ataku wzrasta o ponad 370 000 USD.

Eksperci branżowi twierdzą, że wektorami ataków są najprawdopodobniej ataki typu ransomware lub SQL injection, które mogą wystąpić, gdy złośliwa poczta e-mail, witryna internetowa lub oprogramowanie jest zainstalowane lub uzyskuje dostęp w sieci, często przez niczego niepodejrzewającego użytkownika.

Opieka zdrowotna podatna na ataki ransomware

Branża opieki zdrowotnej jest szczególnie podatna na ataki złośliwego oprogramowania ransomware. W styczniu 2018 r. atak zmusił informatyków w Hancock Health do zamknięcia swoich systemów, podczas gdy informacje umożliwiające identyfikację pacjentów były zakładnikami.

Naruszenie przypisano hakerowi, który korzystał z portalu zdalnego dostępu i danych uwierzytelniających innej firmy, które są głównymi przyczynami cyberataków. Szpital został później zmuszony przez atakującego do zapłacenia 55 000 USD za pomocą bitcoinów.

Prawdziwe niebezpieczeństwo ataków hakerów na placówki opieki zdrowotnej polega na tym, że personel medyczny pilnie potrzebuje dostępu do akt pacjentów na miejscu. W niektórych przypadkach może to być dosłownie kwestia życia i śmierci.

Hakerzy atakujący placówki opieki zdrowotnej wiedzą, że po uzyskaniu dostępu za pośrednictwem sieci VPN, danych uwierzytelniających lub phishingu nie ma możliwości ograniczenia dostępu do napotkanych informacji. Otwarcie tych drzwi oznacza nieograniczony dostęp do dziesiątek, setek, a nawet tysięcy akt pacjentów.

Źródła obejmują:

BleepingComputer.com

SecureLink.com

Upublicznianie w sieci materiałów o dziecku wiąże się z zagrożeniami. Eksperci radzą, jak im zapobiegać

Mimo informacji o kolejnych wyciekach danych oraz o inwigilacji relacjonowanie codziennego życia w mediach

społecznościowych wciąż wydaje się nie tracić na popularności. Na stronie Centrum Informacji Konsumenckiej czytamy, że w Polsce ok. 40 proc. rodziców regularnie korzystających z internetu publikuje materiały dotyczące własnego dziecka. Z kolei według badań dr Anny Brosch z Wydziału Nauk Społecznych Uniwersytetu Śląskiego w Katowicach co czwarty rodzic permanentnie udostępnia w mediach społecznościowych informacje o swoich dzieciach, które traktowane jak „mikrocelebryci" dorastają w przeświadczeniu, że dzielenie się szczegółami z prywatnego życia jest naturalną praktyką.

„Życie na wirtualnym świeczniku"

Zjawisko to nazywa się sharentingiem (ang. share – dzielić się i parenting – rodzicielstwo) i odnosi się do częstego upubliczniania informacji intymnych o dziecku, które naruszają jego prywatność i które mają zasięg publiczny, a więc mogą trafić do anonimowego odbiorcy. Mogą to być np. zdjęcia przedstawiające codzienne życie, ale i zdjęcia prześmiewcze, np. gdy dziecko zaśnie z nosem w talerzu.

Jak informują eksperci, ok. 23 proc. dzieci zaczyna istnieć w sieci jeszcze przed fizycznym przyjściem na świat, ponieważ ich rodzice zamieszczają zdjęcia bądź nagrania z USG. Czasem nawet dzieci przebywające w łonie matki mają już profile w mediach społecznościowych.

Z poradnika „Sharenting i wizerunek dziecka w sieci" wydanego przez Akademię NASK dowiadujemy się, że spora część rodziców zamieszczających w sieci treści o swoim dziecku nie stosuje ograniczeń dotyczących wyświetlania materiałów i udostępnia je większym grupom osób.

Według badań przeprowadzonych przez dr Annę Brosch w 2018 roku w grupie 1036 rodziców dzieci w wieku przedszkolnym, co czwarty z nich nagminnie udostępnia takie informacje. „Nie jest to więc aż tak popularny proceder, ale na pewno zauważalny, bo jeżeli ktoś upowszechnia dziesiątki albo nawet

setki zdjęć swoich dzieci, to odbiorcom wydaje się, że media społecznościowe są nimi zalane” – powiedziała dr Brosch.

Badaczka z Wydziału Nauk Społecznych Uniwersytetu Śląskiego zwraca uwagę, że sharentingiem zajmują się przeważnie matki.

„Dawniej np. w latach 70. XX wieku młode matki siadały przed blokiem na ławce, dzieci bawiły się w piaskownicy, a one rozmawiały o dzieciach. Teraz matki przeniosły się do sieci” – podkreśliła.

W ocenie dr Brosch matki udostępniają zdjęcia swoich dzieci z kilku powodów. Po pierwsze, żeby pokazać innym, jak dobrymi są matkami, że sobie doskonale radzą. Po drugie, poszukują wsparcia i akceptacji społecznej dla tego, co robią.

„Trzeci motyw związany jest z charakterystyczną dla naszych czasów modą na popularność. Chodzi o uzyskanie aprobaty społecznej poprzez lajki, co prowadzi do popularności. Wiele osób w sieci naśladuje innych – znanych tylko z tego, że są znani. Następnie oni sami chcą stać się takimi celebrytami. A że nie mają szansy dzięki sobie, to starają się to uzyskać chociaż dzięki dziecku. Stąd np. te zdjęcia ośmieszające dzieci, które mają po prostu przykuwać uwagę” – tłumaczyła badaczka.

Brosch dodała, że ojcowie w dużo mniejszym stopniu ulegają sharentingowi, a jeżeli już, to najczęściej w sytuacji, gdy starają się o prawa do opieki nad dzieckiem.

Częściej kobiety ulegają sharentingowi niż mężczyźni. Robią to, by pokazać, że są dobrymi matkami, choć wiele z nich poszukuje również akceptacji i popularności. Zdjęcie ilustracyjne (MarieXMartin / Pixabay)

Stacey Steinberg, profesor z Levin College of Law na Uniwersytecie Florydy w Gainesville, podaje, że dla części rodziców sharenting jest rodzajem budowania więzi z rozproszoną rodziną, pomaga w dzieleniu się problemami i niweluje samotność. Badaczka podkreśla jednak, że należy pamiętać także o płynących z takiego działania zagrożeniach.

Jako obrończyni praw dzieci zaznaczyła, że dzieci powinny mieć prawo do decydowania, jakie informacje o nich chcą zamieścić w sieci ich rodzice.

Nawet jeśli w danym przypadku publikowane treści nie narażą dziecka na różnego rodzaju represje, kradzież tożsamości czy może nie trafią na strony z pornografią dziecięcą, to pediatrzy są coraz bardziej świadomi znaczenia ochrony obecności dzieci w cyfrowej rzeczywistości i zwracają uwagę, by nie zapominać o prawie dziecka do prywatności.

Prywatność i „długa pamięć internetu”

„Każdy człowiek powinien mieć możliwość tworzenia własnej tożsamości i wizerunku, także w świecie cyfrowym” – podkreślają Anna Borkowska i Marta Witkowska, autorki poradnika „Sharenting i wizerunek dziecka w sieci”. Wszystkim niezależnie od wieku należy się prawo decydowania, jakie szczegóły z własnej prywatności chce ujawnić. Rodzice nagminnie dokumentujący w mediach społecznościowych życie własnych dzieci pozbawiają je możliwości wyboru, co i czy w ogóle chciałyby opowiedzieć o sobie w wirtualnym świecie.

Ponadto autorki poradnika dla rodziców o upublicznianiu wizerunku dziecka w sieci wymieniają jeszcze inne zagrożenia związane z sharentingiem.

Przypominają, że „internet ma długą pamięć” i w cyberprzestrzeni nic nie ginie, zwłaszcza że treści zyskujące dużą popularność dość szybko są rozpowszechniane, a zatem trudno je całkowicie usunąć.

„Internet nigdy nie zapomina, więc trudno przewidzieć konsekwencje tego procederu dla dzieci w przyszłości. W sieci nic nie ginie, a jeżeli wrzuci się do sieci jakieś zdjęcie, to zaczyna ono żyć własnym życiem. Nie mówiąc o skrajnych, ale jednak [mających miejsce], przypadkach kradzieży tożsamości w internecie czy pedofilach w sieci” – mówi dr Brosch.

Utrata kontroli

Na przykład w 2015 roku w Australii wykazano, że około połowa z 45 mln zdjęć znajdujących się na stronie z pornografią dziecięcą pochodziła bezpośrednio z mediów społecznościowych i były to przeważnie niewinne zdjęcia z codziennej scenerii, które pojawiały się w kontekście niestosownych komentarzy.

Dlatego eksperci podkreślają, by pamiętać, że nad fotografiami

wrzuconymi do sieci, przestaje się mieć pełną kontrolę i nie można być pewnym, kto i w jaki sposób je wykorzysta. Mogą zostać bezprawnie użyte w celach majątkowych bądź przestępczych.

Specjaliści ostrzegają, że „media społecznościowe są bardzo często terenem poszukiwań dla pedofilów, którzy nagminnie pobierają z nich zdjęcia dzieci i handlują nimi na zamkniętych forach internetowych”.

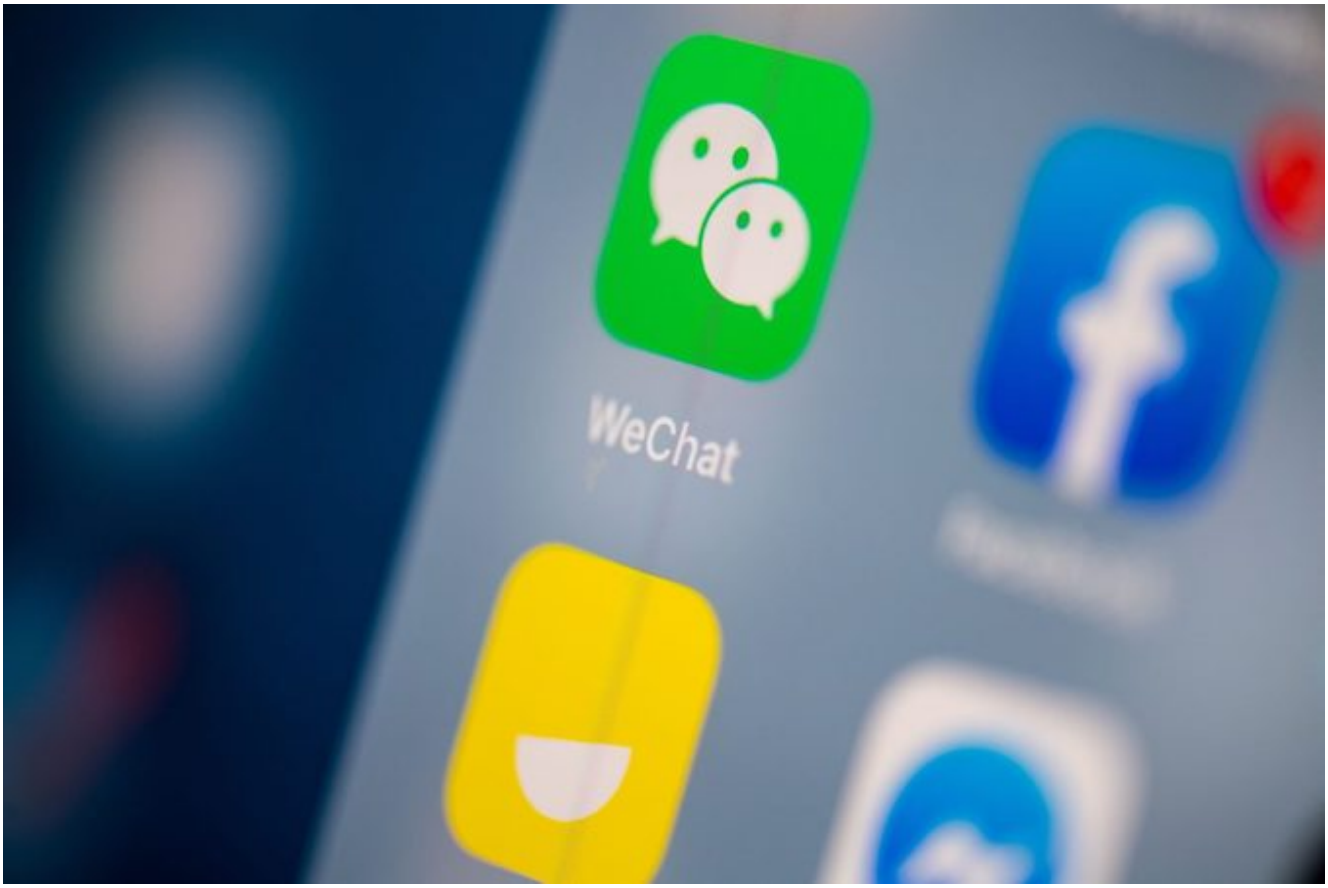
Przestępstwo posługiwania się skradzionym wizerunkiem dziecka w celu realizowania swoich fantazji nazywane jest cyfrowym kidnapingiem (ang. baby role play).

Nie powinniśmy też narażać dzieci na cyberprzemoc. Asumptem do tego może być publikowanie w naszej opinii zabawnych zdjęć dziecka, które jednak w szerszej perspektywie mogą zostać odebrane jako kompromitujące. To może spowodować falę hejtu i agresji ze strony zarówno nieznajomych internautów, jak i rówieśników dziecka oraz wpłynąć na jego samoocenę.

Wykorzystywanie danych osobowych

Pozostaje też kwestia udostępniania danych osobowych, które „wymieniamy” za możliwość korzystania z profilu w mediach społecznościowych. Stanowią one źródło informacji m.in. dla firm marketingowych.

Co więcej, eksperci ds. Chin, a także politycy od lat alarmują, by nie korzystać z chińskich technologii, m.in. TikToka czy WeChata, oraz innych pozornie niegroźnych narzędzi, które gromadzą dane na temat użytkowników, a także pozyskują w nielegalny sposób poufne informacje i wrażliwe dane z różnych instytucji. Gdy takie informacje znajdą się w rękach reżimu komunistycznego, mogą zagrażać bezpieczeństwu krajów oraz ich mieszkańców.



Ilustracja demonstrująca logo chińskiego komunikatora WeChat wyświetlonego na tablecie, 24.07.2019 r. (Martin Bureau/AFP/Getty Images)

Komunistycznej Partii Chin do zbierania danych służą np. platformy społecznościowe, komunikatory, programy do obróbki i „ulepszania" zdjęć lub aplikacje usprawniające pisanie maili.

Władze ChRL wykorzystują „systemy big data do inwigilacji – zwłaszcza w celu sprawdzenia, czy ktoś ma opinie sprzeczne z prezentowanymi przez chiński reżim. Jednym ze sposobów jest analizowanie zakupów w sklepach internetowych" – powiedział profesor nauk politycznych dr Titus C. Chen z Narodowego Uniwersytetu Sun Yat-sena na Tajwanie.

Niemal wszechobecny monitoring w Chinach oraz nadzorowanie aktywności w internecie używane są do tzw. systemu oceny (ang. social credit system). Według niego każdemu obywatelowi są przyznawane punkty „społecznej wiarygodności". Ludziom mogą zostać odjęte punkty z ich wyniku oceny społecznej, jeśli popełnią czyn uznawany przez KPCh za niepożądany, jak

np. przejście przez ulicę w miejscu niedozwolonym. Osoby z niskimi wynikami oceny społecznej są uważane za „niegodne zaufania”, a tym samym pozbawiane dostępu do usług i możliwości. Może chodzić np. o zakaz podróżowania samolotem lub uczęszczania do szkół.

System służy do prześladowania m.in. zwolenników duchowej praktyki Falun Gong, Ujgurów i innych grup, które KPCh próbuje zniszczyć.

Pojawiające się co jakiś czas informacje o wycieku danych pokazują, że KPCh infiltruje nie tylko obywateli ChRL, ale uważnie obserwuje osoby na Zachodzie.

Konsekwencje

Zdaniem dr Anny Brosch sharenting sprawia, że dzieci zaczynają być traktowane jak „mikrocelebryci”, którzy dorastają w przeświadczeniu, że dzielenie się szczegółami z prywatnego życia jest naturalną praktyką.

„Można więc przypuszczać, bo to wymaga jeszcze badań, że gdy w przyszłości sami zostaną rodzicami, będą jeszcze bardziej otwarci i skłonni do samoujawniania. Ale z drugiej strony, to już się dzieje, nastolatkowie proszą rodziców o usunięcie zdjęć i informacji o sobie; za granicą były nawet przypadki sądowych rozpraw” – mówiła dr Brosch.

Badania dr Brosch wykazują, że sharenting się zmienia.

„Coraz mniej już jest zasypywania całymi seriami przypadkowych zdjęć. Teraz są one przemyślane. Wzrasta jednak nastawienie rodziców na zachowania celebryckie i na zyski – im więcej lajków, tym większa popularność i być może możliwość zarabiania pieniędzy z umów na produkty lokowane. W takich przypadkach mogą to być nawet kompromitujące filmy, ale liczy się zasięg” – zauważyła.

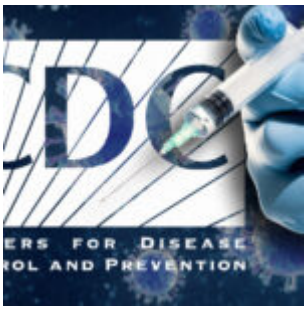
Znawcy przedmiotu doradzają zastanowienie się, jakie treści

o naszych pociechach wrzucamy do sieci i jakie to może mieć konsekwencje w przyszłości. Jeśli decydujemy się na publikację, róbmy to odpowiedzialnie. Pamiętajmy, że nawet najlepsze zabezpieczenia nie dadzą nam pełnej ochrony przed niepożądaną kradzieżą wizerunku.

Dbajmy też o to, by nie narazić dzieci na ostracyzm i uczmy je świadomego podejścia do upubliczniania informacji w cyberprzestrzeni.

Źródła: PAP, Centrum Informacji Konsumenckiej, Akademia NASK, NPR.

Jak CDC manipuluje danymi, aby wzmocnić „skuteczność szczepionki”



Amerykańskie Centrum Kontroli Chorób (CDC) zmienia swoje praktyki rejestrowania i testowania danych pod kątem „Covid19”, aby sprawiać wrażenie, że eksperymentalne „szczepionki” stosowane w terapii genowej są skuteczne w zapobieganiu domniemanej chorobie.

Nie ukrywali tego, ogłaszając zmiany polityki na swojej stronie internetowej na przełomie kwietnia i maja (choć oczywiście bez przyznania dość oczywistej motywacji zmiany).

Sztuczka polega na tym, że zgłaszają to, co nazywają „przełomowymi infekcjami" – to znaczy ludzie, którzy są w pełni „zaszczepieni" przeciwko infekcji Sars-Cov-2, ale i tak zostają zarażeni.

Zasadniczo Covid19 od dawna jest pokazywany – tym, którzy chcą zwrócić uwagę – jako całkowicie stworzona narracja pandemiczna, zbudowana na dwóch kluczowych czynnikach:

1. **Testy fałszywie dodatnie.** Zawodne test PCR można manipulować do zgłaszania dużej liczby fałszywie dodatnich zmieniając próg cyklu (wartość CT).
2. **Zwiększona liczba przypadków.** Niezwykle szeroka definicja „przypadku Covid", stosowana na całym świecie, wymienia każdego, kto uzyska pozytywny wynik testu, jako „przypadek Covid19", nawet *jeśli nigdy nie wystąpiły u niego żadne objawy*.

Bez tych dwóch polityk *nigdy nie byłoby znaczącej pandemii*, a teraz CDC wprowadziło dwie zmiany w polityce, co oznacza, że nie mają one już zastosowania do osób zaszczepionych.

Po pierwsze, **obniżają wartość CT podczas badania próbek z podejrzanych „przełomowych zakażeń".**

Z instrukcji CDC dla stanowych organów ds. Zdrowia dotyczących postępowania z „możliwymi przełomowymi infekcjami" (przesłanych na ich stronę internetową pod koniec kwietnia):

> *W przypadkach ze znaną wartością progową cyklu RT-PCR (Ct) należy przesyłać do CDC **tylko próbki o wartości Ct <28** w celu sekwencjonowania. (Sekwencjonowanie nie jest możliwe przy wyższych wartościach Ct).*

Przez całą pandemię wartości CT przekraczające 35 były normą, a laboratoria na całym świecie sięgały lat czterdziestych.

Zasadniczo laboratoria wykonywały tyle cykli, ile było konieczne, aby osiągnąć pozytywny wynik, pomimo ostrzeżeń

ekspertów, że to bezcelowe (nawet sam Fauci powiedział, że cokolwiek powyżej 35 cykli jest bez znaczenia).

Ale TERAZ i tylko w przypadku osób w pełni zaszczepionych, CDC przyjmie tylko próbki uzyskane z 28 cykli lub mniej. Może to być tylko celowa decyzja mająca na celu zmniejszenie liczby oficjalnie odnotowywanych „zakażeń przełomowych".

Po drugie, **infekcje bezobjawowe lub łagodne nie będą już rejestrowane jako „przypadki zakaźne".**

Zgadza się. Nawet jeśli próbkę pobraną przy niskiej wartości CT wynoszącej 28 można zsekwencjonować do wirusa rzekomo wywołującego Covid19, CDC nie będzie już prowadzić rejestrów przełomowych infekcji, *które nie prowadzą do hospitalizacji ani śmierci*.

Źródło" propaganda.news

Zadbaj o silne hasła do kont. Zniwelujesz zagrożenie cyberatakiem i ochronisz swoje dane, pieniądze

W cyberprzestrzeni coraz częściej przechowujemy wiele cennych

informacji – prywatnych i nie tylko. Od nas zależy, czy odpowiednio je zabezpieczymy. Wydział Promocji Polityki Cyfrowej Kancelarii Prezesa Rady Ministrów (KPRM) przypomina, że internetowi przestępcy atakują nie tylko duże przedsiębiorstwa, lecz także zwykłych ludzi. Eksperci namawiają do stosowania silnych haseł do kont bankowych, poczty elektronicznej, na portalach społecznościowych, a także w telefonie czy w komputerze, by nikt ich nie przejął, nie ukradł tożsamości, nie pozbawił oszczędności bądź nie miał dostępu do naszych prywatnych danych. Jak zatem powinniśmy tworzyć kody zabezpieczające?

Mankamenty haseł

Cyfryzacja KPRM podaje, że część cyberataków uderza właśnie w hasła użytkowników, dlatego należy wystrzegać się najpowszechniejszych błędów, a więc unikać prostych haseł i nie używać tego samego kodu zabezpieczającego do różnych kont. Wskazane jest tworzenie unikatowych haseł dla każdej witryny.

Jakich jeszcze błędów nie powinniśmy popełniać? Nie zabezpieczajmy dostępu do swoich danych najpopularniejszymi hasłami lub oczywistymi wyrażeniami, typu: „hasło”, „123456”, „qwerty”, „piłka nożna”, „wpuscmnie”, ani imieniem własnym bądź kogoś z bliskiego otoczenia, bądź ulubionego zwierzaka. Ta sama zasada dotyczy też danych osobowych, które łatwo zdobyć, takich jak: data urodzenia, numer telefonu, numer rejestracyjny samochodu, nazwa ulicy, numer mieszkania lub domu.

Niewskazane jest stosowanie wyrażeń identycznych z nazwą użytkownika, lub nawet jej częścią, oraz sekwencji kolejnych liter, liczb lub innych znaków, np. „abcde”, „12345”, „QWERTY”, jak również dwóch lub trzech kolejno powtarzających się ciągów znaków, np. „bbbb2bbb”.

Ponadto odradza się używanie pojedynczego wyrazu dowolnego

języka, pisanego normalnie lub wspak, nie wystarczy też, że poprzedzimy lub zakończymy go znakiem specjalnym lub cyfrą.

W komunikacie zwrócono uwagę, by przy zmianie hasła do istniejącego konta nie użyć tego samego sformułowania, co poprzednio lub po niewielkiej modyfikacji, np. zmiana z „hasło1” na „hasło2”.

Cyberklucz

Cyfryzacja KPRM przypomina: „Hasła są jak klucze do sejfu lub domu”. Trzeba dbać, żeby nie dostały się w niepowołane ręce.

Dlatego radzi, aby tworzyć dłuższe hasła, składające się z 12 lub 14 znaków, które będą zawierały co najmniej jeden znak z każdej z następujących grup: małe litery, duże litery, liczby, znaki specjalne.

Konstruując unikatowe hasło, można, jak podpowiadają specjaliści, wykorzystać frazy, wybrać np. łatwy do zapamiętania cytat z piosenki i użyć pierwszych liter poszczególnych słów. Poleca się zastępowanie liter bądź wyrazów liczbami i symbolami.

Podano przykłady: „Mam dwadzieścia lat” można zamienić na M@m2dzie$ciAl4T, a „Mam psa” na M@m%p$@.

Można stosować też metodę łączenia trzech losowych słów, np. „kawatramwajryba”, byleby nie były zbyt proste do odgadnięcia.

Podkreślono, że zabezpieczeń nie powinno się zapisywać na papierze, przesyłać np. w mailu albo wpisywać haseł, gdy ktoś to widzi, bo nawet bardzo silne kody mogą w takich przypadkach okazać się bezużyteczne.

Cyfryzacja KPRM ostrzega przed podszywającymi się np. pod pracowników pomocy technicznej hakerami, którzy próbują wyłudzić dane użytkownika i hasła. Jak zaznaczono: „Wiarygodne witryny i organizacje nigdy

nie poproszą o nazwę użytkownika i hasło w wiadomości e-mail lub przez telefon”.

Hasło powinniśmy bezzwłocznie zmienić, jeśli doszło do jego naruszenia lub nawet jeśli tylko przypuszczamy, że ktoś mógł je wykraść.

Nie należy również wpisywać hasła, gdy korzystamy z cudzego komputera.

Aby dane były bezpieczniejsze, potrzebne jest nie tylko silne hasło, lecz także stosowanie dwuetapowej weryfikacji.

Dodatkowe informacje o zabezpieczaniu danych w cyberprzestrzeni można znaleźć w poradniku „Jak chronić się przed cyberatakami”.

Źródła: PAP, Cyfryzacja KPRM.

Dane 2,4 mln osób z całego świata, w tym Polaków, zgromadziła chińska firma lojalna wobec Komunistycznej Partii Chin

W połowie września 2020 roku wyciekły informacje o tym, że chińska firma Shenzhen Zhenhua Data Technology, powiązana z tajnym oddziałem wojskowym i wywiadowczym Pekinu, zgromadziła gigantyczną bazę danych z plikami dotyczącymi 2,4 mln ludzi z całego świata, w tym dane wpływowych osób i ich rodzin. W ostatnich dniach pojawiły się doniesienia, że ChRL zebrała również dane Polaków.

„Kolekcja" danych z całego globu w komunistycznych rękach

Zhenhua Data Technology, która jest powiązana z Armią Ludowo-Wyzwoleńczą, Ministerstwem Bezpieczeństwa Państwa oraz Komunistyczną Partią Chin (KPCh), zgromadziła bazę skompilowaną głównie z tzw. materiałów open source, takich jak posty w mediach społecznościowych i dane online.

Baza danych okazała się uszkodzona. Australijska firma Internet 2.0, która zajmuje się cyberbezpieczeństwem, odzyskała ponad 10 proc. danych, które były w niej zawarte. Firma ujawniła, że pośród zrekonstruowanych plików znalazły się dane około 52 tys. Amerykanów, 35 tys. Australijczyków, 9 tys. 700 Brytyjczyków i 5 tys. Kanadyjczyków.

W ostatnim tygodniu października „Gazeta Polska" poinformowała w artykule, że otrzymała od Internet 2.0 fragment bazy danych z nazwiskami Polaków. „To spis ponad 3 tys. rekordów zawierających imiona i nazwiska (część się powtarza). Nie wiadomo jednak, z jakiego powodu chiński wywiad wojskowy zlecił Zhenhua zbieranie informacji o tych osobach. Pewne jest jednak, że służba ta ma bardzo dobrą orientację w polskim świecie politycznym. Na liście znajdują się nie tylko byli lub obecni wysocy rangą urzędnicy państwowi, lecz także ich rodziny – małżonkowie, dzieci, rodzice i rodzeństwo" – podaje gazeta.

Internet 2.0 odtworzył zaledwie 10 proc. całej bazy, wydaje się więc, że w tym momencie nie można stwierdzić, czy wśród

odzyskanych rekordów znalazły się wszystkie dane Polaków, które zostały zgromadzone w bazie.

Na kogo „poluje” KPCh na całym świecie?

Zgodnie z raportami globalnego konsorcjum medialnego baza danych obejmuje osoby z różnych sektorów – polityki, biznesu, prawa, środowiska akademickiego i obronności – oraz zawiera szczegółowe dane, takie jak daty urodzenia, adresy, stan cywilny i upodobania polityczne.

Znajdują się tam dane dotyczące zarówno zwykłych biznesmenów, jak i wysokiej rangi osobistości, takich jak oficerowie marynarki wojennej Stanów Zjednoczonych, obserwatorzy Chin w Waszyngtonie, osoby ze środowiska naukowego, członkowie brytyjskiej rodziny królewskiej oraz liderzy przedsiębiorczości.

Ta baza danych, nazywana Overseas Key Information Database (OKIDB), pozwala na dostęp do zagranicznych danych politycznych, wojskowych i biznesowych. Zawiera szczegółowe informacje na temat infrastruktury państw, przemieszczania się zasobów wojskowych, a także analizy opinii publicznej.

Mimo że obecnie nie ma dowodów na to, że reżimowe władze wykorzystują oprogramowanie OKIDB, to jak podkreśla „Washington Post”, z dokumentów marketingowych i rekrutacyjnych Zhenhua można wnioskować, że jest to „firma patriotyczna”, której głównym klientem docelowym jest wojsko.

„The Globe and Mail” po analizie danych dotyczących Kanadyjczyków napisał, że twórcy bazy przypisali osobom z listy „ocenę” w skali od 1 do 3 .

„Wydaje się, że ci, którym przypisano 1, to osoby o bezpośrednim wpływie, takie jak burmistrzowie, posłowie lub wyżsi urzędnicy państwowi, podczas gdy ci, którym przypisano 2, byli często krewnymi osób u władzy […]” – podaje gazeta.

Z kolei ci, których oznaczono numerem 3, to najczęściej osoby skazane, przeważnie za przestępstwa gospodarcze – napisał dziennik.

Tajemnicza baza ujrzała światło dzienne

Baza danych została ujawniona przez źródło w Chinach, a informację przekazano profesorowi Christopherowi Baldingowi. To amerykański naukowiec, który do 2018 roku pracował na Uniwersytecie w Pekinie, skąd udało mu się wyjechać ze względów bezpieczeństwa. To dzięki niemu sprawą zajęła się firma Internet 2.0.

14 września Balding opublikował na swojej stronie oświadczenie, w którym napisał, że zajmował się badaniami doniesień dotyczących Huawei. Trwało to do momentu, zanim w jego badaniach nie nastąpił nagły zwrot. Natknął się na „coś, co dla badaczy Chin jest czymś podobnym do odkrycia Świętego Graala" – otrzymał informację o istnieniu tej potężnej bazy danych.

Przekazał ją konsorcjum mediów w Australii, Stanach Zjednoczonych, Kanadzie, Wielkiej Brytanii, Włoszech i Niemczech.

Balding uważa, że dane potwierdzają utrzymywane od dawna podejrzenia, dotyczące działalności KPCh w zakresie nadzoru i monitorowania. „To, czego nie można lekceważyć, to rozległość i szczegółowość nadzoru [prowadzonego przez] chińskie państwo oraz jego zasięg na całym świecie" – podkreśla.

Jak zauważa: „Świat jest dopiero na początkowych etapach zrozumienia, ile Chiny inwestują w wywiad i jak wpływają na operacje, korzystając z surowych danych, musimy zrozumieć ich cele".

We wcześniejszym wpisie naukowiec zwraca uwagę, że KPCh stanowi „bezprecedensowe wyzwanie dla otwartych, kochających

wolność państw prawa na całym świecie”. Reżim „buduje opresyjne państwo z nadzorem technologicznym, które daje partii komunistycznej potężne środki do kontroli obywateli w kraju” – wyjaśnia.

„Mamy teraz dowody na to, jak chińskie firmy współpracują z agencjami państwowymi w celu monitorowania osób i instytucji na całym świecie” – ocenia Balding.

Reakcja Zhenhua nie zdziwiła ekspertów

Poproszona przez „The Guardian” o komentarz firma Zhenhua zaprzeczyła istnieniu takiej bazy danych, podając, że wszelkie zebrane informacje są danymi ogólnodostępnymi w internecie. Przedstawicielka firmy stwierdziła, że nie zbierają danych i jest to tylko „integracja danych”. Zaznaczyła, że model biznesowy i partnerzy stanowią tajemnicę handlową firmy.

Zanegowała również doniesienia, że Zhenhua ma jakiekolwiek powiązania z chińskimi władzami lub wojskiem, dodając, że ich klientami są organizacje badawcze i grupy biznesowe.

W rozmowie z anglojęzyczną edycją „The Epoch Times” eksperci przyznali, że nie byli zaskoczeni takim stanowiskiem chińskiej firmy.

Według Michaela Shoebridge’a, dyrektora programu obrony, strategii i bezpieczeństwa narodowego w think tanku Australian Strategic Policy Institute (ASPI), stwierdzenie Zhenhua „nie może być przyjmowane za dobrą monetę”, wziąwszy pod uwagę, że tamtejsze prawo zobowiązuje firmy do pomocy chińskim agencjom bezpieczeństwa i wywiadu. Dodaje, że firmy oczywiście muszą publicznie temu zaprzeczać.

W ocenie Caseya Fleminga, dyrektora generalnego firmy BLACKOPS Partners, zajmującej się strategią wywiadowczą i bezpieczeństwa, zgromadzone w bazie informacje są wykorzystywane do wspierania operacji „nieograniczonej wojny hybrydowej” chińskiego reżimu. Obejmuje to szpiegostwo, tajne

zagraniczne kampanie wpływów oraz kradzież zagranicznych innowacji i technologii wojskowej.

Termin nieograniczona wojna hybrydowa nawiązuje do powstałej w latach 90. ubiegłego wieku strategii, którą stworzyli i opisali dwaj chińscy pułkownicy sił powietrznych Qiao Liang i Wang Xiangsui w książce „Unrestricted Warfare". Wydała ją Armia Ludowo-Wyzwoleńcza, siły zbrojne KPCh. Autorzy korzystali z oryginalnych dokumentów wojskowych. Strategia ta opowiada się za zastosowaniem serii niekonwencjonalnych taktyk, stworzonych po to, by osiągnąć cele wojny jednak bez angażowania się w rzeczywistą walkę.

Jak zauważa Fleming, ostatecznym celem tej strategii jest „zniszczenie demokracji po to, by chiński komunizm mógł globalnie przejąć nadzór".

Dyrektorem naczelnym Zhenhua jest Wang Xuefeng, były inżynier IBM. Jak podaje australijski nadawca ABC, wcześniej w chińskich mediach społecznościowych zamieścił wpis o prowadzeniu „wojny hybrydowej" poprzez manipulowanie opinią publiczną i „wojnę psychologiczną".

Zdaniem Nicholasa Eftimiadesa, byłego wysokiego funkcjonariusza sił wywiadowczych USA i autora książki „Chinese Intelligence Operations" (pol. „Chińskie operacje wywiadowcze"), baza danych pomogłaby chińskiemu wywiadowi w namierzeniu tych, którzy nadawaliby się do rekrutacji lub szantażu. Chodzi o osoby ze „słabościami", które można wykorzystać, np. „zapotrzebowanie na pieniądze [lub] sympatie polityczne przeciwne administracji". Reżim mógłby wyszukiwać w mediach społecznościowych posty, które sugerują niezadowolenie z rządu lub trudności finansowe.

W analogiczny sposób działa to w przypadku operacji wywierania wpływu. Wyszukiwani są ludzie publikujący opinie, które popierają politykę reżimu. Kolejnym krokiem jest wspieranie takiej osoby, jej organizacji, a tym samym wzmacnianie jej

poglądów.

Michael Shoebridge zwraca uwagę, że w bazie Zhenhua znajdują się także dane dzieci wpływowych ludzi, m.in. polityków i dyrektorów biznesowych. „To dość niepokojący potencjał wykorzystania takich danych" – zaznacza ekspert. Umożliwia bowiem wywieranie nacisku na te osoby, wykorzystując słabości ich potomstwa.

Ponadto część tych dzieci może w dorosłym życiu piastować eksponowane stanowiska. Zatem na skutek analizowania ich profili już od dzieciństwa „możliwość wykorzystywania tych osób i wpływania na nie jest znacznie większa, ponieważ z biegiem czasu zyskujesz o wiele bardziej wszechstronne ich zrozumienie" – wskazuje Shoebridge.

Kropla w morzu… chińskich baz danych

Eksperci zaznaczają, że gromadzenie danych przez chiński reżim komunistyczny odbywa się na masową skalę, znacznie większą, niż jesteśmy w stanie sobie wyobrazić, a wyciek danych z Zhenhua, to jedynie przysłowiowa kropla w morzu tego, co tam się dzieje.

Shoebridge porównał bazę danych do pojedynczej plastikowej piłeczki w ogromnym basenie. Jak twierdzi, ten zbiór danych byłby łączony z danymi, które zebrały inne chińskie podmioty w celu ich wykorzystania do różnych operacji, mających wesprzeć interesy reżimu.

„To interakcja firm posiadających takie dane z innymi firmami i danymi rządowymi daje władzę" – skomentował ekspert.

Michael Shoebridge tłumaczy, że strategia ta znajduje odzwierciedlenie w doktrynie reżimu o „fuzji cywilno-wojskowej". Dzięki niej władze wykorzystują innowacje prywatnych przedsiębiorstw do napędzania rozwoju wojskowego.

W październiku 2019 roku Australian Strategic Policy Institute

opublikował raport „Engineering global consent”, napisany przez Samanthę Hoffman. Stwierdzono w nim, że reżim tworzy „masowy i globalny ekosystem gromadzenia danych”, wykorzystując możliwości przedsiębiorstw państwowych i prywatnych chińskich firm technologicznych.

Wymienia się w nim Global Tone Communication Technology Co., spółkę zależną chińskiego przedsiębiorstwa państwowego, nadzorowanego przez centralny wydział propagandy KPCh.

W wywiadzie udzielonym pod koniec zeszłego roku polskiej edycji „The Epoch Times” gen. Robert Spalding powiedział, że Global ToneCommunication, to firma prowadząca usługi tłumaczeniowe, która „w rzeczywistości przy użyciu sztucznej inteligencji gromadzi wielki zbiór danych”. Jak dodał: „Czasami ma tę funkcję wbudowaną na podobnych zasadach co produkty Huawei, jako most telekomunikacyjny, lub może bazować na oprogramowaniu opartym na tzw. chmurze”.

Poza gromadzeniem ogromnych baz danych z całego świata w ponad 65 językach, które przetwarza na użytek Pekinu do celów wywiadowczych, bezpieczeństwa i propagandy, firma koncentruje się na technologiach sztucznej inteligencji, takich jak rozpoznawanie twarzy.

W opinii Nicholasa Eftimiadesa chińskich firm zaangażowanych w gromadzenie dużych ilości danych na potrzeby reżimu są prawdopodobnie dziesiątki, jeśli nie setki. Nie wliczając w to działań prowadzonych przez chińskie agencje bezpieczeństwa, które za pośrednictwem zaawansowanego technologicznie aparatu nadzoru tego kraju zbierają dane na temat wszystkich obywateli, a więc 1,4 mld ludzi.

Eftimiades twierdzi, że dane dziesiątek milionów Amerykanów zostały wykradzione przez chińskich hakerów. Zostały one wprowadzone do baz w Chinach i służą do doskonalenia narzędzi sztucznej inteligencji. Wśród ataków wyliczyć można włamanie do amerykańskiego Urzędu Zarządzania Personelem (ang. Office

of Personnel Management, OPM) w 2014 roku, federalnej agencji ds. personelu, naruszenie obowiązku sprawozdawczego firmy Equifax w 2017 roku, a także cyberatak na ubezpieczyciela zdrowotnego Anthem w 2016 roku.

W lutym 2016 roku anglojęzyczna edycja „The Epoch Times", powołując się na poufne źródło w Chinach, poinformowała, że chińskie agencje bezpieczeństwa stworzyły bazę danych wykorzystywaną do przetwarzania skradzionych danych Amerykanów. Zawiera ona także poufne dane osobowe, wyszczególnione w poświadczeniach bezpieczeństwa 21 mln obecnych i byłych pracowników federalnych, pochodzące z włamania do Urzędu Zarządzania Personelem (OPM) oraz osobiste dane prawie 80 mln obecnych i byłych klientów i pracowników Anthem.

Ta baza danych funkcjonuje na potężnym oprogramowaniu zdolnym do przyjmowania ogromnych ilości danych. Zgromadzone zasoby analizuje się pod kątem relacji między różnymi osobami i zdarzeniami.

Wyciek danych z Zhenhua Data Technology jest dla wszystkich, niezależnie od statusu społecznego, okazją do zastanowienia się nad zamieszczanymi treściami w mediach społecznościowych. Jak widać, mogą one nieoczekiwanie stać się pożywką dla podmiotów gromadzących dane. Mogą zostać wykorzystane przeciwko nam, zwłaszcza jeśli trafią do państwa totalitarnego, jakim są Chiny.

Źródła:

Military-Linked Chinese Company Collected Personal Data On Thousands of Canadians

How Chinese Data Trove on 2 Million People Serves Beijing's Unrestricted Warfare

„Gazeta Polska"

The Washington Post

The Globe and Mail

The Guardian

Ekspert UODO: Podczas lekcji online dbajmy o swą prywatność

Podczas lekcji online uczniowie i nauczyciele powinni dbać o swoją prywatność. Kamerka internetowa powinna pokazywać jak najmniej z ich otoczenia – zaleca radca Urzędu Ochrony Danych Osobowych Piotr Drobek. Przypomina, że uczniowie i rodzice nie mogą bez zgody nauczyciela publikować w sieci nagrań zdalnych lekcji.

Od poniedziałku zdalne nauczanie wróciło na większą skalę: w szkołach średnich w czerwonej strefie jest obowiązkowe, w liceach i technikach w żółtej strefie ma być łączone z nauką w szkolnych murach. W czwartek ma być ogłoszona decyzja w sprawie szkół podstawowych. Zgodnie z zapowiedziami premiera Mateusza Morawieckiego, wyższe klasy podstawówek będą uczyć się zdalnie lub w systemie hybrydowym.

Drobek zaznaczył w rozmowie z PAP, że zdalne kształcenie

i wykorzystywane do tego narzędzia rodzą nowe zagrożenia związane z ochroną danych osobowych w oświacie. Uwydatniły się też problemy, które w wielu szkołach nie były wcześniej rozwiązane, jak to, czy nauczyciel może korzystać z prywatnego sprzętu w domu, np. logując się do elektronicznego dziennika.

> *„Warto podkreślić, że RODO nie zakazuje wykorzystywania sprzętu prywatnego. Szkoła powinna wprowadzić zasady posługiwania się takim sprzętem i przeprowadzić szkolenia nauczycieli, jak mają bezpiecznie z niego korzystać” – powiedział Drobek.*

Dodał, że wykorzystywanie dziennika elektronicznego do kontaktowania się z rodzicami zapewnia większe bezpieczeństwo niż używanie poczty elektronicznej i wyklucza wcześniej zdarzające się często naruszenia, jak wysyłanie korespondencji zbiorowej z podaniem wszystkich adresatów.

Ekspert podkreślił, że bez względu na to, czy nauka odbywa się w szkolnym budynku, czy jest prowadzona zdalnie,

administratorem danych osobowych jest szkoła, a kierujący placówką dyrektor odpowiada za bezpieczeństwo ich przetwarzania.

„Nauczyciel nie jest odrębnym administratorem danych, dlatego jeśli wykorzystuje narzędzia zdalnej edukacji, powinien to robić w porozumieniu z dyrektorem szkoły" – wskazał.

„Większość szkół, przechodząc na zdalną edukację, nie miało wdrożonych ani nie wdrożyło w jednolity sposób służących do tego celu platform lub narzędzi. Z tego powodu poszczególni nauczyciele samodzielnie wybierali narzędzia lub aplikacje wykorzystywane do zdalnej edukacji, choć nie zawsze byli w stanie zdiagnozować ryzyko związane z ich wykorzystywaniem" – mówił Drobek.

Zaznaczył, że z czasem coraz więcej szkół, a także organów prowadzących, zaczęło wprowadzać w swoich placówkach jednolite platformy edukacyjne czy aplikacje.

„To pozwala zapewnić bezpieczeństwo w ramach jednego narzędzia, bez względu na to, jakie nauczyciele czy uczniowie mają umiejętności" – wskazał radca UODO.

Oprócz określenia jednolitego narzędzia do edukacji zdalnej szkoły powinny też ustalić zasady ochrony danych osobowych podczas zdalnych lekcji, wskazać, jak nauczyciel powinien reagować w sytuacji np. nagrywania lekcji czy naruszenia ochrony danych osobowych.

Ekspert zwrócił uwagę, że rodzic może w porozumieniu z nauczycielem nagrać lekcję online po to, by np. utrwalić z dzieckiem wiedzę czy odrobić lekcje. W żadnym wypadku takie nagranie nie może być jednak bez zgody nauczyciela udostępnione w sieci – ani przez rodzica, ani przez ucznia.

Drobek zauważył, że uczniom powinno się też przypominać o zachowaniu prywatności podczas korzystania z mediów społecznościowych czy gier sieciowych, a także podczas lekcji

online.

„Pamiętajmy, kiedy podczas lekcji online korzystamy z kamerek internetowych, w taki sposób zaaranżujmy swoje otoczenie, żeby zachować swoją prywatność. Zastanówmy się, jakie elementy niekoniecznie chcemy pokazywać klasie” – zalecił uczniom. Dodał, że o tym samym powinni pamiętać nauczyciele.

Autor: *Karolina Mózgowiec*