
LEX ARTIST

RODO - aktualności

[11.06.2024]

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 Olbrzymi wyciek z Ticketmaster i Santander

02 50 000 zł kary dla Wójta Gminy za rażące niedbalstwo

03 PUODO: Niezależność IOD musi być standardem

04 Upomnienie dla PZU za przetwarzanie niewłaściwych danych klienta

05 Optymizm polskich firm wobec poziomu ochrony przed cyberatakami jest wyjątkowo wysoki

01 Olbrzymi wyciek z Ticketmaster i Santander

- Santander i Ticketmaster (LiveNation) to firmy, które zostały zhackowane i wykradziono im dane kilkudziesięciu milionów (!) klientów lub pracowników. Wyciekły informacje o rachunkach, numery kart płatniczych i oczywiście dane osobowe.
- Włamywacze, kryjący się pod nazwą ShinyHunters (UNC5537), twierdzą, że zhackowali pracownika firmy Snowflake i dzięki temu byli w stanie wygenerować tokeny, które pozwoliły im ominąć uwierzytelnienie przez Oktę i dały im dostęp do baz klientów chmury Snowflake, w tym Santandera i Ticketmastera (ale ofiar jest więcej). Snowflake zaprzecza i podaje IoC, po których klienci mogą sprawdzić, czy byli celem ataków tej grupy.
- Z analizy dumpu udostępnionego przez włamywacza wynika, że pozyskano 1,3 TB danych z informacjami na temat 560 milionów klientów. Oto rodzaje pozyskanych danych: Imię i nazwisko, adres e-mail, adres zamieszkania, numer telefonu, hash numeru karty płatniczej oraz 4 ostatnie cyfry, historia transakcji;
- Santander miał ten sam problem. Bank wydał oficjalne oświadczenie w sprawie ataku. W Polsce o tym wycieku niewiele mówiono bo dotyczył on klientów z Chile, Hiszpanii i Urugwaju oraz niektórych byłych pracowników banku. Wykradzione dane mają obejmować rekordy o 30 milionach klientów, 6 milinach kont i 28 milionach kart kredytowych.
- Ani Ticketmaster, ani Santader w swoich oświadczeniach nie wskazały na to, że źródłem wykradzionych danych jest Snowflake. Skąd to wiadomo? Bo taką informację, powołując się na rozmowę z włamywaczem, opublikowała firma Hudson Rock.
- W oświadczeniu, które jest wspólnym oświadczeniem zarówno Snowflake jak i CrowdStrike oraz Mandiant, przeczytać można, że: miała miejsce “kampania” zorientowana na użytkowników niekorzystających z 2FA oraz faktycznie, znaleziono dowody na to, że sprawca zdobył dane uwierzytelniające i uzyskał dostęp do kont demo należących do byłego pracownika Snowflake.

Źródło: » Olbrzymi wyciek z Ticketmaster i Santander, czyli zhackowana chmura od Snowflake -- Niebezpiecznik.pl --

02 50 000 zł kary dla Wójta Gminy za rażące niedbalstwo

- Pewien pracownik Urzędu Gminy otworzył zainfekowany link, co skutkowało uruchomieniem oprogramowania złośliwego ransomware X., który zaszyfrował serwer. W toku dalszych czynności wyjaśniających Administrator otrzymał potwierdzenie wycieku czterech baz danych, w których znajdują się dane osobowe pracowników oraz byłych pracowników Urzędu Gminy.
- Prezes Urzędu Ochrony Danych Osobowych stwierdził: naruszenie przez Wójta Gminy Nowiny przepisów art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 RODO polegające na niezastosowaniu przez Wójta Gminy Nowiny odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych, w szczególności w zakresie wdrożenia zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania oraz zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, co skutkuje naruszeniem zasady integralności i poufności oraz zasady rozliczalności,
- PUODO nałożył także administracyjną karę pieniężną w kwocie 50 000 złotych.
- Zdaniem Prezesa UODO wójt powinien i jest w stanie ponieść konsekwencje swoich zaniedbań w sferze ochrony danych, stąd nałożenie kary w wysokości 50 000 złotych (pięćdziesięciu tysięcy złotych) jest w pełni uzasadnione,
- W swojej decyzji Prezes UODO stanowczo wskazał, że istotny wpływ na wystąpienie przedmiotowego naruszenia miało rażące niedbalstwo organu samorządu terytorialnego.

Źródło: https://www.linkedin.com/posts/piotr-liwszic_orzecznictwo-rodo-w-jednym-miejscu-activity-7206154486321524736-LzvW?utm_source=share&utm_medium=member_desktop

03 PUODO: Niezależność IOD musi być standardem

- Kwestia niezależności inspektorów ochrony danych (IOD) w świetle krajowego raportu z przeprowadzonego w 2023 r. skoordynowanego działania EROD CEF DPO była głównym tematem zorganizowanego przez UODO 9 kwietnia br. spotkania ze środowiskiem IOD.
- Na spotkaniu przedstawiciele UODO omówili standardy w zakresie niezależności IOD wynikające z przepisów o ochronie danych osobowych oraz występujące w praktyce problemy, takie jak: nakładanie na IOD obowiązków administratora, zawieranie umowy powierzenia przetwarzania danych osobowych pomiędzy administratorem a inspektorem ochrony danych, występowanie przez IOD w roli pełnomocnika administratora.
- W opinii organu nadzorczego warto, aby w działania na rzecz niezależności IOD włączali się również sami inspektorzy. Od specjalistów w dziedzinie ochrony danych osobowych, jakimi są, powinno się bowiem oczekiwać odpowiedzialnej postawy, stania na straży przestrzegania przepisów prawa oraz zwiększonej rzetelności w zakresie funkcji doradczej i monitorowania przestrzegania prawa.
- Zawodowy charakter tej funkcji powinien za sobą pociągać zwiększony zakres wymagań co do umiejętności, wiedzy i zapobiegliwości w dziedzinie ochrony danych osobowych. Przykładowo inspektor ochrony danych - z uwagi na swoją rolę fachowego doradcy i podmiotu monitorującego w sposób niezależny przestrzeganie przepisów o ochronie danych osobowych - powinien ze swej strony odpowiednio wcześnie identyfikować i sygnalizować administratorowi zagrożenia dla niezależności IOD (np. ryzyko wystąpienia konfliktu interesów), by możliwe było odpowiednio wczesne im zapobieganie.
- Prezes UODO wyraził też przekonanie, że wypracowywane przez lata, we współpracy z inspektorami ochrony danych i administratorami, wskazówki zamieszczane na stronie internetowej organu były i będą dla organizacji zrzeszających IOD niezbędną podbudową dla projektów mających na celu doskonalenie i upowszechnianie standardów w zakresie zgodnego z prawem realizowania obowiązków administratorów wobec IOD.

Źródło: Aktualności – UODO; https://uodo.gov.pl/pl/file/4880

04 Upomnienie dla PZU za przetwarzanie niewłaściwych danych klienta

- Prezes UODO upomniał PZU SA za sposób, w jaki potraktował klienta, który zalegał z opłatami za OC samochodu. Przekazał jego dane do Krajowego Rejestru Długów, bowiem pomylił jego adresy i całą korespondencję o długu kierował na niewłaściwy adres.
- Problem wziął się stąd, że PZU dysponował dwoma adresami klienta. Starym, archiwalnym, z polisy zawartej przed 2006 roku i nowym, z polisy OC na samochód z 2020 roku. Tej ostatniej polisy klient nie zamierzał przedłużać. Niestety, wypowiedzenie umowy złożył już po wygaśnięciu polisy, a zgodnie z ustawą o ubezpieczeniach obowiązkowych (art. 28 ust. 1) PZU musiał tę polisę wznowić automatycznie. W efekcie powstało zadłużenie w wysokości ok. 400 zł. PZU wpisał więc swego klienta (pod niewłaściwym adresem) do Krajowego Rejestru Długów Biura Informacji Gospodarczej SA (zwanego dalej: BIG). W postępowaniu przed UODO Zakład wyjaśnił, że sam klient, kiedy dowiedział się o sprawie zadłużenia, odpisał też z tego adresu.
- Prezes UODO wydając decyzję o upomnieniu wskazał, że

➢ PZU samowolnie wykorzystał adres archiwalny do przedłużenia umowy ubezpieczenia, podczas gdy w umowie pierwotnej wskazany został przez Skarżącego inny adres.

➢ To, że Skarżący podał potem ten stary adres w korespondencji z PZU, nie ma znaczenia. Skarżący zrobił to po to, by PZU go prawidłowo zidentyfikował.

➢ Każdy ma prawo do wskazania swojego adresu do korespondencji, gdyż ponosi odpowiedzialność a późniejsze odbieranie korespondencji. Na administratorze ciąży natomiast obowiązek przetwarzania prawidłowych i aktualnych danych adresowych.

➢ W przedmiotowej sprawie doszło do naruszenia przez PZU przepisów o ochronie danych osobowych polegających na przetwarzaniu nieprawidłowych danych osobowych Skarżącego w zakresie jego nieaktualnego adresu.

Źródło: Biuletyn UODO 05/2024 https://uodo.gov.pl/pl/file/4872

05 Optymizm polskich firm wobec poziomu ochrony przed cyberatakami jest wyjątkowo wysoki

- Wskaźnik tegorocznego „Monitora Transformacji Cyfrowej Biznesu" w zakresie cyberbezpieczeństwa i ryzyka wyniósł 4,9 pkt. To o 0,5 pkt więcej niż przed rokiem. Firmy dostrzegają czyhające niebezpieczeństwa i skupiają się na budowaniu dedykowanych zespołów ds. cyberbezpieczeństwa, sformalizowanych procedurach oraz systemach monitorowania zagrożeń.
- 72% ankietowanych deklaruje, że w ich firmach stworzono i wdrożono polityki oraz procedury w obszarze cyberbezpieczeństwa. Odsetek tych organizacji wzrósł w ciągu roku o 12 punktów procentowych. Najlepiej pod tym względem wypadają sektory finansowy i motoryzacyjny, gdzie formalne zarządzanie cyberbezpieczeństwem deklaruje 87% respondentów, oraz branża life sciences, z 86% takich odpowiedzi.
- 40% ankietowanych twierdzi też, że w ich firmach istnieje dział lub zespół ds. cyberbezpieczeństwa, co stanowi wzrost o 13 punktów procentowych w porównaniu z ubiegłym rokiem. Ponownie na prowadzaniu znajduje się sektor finansowy, w którym odsetek takich firm wzrasta do 80%.
- Jak pokazuje badanie, respondenci ufają swoim pracownikom. Aż 42% z nich zgadza się w bardzo dużym lub dużym stopniu ze stwierdzeniem, że znajomość procedur reagowania na cyberincydenty przez pracowników jest wysoka. Kolejne 39% ankietowanych uważa tak w stopniu umiarkowanym. Optymizmem może napawać fakt, że jedynie według 19% organizacji, ich pracownicy nie są przygotowani lub są przygotowani w małym stopniu do zapobiegania atakom cyberprzestępców.
- Niepokojący jest jednak fakt, że pomimo poprawy względem zeszłorocznych wyników badania, wciąż jedynie 37% firm w dużym lub bardzo dużym stopniu uwzględnia analizę ryzyka przy podejmowaniu decyzji strategicznych czy operacyjnych dotyczących wykorzystania nowych technologii. Dopracowana analiza zapewni optymalną inwestycję w cyberbezpieczeństwo, czyli taką, która w największym stopniu ograniczy ryzyko operacyjne.

Źródło: Monitor Transformacji Cyfrowej Biznesu 2024 (kpmg.com)