Oprogramowanie trzeba regularnie aktualizować

Posted on 2025-05-30

Regularna aktualizacja oprogramowania to wynikający z RODO obowiązek administratora i podmiotu przetwarzającego. Powinna ona stanowić integralny element każdej strategii ochrony danych osobowych. Zaniedbania w tym obszarze mogą prowadzić do poważnych naruszeń bezpieczeństwa danych, a w konsekwencji do odpowiedzialności prawnej z tego tytułu.

W świetle ogólnego rozporządzenia o ochronie danych (RODO) administrator oraz podmiot przetwarzający zobowiązani są do zapewnienia bezpieczeństwa przetwarzanych danych osobowych. W tym celu – stosownie do art. 24 ust. 1 RODO – powinni wdrożyć środki techniczne i organizacyjne odpowiednie do zidentyfikowanego ryzyka. Środki te powinny być w razie potrzeby poddawane przeglądom i uaktualniane. Również art. 32 ust. 1 lit. d RODO wprost wskazuje na konieczność regularnego testowania, mierzenia i oceniania skuteczności wdrożonych zabezpieczeń.

Na konieczność utrzymywania aktualnego oprogramowania wskazują również przepisy ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, a także Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Fundamentalne znaczenie aktualizacji

Zagrożenia cybernetyczne nieustannie ewoluują, a przestępcy są coraz lepiej zorganizowani i kreatywni w swoich działaniach. W miarę jak opracowują coraz bardziej zaawansowane i wyrafinowane sposoby i techniki ataków, programiści wydają aktualizacje oprogramowania, których głównym celem jest naprawa wykrytych luk bezpieczeństwa i wprowadzenie nowych funkcji ochronnych. Korzystanie z najnowszych wersji oprogramowania jest zatem niezbędne dla skutecznej ochrony danych osobowych przed nieuprawnionym dostępem, uszkodzeniem czy utratą.

Ponadto aktualizacje:

- • dostosowują oprogramowanie do aktualnych regulacji prawnych dotyczących ochrony danych,
- • poprawiają ogólną wydajność systemu, co zmniejsza ryzyko awarii mogących prowadzić do utraty danych,
- • zapewniają lepszy dostęp do pomocy technicznej, co może być istotne w przypadku wystąpienia incydentu bezpieczeństwa,
- • zawierają optymalizacje, które znacząco zwiększają efektywność działania, eliminują znane błędy wpływające na stabilność pracy oraz wprowadzają dodatkowe funkcjonalności zwiększające użyteczność programów,

Instalacja najnowszych aktualizacji powinna odbywać się na bieżąco, z chwilą ich pojawienia się. Dzięki temu minimalizujemy ryzyko wykorzystania luki w zabezpieczeniach do ataków hakerskich.

Naruszenia bezpieczeństwa spowodowane brakiem aktualizacji

Urząd Ochrony Danych Osobowych konsekwentnie zwraca uwagę, że regularne aktualizowanie programów antywirusowych, oprogramowania typu firewall, przeglądarek, a także innych aplikacji
i całych systemów operacyjnych stanowi nieodzowny element zapewniający bezpieczną pracę
i ochronę danych osobowych.

Brak regularnych aktualizacji oprogramowania może prowadzić do poważnych naruszeń bezpieczeństwa danych osobowych. Dowodzą tego m.in. sprawy prowadzone w UODO. W jednej z nich (DKN.5131.56.2022) przyczyną wystąpienia ataku ransomware było wykorzystanie istniejącej w systemie teleinformatycznym podatności spowodowanej niezaktualizowaniem bazy wirusów programu antywirusowego. W innej (DKN.5112.35.2021) – brak aktualizacji oprogramowania. Kolejne przykłady (DKN.5130.2815.2020, DKN.5131.34.2022) dotyczą naruszeń bezpieczeństwa, do których doszło na skutek korzystania
z systemu operacyjnego, który utracił wsparcie producenta.

Regularne testowanie i ocena skuteczności środków bezpieczeństwa

Oprócz samego aktualizowania oprogramowania, równie istotne jest regularne testowanie, mierzenie i ocenianie skuteczności wdrożonych środków technicznych i organizacyjnych. Obowiązek ten wynika bezpośrednio z art. 32 ust. 1 lit. d) RODO i jest podstawowym obowiązkiem każdego administratora oraz podmiotu przetwarzającego.

Administrator zobowiązany jest do weryfikacji zarówno doboru, jak i poziomu skuteczności stosowanych środków technicznych na każdym etapie przetwarzania danych. Kompleksowość tej weryfikacji powinna być oceniana przez pryzmat adekwatności do istniejących ryzyk oraz proporcjonalności w stosunku do aktualnego stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania. Jak wskazał Wojewódzki Sąd Administracyjny w Warszawie w wyroku z 27 lutego 2024 r. (sygn. akt II SA/Wa 1404/23) „wdrożenie przez administratora środków technicznych i organizacyjnych nie jest działaniem jednorazowym, ale powinno przybrać postać procesu, w ramach którego administrator dokonuje przeglądu i w razie potrzeby uaktualnia przyjęte wcześniej zabezpieczenia. Prawodawca unijny nie wskazuje terminu, w jakim powinien zostać przeprowadzony przegląd czy aktualizacja, pozostawiając w tym zakresie swobodę administratorowi, który w razie dostrzeżenia potrzeby powinien dokonać przeglądu i ewentualnego uaktualnienia”.

Z kolei Wojewódzki Sąd Administracyjny w Warszawie w wyroku z 10 kwietnia 2025 r. (sygn. akt II SA/Wa 1266/24) podtrzymującym decyzję Prezesa UODO nakładającą na spółkę

karę finansową zwrócił uwagę, że na żadnym etapie postępowania, spółka ta „nie twierdziła ani nie wykazywała, że prowadzi regularne testowanie, mierzenie i ocenianie przyjętych środków technicznych
i organizacyjnych. Odwoływała się jedynie do przeprowadzonego audytu w związku z przedłużeniem ważności posiadanego przez spółkę certyfikatu ISO/IEC 27001:2013. Organ nie kwestionował, że taki audyt został w spółce przeprowadzony, jednak stał na stanowisku, że jego przeprowadzenie nie może zastąpić realizacji obowiązku regularnego testowania, mierzenia i oceniania wynikającego z art. 32 ust. 1 lit. d) rozporządzenia nr 2016/679. Tę ocenę organu Sąd w całości podziela.

Z akt administracyjnych nie wynika, by spółka tego rodzaju działania regularnie podejmowała, co w konsekwencji doprowadziło, do niezastosowania przez spółkę odpowiednich środków technicznych i organizacyjnych odpowiadających ustalonemu prawidłowo poziomowi ryzyka dla praw i wolności osób fizycznych. Sam fakt zawarcia w dokumentach spółki wskazań co do konieczności prowadzenia regularnych testów nie oznacza, że tego rodzaju testy były prowadzone, a skarżącą takiej okoliczności nie wykazała.”

Odpowiedzialność administratora za aktualizację

Pełną odpowiedzialność za zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych ponosi administrator. Zatem to jego obowiązkiem jest regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i

organizacyjnych mających zapewnić bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym aktualizowanie używanego oprogramowania.

W przypadku naruszenia ochrony danych osobowych spowodowanego brakiem aktualności oprogramowania administrator może zostać pociągnięty do odpowiedzialności administracyjnej. Prezes Urzędu Ochrony Danych Osobowych, korzystając ze swoich uprawnień, może m.in. udzielić mu upomnienia lub nałożyć karę pieniężną, której wysokość zależy od wielu czynników, w tym od
charakteru i wagi naruszenia oraz od działań podjętych przez administratora w celu zminimalizowania szkody.

Administrator musi również liczyć się z odpowiedzialnością cywilną. Każdej osobie, która uważa, że naruszone zostały jej określone w RODO prawa, przysługuje bowiem możliwość ich ochrony przed sądem cywilnym. Ma ona także prawo żądać odszkodowania za naruszenie przepisów o ochronie danych osobowych, które spowodowało szkodę majątkową lub niemajątkową. Potwierdzają to nie tylko wymienione wyżej decyzje Prezesa UODO, na mocy których administratorów ukarano administracyjną karą pieniężną lub upomnieniem, ale również orzecznictwo.

Trybunał Sprawiedliwości Unii Europejskiej w wyroku z 14 grudnia 2023 r. (C-340/21) wskazał, że administrator danych może ponieść odpowiedzialność za szkodę niemajątkową osoby, której dane zostały udostępnione w wyniku ataku hakerskiego. Co istotne, Trybunał uznał, że nawet sama obawa o skutki wycieku danych osobowych może być uznana za szkodę niemajątkową w rozumieniu RODO, co otwiera drogę do dochodzenia roszczeń odszkodowawczych przez osoby, których dane zostały narażone na ryzyko w wyniku zaniedbań administratora.

Praktyczne zalecenia dotyczące aktualizacji oprogramowania i sprzętu

Mając na uwadze obowiązki administratora oraz potencjalne konsekwencje zaniedbań w obszarze aktualizacji oprogramowania, warto przyjąć systematyczne podejście do tego zagadnienia. Przede wszystkim należy regularnie monitorować dostępność aktualizacji dla wszystkich używanych systemów operacyjnych, aplikacji i urządzeń, a także wdrażać je niezwłocznie po ich opublikowaniu przez producenta. Szczególną uwagę należy zwrócić na aktualizacje dotyczące bezpieczeństwa, które usuwają znane luki w zabezpieczeniach. Producenci oprogramowania regularnie publikują informacje o wykrytych podatnościach oraz wydają odpowiednie poprawki. Dlatego śledzenie tych komunikatów powinno stanowić element procedur bezpieczeństwa w każdej organizacji przetwarzającej dane osobowe.

W przypadku systemów operacyjnych należy również pamiętać o terminach końca wsparcia technicznego. Korzystanie z systemu, który utracił wsparcie producenta, oznacza brak dostępu do krytycznych aktualizacji bezpieczeństwa, co istotnie zwiększa ryzyko naruszenia ochrony danych. W takiej sytuacji administrator powinien rozważyć migrację do nowszych wersji lub wykorzystanie alternatywnych rozwiązań, które nadal otrzymują aktualizacje bezpieczeństwa. Korzystanie z nieaktualnych systemów operacyjnych, po zakończeniu wsparcia technicznego, może zostać uznane za naruszenie art. 32 RODO i skutkować nałożeniem kary administracyjnej przez organ nadzorczy.

Podsumowując, regularne testowanie, mierzenie i ocenianie skuteczności wdrożonych środków bezpieczeństwa oraz regularne aktualizacje oprogramowania i sprzętu stanowią nie

tylko dobrą praktykę w zakresie cyberbezpieczeństwa, ale również prawny obowiązek administratora danych wynikający z przepisów RODO. Zaniedbania w tym obszarze mogą prowadzić do poważnych naruszeń bezpieczeństwa danych osobowych, a w konsekwencji skutkować odpowiedzialnością administratora z tego tytułu. Dlatego też systematyczne podejście do aktualizacji powinno stanowić integralny element każdej strategii ochrony danych osobowych.