
LEX ARTIST

RODO - aktualności

[04.03.2024]

UWAGA!

Tezy przedstawione w artykułach, zamieszczone w niniejszym materiale i niebędące wytycznymi organu nadzorczego albo orzeczeniami sądów lub organów administracji publicznej, stanowią wyłącznie opinię ich autorów i nie są oficjalnym stanowiskiem Lex Artist Sp. z o.o.

01 Już ponad 2 mln osób zastrzegło numer PESEL

02 Większa obecność UODO w mediach społecznościowych

03 NSA: Gmina jest administratorem, nawet jeśli to nie ona zamawiała BIP

04 Wyciek danych i ataki na dostawców Glovo, Uber i innych platform

05 Nowy sposób ataku na zabezpieczenia biometryczne - odciski palców można odtworzyć na podstawie dźwięków

06 USA wytaczają ciężkie działo w ochronie danych osobowych

01 Już ponad 2 mln osób zastrzegło numer PESEL

- Rośnie liczba osób, które decydują się na zastrzeżenie swojego numeru PESEL. Możliwość taką wprowadzono 17 listopada 2023 roku na podstawie przepisów ustawy z dnia 7 lipca 2023 r. o zmianie niektórych ustaw w celu ograniczania niektórych skutków kradzieży tożsamości.
- Jeśli obywatel zastrzeże swój numer PESEL, znajdzie się on w specjalnym rejestrze.
- Od 1 czerwca rejestr ten – przed podpisaniem umowy z klientem – będzie musiał być sprawdzany przez każdą instytucję objętą ustawą z dnia 7 lipca 2023 r. czyli np. banki, instytucje kredytowe, ale też operatorów telekomunikacyjnych i notariuszy.
- Jeśli instytucje nie dopełnią tego obowiązku lub – pomimo aktywnego zastrzeżenia – udzielą np. pożyczki na skradzione dane, poszkodowana osoba nie będzie musiała spłacać zadłużenia powstałego wskutek oszustwa. To działanie prewencyjne, ma uniemożliwić zawarcie umowy, jeżeli PESEL jest zastrzeżony. Jeśli natomiast do zawarcia takiej umowy dojdzie (mimo aktywnego zastrzeżenia), ochroni osobę poszkodowaną przed koniecznością spłaty zadłużenia zaciągniętego przez złodziei.
- Zastrzeżenie PESEL uniemożliwi także np. wyrobienie duplikatu karty SIM, zawarcie umowy u notariusza przy sporządzaniu dokumentów dotyczących sprzedaży nieruchomości czy podpisanie umowy leasingowej.

Źródło: Ile osób zastrzegło numer PESEL? (prawo.pl)

02 Większa obecność UODO w mediach społecznościowych

- Bieżące informacje, edukacja w zakresie ochrony danych osobowych, poszerzanie świadomości na temat działań i roli Prezesa UODO – to główne cele coraz większej aktywności UODO w mediach społecznościowych.
- Od 1 marca UODO jest dostępny także na platformie LinkedIn oraz Mastodon. Celem większej aktywności w mediach społecznościowych jest dotarcie do większej i bardziej zróżnicowanej liczby odbiorców.
- Obok strony internetowej Urzędu Ochrony Danych Osobowych, która stanowi główne źródło informacji o działalności organu nadzorczego, rozwijane są profile w mediach społecznościowych. Od jakiegoś czasu UODO ma swój profil na platformie X (dawniej Twitter), z którego odbiorcy mogą dowiedzieć się o bieżącej aktywności Prezesa UODO, najważniejszych wydarzeniach bądź ich zapowiedziach.
- Niedawno został reaktywowany kanał UODO na YouTube, który stanowi dodatkowe źródło wiedzy. Został on uzupełniony o minione wydarzenia, by odbiorcy tego medium mogli zapoznać się z konferencjami czy webinarami organizowanymi przez UODO. Będzie on na bieżąco uzupełniany o kolejne materiały filmowe. Kanał UODO można obejrzeć pod linkiem: Urząd Ochrony Danych Osobowych - YouTube

Źródło: Aktualności - UODO

03 NSA: Gmina jest administratorem, nawet jeśli to nie ona zamawiała BIP

- Sąd orzekł, że dostęp do informacji publicznej podlega przepisom RODO. I podtrzymał 40 tys. zł kary dla burmistrza Aleksandrowa Kujawskiego.
- UODO ukarał Aleksandrów Kujawski za kilka naruszeń przepisów RODO. Przede wszystkim chodziło o to, że udostępnianie danych osobowych Biuletynu Informacji Publicznej Urzędu Miejskiego w Aleksandrowie Kujawskim firmom prowadzącym stronę internetową BIP odbywało się bez uprzedniego zawarcia z tymi podmiotami umowy powierzenia danych osobowych, o której mowa w art. 28 ust. 3 RODO. W takiej umowie powinny zostać określone m.in.: czas trwania przetwarzania, charakter i cel, rodzaj danych osobowych czy prawa i obowiązki administratora.
- Podczas kontroli w Aleksandrowie organ ochrony danych dopatrzył się też m.in. braku procedur wewnętrznych, które zapewniłyby przetwarzanie danych zgodnie z zasadą ograniczonego przechowywania. W rezultacie dane osobowe były dostępne na stronie BIP zbyt długo. Chodziło m.in. o kwestię publikacji w BIP oświadczeń majątkowych radnych. Zgodnie z art. 24h ust. 6 ustawy o samorządzie gminnym przechowuje się je przez sześć lat – podczas gdy najstarsze dostępne w kontrolowanym BIP pochodziły z 2010 r.
- Miasto argumentowało, że ustawowy okres dotyczy przechowywania, a nie publikacji, i że oświadczenia muszą być dostępne w czasie pięcioletniej kadencji radnych. Dopiero po jej zakończeniu zaczyna biec sześcioletni termin przechowywania. Realizowane przez województwo kujawsko-pomorskie zamówienie publiczne na internetowy system BIP obejmowało wszystkie gminy. Burmistrz Aleksandrowa nie uważał się więc za podmiot odpowiedzialny za zawarcie z wykonawcami serwisu umowy powierzenia danych osobowych.
- Zdaniem UODO i WSA wyłączenie (spod przepisów RODO) ma charakter wyjątkowy i w niniejszej sprawie nie znajduje zastosowania. NSA nie ma też wątpliwości, że burmistrz jest administratorem danych osobowych i uznał za wystarczające uzasadnienie sądu I instancji dla podtrzymania wymierzonej przez UODO kary pieniężnej.

Źródło: Gmina jest administratorem, nawet jeśli to nie ona zamawiała BIP - GazetaPrawna.pl

04 Wyciek danych i ataki na dostawców Glovo, Uber i innych platform

- Ktoś uzyskał nieuprawniony dostęp do danych dostawców Bolta, Glovo, Ubera, Wolta, którzy korzystali z aplikacji AppJobs.Work, dzięki której mogli świadczyć swoje usługi dostaw. Tysiące osób może paść ofiarą przestępstwa, a winny całej sytuacji jest prawdopodobnie były pracownik AppJobs.
- AppJobs, to aplikacja dla dostawców, którzy współpracują firmami, jak Wolt, Uber, Glovo czy Bolt (i nie tylko z tymi). Chodzi o to, aby kierowca czy kurier mógł podpisać umowę w jednym miejscu dla wszystkich usług tego typu. Aplikacja zbiera dane o kierowcy lub kurierze i te właśnie dane wyciekły.
- Kurierzy korzystający z AppJobs zaczęli otrzymywać od twórców aplikacji wiadomość o skierowanym na kurierów ataku phishingowym. Był to atak ukierunkowany, a link w wiadomości kierował do strony wyłudzającej pieniądze.
- Podczas ataku nie ujawniono żadnych haseł ani danych logowania, natomiast przestępcy mogli pozyskać informacje, do których hasła broniły dostępu, m.in.: nazwiska i imiona, dane wynikające z umowy z Appjobs, dane o obywatelstwie, adresy zamieszkania, dane dotyczące pojazdów, numery PESEL, numery dokumentu tożsamości, numery rachunku bankowego i dane o wynagrodzeniach,
- AppJobs ostrzegł, że kurierzy powinni uważać na dalszy phishing, zastrzec dokumenty i PESEL i muszą liczyć z wyłudzeniami kredytów.
- Wszystko wskazuje na to, że naruszenie zostało dokonane przez osobę, która miała wcześniej autoryzowany dostęp do naszych systemów. Jego działania były możliwe dzięki stopniowemu i systematycznemu uzyskiwaniu dostępu do różnych elementów infrastruktury IT. Atak phishingowy i potencjalne wykorzystanie danych użytkowników do oszustw finansowych nastąpiły już po wycieku danych spowodowanego działaniami wewnętrznymi.

Źródło: » Wyciek danych i ataki na dostawców Glovo, Uber i innych platform -- Niebezpiecznik.pl --

05 Nowy sposób ataku na zabezpieczenia biometryczne - odciski palców można odtworzyć na podstawie dźwięków

- Interesujący nowy sposób ataku na zabezpieczenia biometryczne został opisany przez grupę badaczy z Chin i USA. Jest nim PrintListener: odkrywanie luki w zabezpieczeniach uwierzytelniania odcisków palców za pomocą dźwięku tarcia palca. Atak wykorzystuje charakterystykę dźwięku przesuwania palcem użytkownika po ekranie dotykowym w celu wyodrębnienia cech wzoru odcisku palca.
- Po przeprowadzeniu testów naukowcy twierdzą, że mogą skutecznie zaatakować "do 27,9% częściowych odcisków palców i 9,3% kompletnych odcisków palców w ciągu pięciu prób przy najwyższym poziomie bezpieczeństwa FAR [False Acceptance Rate] wynoszącym 0,01%". Jest to pierwsza praca naukowa, która opisuje wykorzystywanie dźwięków przesuwania palców po ekranie do wnioskowania o informacjach o odciskach palców.
- Jak atakujący może mieć nadzieję na uzyskanie jakichkolwiek danych o odciskach palców, jeśli nie ma odcisków ani zdjęć szczegółów palców?
- Źródłem dźwięków przesuwania palcem mogą być popularne aplikacje, takie jak Discord, Skype, WeChat, FaceTime itp. Dowolna aplikacja do czatowania, w której użytkownicy bezmyślnie wykonują czynności przesuwania palca po ekranie, gdy mikrofon urządzenia jest włączony. Stąd nazwa ataku - kanałem bocznym (side-channel).

Źródło: Your fingerprints can be recreated from the sounds made when you swipe on a touchscreen — Chinese and US researchers show new side channel can reproduce fingerprints to enable attacks | Tom's Hardware (tomshardware.com)

06 USA wytaczają ciężkie działo w ochronie danych osobowych

- Prezydent USA Joe Biden podpisał rozporządzenie wykonawcze, które ma ochronić Amerykanów przed sprzedażą ich wrażliwych danych osobowych do krajów wrogich USA. Obecnie taka praktyka jest legalna, dzięki czemu informacje te mogą być pozyskiwane przez obce służby wywiadowcze.
- Według Białego Domu rozporządzenie jest najbardziej znaczącym w historii działaniem władz USA, by ograniczyć zagrożenie związane z używaniem danych osobowych Amerykanów przez wrogie państwa.
- Rozporządzenie nakazuje resortowi sprawiedliwości i innym ministerstwom przygotować regulacje mające ustanowić "jasną ochronę" danych osobowych - w tym danych genetycznych, biometrycznych, zdrowotnych, finansowych i geolokacyjnych - przed trafieniem w ręce "krajów budzących obawy". Jak powiedziała rzeczniczka Białego Domu Karine Jean-Pierre, obecne prawo pozwala podmiotom z krajów takie jak Chiny do kupowania wrażliwych informacji od firm handlujących danymi, co budzi obawy o bezpieczeństwo narodowe.
- "Komercyjni brokerzy danych i inne firmy mogą sprzedawać te dane do krajów budzących obawy lub podmioty kontrolowane przez te kraje, przez co mogą trafić w ręce obcych służb wywiadowczych, wojsk i firm kontrolowanych przez obce rządy" - stwierdziła rzeczniczka. Zaznaczyła jednak, że do pełnego zatkania luki w prawie potrzebna jest ustawa Kongresu. Przyznała też, że jest to reakcja na obawy związane z działalnością m.in. chińskich firm na amerykańskim rynku, takich jak platforma TikTok, czy zyskujący popularność portal e-commerce Temu.

Źródło: Biden podpisał rozporządzenie. Chodzi o ochronę przed krajami wrogimi USA (msn.com)