
LEX ARTIST

RODO - aktualności

[15.08.2023]

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 Adam Niedzielski złożył rezygnację z funkcji ministra zdrowia

02 QRishing – trudniej go wykryć i rzadziej się przed nim ostrzega

03 Atak na klientów dwóch dużych banków. Żabka też na celowniku cyberoszustów

04 DSA zacznie obowiązywać za kilka dni. Czy Big Techy znów zignorują regulacje?

05 X (Twitter) zweryfikuje twoją tożsamość. Będzie wymagał skanu dowodu osobistego

01 Adam Niedzielski złożył rezygnację z funkcji ministra zdrowia

- W piątek, 4 sierpnia, minister zdrowia Adam Niedzielski ujawnił na platformie X (dawniej Twitter), na jakiego typu leki wypisał sobie receptę lekarz Piotr Pisula. Post miał 4,4 mln wyświetleń.
- Dymisja Adama Niedzielskiego nastąpiła po krytyce upublicznienia przez niego w mediach społecznościowych danych wrażliwych lekarza. Prezes NRL złożył w tej sprawie zawiadomienie do prokuratury o możliwości popełnienia przez Adama Niedzielskiego przestępstwa.
- Wcześniej środowisko lekarskie zbulwersowała sprawa możliwego naruszenia tajemnicy lekarskiej przez ministra Niedzielskiego, ze względu na upublicznienie w mediach społecznościowych recepty, na której znajdowały się dane wrażliwe lekarza oraz inne informacje. Prezes Naczelnej Rady Lekarskiej Łukasz Jankowski zwrócił się w tej sprawie do prokuratury, Urzędu Ochrony Danych Osobowych, Rzecznika Praw Obywatelskich i Rzecznika Praw Pacjenta.
- Zdaniem prawników doszło do popełnienia przestępstwa z art. 107 ustawy o ochronie danych osobowych zagrożonych karą do trzech lat pozbawienia wolności. Zgodnie z tym artykułem karze grzywny lub pozbawienia wolności podlega ten, kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności.
- Ponadto za brak podjęcia odpowiednich działań prezes UODO może wymierzyć karę Ministerstwu Zdrowia w wysokości do 100 tys. zł. Prezes UODO podjął decyzję o wszczęciu postępowania wyjaśniającego w tej sprawie.

Źródło: Jest reakcja UODO. Będzie postępowanie w sprawie ujawnienia danych przez ministra zdrowia (businessinsider.com.pl) Jakie przepisy złamał minister Niedzielski? Lista jest długa (businessinsider.com.pl)

02 QRishing – coraz więcej niebezpiecznych kodów QR

- Firma Cofense poinformowała o zidentyfikowaniu dużej kampanii phishingowej wykorzystującej kody QR. Jej celem było m.in. duże amerykańskie przedsiębiorstwo z branży energetycznej oraz inne firmy z branż: produkcyjnej, ubezpieczeniowej, technologicznej i finansowej. Wydaje się, że warto omówić zarówno tę konkretną kampanię jak i specyficzny rodzaj phishingu, który wykorzystuje kody skanowane telefonem. Już przed laty ukuto dla tego oszustwa termin qrishing, ale nie było powodów by często tego terminu używać.
- W przypadku rzeczonej kampanii atakującej przedsiębiorstwo energetyczne pracownicy firmy dostawali e-maile z kodem w pliku PNG. Maile przekonywały, że w związku z procedurami bezpieczeństwa konieczne jest włączenie weryfikacji 2FA poprzez zeskanowanie kodu QR. Oczywiście po zeskanowaniu kodu należało się zalogować i tu pojawił się problem – kod kierował użytkownika do strony fałszywej, służącej wyłudzeniu danych uwierzytelniających.
- Przestępcy byli sprytni. Zastosowali link z przekierowaniem przez domenę Bing.com. Takie adresy URL, tworzone zwykle w celach marketingowych, zaczynają się od adresu bing.com, potem mają pewien ciąg znaków istotny dla działań marketingowych, a dopiero na końcu mają doklejony adres e-mail ofiary oraz link do strony docelowej.
- Firmę Cofense zaniepokoiła nie tyle użyta technika (wcale nie nowatorska) ile wyraźny wzrost liczby wiadomości tego typu. W maju wynosił on 270% w ujęciu miesiąc do miesiąca. W czerwcu skoczył do 500%, a w kolejnym miesiącu o kolejne 155%.
- Kody QR często nie zostają wykryte przez systemy anty-phishingowe jako niebezpieczne linki w mailu, dlatego należy zachować ostrożność.

Źródło: » QRishing – trudniej go wykryć i rzadziej się przed nim ostrzega -- Niebezpiecznik.pl --

03 Atak na klientów dwóch dużych banków. Żabka też na celowniku cyberoszustów

- Cyberprzestępcy wykorzystują witryny naśladujące strony bankowości elektronicznej BOŚ i Credit Agricole, by wyłudzać loginy i hasła użytkowników - ostrzegł Zespół CSIRT Komisji Nadzoru Finansowego.
- W osobnym, wcześniejszym wpisie Zespół przestrzegł również konsumentów przed fałszywymi reklamami inwestycyjnymi wykorzystującymi wizerunek sieci Żabka.
- „Oszuści w fałszywych reklamach oferują wysokie zyski i zachęcają do zainwestowania pieniędzy. Wejście w reklamę prowadzi na niebezpieczną stronę, na której wymagane jest dokonanie rejestracji. Nie ufajcie w tego typu oferty i bądźcie ostrożni!" - przestrzegli specjaliści.
- Zespół CSIRT KNF realizuje zadania Sektorowego Zespołu Cyberbezpieczeństwa we współpracy z podmiotami krajowego systemu cyberbezpieczeństwa, a w szczególności zespołami CSIRT poziomu krajowego. Sektorowy Zespół Cyberbezpieczeństwa został utworzony przez KNF. (PAP)

Źródło: Atak na klientów dwóch dużych banków. Żabka też na celowniku cyberoszustów - Bankier.pl

04 DSA zacznie obowiązywać za kilka dni. Czy Big Techy znów zignorują regulacje?

- Już 25 sierpnia zaczną obowiązywać przepisy ważnej unijnej regulacji - Aktu o usługach cyfrowych (DSA).
- Regulacja ma na celu zmusić wielkie firmy technologiczne do tego, aby w końcu wzięły odpowiedzialność za treści publikowane na platformach (DSA) i zaangażowały się w ochronę użytkowników przed nadużyciami, również tymi wynikającymi z nieprawidłowego przetwarzania ich danych, jak i o to, aby zaczęły zachowywać się w sposób umożliwiający konkurencję wolnorynkową, a nie budowały monopole i oligopole (DMA).
- Najwięksi gracze na rynku zapowiedzieli już zmiany. Wall Street Journal (WSJ) pisze, że koncern Meta m.in. wprowadzi narzędzia pozwalające użytkownikom na łatwiejsze odwoływanie się od arbitralnie podejmowanych decyzji o blokowaniu kont lub treści, a także zaniżaniu ich widoczności. Z kolei producent sprzętów elektronicznych Apple umożliwi z kolei instalowanie aplikacji spoza do tej pory jedynego legalnego źródła, czyli sklepu z oprogramowaniem App Store na iPhone'y i iPady.
- Amazon - największy sklep internetowy świata - wprowadzi mechanizm dla klientów pozwalający na informowanie administracji o potencjalnie podrabianych lub nielegalnych produktach, co od wielu lat było dla platformy sporym problemem.
- Co ciekawe, nie wszystkie platformy pogodziły się z losem - niektóre się odwołały, jak np. Amazon i Zalando.
- Wielkie platformy nie będą mogły projektować swoich serwisów w sposób, który zwodzi lub w inny sposób ogranicza możliwość podejmowania swobodnych decyzji. Nie chodzi tylko o wyskakujące okienka służące wyłudzeniu zgody na przetwarzanie danych osobowych, ale też np. o aplikacje łatwe do uruchomienia, a trudne do wyłączenia.

Źródło: DSA i DMA w pigułce – co warto wiedzieć o prawie, które ma poskromić cybergigantów | Fundacja Panoptykon; DSA zacznie obowiązywać za kilka dni. Czy Big Techy znów zignorują regulacje? | CyberDefence24

05 X (Twitter) zweryfikuje twoją tożsamość. Będzie wymagał skanu dowodu osobistego

- Ten przymus ma wiązać się z zamieszaniem, które pojawiło się po uruchomieniu programu Twitter Blue.
- Po zmianach w platformie o wiele łatwiej można było podszyć się pod znane osoby publiczne czy instytucje. To spowodowało prawdziwy zalew fałszywych informacji publikowanych przez internetowych trolli. Jak pisaliśmy wcześniej na łamach Bankier.pl, straty (dla X i innych firm) spowodowane tymi działaniami można było liczyć w milionach dolarów.
- Weryfikacja wiązałaby się z wykonaniem selfie oraz zdjęcia dowodu osobistego. Dodatkowo trzeba wyrazić zgodę na przetwarzanie danych osobowych oraz biometrycznych i ich przechowywanie przez maksymalnie 30 dni.
- Na ten moment nikt z X nie potwierdził tych doniesień i nie wiadomo, kiedy taka weryfikacja miałaby zostać wprowadzona. Choć ta platforma nie jest pierwszą, która wymaga tego typu weryfikacji, warto zawsze wziąć pod uwagę ryzyko wiążące się z podawaniem danych wrażliwych. W przypadku cyberprzestępstwa mogą one wpaść w niepowołane ręce.

Źródło: X (Twitter) zweryfikuje twoją tożsamość. Będzie wymagał skanu dowodu osobistego - Bankier.pl