Mądry Polak po szkodzie — jak poradzić sobie z wyciekiem danych?

W TYM WYDANIU:

Aleksander Markiewicz

Weryfikacja partnerów biznesowych — czy warto?

Jednym z elementów systemu compliance w organizacji powinna być procedura oceny wiarygodności podmiotów, z którymi organizacja współpracuje. Do grona tych podmiotów należy zaliczyć partnerów biznesowych, podwykonawców, dostawców i kontrahentów. Dokonanie weryfikacji powyższych podmiotów przed nawiązaniem współpracy, jak również okresowo w czasie jej trwania, ma na celu uniknięcie negatywnych konsekwencji związanych z nawiązaniem stosunków gospodarczych z podmiotem nierzetelnym. Dlatego też uważa się, że weryfikacja ma charakter prewencyjny.

Ryzyko

Zadaniem procesu weryfikacji partnera powinno być zminimalizowanie ryzyka wystąpienia negatywnych następstw wynikających z niewiarygodności, nierzetelności lub niestabilności biznesowej i finansowej partnera. Od poziomu ryzyka powinny być uzależnione działania mające na celu weryfikację naszego potencjalnego kontrahenta. Na poziom ryzyka wpływ powinna mieć nie tylko wiarygodność partnera, ale również przedmiot umowy, jego znaczenie dla naszej organizacji oraz wpływ na naszą ciągłość działania (łańcuch dostaw) i płynność finansową. Dlatego też przy zawieraniu umów, mających kluczowe i strategiczne znaczenie dla naszej organizacji, powinniśmy zadbać o możliwie najdokładniejsze zweryfikowanie partnera, ale także przewidzieć ewentualne skutki nieplanowanego zakończenia współpracy oraz ich wpływ na naszą organizację.

Jak każdy proces, ten związany z oceną kontrahenta, również jest dla organizacji kosztem. Dlatego planując go, należy dostosować go do specyfiki naszych usług lub towarów, branży, w jakiej działamy, naszych zasobów, a także jasnych i sprecyzowanych kryteriów oceny wraz z przypisaniem osób odpowiedzialnych za proces.

Proces weryfikacji kontrahentów jest procesem, który można łatwo outsourcować do podmiotu, który zajmuje się tym w sposób profesjonalny i będzie wiedział, jaki sposób weryfikacji dobrać dla danego partnera, w jaki sposób szacować ryzyko i jakie ryzyka mogą wystąpić przy danym typie usług.

Obowiązek weryfikacji

Weryfikacja partnerów biznesowych nie jest obowiązkowa, tzn. nie jest obowiązkiem powszechnym. W pewnych branżach taki obowiązek jest wskazany wprost w przepisach prawa, za przykład może tu posłużyć obowiązek identyfikacji i weryfikacji podmiotów dostarczających drewno oraz produkty z drewna. Obowiązek ten wynika

z rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 995/2010 z dnia 20 października 2010 r. ustanawiające obowiązki podmiotów wprowadzających do obrotu drewno i produkty z drewna.

W przypadkach, gdy obowiązek weryfikacji partnerów nie jest wprost wskazany w przepisach, należy pamiętać o należytej staranności każdego profesjonalnego podmiotu. Przykładem wyrazu należytej staranności może być weryfikacja kontrahentów na potrzeby minimalizacji lub wyłączenia ryzyka nieświadomego udziału w karuzeli podatkowej VAT. Należy podkreślić, że dla zachowania należytej staranności nie jest wystarczające posiadanie i wdrożenie procedury weryfikacji partnerów biznesowych, najistotniejsze jest stosowanie takiej procedury oraz dobór adekwatnych środków weryfikacji do danych okoliczności.

> **Dla zachowania należytej staranności nie jest wystarczające posiadanie i wdrożenie procedury weryfikacji partnerów biznesowych, najistotniejsze jest stosowanie takiej procedury oraz dobór adekwatnych środków weryfikacji do danych okoliczności.**

Procedura weryfikacji

Do skutecznej weryfikacji kontrahentów niezbędna jest procedura, która będzie określała najistotniejsze elementy i etapy procesu weryfikacji. Prawidłowo przygotowana procedura powinna określać m.in.:

- cel procedury;
- osoby odpowiedzialne za weryfikację partnera;
- kategorie podmiotów podlegających weryfikacji;
- system oceny i dalsze kroki przewidziane dla danej oceny;
- sposób weryfikacji i jej zakres;
- etapy weryfikacji;
- narzędzia wykorzystywane w procesie weryfikacji;
- częstotliwość weryfikacji – może ona być uzależniona od ostatniej oceny danego podmiotu;
- przesłanki stanowiące czerwoną flagę – okoliczności wskazujące, że dany podmiot jest podmiotem wysokiego ryzyka;
- finalny efekt procedury – raport z weryfikacji i jego wzór.

Źródła informacji o kontrahentach

Źródła, z których pozyskujemy informacje, niezbędne w procesie weryfikacji kontrahentów możemy podzielić na wewnętrzne i zewnętrzne. Te drugie możemy podzielić na płatne i bezpłatne.

Informacje ze źródeł wewnętrznych to informacje, które pozyskujemy z wewnątrz naszej organizacji, np. historia współpracy z danym kontrahentem, historia zaległości w płatnościach, opóźnień w wykonaniu umowy, postępowań sądowych, a także dokumenty przedkładane przez weryfikowanego kontrahenta.

Informacje, których pochodzeniem są źródła zewnętrzne, można podzielić, jak wyżej wskazano, na płatne i bezpłatne. Bezpłatne źródła to informacje pozyskiwane z powszechnie dostępnych rejestrów, baz danych czy mniej oficjalnych źródeł jak np. profil kontrahenta w social mediach. Do bezpłatnych źródeł są zaliczane w szczególności: Krajowy Rejestr Sądowy, Centralna Ewidencja i Informacja o Działalności Gospodarczej, biała lista podatników VAT, strona internetowa kontrahenta, profil w portalach społecznościowych, opinie Google, rejestry/giełdy długów, serwisy z opiniami.

Wśród odpłatnych źródeł informacji o kontrahencie należy wskazać Biura informacji gospodarczej, np. Krajowe Biuro Informacji Gospodarczej, ERIF, Krajowy Rejestr Długów czy Krajową Informację Długów Telekomunikacyjnych. Innym odpłatnym źródłem mogą być wywiadownie gospodarcze, np. Bisnode czy Eurel Hermes.

Kontrahenci zagraniczni

Dla potrzeb weryfikacji kontrahentów zagranicznych (niezarejestrowanych w Polsce) część wyżej wskazanych źródeł informacji nie będzie miało zastosowania m.in. KRS i CEiDG, w związku z tym konieczne będzie skorzystanie ze źródeł, które pozwolą nam na uzyskanie informacji o podmiotach zagranicznych, np. VIES – czyli wyszukiwarka weryfikująca nr VAT podmiotów z UE. Dla weryfikacji

podmiotów zagranicznych zaleca się skorzystanie z zagranicznych wywiadowni gospodarczych, które mogą przygotować kompleksowy raport na temat wskazanego podmiotu.

Czerwone flagi

Przez czerwone flagi rozumie się informacje, które powinny być sygnałem ostrzegawczym o nierzetelności lub braku wiarygodności kontrahenta. Do sygnałów ostrzegawczych należy zaliczyć m.in. brak zarejestrowanej działalności (brak wpisu w KRS lub CEiDG), minimalny kapitał zakładowy, brak sprawozdań finansowych w KRS, ogłoszenie upadłości kontrahenta, likwidacja kontrahenta, zawieszona działalność, umowa niezwiązana z głównym przedmiotem działalności kontrahenta, siedziba kontrahenta w raju podatkowym. Oczywiście powyższy katalog jest jedynie katalogiem przykładowymi i w praktyce występuje wiele innych informacji, które mogą być dla nas sygnałem ostrzegawczym przed nierzetelnym kontrahentem. W przypadku identyfikacji powyższych danych powinniśmy być świadomi, że wejście w stosunki handlowe z badanym kontrahentem może być dla naszej organizacji ryzykowne.

RODO a weryfikacja kontrahentów

W procesie weryfikacji kontrahentów może dochodzić do przetwarzania danych osobowych. Podstawą takiego przetwarzania będzie art. 6 ust. 1 lit. c — uzasadniony interes administratora, a więc podmiotu dokonującego weryfikacji. Uzasadnionym interesem jest ochrona własnego przedsiębiorstwa przed naruszeniami powszechnie obowiązującego prawa i nadużyciami finansowymi.

W pewnych przypadkach, gdy organizacja jest zobowiązana przepisami prawa do weryfikacji kontrahentów, podstawą przetwarzania będzie wykonanie obowiązku prawnego – art. 6 ust. 1 lit. c, w takim przypadku należy jednak mieć na względzie, że zakres przetwarzanych danych w procesie weryfikacji powinien być zbieżny z zakresem (o ile został wskazany) określonym w przepisach prawa.

Podsumowanie

Podsumowując, proces weryfikacji kontrahenta może okazać się narzędziem, które uchroni naszą organizację przed wejściem w stosunki gospodarcze z niewiarygodnym i nierzetelnym kontrahentem. Osoby odpowiedzialne za kierowanie przedsiębiorstwem mogą, przez stosowanie tego narzędzia, wykazać należytą staranność, a tym samym zwolnić siebie z ewentualnej odpowiedzialności.

Należy również pamiętać, że weryfikacja kontrahenta nie chroni nas wyłącznie przed stratą finansową, utratą ciągłości działania, ale również przed stratą wizerunkową, która dzisiaj może mieć poważniejsze skutki niż dwa pozostałe wskazane ryzyka.

LexDigital

Drodzy czytelnicy, specjalnie dla Was przygotowaliśmy prezent!

Jest to kompletny i merytoryczny poradnik "Co powinien zrobić administrator w przypadku wycieku danych?" Znajdziecie w nim między innymi:

- jakie mogą być skutki wycieku danych;
- jak zabezpieczyć dane, które powierzasz do przetwarzania innym firmom;
- 5 kroków, które musisz podjąć, jeśli doszło do wycieku;

Poradnik znajdziecie na następnych stronach newslettera. Możecie go również pobrać — link poniżej.

Pobierz poradnik w PDF!

Co powinien zrobić administrator w przypadku wycieku danych?

poradnik LexDigital

Skąd się biorą wycieki danych? Jakie są ich skutki i konsekwencje dla administratora? Kroki, które musisz podjąć w przypadku wycieku.

Kim jest administrator danych osobowych?

Zgodnie z art. 4 RODO, administratorem danych osobowych można nazwać osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Prowadzisz jednoosobową działalność gospodarczą? Jeśli tak, jesteś administratorem danych osobowych. Będąc administratorem danych, jesteś odpowiedzialny za dane, które przetwarzasz, ich bezpieczeństwo oraz minimalizację ryzyka wycieku. Twoim zadaniem jest ochrona danych osób, które Ci je powierzyły.

Za co odpowiada administrator?

Administrator danych osobowych jest odpowiedzialny za wybór i wdrożenie odpowiednich środków technicznych i organizacyjnych, adekwatnie do ryzyka, które jest związane z przetwarzaniem danych.

Aby zagwarantować zgodność z przepisami RODO, administrator dokładnie analizuje sposób przetwarzania danych, zgodnie z zasadami wynikającymi z artykułu 5 RODO, takimi jak minimalizacja danych, ograniczenie czasu przechowywania oraz utrzymanie dokładności danych.

Jeśli jednak dojdzie do naruszenia ochrony danych osobowych, które może być związane z wysokim ryzykiem naruszenia praw podmiotów danych, to właśnie administrator danych składa zawiadomienie do Prezesa Urzędu Ochrony Danych Osobowych. Jeżeli naruszenie wynika z naruszenia przepisów prawa w zakresie ochrony danych osobowych, administrator może ponieść konsekwencje np. w postaci kary administracyjnej nakładanej przez organ nadzorczy.

Administrator powinien zabezpieczyć dane przed:

- udostępnieniem ich osobom nieupoważnionym,
- zabraniem przez osoby nieuprawnione,
- przetwarzaniem niezgodnym z prawem,
- zniszczeniem,
- kradzieżą oraz atakami hakerskimi,
- utratą lub uszkodzeniem.

Przez ostatnie 5 lat polski organ nadzorczy wydał 50 decyzji nakładających na administratorów danych kary administracyjne. Jest to 8 miejsce w Europie.

W spełnieniu powyższych wymagań może pomóc powołany u administratora Inspektor Ochrony Danych Osobowych (IOD). W niektórych przypadkach jego wyznaczenie jest obowiązkowe (kryteria znajdziesz bezpośrednio w RODO). Osoba taka powinna dysponować fachową wiedzą z zakresu przetwarzania danych osobowych i może pomóc w procesie zarządzania systemem ochrony danych u administratora.

Administrator powinien prowadzić dokumentację, która opisuje, w jaki sposób przetwarza dane oraz jakie środki stosuje w celu ich ochrony. Powinien zachować szczególną ostrożność w przypadku przetwarzania danych dotyczących prywatnych aspektów, takich jak orientacja seksualna, pochodzenie, poglądy czy stan zdrowia (dane szczególnej kategorii).

Jakie mogą być skutki wycieku danych?

Skutki wycieku danych osobowych mogą być mniej lub bardziej dotkliwe dla podmiotów danych. Administrator danych powinien podjąć szybkie działania w celu ich minimalizacji. Zaniechania w tym obszarze mogą prowadzić do poważnych konsekwencji np. w postaci kary nałożonej przez Urząd Ochrony Danych Osobowych (UODO). Osoba, której dane wyciekły, może napotkać różne zagrożenia.

Mogą to być na przykład:

- kradzież lub sfałszowanie tożsamości,
- utrata kontroli nad własnymi danymi,
- strata finansowa,
- szkody społeczne lub gospodarcze,
- naruszenie dobrego imienia,
- naruszenie poufności danych.

W zależności od rodzaju danych, które wyciekną, osoby nieuprawnione mogą wykorzystać je do różnych celów, na przykład wynająć pokój w hotelu lub samochód, a nawet wziąć kredyt lub popełnić przestępstwo, podając się za osobę, której dane pozyskały. Ważne jest więc, aby jak najszybciej podjąć działania w celu zabezpieczenia danych i zapobieżenia dalszemu ich wykorzystywaniu.

Nie bagatelizuj naruszeń bezpieczeństwa danych osobowych w firmie. Podejmij szybkie, stanowcze kroki, aby zminimalizować skutki wycieku.

Kroki, które musisz podjąć, jeśli doszło do wycieku danych:

1. Weryfikacja i zabezpieczenie

Natychmiast zweryfikuj źródło i zakres wycieku danych. Zabezpiecz wszelkie źródła wycieku, aby zapobiec dalszemu dostępowi do danych. Oceń wagę zaistniałego zdarzenia. Każdy wyciek danych można zakwalifikować do jednej z dwóch kategorii: incydentu lub naruszenia.

Incydent — zdarzenie lub seria zdarzeń niepożądanych. Może stworzyć potencjalne zaburzenie realizacji zadań lub zagrozić bezpieczeństwu informacji.

Naruszenie — przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, ujawnienie lub nieuprawniony dostęp do przetwarzanych danych osobowych. Posiada negatywne konsekwencje dla osoby, której dane dotyczą.

2. Analiza ryzyka i ustalenie dalszych działań

Oceń ryzyko naruszenia praw i wolności osoby, którą zdarzenie dotknęło. To pozwoli Ci podjąć decyzję dotyczącą zgłoszenia zaistniałego incydentu do Urzędu Ochrony Danych Osobowych oraz poinformowania osoby, której dane zostały naruszone.

Przeprowadź szczegółową analizę wycieku, aby zrozumieć, jakie dane zostały naruszone i jakie mogą być potencjalne skutki tego wycieku. Wykonaj odpowiednie działania, aby oczyścić system z wszelkich zagrożeń i luki w zabezpieczeniach.

3. Udokumentowanie

Zbieraj dokumentację odnośnie każdego naruszenia lub jego podejrzenia. Jest to Twój obowiązek jako administratora. Informacja powinna zawierać szczegóły incydentu, jego skutki, a także kroki podjęte w celu zaradzenia naruszeniu.

4. Kontakt z PUODO

Jeśli Twoja ocena wykaże konieczność zgłoszenia zajścia do Prezesa UODO, zrób to w przeciągu maksymalnie 72 godzin od wykrycia incydentu.

5. Poinformowanie osób dotkniętych wyciekiem

Jeżeli w związku z wyciekiem danych (np. ze względu na ich zakres czy rodzaj) administrator stwierdzi wysokie ryzyka dla podmiotu danych, ma obowiązek poinformowania osoby o zaistniałej sytuacji. Danymi, których wyciek może stanowić zagrożenie są np. nr PESEL, dane konta bankowego, dane z dowodu osobistego.

Żądania osób, których dane wyciekły

Zgodnie z RODO, każda osoba, której dane wyciekły ma prawo domagać się od administratora szczegółowych informacji związanych ze zdarzeniem.

Osoba, której dane dotyczą może Cię zapytać:

- Jak doszło do wycieku?
- Kto lub co za niego odpowiada?
- Czy było to zamierzone (np. kradzież, atak hakera) czy niezamierzone działanie?
- Jakie środki podjąłeś w celu minimalizacji skutków?
- Które konkretnie dane zostały ujawnione wskutek incydentu?
- Czy sprawa została zgłoszona do Prezesa Urzędu Ochrony Danych Osobowych?
- Jakie kroki zamierzasz podjąć w przyszłości, aby uniknąć podobnych sytuacji?

Klauzula poufności

Pamiętaj, że źródłem wycieku danych może być twój pracownik. Jego działania mogą być celowe lub przypadkowe. W związku z tym, zgodnie z RODO, osoby z dostępem do danych osobowych powinny się zobowiązać do zachowania tajemnicy jeszcze zanim rozpoczną pracę z danymi osobowymi, których jesteś administratorem. Zobowiązanie do zachowania tajemnicy można zabezpieczyć osobną umową lub klauzulą poufności w umowie o współpracy lub zawrzeć odpowiednie zapisy w upoważnieniu.

Skąd się biorą wycieki danych?

Za większość wycieków danych w firmie odpowiadają pracownicy. Nie zawsze jest to celowe działanie na szkodę drugiej osoby. Często incydenty wynikają z niewiedzy lub niezachowania należytej ostrożności.

Twoją rolą jako administratora jest nie tylko dbanie o bezpieczeństwo danych, lecz także edukowanie pracowników. Jeśli chcesz zrobić to szybko i sprawnie skorzystaj z naszego szkolenia dla pracowników. Szkolenie zawiera test, więc możesz sprawdzić poziom wiedzy osób zatrudnionych w swojej firmie.

Dobrą decyzją na rzecz ochrony danych jest powołanie Inspektora Danych Osobowych. Do pełnienia tej funkcji możesz zatrudnić także firmę zewnętrzną. Kliknij i zapoznaj się z naszą ofertą.

LexDigital Sp. z o.o.
ul. Grodziska 8; 60-363; Poznań
biuro@lexdigital.pl
LexDigital Sp. z o.o.

Jak zabezpieczyć dane, które powierzasz do przetwarzania innym firmom?

Pamiętaj: za bezpieczeństwo danych powierzanych do przetwarzania również odpowiada Administrator danych. Dlatego dobieraj podmioty przetwarzające skrupulatnie, korzystaj ze swoich praw i przeprowadzaj u nich audyty.

Bądź uważny i sprawdzaj, czy podmioty, którym powierzasz przetwarzanie danych:

- wdrożyły odpowiednie środki techniczne i organizacyjne (art. 28 RODO);
- posiadają fachową wiedzę w zakresie bezpiecznego przetwarzania danych (motyw 81 preambuły do RODO);
- są uprawnione do przetwarzania danych wyłącznie w zakresie celów i sposobów przetwarzania określonych przez Administratora w umowie (podstawą prawną powierzenia danych osobowych jest przede wszystkim umowa powierzenia przetwarzania)

Konsekwencje dla administratora

W związku z zaistniałym wyciekiem danych, Ty jako administrator możesz odczuć konsekwencje finansowe, wizerunkowe, lub prawne.

Wyciek danych może spowodować spadek zaufania klientów wobec Twojej firmy, a co za tym idzie, straty pieniężne. Bardziej odczuwalne natomiast są kary od Prezesa Urzędu Ochrony Danych Osobowych. Taka kara może wynosić nawet do 10 lub 20 mln euro, do 2 lub 4% całkowitego rocznego obrotu firmy z poprzedniego roku.

Potrzebujesz zweryfikować poziom bezpieczeństwa przechowywanych danych w Twojej firmie?
Nasi specjaliści Ci w tym pomogą.
Napisz do nas maila: biuro@lexdigital.pl
lub zadzwoń: +48 500 214 942.

Największy wyciek danych w historii Internetu, znany jako "Collection #1", miał miejsce w styczniu 2019 roku. W tym incydencie skradzionych zostało ponad 770 milionów adresów e-mail i ponad 21 milionów haseł z różnych witryn internetowych.

Ochrona danych w erze cyfrowej: przydatne rozwiązania na straży prywatności

Aby zapobiec niepożądanemu wyciekowi danych w Twojej firmie, musisz zadbać o odpowiednie środki bezpieczeństwa. Skoncentruj się na wykorzystaniu nowoczesnych technologii informatycznych oraz dostępnych na rynku przydatnych rozwiązań.

Multi-factor Authentication

Metoda uwierzytelniania, która wymaga od użytkownika przedstawienia co najmniej dwóch różnych form identyfikacji, aby dostać dostęp do określonego konta lub systemu. Może to być połączenie czegoś, co użytkownik wie (np. hasło), coś, co użytkownik ma (np. urządzenie autoryzacyjne), oraz biometrii.

Pseudonimizacja

Przetwarzanie danych w taki sposób, aby nie można było ich przypisać konkretnej osobie, której dane dotyczą bez użycia dodatkowych informacji. Zidentyfikowanie osoby jest jednak możliwe przy pomocy zastosowania dodatkowych informacji przechowywanych w osobnym miejscu.

Data Leak Prevention

To zestaw technologii i polityk, które zapobiegają niepożądanym wyciekom danych poprzez monitorowanie, kontrolowanie i ograniczanie przepływu informacji w organizacji oraz wykrywanie i blokowanie potencjalnych zagrożeń związanych z naruszeniem poufności danych.

Szyfrowanie end-to-end

Technika, w której informacje są szyfrowane na urządzeniu nadawcy i pozostają zaszyfrowane przez całą trasę przesyłania, aż do urządzenia odbiorcy, gdzie są odszyfrowane. Tylko nadawca i odbiorca mają klucze do deszyfrowania danych, co zapewnia pełną poufność i bezpieczeństwo komunikacji.

Firewall z zaawansowanym filtrowaniem treści

Rodzaj zapory sieciowej, która potrafi analizować oraz filtrować zawartość przesyłanych danych. Dzięki temu może blokować dostęp do niebezpiecznych stron internetowych, wykrywać i zablokować próby przesyłania poufnych informacji.

Szyfrowanie danych

Przekazywana informacja jest możliwa do odczytu jedynie przez osoby uprawnione do dostępu. Stosowany jest mechanizm kodowania treści. Przypadkowa osoba postronna nie odczyta takiej informacji, ponieważ nie posiada odpowiedniego klucza dekodującego.

Prasówka

Google znowu wywija się z pozwów o naruszenie prywatności

Google zawarł ugodę w sprawie, w której oskarżano firmę o naruszenie prawa prywatności poprzez tajne zbieranie danych użytkowników w trybie "incognito" na przeglądarce internetowej Chrome. Pozew, domagający się co najmniej 5 miliardów dolarów, twierdzi, że narzędzia analityczne, pliki cookie i aplikacje Google kontynuowały śledzenie użytkowników nawet w trybach "Incognito" lub "prywatnym" przeglądaniu. Wstępna ugoda między Google a konsumentami spowodowała zawieszenie zaplanowanego na 5 lutego 2024 r. procesu sądowego. Warunki ugody nie zostały ujawnione, ale prawnicy planują przedstawić formalne porozumienie do zatwierdzenia przez sąd do 24 lutego 2024 r. Pozew, złożony w 2020 r., obejmował "miliony" użytkowników Google od 1 czerwca 2016 r. i domagał się co najmniej 5000 dolarów odszkodowania dla każdego użytkownika za naruszenia federalnych przepisów dotyczących podsłuchiwania oraz prawa prywatności Kalifornii.

Ugoda ta ma miejsce w kontekście szeregu kompromitujących informacji na temat działań firmy, które wyszły na jaw w wyniku różnych procesów sądowych w ostatnich miesiącach. W ramach procesu antytrustowego przeciwko Google prowadzonego przez rząd USA, przedstawiono dowody wskazujące, że firma rozważała opóźnienie lub cofnięcie ulepszeń wyników wyszukiwania w celu zwiększenia przychodów z reklam. Niedawno sędzia nadzorujący proces antytrustowy wytoczony przez twórcę gry Fortnite, firmę Epic Games, skrytykował Google za usuwanie dokumentów istotnych dla sprawy. Google przegrało sprawę z firmą Epic, ale planuje się odwołać.

Wypowiedzi analityków sugerują, że Google traci swoją kulturę lidera produktowego i może odchodzić od starej zasady "nie róbmy zła"

Źródło: https://bit.ly/3HcyXww

Ukraińscy hakerzy opublikowali dane osobowe ponad 24 milionów klientów rosyjskiego Alfa Banku

Ukraińska grupa hakerska Kiborg opublikowała w domenie publicznej pełną bazę klientów Alfa-Banku. W październiku 2023 r. hakerzy Kiborg uzyskali dostęp do danych wszystkich klientów Alpha Bank, a następnie opublikowali dane osobowe prawie 44 tysięcy klientów banku. Bank nazwał raporty o wycieku informacji „fałszywymi”.

Baza danych, którą ujawnili hakerzy, zawiera informacje o nazwiskach, datach urodzenia, numerach telefonów, kartach i kontach ponad 24 milionów klientów indywidualnych, a także informacje o kontach ponad 13 milionów osób prawnych. Dziennikarze potwierdzają, że opublikowane dane rzeczywiście odnoszą się do prawdziwych mieszkańców Rosji.

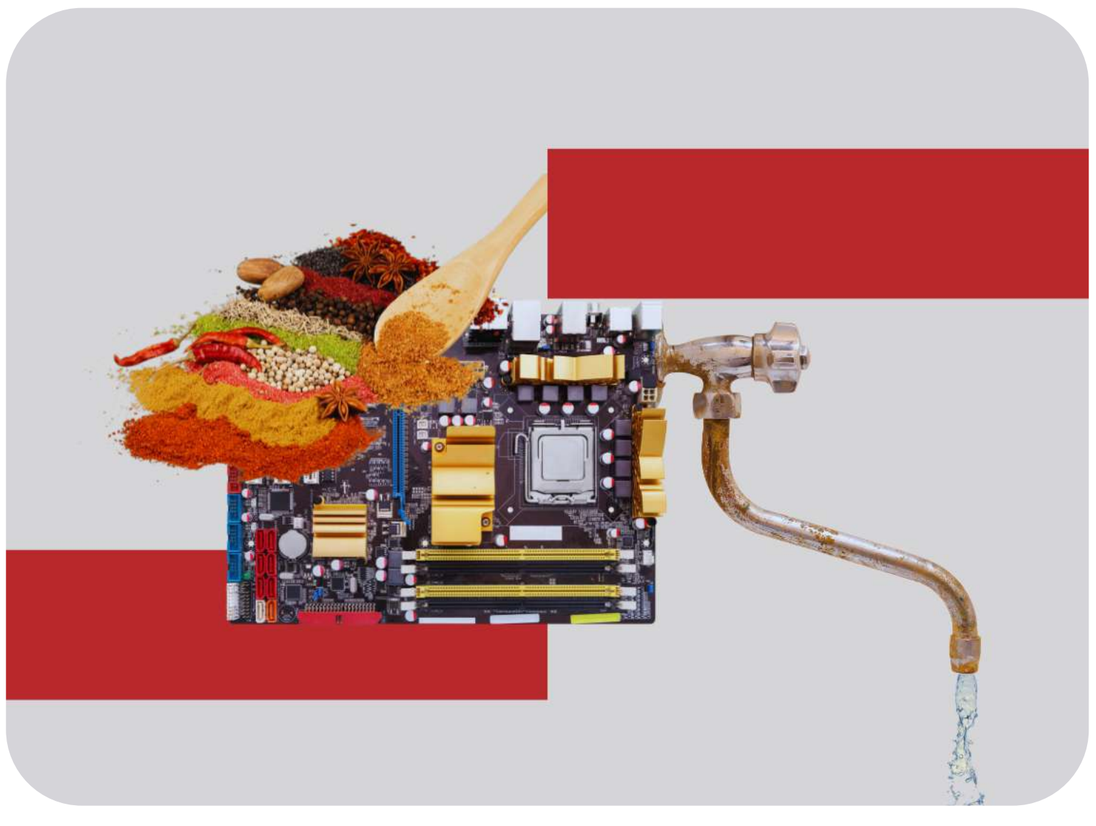
Grupa hakerów Kiborg znana jest z włamania się do bazy danych Siren-Travel z informacjami o pasażerach rosyjskich linii lotniczych. Hakerzy twierdzili, że uzyskali dostęp do 664,6 miliona rejestrów podróży lotniczych w latach 2007-2023. Wśród ujawnionych danych były nazwiska i telefony pasażerów, trasy, taryfy, informacje o cenie biletów.

Źródło: https://bit.ly/41TwGju

Masowy wyciek danych z indyjskiego portalu emerytalnego SPARSH naraża personel obronny na ryzyko

W wyniku znaczącego naruszenia bezpieczeństwa, portal Systemu Zarządzania Emeryturą Raksha (SPARSH) w Indiach, będący kluczowym narzędziem do automatyzacji procesów emerytalnych dla personelu obronnego, doświadczył masowego wycieku danych. Wyciek obejmuje informacje tysięcy pracowników zbrojnych, w tym Armii, Marynarki Wojennej, Sił Powietrznych oraz personelu cywilnego, podnosząc poważne obawy dotyczące prywatności i bezpieczeństwa osób, które pełniły służbę w siłach zbrojnych.

Portal SPARSH, opracowany przez Tata Consultancy Services (TCS), jedną z najważniejszych firm informatycznych w Indiach, stał się miejscem wycieku wrażliwych danych, takich jak nazwy użytkowników, hasła, adresy URL i numery emerytalne. Te informacje trafiły nawet na platformę Telegram, zwiększając ryzyko nadużycia i manipulacji kluczowymi procesami związanymi z emeryturami.



Co istotne, dane z wycieku są również oferowane na rosyjskim rynku za 9,00 dolarów, co rodzi obawy o potencjalne zaangażowanie rosyjskich grup hakerskich. Wyciek dotyczy głównie danych osobowych personelu obronnego w Kerali, co nadaje sytuacji wymiar międzynarodowy i zwiększa obawy dotyczące szerokich konsekwencji oraz potencjalnego nadużycia ujawnionych informacji.

Naruszenie bezpieczeństwa SPARSH stawia pod znakiem zapytania skuteczność systemu Centralized Pension Disbursement System (CPDS). Wyciek danych może poważnie wpłynąć na kluczowe funkcje portalu, takie jak zarządzanie profilami emerytów, weryfikacja danych emerytalnych, śledzenie wniosków o emeryturę, wypłata emerytur oraz składanie certyfikatów życiowych.

W kontekście ogólnokrajowych wyzwań związanych z cyberbezpieczeństwem, ten incydent wpisuje się w niepokojący trend ataków na portale rządowe w Indiach. Przypomnijmy, że w 2023 roku doszło do ataku na Departament Dochodów Podatkowych Indii, a grupa Phoenix, związana z rosyjską grupą hakerską Killnet, twierdziła, że przeprowadziła liczne ataki cybernetyczne na Ministerstwo Zdrowia w Indiach. W obliczu tych wydarzeń, wszyscy użytkownicy portalu SPARSH są zaleceni do natychmiastowej zmiany haseł, a władze powinny przeprowadzić dogłębne śledztwo, wzmocnić środki bezpieczeństwa portalu oraz podjąć szybkie działania przeciwko odpowiedzialnym za wyciek danych SPARSH.

Źródło: https://bit.ly/3NQwyLt

Jak świat probuje kontrolować AI?

Globalne podejście do regulacji sztucznej inteligencji (SI) obejmuje różnorodne strategie, z wyróżnieniem historycznego aktu UE w grudniu, klasyfikującego systemy SI według ich potencjalnego wpływu. W USA, dekret wykonawczy Bidena z października podkreśla bezpieczeństwo i równość, jednak brakuje mu mocy wiążącej federalnej ustawy.

W Bletchley Park odbył się pierwszy globalny szczyt dotyczący bezpieczeństwa SI, z udziałem 28 krajów, w tym Chin, z poparciem dla współpracy w zarządzaniu ryzykiem SI. Trzy kluczowe ramy prawne, w tym Akt SI UE, podkreślają bardziej wyważone zrozumienie SI, dbając o zgodność z wartościami ludzkimi. Dążą one do równowagi między postępem technologicznym a etyczną regulacją, zapewniając transparentność i odpowiedzialność.

Oczekuje się, że przyszłe szczyty w Seulu i Paryżu doprecyzują kwestie związane z działaniem SI, rysując kierunek dla globalnej regulacji SI. Ważnym elementem jest także debata nad kontrolą ludzką wobec filozofii "efektywnego akceleracjonizmu", który sprzyja szybkiemu postępowi technologicznemu, pomijając surową regulację.

Ostateczne kształtowanie regulacji SI będzie wynikiem równowagi między innowacjami a bezpieczeństwem, kierując przyszłość integracji SI w społeczeństwo.

Źródło: https://reut.rs/4aLMOr9

Złośliwe oprogramowanie Chameleon dla systemu Android może wyłączyć odblokowywanie odciskiem palca dla kradzieży kodu PIN

Nowa wersja malware Chameleon na platformie Android umożliwia omijanie zabezpieczeń odcisku palca, pozwalając cyberprzestępcom przejąć kod PIN. Według badań ThreatFabric, złośliwe oprogramowanie to podszywa się pod legalne aplikacje, przekonując użytkowników do włączenia usług dostępności. Następnie atakujący zmieniają zabezpieczenia telefonu z biometrycznych na kod PIN, umożliwiając kradzież hasła. Złośliwe oprogramowanie głównie rozprzestrzenia się za pomocą plików Android Package (APK) z nieoficjalnych źródeł. Użytkownicy są ostrzegani, aby ostrożnie weryfikować legalność używanych aplikacji, zwłaszcza tych związanych z bankowością. ThreatFabric zauważa, że ta nowa wersja Chameleon staje się bardziej zaawansowanym zagrożeniem w dziedzinie mobilnych trojanów bankowych.

Źródło: https://bit.ly/3ROZMM1

Nowy raport NIST alarmuje o rosnącym zagrożeniu atakami AI

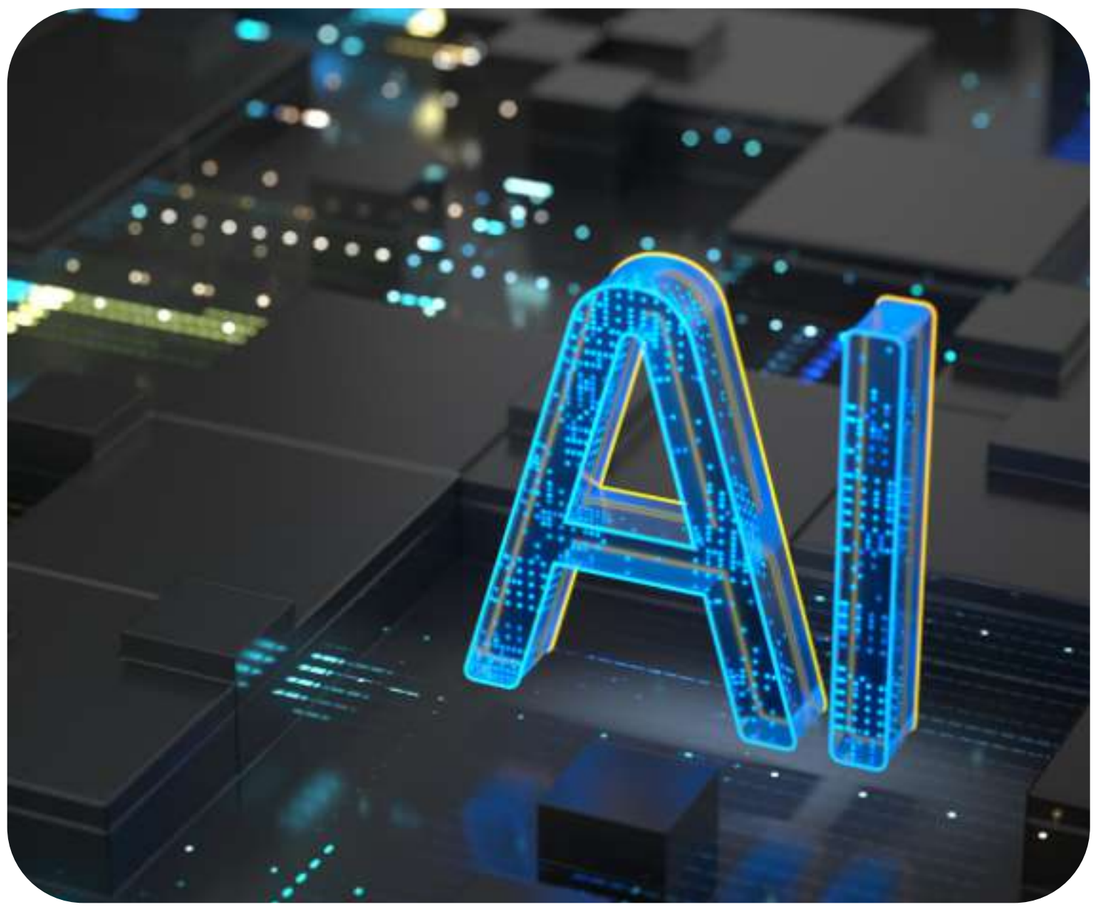
National Institute of Standards and Technology (NIST) wydał pilny raport mający pomóc w obronie przed narastającym zagrożeniem dla systemów sztucznej inteligencji (SI). Raport, zatytułowany "Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations," przychodzi w krytycznym momencie, gdy systemy SI są bardziej potężne i bardziej podatne niż kiedykolwiek wcześniej. Adversarial machine learning to technika, której używają atakujący, aby wprowadzić w błąd systemy SI poprzez subtelne manipulacje, które mogą mieć katastrofalne skutki.

Raport szczegółowo omawia, jak takie ataki są przeprowadzane, kategoryzując je na podstawie celów, zdolności i wiedzy atakujących dotyczącej docelowego systemu SI. Ataki mogą wprowadzać zamieszanie lub nawet "zatruwać" sztuczne systemy inteligencji, wykorzystując słabości w ich tworzeniu i wdrożeniu. Raport omawia ataki, takie jak "zatrucie danych", gdzie przeciwnicy manipulują danymi używanymi do trenowania modeli SI.

Kolejnym zagrożeniem są "ataki z tylnymi drzwiami", gdzie w danych szkoleniowych zostają zasadzone wyzwalacze, indukujące określone błędne klasyfikacje. Raport NIST podkreśla również ryzyka prywatności związane z systemami SI. Techniki takie jak "ataki na inferencję członkostwa" mogą określić, czy próbka danych została użyta do trenowania modelu. NIST ostrzega, że "jeszcze nie istnieje niezawodny sposób ochrony SI przed wprowadzeniem w błąd".

Choć SI obiecuje transformację branż, eksperci ds. bezpieczeństwa podkreślają konieczność ostrożności. Raport NIST ma na celu ustanowienie wspólnego języka i zrozumienia problemów związanych z bezpieczeństwem SI. Ten dokument prawdopodobnie posłuży jako ważne odniesienie dla społeczności ds. bezpieczeństwa SI w pracy nad rozwiązywaniem nowych zagrożeń. Eksperci zaznaczają, że w obliczu wszechobecnych zagrożeń bezpieczeństwa SI wchodzimy w nową erę, gdzie systemy SI będą potrzebować znacznie skuteczniejszej ochrony przed szerokim wdrożeniem w różnych branżach. Ryzyko jest po prostu zbyt duże, by je ignorować.

Źródło: https://bit.ly/3H9t2sb



Polska

PUODO nałożył administracyjną karę pieniężną w wysokości 100 000 zł za nielegalne pozyskanie danych osobowych.

Prezes Urzędu Ochrony Danych Osobowych orzekł, że Minister Zdrowia naruszył przepisy dotyczące ochrony danych osobowych. Naruszenia obejmują nielegalne pozyskiwanie danych osobowych z Elektronicznej Platformy, publikację tych danych na platformie społecznościowej bez odpowiedniej podstawy prawnej oraz brak wdrożenia odpowiednich środków bezpieczeństwa. W związku z tym nałożono karę pieniężną w wysokości 100 000 zł oraz nakazano wdrożenie środków mających na celu minimalizację ryzyka związanego z przetwarzaniem danych osobowych. Minister Zdrowia ma również obowiązek poinformowania osób, których dane zostały ujawnione, o naruszeniu ochrony danych osobowych i przekazania im odpowiednich informacji.

Źródło: https://bit.ly/3vA1Ujb

Świat

Hiszpański organ ds. ochrony danych (DPA) ukarał bank karą w wysokości 70 000 euro za złamanie przepisów RODO, w tym artykułów 5(1)(b), 32 i 5(1)(f). Naruszenie wynikało z ujawnienia przez bank prywatnego adresu prawnika, będącego jednocześnie klientem, podczas udzielania odpowiedzi innemu klientowi reprezentowanemu przez tego samego prawnika.

Adwokat, będący również klientem banku, złożył skargę w listopadzie 2020 r. w imieniu swojego klienta. W odpowiedzi udzielonej 1 grudnia 2020 r. bank nieumyślnie ujawnił prywatny adres adwokata, który znajdował się w prywatnym pliku klienta.

Hiszpański organ ds. ochrony danych uznał bank za naruszające zasadę "ograniczenia celu" określoną w artykule 5(1)(b), ponieważ przetwarzanie danych osobowych adwokata, zwłaszcza jego adresu domowego, w kontekście obsługi skargi klienta, stanowiło naruszenie tej zasady. Dodatkowo organ ds. ochrony danych zidentyfikował naruszenie artykułu 32, podkreślając niewystarczające środki techniczno-organizacyjne w celu zapobieżenia nieautoryzowanemu dostępowi. Bank został także oskarżony o złamanie artykułu 5(1)(f), dotyczącego "zasady integralności i poufności".

Organ ds. ochrony danych nałożył karę w wysokości 50 000 euro za naruszenia artykułów 5(1)(b) i 5(1)(f) oraz dodatkowe 20 000 euro za naruszenie artykułu 32. Pomimo twierdzeń banku, że incydent był jednorazowym błędem, organ ds. ochrony danych uznał go za odpowiedzialnego, wskazując na brak staranności w przestrzeganiu przepisów.

Źródło: https://bit.ly/3NUCnb2

Włoski organ ds. ochrony danych (DPA) nałożył karę w wysokości 40 000 euro na GEICO S.p.A. za nielegalny dostęp do kont email trzech byłych pracowników, naruszając art. 5(1) i art. 13 RODO. Pomimo deaktywacji kont po zakończeniu zatrudnienia, firma nie zarchiwizowała ich, umożliwiając nadal dostęp do wiadomości. Naruszenie zostało zauważone dzięki systemowi powiadomień, co skłoniło byłych pracowników do złożenia skargi.

DPA uznał, że GEICO naruszyło zasadę uczciwości i przejrzystości (art. 5(1)(a) RODO), nie informując byłych pracowników o dalszym przetwarzaniu ich danych po zakończeniu zatrudnienia. Dodatkowo, firma nie poinformowała o sposobie przetwarzania danych i odbiorcach (art. 13 RODO).

Organ stwierdził, że GEICO nie przedstawiło dowodów uzasadniających podejrzane zachowanie byłych pracowników. Brak konkretnego, jasnego i uzasadnionego celu przetwarzania doprowadził do naruszenia zasady ograniczenia celu (art. 5(1)(b) RODO) i zasady minimalizacji danych (art. 5(1)(c) RODO).

DPA skrytykował również politykę firmy dotyczącą przekierowywania e-maili z dezaktywowanych kont, uznając ją za naruszenie zasady integralności i poufności danych (art. 5(1)(f) RODO).

Mimo współpracy i braku wcześniejszych naruszeń, DPA nałożył karę w wysokości 40 000 euro zgodnie z art. 83 RODO.

Źródło: https://bit.ly/3HiqBDn

Włoski organ ds. ochrony danych (DPA) ukarał firmę Cluster S.r.l. karą w wysokości 18 000 euro za naruszenie zabezpieczeń przetwarzania danych, obejmujące dane wrażliwe i informacje o przestępstwach popełnionych przez nieletniego. Firma nie zadbała o bezpieczeństwo materiałów szkoleniowych, co było sprzeczne z art. 32 ust. 1 lit. b) i lit. d) RODO.

Cluster S.r.l. zorganizowała warsztaty dla studentów podyplomowych z psychiatrii. Materiały szkoleniowe zawierały opinię eksperta z przypadku z zakresu sprawiedliwości nieletnich, obejmującą szczegóły medycznej i kryminalnej historii zmarłego nieletniego (osoba, której dane dotyczyły), a także dane osobowe członków jego rodziny. Opinia nie została odpowiednio zanonimizowana, ujawniając nazwisko osoby danych. Dodatkowo dane zostały opublikowane na stronie trzeciej.

Skargę do organu ds. ochrony danych wniosła matka osoby, której dane dotyczyły. W odpowiedzi na prośbę o informacje DPA, firma wyjaśniła, że materiał ten był udostępniany wyłącznie dla uczestników kursu w celach szkoleniowych, którzy byli również objęci tajemnicą zawodową, a ujawnienie go było wyraźnie zabronione. Firma dodała również, że nie wiedziała, iż materiał ten został opublikowany na stronie trzeciej. Firma dalej wyjaśniła, że wgrała opinię eksperta do swojego systemu wewnętrznego, aby umożliwić dostęp na warsztatach i wysłała studentom URL do dostępu do tej informacji na żądanie jednego z prelegentów. System firmy nie był publicznie dostępny z Internetu, a URL był jedynym sposobem, aby publiczność miała dostęp do opinii eksperta. Jednak firma przyznała, że nie sprawdziła, czy prelegent usunął wszystkie dane osobowe osoby, której dane dotyczyły i jej matki. Wreszcie firma sugerowała, że niektórzy studenci mogli udostępnić URL w Internecie. Po dowiedzeniu się o tych problemach firma natychmiast usunęła opinię eksperta ze swojego systemu.

Na podstawie dostarczonych informacji włoski organ ds. ochrony danych stwierdził, że bez uszczerbku dla braku oceny poprawności zdezaktywowania danych, firma była zobowiązana do wprowadzenia odpowiednich środków technicznych i organizacyjnych zapewniających poziom bezpieczeństwa adekwatny do ryzyka przetwarzania danych. To obejmuje zapewnienie poufności przetwarzania oraz regularne testowanie i ocenę skuteczności środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa przetwarzania, zgodnie z art. 32 ust. 1 lit. b) i lit. d) RODO.

W tym przypadku DPA zauważyła, że firma przetwarzała dane osobowe osoby danych i członków jej rodziny w sposób naruszający RODO, ponieważ nie dostarczyła odpowiednich środków zapewniających poufność i nie zweryfikowała skuteczności środków technicznych i organizacyjnych podjętych w tym zakresie. Firma nie miała procedury uwierzytelniania ograniczającej dostęp do opinii eksperta, ani nie oceniła adekwatności środków anonimizacji.

W związku z tym, biorąc pod uwagę czas trwania naruszenia i kategorie danych osobowych objętych naruszeniem, poziom powagi naruszenia popełnionego przez firmę był wysoki. Dlatego DPA nałożyła na firmę karę w wysokości 18 000 euro za niezapewnienie bezpiecznego przetwarzania danych osobowych, naruszając art. 5 ust. 1 lit. f) RODO oraz art. 32 ust. 1 lit. b) i lit. d) RODO.

Dwa aspekty decyzji są interesujące. Po pierwsze, osoba, której dane dotyczyły zmarła przed wniesieniem skargi. RODO obejmuje dane osobowe zmarłych ze względu na konkretne przepisy prawa włoskiego.

Po drugie, skarga została złożona długo po zakończeniu warsztatów. Firma twierdziła, że przedawnienie przestępstwa administracyjnego już minęło. Jednak organ stwierdził, że naruszenie trwało do momentu usunięcia danych osobowych z systemu. W rezultacie firma mogła zostać ukarana.

Źródło: https://bit.ly/3tN1Dcm