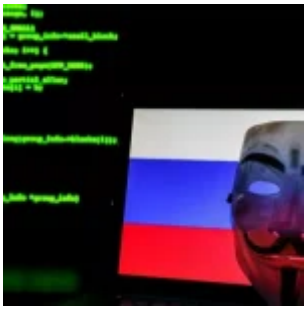
Anonymous włamali się do kolejnego rosyjskiego banku. 800 GB danych



Anonymous poinformowało, że udało im się włamać do bazy danych banku kraju-agresora Rosji. Zagrozili wyciekiem do sieci 800 GB poufnych informacji.

Stało się to znane z anonimowej wiadomości na portalu społecznościowym Twitter . Został opublikowany w poniedziałek 18 kwietnia.

Mówimy o Społecznym Banku Handlowym w Petersburgu – PSCB. Klientami tej instytucji finansowej są rosyjscy oligarchowie.

https://twitter.com/Anonymous_Link/status/1516116675078377474?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1516116675078377474%7Ctwgr%5E%7Ctwcon%5Es1
„Anonymous złamał inny rosyjski bank. Planujemy uwolnić 800 GB poufnych danych! Zespół hakerów podpisujących papiery wartościowe Anonymous złamał rosyjski bank JSC Bank PSKB, z którego korzystają oligarchowie" – podał portal społecznościowy.

W przeddzień okazało się, że Anonymous złamał jedną z firm Gazpromu . Hakerzy umieścili w Internecie 768 000 listów od pracowników Gazprom Linde Engineering, które są częścią rosyjskiego giganta gazowego. Firma specjalizuje się w projektowaniu obiektów dla rafinerii ropy naftowej.

Ponadto otrzymali dostęp do 700 GB danych rządu rosyjskiego. Anonymous przejął także kontrolę nad systemem monitoringu Kremla i pokazał pierwszy materiał filmowy z wnętrza.

Memorandum budapesztańskie: jak Ukraina oddała broń nuklearną za gwarancje bezpieczeństwa?

Był grudzień 1994 roku. Na gruzach po zimnowojennej rzeczywistości formułowano nowe porządki. Ukraina zobowiązała się do przekazania broni nuklearnej Rosji. Z kolei imperium to, a także Stany Zjednoczone i Wielka Brytania do poszanowania suwerenności i integralności terytorialnej Ukrainy. W efekcie doszło do podpisania memorandum budapesztańskiego.

Ukraina ogłosiła niepodległość 24 sierpnia 1991 roku. W tym czasie na jej terenie znajdowało się 176 pocisków wielogłowicowych, blisko 2 tysiące głowic bojowych i 44 bombowce, zdolne do przenoszenia broni jądrowej. Był to potężny arsenał (być może większy niż ówcześnie brytyjski, francuski i chiński łącznie), z którym liczyły się wszystkie światowe mocarstwa. W ich interesie było zmniejszanie dostępu

do tego typu broni wśród pozostałych państw. Jak wskazuje Rafał Kopeć, z broni nuklearnej do 1998 roku zrezygnowały: Republika Południowej Afryki, Kazachstan, Białoruś i Ukraina.

Memorandum budapesztańskie: głowice wyjeżdżają do Rosji
Ukraina pod naciskiem Rosji i USA zdecydowała się na rozpoczęcie procesu proliferacji broni masowego rażenia. Działania te zaczęły się w 1992 roku, wraz z podpisaniem przez Ukrainę, Białoruś i Kazachstan artykułu piątego Protokołu Lizbońskiego, który zobowiązywał postsowieckie państwa do denuklearyzacji.

Dopiero dwa lata później, w grudniu 1994 roku udało się przybliżyć do realizacji zainicjowanych wcześniej ustaleń. Przedstawiciele Rosji, Stanów Zjednoczonych, Wielkiej Brytanii oraz Ukrainy, Kazachstanu i Białorusi podpisali porozumienie, określane jako memorandum budapesztańskie. Był to dokument, który w ujęciu prawa międzynarodowego stanowił niewiążące porozumienie, co – jak pokazały późniejsze wydarzenia – miało bardzo poważne konsekwencje dla pozycji poszczególnych sygnatariuszy, a najtragiczniejsze dla Ukrainy.

Głównym założeniem memorandum było przekazanie broni nuklearnej Rosji. Ukraina w zamian domagała się gwarancji niepodległości ze strony USA. Stany Zjednoczone rzeczywiście podpisały dokument dotyczący integralności i suwerenności Ukrainy, jednak w zupełnie innej randze niż oczekiwałby Kijów. W ramach negocjacji Ukrainie udało się jeszcze zapewnić dostarczenie paliw do elektrowni jądrowych (od Rosjan) oraz pokrycie kosztów procesu przekazania broni (przez Amerykanów i Rosjan). USA wspólnie z Wielką Brytanią dbały przede wszystkim o własny interes, jakim była denuklearyzacja Ukrainy, a nie obrona tego państwa. Należy ocenić, że największym beneficjentem podpisanego w Budapeszcie memorandum była jednak Rosja, która przejęła po dawnym państwie satelitarnym arsenał, z jednej strony wzmacniając własną zdolność bojową, z drugiej radykalnie osłabiając potencjalnego przeciwnika.

Wbrew pozorom współczesna ocena porozumienia podpisanego w Budapeszcie jest niejednoznaczna. Wydawać by się mogło, że Ukraina w zamian za niejasne i niewiążące gwarancje bezpieczeństwa, dobrowolnie oddała swoją najgroźniejszą broń. Trudności w ocenie odnoszą się przede wszystkim do kwestionowania zdolności bojowej użycia przez Ukrainę arsenału nuklearnego. Część badaczy jest zdania, że Ukraina nie była w stanie wykorzystać głowic do potencjalnego ataku, co stawiałoby podpisanie memorandum w całkiem innym kontekście. Co ważne, jak wskazuje Eugeniusz Mironowicz, już w swojej deklaracji o suwerenności z 1990 roku Ukraina proklamowała status państwa niepodległego, które nie dysponuje bronią atomową. Z pewnością duża była też siła nacisków zewnętrznych na podpisanie dokumentu, tym bardziej, że interes Rosji był zbieżny z oczekiwaniami państw Zachodnich. Ostatecznie Ukraina podpisała porozumienie 5 grudnia 1994 roku, rozpoczynając proces całkowitej denuklearyzacji kraju.

Polityczne echa tej decyzji i pytania o jej słuszność powracały przy okazji kolejnych napięć z Rosją m.in. jeszcze w latach 90. podczas podziału Floty Czarnomorskiej. Kwestię gwarancji bezpieczeństwa przywołano zaś po rosyjskiej agresji na wschodnią część Ukrainy w 2014 roku – za nieważne uznał je wówczas Władimir Putin. Także w 2022 roku po zaatakowaniu Ukrainy przez Rosję, wielu komentatorów przypomniało o gwarancjach, jakich Zachód i Rosja udzielali Kijowowi niespełna 30 lat wcześniej.

Ostatecznie memorandum budapesztańskie pozbawiło Ukrainę groźnej broni, nie dając jej wiele w zamian. Zamiast umowy międzynarodowej, jak wskazuje Agata Kleczkowska, podpisano porozumienie polityczne, którego treść i moc prawna w obliczu agresji rosyjskiej, nie zmusza Stanów Zjednoczonych ani Wielkiej Brytanii do obrony Ukrainy. Osobną kwestią jest moralny wymiar tego porozumienia, który w odniesieniu do Rosji nie pozostawia wątpliwości co do jej fałszywych intencji. W obliczu toczącej się wojny poddaje w wątpliwość także

długofalową wizję bezpieczeństwa regionu, na którą liczył Zachód.

Oto pełna treść memorandum Budapesztańskiego:

Witając przystąpienie Ukrainy do Układu o Nierozprzestrzenianiu Broni Jądrowej jako Państwa Nienuklearnego,
Mając na uwadze zaangażowanie Ukrainy w eliminacje broni jądrowej z jej terytorium w określonym terminie, Zauważając zmiany w sytuacji bezpieczeństwa światowego, obejmujące zakończenie zimnej wojny, które doprowadziły do powstania warunków do głębokiej redukcji sił nuklearnych,
Potwierdzają co następuje: 1. Federacja Rosyjska, Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej oraz Stany Zjednoczone Ameryki potwierdzają swoje zaangażowanie, zgodnie z zasadami Aktu Końcowego Konferencji Bezpieczeństwa i Współpracy w Europie, w poszanowanie niezależności i suwerenności istniejących granic Ukrainy;

2. Federacja Rosyjska, Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej oraz Stany Zjednoczone Ameryki potwierdzają swoje zobowiązanie do powstrzymania się od stosowania groźby lub użycia siły przeciw integralności terytorialnej bądź politycznej niezależności Ukrainy, i że żadna broń w ich posiadaniu nigdy nie zostanie użyta przeciw Ukrainie, chyba że w samoobronie lub w przypadkach zgodnych z Kartą Narodów Zjednoczonych;
3. Federacja Rosyjska, Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej oraz Stany Zjednoczone Ameryki potwierdzają swoje zaangażowanie, zgodnie z zasadami Aktu Końcowego Konferencji Bezpieczeństwa i Współpracy w Europie, w powstrzymanie się od przymusów ekonomicznych zmierzających do podporządkowania swoim własnym interesom realizacji przez Ukrainę praw nieodłącznie związanych z jej suwerennością aby w ten sposób osiągnąć korzyści jakiegokolwiek rodzaju;

4. Federacja Rosyjska, Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej oraz Stany Zjednoczone Ameryki potwierdzają swoje zaangażowanie w poszukiwanie natychmiastowych działań Rady Bezpieczeństwa Narodów Zjednoczonych celem dostarczenia pomocy Ukrainie, jako Państwu Nienuklearnemu stronie Układu o Nierozprzestrzenianiu Broni Jądrowej, gdyby Ukraina stała się ofiarą aktu agresji lub obiektem groźby agresji, w których stosowana jest broń jądrowa;
5. Federacja Rosyjska, Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej oraz Stany Zjednoczone Ameryki potwierdzają, w przypadku Ukrainy, swoje zaangażowanie do nie stosowania broni jądrowej przeciw jakiemukolwiek Państwu Nienuklearnemu stronie Układu o Nierozprzestrzenianiu Broni Jądrowej, chyba że w przypadku zaatakowania ich, ich terytoriów zależnych, ich sił zbrojnych lub ich sojuszników przez takie państwo w połączeniu lub w sprzymierzeniu z Państwem Nuklearnym;

   6 Ukraina, Federacja Rosyjska, Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej oraz Stany Zjednoczone Ameryki będą się konsultowały w przypadku powstania sytuacji, w której pojawiłyby się wątpliwości dotyczące powyższych zobowiązań.

   Memorandum wchodzi w życie po jego podpisaniu. Podpisano w czterech kopiach o równej ważności w językach ukraińskim, angielskim i rosyjskim.

   Za Ukrainę: (podpis) Łeonid D. KUCZMA

   Za Federację Rosyjską: (podpis) Boris N. JELCYN

   Za Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej: (podpis) John MAJOR

   Za Stany Zjednoczone Ameryki: (podpis) William J. CLINTON

Tłumaczenie oparte jest na The Council on Foreign Relations (CFR)

Bibliografia:

P. Andrusieczko, J. Prokopiuk, Flota Czarnomorska i Krym w kontekście bezpieczeństwa Ukrainy, „Przegląd Naukowo-Metodyczny. Edukacja dla bezpieczeństwa” nr. 3, 2010, s. 65-74.
A. Kleczkowska, Memorandum Budapesztańskie – umowa międzynarodowa czy niewiążące porozumienie?, „Władza Sądzenia” nr. 20, 2021 s. 144-165.
R. Kopeć, Strategie nuklearne w okresie pozimnowojennym, Kraków 2014.
E. Mironowicz, Polityka zagraniczna Ukrainy 1990-2010, Białystok, 2012.

Źródło: Histmag.org

Amerykańskie eksperymenty wojskowe ze sztuczną inteligencją, która może przewidzieć przyszłość

Departament Obrony testuje programy sztucznej inteligencji, które mogłyby, gdyby zostały w pełni rozwinięte, „zobaczyć przyszłość.”

United States Northern Command (USNORTHCOM) przeprowadziło ostatnio serię eksperymentów z Pentagonem i Północnoamerykańskim Dowództwem Obrony Kosmicznej (NORAD). Testy te były znane jako Global Information Dominance Experiments (GIDE).

GIDE połączyło globalne sieci czujników, systemy sztucznej inteligencji i programy do przetwarzania w chmurze. Celem eksperymentów było „osiągnięcie dominacji informacyjnej" i „wyższości decyzyjnej" na symulowanych polach walki.

Technologia sztucznej inteligencji analizuje ogromne ilości danych, aby tworzyć prognozy

Generał Glen D. VanHerck, dowódca USNORTHCOM i NORAD, powiedział niedawno dziennikarzom, że najnowszy test GIDE był w rzeczywistości trzecim takim eksperymentem. Zawierał przedstawicieli wszystkich 11 dowództw bojowych w Pentagonie.

Pentagon nie ujawnił wielu szczegółowych informacji dotyczących GIDE ze względu na obawy związane z bezpieczeństwem. Wiadomo jednak, że trzecia próba jest do tej pory najbardziej ekspansywną. Skoncentrowano się na rozwiązywaniu scenariuszy, w których „kwestionowana logistyka" może stanowić problem. Jedna z symulacji podczas testu dotyczyła tego, co by się stało, gdyby komunikacja w rejonie Kanału Panamskiego została zakłócona i przejęta przez wroga.

„To, co widzieliśmy, to zdolność zajść znacznie dalej – to, co nazywam byciem z dala – z dala od bycia reaktywnym do faktycznego bycia proaktywnym" – powiedział VanHerck podczas briefingu z dziennikarzami w Pentagonie. „I nie mówię o minutach i godzinach – mówię o dniach."

„Zdolność widzenia z kilkudniowym wyprzedzeniem tworzy przestrzeń decyzyjną. Dla mnie jako dowódcy operacyjnego

przestrzeń decyzyjna do potencjalnego ustawienia sił w celu stworzenia opcji odstraszania, aby zapewnić to [sekretarzowi obrony] lub nawet prezydentowi" – □□powiedział VanHerck. „Aby wykorzystać wiadomości, przestrzeń informacyjną do tworzenia opcji odstraszania i przesyłania wiadomości, a jeśli to konieczne, aby iść dalej i ustawiać się na porażkę".

VanHerck podkreślił, że system sztucznej inteligencji tak naprawdę nie wiąże się z wykorzystaniem żadnej nowej technologii. To, co rozwija wojsko, to po prostu nowe podejście do wykorzystywania istniejącej technologii do przetwarzania wielu informacji i przewidywania na podstawie tych informacji.

„Dane istnieją" – powiedział VanHerck. „To, co robimy, to udostępnianie tych danych i udostępnianie ich w chmurze, w której patrzą na nie uczące się maszyny i sztuczna inteligencja. I przetwarzają to naprawdę szybko i dostarczają decydentom, co nazywam wyższością decyzji".

Jeśli proces ten zostanie udoskonalony, VanHerck twierdzi, że może to spowodować, że kraj otrzyma wyprzedzające ostrzeżenia o dni, zanim pojawi się jakiekolwiek potencjalne zagrożenie.

Technologia predykcyjna może być wkrótce zastosowana

VanHerck powiedział, że platforma sztucznej inteligencji może wkrótce zostać wprowadzona do użytku w świecie rzeczywistym. Uważał, że wojsko jest gotowe do wykorzystania oprogramowania na obecnych polach bitew i może je zweryfikować podczas kolejnego testu GIDE wiosną 2022 roku.

VanHerck wyjaśnił, dlaczego ten rodzaj szybkiego systemu przetwarzania informacji jest bardzo potrzebny w dzisiejszym współczesnym krajobrazie wojennym.

„Dzisiaj znajdujemy się w środowisku reaktywnym, ponieważ

spóźniamy się z danymi i informacjami. A więc zbyt często reagujemy na ruch konkurenta” – wyjaśnił. „W tym przypadku pozwala nam to na tworzenie odstraszania, które zapewnia stabilność dzięki wcześniejszej świadomości tego, co [wróg] faktycznie robi”.

Ale pomimo swoich wyraźnych zalet, predykcyjny system sztucznej inteligencji wciąż ma swoje ograniczenia. Musi szukać danych, które są niezwykłe. Nie jest w stanie powiedzieć z całą pewnością, co się dzieje. Analitycy muszą być mocno zaangażowani, aby wszelkie przewidywania miały sens.

Mimo to VanHerck uważa, że □□system sztucznej inteligencji może nadal być opłacalny, zwłaszcza jeśli może przewidzieć i zapobiec atakowi.

Źródła

TheDrive.com

CNet.com

EnGadget.com

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

Bądź bezpieczny: nie odwiedzaj umierającego rodzica. Nie wychodź z domu. Nie wychodź za mąż. Nie …

Jak zauważyło wielu obserwatorów, zachowanie bezpieczeństwa stało się religią. „Bezpieczeństwo”, jak to się czasem nazywa, jak wszystkie religie, stawia to, co ceni – w tym przypadku bezpieczeństwo – ponad innymi wartościami. Safetyism wyjaśnia gotowość Amerykanów do wyrzeczenia się swoich najbardziej cenionych wartości – w tym wolności – w imię bezpieczeństwa przez ostatnie półtora roku.

Miliony Amerykanów nie tylko zrezygnowały z prawa do chodzenia do pracy, zarabiania na życie, chodzenia do kościoła lub synagogi oraz odwiedzania przyjaciół i krewnych, ale nawet zrezygnowały z prawa do odwiedzania umierających krewnych i przyjaciół. Można założyć, że prawie każda osoba zarejestrowana jako zmarła na COVID-19 zmarła bez ani jednej bliskiej osoby przy łóżku od momentu wejścia do szpitala aż do śmierci. Akceptację takiego okrucieństwa – można by dodać – irracjonalnego i nienaukowego okrucieństwa – można wytłumaczyć

jedynie niepowodzeniem pokoleń szkół i rodziców w nauczaniu wolności, przy jednoczesnym skutecznym nauczaniu kultu bezpieczeństwa. Jeśli twój ojciec musiał umrzeć sam, to było tego warte ze względu na bezpieczeństwo; jeśli twoja matka musiała przebywać w odosobnieniu w domu opieki dłużej niż rok, to również było tego warte ze względu na bezpieczeństwo. I oczywiście, jeśli przywódcy polityczni i liderzy w nauce i medycynie muszą kłamać ze względu na bezpieczeństwo, niech tak będzie; prawda też jest mniej ważna niż bezpieczeństwo.

Nic z tego nie jest nowe. Dwadzieścia pięć lat temu pisałem i relacjonowałem chęć Amerykanów do oglądania indywidualnych praw łamanych w wojnie przeciwko paleniu, a zwłaszcza akceptowania absurdalności rzekomo śmiertelnych niebezpieczeństw biernego palenia. Nikt nie zaprzecza, że intensywne narażenie na bierne palenie może zaostrzyć istniejące wcześniej choroby, takie jak astma. Ale twierdzenie antynikotynowych zapaleńców, że 50 000 Amerykanów umiera każdego roku z powodu biernego palenia, jest nonsensem. Na przykład w 2013 r. Journal of the National Cancer Institute poinformował, że nie ma statystycznie istotnego związku między rakiem płuc a narażeniem na bierne palenie.

Jednak, w imię tego bezsensownego twierdzenia o 50 000 rocznie, ludziom zabroniono nie tylko palić w samolotach – co było właściwe tylko ze względów grzecznościowych – ale nawet w 'smoke shopach'. W mieście Burbank w Kalifornii, rządzonym od dziesięcioleci przez lewicowców, którzy, jak wszyscy lewicowcy, gardzą wolnością osobistą, palenie jest zakazane nawet w sklepach z cygarami. Pomimo tego, że nikt nie jest zmuszany do pracy w żadnym sklepie z cygarami, a nawet jeśli sklep jest dobrze wentylowany, nie wolno w nim palić.

Należy zauważyć, że te irracjonalne zakazy dotyczące wolności osobistej nie przeszkadzały nikomu poza palaczami. Liczba niepalących obywateli Burbank, którzy sprzeciwili się tym przepisom, wynosiła prawdopodobnie zero. Gdyby Burbank ogłosił zakaz spożywania alkoholu, doszłoby do buntu – pomimo faktu,

że co najmniej połowie przypadków maltretowania małżonków i dzieci towarzyszy alkohol, a każdemu zgonowi, uszkodzeniu mózgu, paraliżowi i innym trwałym obrażenia spowodowane przez pijanego kierowcę są spowodowane przez alkohol. Czy ktoś został zabity przez palącego kierowcę? Czy ktoś został zamordowany lub jakiekolwiek dziecko lub współmałżonek był molestowany lub bity, ponieważ morderca lub oprawca palił?

Tak więc fanatycy bezpieczeństwa nauczyli się z krucjaty antynikotynowej i anty-biernemu paleniu wielkiej lekcji, że jeśli powiesz Amerykanom, że coś nie jest bezpieczne, możesz pozbawić ich praw, a oni chętnie się z tym pogodzą. I, dla przypomnienia, jest to równie prawdziwe w praktycznie każdym kraju na świecie. „Bezpieczeństwo Uber Alles".

Nauczyli się tej lekcji nie tylko od fanatyków antynikotynowych. Od dwóch pokoleń bezpieczeństwo coraz bardziej pozbawia Amerykanów radości i wolności. Zwłaszcza dzieci były tak rozpieszczane, że amerykańskie dzieci ostatnich dwóch pokoleń prawdopodobnie miały znacznie mniej radości i znacznie więcej strachu niż dzieci jakiegokolwiek poprzedniego pokolenia Amerykanów. Małe dzieci nie mogą samodzielnie chodzić na spacery, aby nie wezwać służby ochrony dzieci; trampoliny, które kiedyś znajdowały się na prawie każdym domowym basenie, są powszechnie zakazane; Z placów zabaw usunięto drabinki i huśtawki. Jak czytamy w artykule w australijskiej witrynie Babyology, zatytułowano: „Małpie bary są niebezpieczne i muszą być usuwane z placów zabaw, mówią eksperci".

Młodzi ludzie do 15 roku życia nie mogą latać bez nadzoru linii lotniczej przez osoby dorosłe. Dlaczego nie? Leciałem sam z Miami do Nowego Jorku, kiedy miałem 7 lat i nikt nie myślał, że moi rodzice zachowali się w jakikolwiek sposób nieodpowiedzialnie.

Dwoje norweskich naukowców, Ellen Sandseter (Queen Maud University College of Early Childhood Education) i Leif

Kennair (Norweski Uniwersytet Nauki i Technologii), napisało badanie na temat dzieci i ryzykownych zabaw, opublikowane w „Evolutionary Psychology", w którym doszli do wniosku: „Możemy zaobserwować zwiększony neurotyzm lub psychopatologie w społeczeństwie, jeśli dzieciom przeszkadza się w uczestniczeniu w ryzykownych zabawach odpowiednich do wieku".

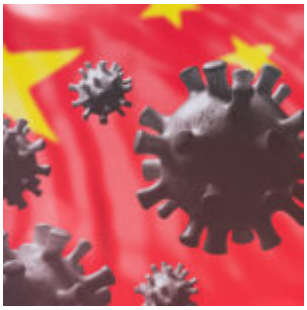
Chęć prowadzenia jak najbezpieczniejszego życia jest głównym czynnikiem wyjaśniającym, dlaczego coraz mniej młodych Amerykanów zawiera małżeństwa, a jeszcze mniej ma dzieci. Ani małżeństwo, ani posiadanie dzieci nie są bezpieczne. Oba są pełne ryzyka. Nagłówek artykułu z zeszłego tygodnia na stronie programu NBC „Today" głosi: „Dorośli bez dzieci są tak samo szczęśliwi jak rodzice, jak wynika z badań". Pomijając pytanie, czy można porównać szczęście dwóch grup ludzi o zupełnie różnych doświadczeniach (czy byłoby sensowne stwierdzenie, że większość psów jest szczęśliwsza od ludzi?) – czy nawet można oczekiwać szczerych odpowiedzi (ile ludzi twierdzi, że ich życiowe wybory uczyniły ich nieszczęśliwymi?) – artykuł dobrze ilustruje sens tej kolumny. „Bądź bezpieczny"

Możesz żyć bezpiecznie. Albo możesz żyć pełnią życia. Nie możesz żyć jednym i drugim.

Artykuł przetłumaczono z: townhall.com

Tuszowanie KORONY: Dziesiątki próbek testowych z najwcześniejszych

potwierdzonych przypadków koronawirusa usuniętych z bazy danych NIH



Stwierdzono, że dziesiątki próbek testowych od najwcześniejszych potwierdzonych pacjentów z koronawirusem (COVID-19) w Wuhan w Chinach zostały usunięte z bazy danych *Narodowego Instytutu Zdrowia* (NIH) wykorzystywanej do śledzenia rozwoju SARS-CoV-2.

Pliki mogły dostarczyć istotnych wskazówek na temat powstania wirusa i czasu jego rozprzestrzeniania się przed wybuchem w grudniu 2019 r.

Jesse Bloom, wirusolog z Fred Hutchinson Cancer Research Center w Seattle, zauważył usunięcie i udało mu się odzyskać część danych. Powiedział, że wierzy, że Chiny usunęły pliki, aby „zaciemnić ich istnienie".

Czterdzieści pięć pozytywnych próbek zostało pierwotnie przesłanych do archiwum odczytu sekwencji NIH przez *Uniwersytet Wuhan* w marcu 2020 r.

Próbki zostały opublikowane w ramach badania dotyczącego diagnozowania pacjentów z COVID za pomocą testów PCR – zaledwie kilka dni przed wydaniem przez rząd chiński nakazu zatwierdzenia publikacji wszystkich danych dotyczących koronawirusa.

Bloom zauważył, że wszystkie 45 próbek zostało od tego czasu

pobrane z bazy danych, bez „żadnego wiarygodnego naukowego powodu”. Szczegóły zatuszowania opisał w artykule naukowym zatytułowanym „Odzyskiwanie usuniętych danych z głębokiego sekwencjonowania rzuca więcej światła na wczesną epidemię SARS-CoV-2 w Wuhan”.

NIH potwierdził, że sekwencje zostały usunięte w czerwcu 2020 r. na prośbę badacza, który pierwotnie przedstawił je w marcu 2020 r., i powiedział, że zezwalanie na to jest standardową praktyką.

Wiadomość o chińskiej próbie zatuszowania śladów wirusa pojawiła się pośród narastającego podejrzenia, że □□SARS-CoV-2 mógł przypadkowo wycieknąć z laboratorium bezpieczeństwa biologicznego wysokiego poziomu w Wuhan – uznanym punkcie zerowym pandemii.

Odzyskane próbki wykazują różnice genetyczne w stosunku do wirusa, który rozprzestrzenił się na całym świecie

Bloom był w stanie częściowo odzyskać 13 usuniętych próbek za pomocą Google Cloud i przystąpił do sekwencjonowania wirusów. Zauważył kilka różnic genetycznych między szczepami w usuniętych próbkach a wirusem, który ostatecznie rozprzestrzenił się na całym świecie.

Wirusolog powiedział, że większość odzyskanych danych sugeruje, że wirus krążył na długo przed oficjalnym harmonogramem Chin.

Odkrył, że wczesne próbki wirusa były bardziej rozwinięte, niż można by się spodziewać po patogenie, który niedawno przeskoczył ze zwierząt na ludzi – ale nie powiedział, że nadało to większej wagi teorii wycieku z laboratorium.

„To badanie nie dostarcza żadnych dodatkowych mocnych dowodów na korzyść naturalnej choroby odzwierzęcej lub wypadku laboratoryjnego” – powiedział Bloom w e-mailu do *CNN*.

„Pokazuje raczej, że istnieją dodatkowe sekwencje ze stosunkowo wczesnego wybuchu epidemii, które są wciąż nieznane, a w niektórych przypadkach mają mutacje, które sugerują, że prawdopodobnie są ewolucyjnie starsze niż wirusy z 'mokrego targu' w Huanan".

Bloom odkrył, że te wirusy mają trzy dodatkowe mutacje, których brakuje w próbkach SARS-CoV-2 pobranych kilka tygodni później. Te późniejsze wirusy bardziej przypominają koronawirusy znalezione u nietoperzy. „Są o trzy kroki bardziej podobne do koronawirusów nietoperzy niż wirusy z Huanan" – powiedział Bloom.

Ustalenia Blooma sugerują, że COVID rozprzestrzeniał się przed grudniem 2019 r.

W wątku na Twitterze opisującym swoje odkrycia Bloom napisał: „Chociaż wydarzenia, które doprowadziły do □□pojawienia się #SARSCoV2 w Wuhan, są niejasne (zoonoza a wypadek w laboratorium), wszyscy zgadzają się, że głębokimi przodkami są koronawirusy nietoperzy.

„Dlatego spodziewaliśmy się, że pierwsze sekwencje #SARSCoV2 będą bardziej podobne do koronawirusów nietoperzy, a ponieważ #SARSCoV2 będzie dalej ewoluował, stanie się bardziej odmienny od tych przodków. Ale tak nie jest!

„Zamiast tego wczesne wirusy Huanan Seafood Market #SARSCoV2 różnią się bardziej od koronawirusów nietoperzy niż wirusy #SARSCoV2 zebrane później w Chinach, a nawet w innych krajach".

Brytyjscy eksperci komentujący badanie powiedzieli, że potwierdziły od dawna podejrzenia, że □□COVID rozprzestrzeniał się przed grudniem 2019 r. Ostrzegali również, że podkreślono wady w dochodzeniu *Światowej Organizacji Zdrowia* w sprawie pochodzenia COVID, które jest uważnie nadzorowane przez Chiny.

„Badanie dodatkowo potwierdza fakt, że wirus krążył w Wuhan

przed grudniową epidemią” – powiedział *MailOnline* Lawrence Young, biolog molekularny z *University of Warwick*.

„To tylko pokazuje, jak ważne jest zrozumienie wczesnego rozprzestrzeniania się wirusa, a każde przyszłe dochodzenie naprawdę musi poważnie przyjrzeć się całej sprawie. Szczególnie niepokojące jest to, że kluczowe dane zostały przesłane, a następnie usunięte. To dziwne zachowanie.

Źródła:

DailyMail.co.uk

9News.com.pl

NYTimes.com

Artykuł przetłumaczono z: naturalnews.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".

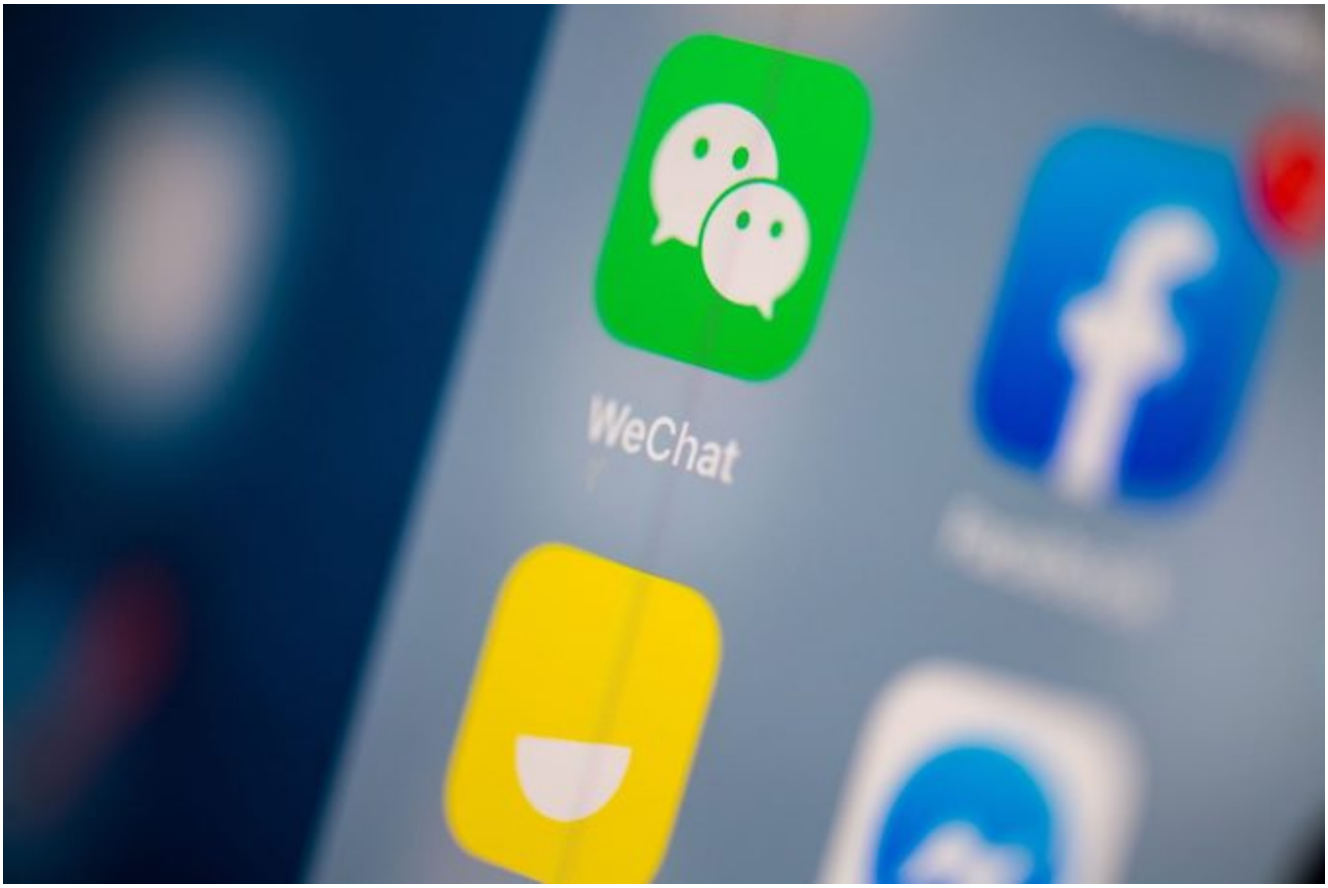
Przestępstwo posługiwania się skradzionym wizerunkiem dziecka w celu realizowania swoich fantazji nazywane jest cyfrowym kidnapingiem (ang. baby role play).

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.

Upewnij się, że dobrze to rozumiesz. TO nie jest szczepionka tylko fabryka syntetycznych patogenów!

Dr. Mikovits: **„Dosłownie – wstrzykuje się chorobę.”**

Nasi rządzący, którzy aktywnie uczestniczą w tym wykroczeniu, muszą mieć świadomość, że takie uczestnictwo będzie miało konsekwencje. Ten rodzaj współudziału nie różni się od tego, o który oskarżano i sądzono niemieckich lekarzy i naukowców w Norymberdze.

Dr David Martin dał światu dymiącą broń.

Dr David Martin dał nam również wgląd, aby pomóc „nam, ludziom” w przejęciu narracji.

„Rocco, upewnijmy się, że jedna rzecz jest jasna. Musimy zastrzec, że **to nie jest szczepionka**. Potrzeba to wyjaśnić. Używamy określenia „szczepionka,” żeby wpasować to pod kryteria wykluczeń w zakresie zdrowia publicznego. **To jest mRNA zapakowane w otoczkę tłuszczową, które jest dostarczane do komórki.** Jest to **urządzenie medyczne, mające na celu pobudzenie ludzkich komórek do tego, żeby stały się wytwórcą patogenów.**

To nie jest szczepionka, szczepionka jest terminem, określonym w prawie dotyczącym zdrowia publicznego, jest terminem, określonym w standardach CDC i FDA. Szczepionka musi pobudzić zarówno odporność u osoby, która ją przyjmuje, ,jak i zakłócić rozprzestrzenianie się wirusa. To ten produkt nie jest. Bardzo jasno i wielokrotnie mówiono, że nić mRNA nie zatrzyma rozprzestrzeniania się. Jest to terapia. Jeśli jednak mówilibyśmy o niej jak o środku leczniczym, nie spotkałoby się to z przychylnością władz z obszaru zdrowia publicznego, ponieważ ludzie pytaliby wówczas, jakie są inne sposoby leczenia. Stosowanie określenia „szczepionka” jest nie do zrozumienia zarówno pod względem prawa, jak i dlatego, że ono mogłoby rozpocząć debatę publiczną. Kiedy mówi się „szczepionka” wpada się w kategorie, że ktoś jest albo zwolennikiem, albo przeciwnikiem szczepień.

Pamiętajcie, a ludzie o tym zapominają, Moderna została założona jako firma produkująca chemioterapię na raka, a nie firma produkująca szczepionki na SARS. Jeśli powiedzielibyśmy ludziom, że damy im profilaktycznie chemioterapię na raka, którego nie mają, śmiech słyszałbyś długo jeszcze po wyjściu z sali. Bo jest to głupi pomysł. Tu jest dokładnie tak samo. Jest to mechaniczne urządzenie w postaci bardzo małego pakietu technologii, wprowadzane jest do ludzkiego organizmu, żeby

uruchomić komórki tak, aby stały się fabryką produkującą patogeny. I odmawiam uznawania w jakiejkolwiek rozmowie, że jest to kwestia szczepień. To określenie jest używane tylko jako nadużycie wyroku sądu w sprawie Jacobsona z 1905 r., który jest błędnie przedstawiany od czasu, kiedy został napisany.

Jeśli bylibyśmy w tej kwestii uczciwi, nazwalibyśmy rzeczy po imieniu. Jest to urządzenia chemiczne patogenne, służące do uruchomienia aktywności komórki polegającej na produkowaniu związków chemicznych. Jest to urządzenie medyczne, nie lek, ponieważ spełnia kryteria określenia „Urządzenie: zgodnie z CDRH". Nie jest to żywy układ, nie jest to biologiczny organizm. Pod względem fizycznym jest to technologia, tyle że jest rozmiaru pakietu cząsteczek. Dlatego musimy mówić bardzo jasno, żeby nie wpaść w pułapkę grania w ich grę. A ich grą polega na tym, że kiedy nazywamy to szczepionką, rozmowa staje się rozmową o szczepieniach. Tylko dlatego, że oni to tak nazwali, to nie stało się szczepionką. Musi być to jasne dla wszystkich słuchaczy, że my nie będziemy powtarzać fałszywych określeń, tak samo, jak nie przystaniemy na ich chemiczno-przemysłową definicję zdrowia. Bo one oba są oszukańcze i są jaskrawym pogwałceniem przepisów dotyczących produktu, jaki jest wykorzystywany.

R: Judy, czy Ty jako naukowiec, mogłabyś powiedzieć nam to bardziej po angielsku, jak prostemu człowiekowi. Ja to wyjaśnienie, przyjmuję, jest świetne, ale tym, którzy mogą nie być w stanie nadążyć za tą inteligentną analizą – i nie mówię tego obraźliwie, Dave- drażni mnie, kiedy słyszę, jak prawnicy, aktywiści itp mówią: „będziemy walczyć przeciwko szczepionce". Jeśli przyznasz, że jest to szczepionka, od razu przegrałeś bitwę. To nie jest szczepionką.

R: Jak więc powinienem to nazywać? Substancja chemiczna

JM: Tak, jest to **syntetyczny patogen.** Dosłownie **wstrzykują bardzo chorobotwórczą część wirusa do każdej komórki ciała**.

RG: Syntetyczny patogen – robi mi się od tego nie dobrze.

JM: Tak.

DM: Od tego ma być ci nie dobrze.

Roco, pamiętaj 80% osób rzekomo narażonych na rzekomego wirusa SARS-COV-2 w ogóle nie ma objawów. Nazywają ich nosicielami bezobjawowymi. 80% osób, którym się to wstrzykuje ma kliniczne skutki uboczne.

Wstrzykuje się im substancję chemiczną, po to żeby wywołać chorobę, a nie żeby wywołać odpowiedź odpornościową i nieprzenoszenie wirusa. Mówiąc inaczej, nic z tego nie powstrzyma rozprzestrzeniania się czegokolwiek.

Tu chodzi o to, żebyś się pochorował i o to, żeby to Twoje komórki spowodowały chorobę.

RG: Więc to wywoła reakcję autoimmunologiczną?

JM: **Między innymi. Może bezpośrednio wywołać stwardnienie rozsiane, stwardnienie zanikowe boczne, chorobę Alzheimera, to taka jest ekspresja tego patogenu w otoczce, może spowodować przyspieszoną chorobę nowotworową, taka może być ekspresja tego wirusa, tej syncytyny, to wiadomo od dziesięcioleci.**

Dosłownie – wstrzykuje się chorobę.

„Kiedy przemysł jest odpowiedzialny za rozpowszechnianie informacji, tracimy. Bo jedyną narracją jest ta, która zostanie zrekompensowana przez osoby podpisujące czek. Dotyczy to naszych polityków… i naszych mediów – otrzymali zapłatę – jeśli podążasz za pieniędzmi, zdajesz sobie sprawę, że w żadnej sieci nie ma głosu niekonfrontacyjnego ”.

– Dr David Martin , 5 stycznia 2021 r.,

Źródło:

cioz-dobrostan.pl

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.

Google śledzi użytkowników Chrome nawet w trybie „incognito”

Jeśli używasz przeglądarki Google Chrome do surfowania po sieci i robisz to „incognito”, co ma oznaczać przeglądanie prywatne, powinieneś wiedzieć, że gigant z Doliny Krzemowej nadal potajemnie śledzi twoją aktywność w sieci.

Firma Alphabet Inc. twierdzi, że aktywacja trybu „stealth” w Chrome oznacza po prostu, że firma nie „zapamięta Twojej aktywności”. Nie oznacza to, że Google nie jest w stanie zobaczyć, które strony odwiedzasz i jak często je odwiedzasz, co dla niektórych może być zaskoczeniem.

Sędzia okręgowy USA Lucy Koh, znana z tego, że wzięła się za Big Tech, które jest winne zbrodni przeciwko ludzkości, odpowiedziała na pozew zbiorowy przeciwko Google, mówiąc, że jest „zaniepokojona” praktykami gromadzenia danych przez międzynarodową korporację, które w najlepszym przypadku są zwodnicze.

Pozew domaga się 5000 dolarów odszkodowania za każdego z milionów użytkowników Chrome, których prywatność została naruszona od czerwca 2016 roku. Koh mówi, że uważa za „niezwykłe” to, że Google dokłada „dodatkowego wysiłku” w celu

zebrania takich danych, jeśli rzekomo tego nie robi aby profilować użytkowników i kierować do nich reklamy.

Firma Google jest i była uwikłana w liczne procesy sądowe dotyczące jej praktyk monopolistycznych, w tym naruszania prywatności w reklamach cyfrowych i wyszukiwaniu online. W jednym z nich Koh skutecznie zmusiła Google do ujawnienia skanowania prywatnych wiadomości e-mail w celu tworzenia profili i kierowania reklam.

W tym przypadku Google jest oskarżany o osadzanie kodu w witrynach internetowych, które wykorzystują jej usługi analityczne i reklamowe do pobierania danych z rzekomo prywatnej historii przeglądania użytkowników i przekazywania ich na serwery Google w celu przetworzenia.

Google sprawia wrażenie, jakby tryb przeglądania prywatnego zapewniał użytkownikom większą kontrolę nad ich danymi, mówi prawniczka Amanda Bonn, ale w rzeczywistości „Google twierdzi, że w zasadzie niewiele można zrobić, aby uniemożliwić nam gromadzenie Twoich danych, i właśnie to powinieneś założyć”

Google to zło; przestań używać ich produkty

Andrew Shapiro, prawnik Google, twierdzi, że polityka prywatności jego klienta „wyraźnie ujawnia” fakt, że podczas korzystania z produktu Google prawie nic nie jest prywatne.

„Gromadzenie danych, o którym mowa, zostało ujawnione” – mówi.

Stephen Broome, inny prawnik Google, mówi, że strony internetowe, które zawierają umowę z Google na korzystanie z jej narzędzi analitycznych lub innych usług, doskonale znają praktyki gromadzenia danych jego klientów i nie jest to tajemnicą.

Broome próbował bagatelizować obawy powodów, a także sądu dotyczące prywatności, wskazując, że własna strona internetowa federalnego sądu korzysta z usług Google. Ta taktyka

przyniosła jednak odwrotny skutek, gdy sędzia zażądał wyjaśnienia „co dokładnie robi Google”, wyrażając jednocześnie obawy, że osoby odwiedzające witrynę sądu nieświadomie ujawniają Google prywatne informacje.

„Chcę oświadczenia od Google na temat tego, jakie informacje gromadzą o użytkownikach witryny sądu i do czego są one wykorzystywane” – powiedziała Koh prawnikom Google.

Wniosek z tego wszystkiego jest taki, że Google nie można i nie powinno się ufać. Wszystko, co robi, ma na celu zarabianie pieniędzy, przejęcie władzy, eliminację praw ludzi i ostatecznie osiągnięcie dominacji nad światem.

„Ponadto Google i Alphabet ukradły kod Oracle, więc cała ich działalność opiera się na tej kradzieży” – zauważył jeden z naszych komentatorów o kolejnej króliczej dziurze Google.

„Sprawa jest w tej chwili w Sądzie Najwyższym i wkrótce zostanie rozpatrzona. Naprawdę łatwo to udowodnić, Google jest skończone. Nawet przestępcy w Sądzie Najwyższym nie mogą pozwolić sobie na to. To zbyt oczywiste”.

Inny komentator zgodził się z tym, dodając, że „dni Google są policzone”, ponieważ „nigdy nie nauczą się, że wahadło może wychylać się tylko daleko w jednym kierunku, i musi wrócić”.

Źródła tego artykułu obejmują:

BNNBloomberg.ca

NaturalNews.com