Warszawa, 29 listopada 2023 r.

O bezpieczeństwie informacji w e-commerce – porady praktyczne

O przepisach RODO w branży e-commerce napisano już bardzo dużo tekstów prawniczych. Nie negując ich użyteczności, pamiętać należy, że oprócz kwestii prawnych firma prowadząca sklep internetowy musi również pamiętać o szeregu praktycznych konsekwencji obowiązujących przepisów. W tym obszarze szczególnie ważne jest realne zapewnienie bezpieczeństwa przetwarzanych danych – nie tylko tych osobowych. A zatem nie tylko opracowujemy procedury i podpisujemy umowy, ale i pilnujemy ich przestrzegania. W dobie coraz częstszych ataków hackerskich zaufanie klienta do sklepu jest niezwykle istotne. Celem niniejszego tekstu jest przedstawienie – na praktycznych przykładach – jak uniknąć zagrożeń w bieżącej działalności i zminimalizować ryzyko wystąpienia nie tylko kar, ale przede wszystkim strat wizerunkowych.

Zbyt pomocna technologia – ale nie SI

Pomijając korzystanie do pracy ze sztucznej inteligencji, warto zwrócić uwagę na pewne aspekty automatyzacji, które zamiast pracę ułatwić, potrafią ją zaskakująco skomplikować. Prostym przykładem są popularne aplikacje do obsługi poczty elektronicznej. Prawie każda z nich przy wpisywaniu adresata wiadomości ochoczo podpowiada dane ze swojej książki adresowej. Gdy chcemy wysłać e-mail do Jana Kowalskiego, po wpisaniu [Jan K] program podpowie nam pełen adres Jana Kowalskiego. To świetna funkcja, która pozwala zaoszczędzić kilka sekund przy pisaniu każdej wiadomości. Przy pisaniu choćby tuzina maili dziennie skaluje się zapewne do co najmniej paru godzin zaoszczędzonego czasu rocznie. Problem pojawia się jednak, gdy w książce adresowej obok Jana Kowalskiego (z firmy X) mamy również Jana Kowalczyka (z firmy Y). I chcemy do niego wysłać pilną wiadomość e-mail.

Z uwagi na fakt, iż „odkręcenie" wysłania danych osobowych/informacji objętych tajemnicą przedsiębiorstwa firmy X do firmy Y zajmuje dużo więcej czasu niż te parę sekund oszczędności na jednym mailu, gorąco rekomendujemy wyłączanie tej funkcji.

Zbyt pomocna technologia 2 – ale jednak o SI

Sztuczna inteligencja zdobyła w ostatnim czasie taki rozgłos, że trudno jednak ją pominąć. Widząc wszystkie zalety tego rozwiązania nie możemy zapominać o ryzykach z nimi związanych. Jednym z nich jest to, że sztuczna inteligencja potrafi… opowiadać głupoty. Znana jest przygoda prawnika z USA, który z użyciem SI wygenerował pismo procesowe w postępowaniu cywilnym. Pismo wyglądało bardzo uczenie i sensownie, ale niestety algorytm na uzasadnienie swojego wywodu prawnego przywołał zmyślone przez siebie, nieistniejące precedensowe wyroki[1]. Ale pomijając takie anegdoty, każdy korzystający z modeli językowych opartych na sztucznej inteligencji powinien pamiętać, że te aplikacje zapisują wszystko co do nich napiszemy. Zatem jeżeli wprowadzimy tam dane osobowe będące w naszej dyspozycji, to na gruncie RODO ma to dwie bardzo doniosłe konsekwencje:

[1] https://www.forbes.com/sites/mollybohannon/2023/06/08/lawyer-used-chatgpt-in-court-and-cited-fake-cases-a-judge-is-considering-sanctions/ [dostęp 17.11.2023 r.]

- Właśnie udostępniliśmy dane osobowe. Czy osoby, których dane dotyczą, wiedziały że to zrobimy i możemy to udowodnić? I czy serwery dostawcy chatbota wykorzystującego SI nie znajdują się przypadkiem poza Europejskim Obszarem Gospodarczym?
- Co się stanie, jeżeli nasze dane wyciekną/zostaną skradzione od dostawcy naszego rozwiązania opartego na SI?

Szczególnie ten drugi problem może być bardzo dotkliwy. Nie jest też całkowicie hipotetyczny – wiemy już o dużych wyciekach danych z tego typu usług[2]. W jednym takim przypadku programiści z naruszeniem wewnętrznych zasad wrzucali do chatbota niejawny kod aplikacji, nad którą pracowali[3]. W tym konkretnym przypadku nie doszło do naruszenia ochrony danych osobowych, ale utrata kontroli nad fragmentami tajnego kodu aplikacji może okazać się dużo bardziej dotkliwa.

Reasumując: poza prawnymi aspektami korzystania ze sztucznej inteligencji (oraz jej skłonności do konfabulacji) należy bezwzględnie pamiętać, że dysponent danych używanych do korzystania z niej faktycznie traci kontrolę nad swoimi danymi. I udostępniać tam tylko takie materiały, których ujawnienie nie narazi firmy na straty.

Szyfrowanie

Bardzo dobrą praktyką przy przesyłaniu ważnych danych jest dodanie ich do zaszyfrowanego pliku archiwum oraz przekazanie hasła innym kanałem komunikacji niż samego pliku. Doświadczenie uczy, że taka metoda – choć naprawdę świetna i słusznie popularna – napotyka dwa duże problemy w praktyce.

Pierwszym jest chęć zaoszczędzenia na czasie. Bo chyba tylko tym można wyjaśnić wysłanie zaszyfrowanego pliku w jednej wiadomości e-mail a hasła – minutę później w drugiej wiadomości e-mail, do tego samego odbiorcy. Takie działanie całkowicie niweczy sens szyfrowania danych. Jeżeli bowiem haker uzyska dostęp do naszej bądź adresata skrzynki e-mail – to od ręki będzie mógł zaszyfrowany plik odczytać. Autorowi niniejszego tekstu znany jest też przypadek incydentu ochrony danych osobowych polegającego na omyłkowym wysłaniu do niewłaściwego odbiorcy (przykład jak z Janem Kowalczykiem powyżej) zaszyfrowanego pliku, w ślad za którym hasło zostało wysłane mailem na ten sam nieprawidłowy adres.

Drugą niezwykle istotną kwestią jest jakość stosowanych haseł. Pamiętać należy, że przy stale wzrastającej mocy obliczeniowej komputerów długość hasła, które można złamać w sensownym okresie czasu po prostu próbując wszelkich możliwych kombinacji ciągle rośnie. Hasła o długości do 8 znaków (z dużą i małą literą, cyfrą i znakiem specjalnym) są do złamania w czasie paru minut, względnie poniżej jednego dnia. Relatywne bezpieczeństwo uzyskujemy dopiero powyżej dwunastu znaków[4]. Przy wybieraniu hasła warto kierować świetnym zestawem porad opublikowanym przez jednych z najlepszych polskich specjalistów od cyberbezpieczeństwa – CERT NASK.

[2] https://www.cshub.com/data/news/openai-confirms-chatgpt-data-breach [dostęp 17.11.2023 r.]
[3] https://www.cshub.com/data/news/iotw-samsung-employees-allegedly-leak-proprietary-information-via-chatgpt [dostęp 17.11.2023 r.]
[4] https://forsal.pl/lifestyle/technologie/artykuly/8308953,bezpieczne-haslo-zlamanie-dobrego-hasla-zajmie-34-tys-lat.html [dostęp 17.11.2023 r.]

Podsumowując

Lata doświadczeń na odcinku ochrony danych osobowych i niezliczone przeprowadzone audyty pozwalają nam na poczynienie pewnych uwag. Bezpieczeństwo informacji to nie tylko klauzule informacyjne, polityki i procedury. Choćby były one niedoskonałej napisane, nie zdadzą się na nic, jeżeli pracownicy ich nie przestrzegają albo popełniają proste, niewymuszone błędy. Nie jest to tylko pogląd autora – Prezes Urzędu Ochrony Danych Osobowych dawał już do zrozumienia, że posiadanie dobrych procedur gdzieś w szufladzie i ignorowanie ich w codziennym działaniu nie jest akceptowalną praktyką. O takich sytuacjach powinni pamiętać szczególnie przedsiębiorcy działający w branży nowych technologii, jak i prowadzących handel internetowy. Firmy te są szczególnie uzależnione od przekazywania znacznych ilości informacji za pośrednictwem elektronicznych środków komunikacji. Zapewnienie bezpieczeństwa w tej komunikacji jest czymś więcej niż tylko obowiązkiem wynikającym z RODO.

Daniel Taberski - radca prawny, specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.