Aktualizacje oprogramowania pomagają zapewnić bezpieczeństwo danych

Aktualizacje są nieodłącznym aspektem w świecie informatycznym dlatego należy zdawać sobie sprawę z tego, że regularne aktualizowanie programów antywirusowych, oprogramowania typu firewall, przeglądarek, a także innych aplikacji i całych systemów operacyjnych, z których korzystamy na co dzień, jest jednym z kluczowych warunków zapewniających bezpieczną i stabilną pracę naszego komputera.

Urząd Ochrony Danych Osobowych przypomina, że zgodnie z art. 32 RODO administrator i podmiot przetwarzający musi wdrożyć odpowiednie środki organizacyjne i techniczne, aby zapewnić odpowiedni stopień bezpieczeństwa danych. Wśród wymienionych przykładowo środków znalazła się zdolność do zapewnienia poufności, integralności i odporności systemów i usług przetwarzania. Za bezpieczeństwo danych przetwarzanych w systemach komputerowych odpowiada administrator i podmiot przetwarzający, którzy powinni zapewnić aktualne oprogramowania oraz regularne testowanie środków bezpieczeństwa.

Do bezpieczeństwa informatycznego należy podchodzić wielopłaszczyznowo. Przestępcy wprowadzają do systemów często złośliwe oprogramowania, które po zaszyfrowaniu danych blokują do nich dostęp. Trzeba zwrócić szczególną uwagę na trzy istotne elementy, które składają się na budowanie i utrzymanie wysokiego poziomu bezpieczeństwa – są to procesy, technologia i przede wszystkim ludzie, którzy są odpowiedzialni za ochronę systemów.- powiedział **Tomasz Soczyński**, **Dyrektor Departamentu Informatyki w Urzędzie Ochrony Danych Osobowych.**

Powyższe zasady dotyczą nie tylko administratorów, jakimi są duże firmy, korporacje czy urzędy. Zasady te powinni stosować również osoby fizyczne, które w związku ze swoją działalnością, czasem także pozazawodową, przetwarzają dane innych osób, które powinni chronić.

O ile w wielu przedsiębiorstwach, każda aktualizacja oprogramowania wykonywana jest przez dział IT, który dba o bezpieczeństwo informatyczne o tyle sami musimy zadbać o aktualizacje na naszym prywatnym sprzęcie.

Wiele osób niestety nie zdaje sobie sprawy z konieczności regularnego aktualizowania systemu operacyjnego i zainstalowanego na nim oprogramowania. Należy podkreślić, że użytkownicy regularnie aktualizowanych programów są mniej podatni na próby oszustwa.

Nasze dane mogą trafić w ręce cyberprzestępców poprzez luki w przeglądarkach internetowych, programach pocztowych czy biurowych. I choć niewiele aktualizacji polega na usprawnieniu działania pewnych funkcji, to są wśród nich takie, które dotyczą kwestii bezpieczeństwa.

Producenci co jakiś czas udostępniają nowe wersje systemu, regularnie wycofując wsparcie dla starszych wersji. W takiej sytuacji pozostaje nam przejście na nowszy system operacyjny tego samego producenta lub skorzystanie z rozwiązań typu open source (zazwyczaj jest ono darmowe).

Praca na aktualnym systemie operacyjnym jest o tyle istotna, że niektóre z poprawek nie dotyczą wyłącznie kwestii bezpieczeństwa tego oprogramowania, ale również „załatania” luk wykrytych w konstrukcji podzespołów komputerowych. Istnieją rozwiązania, które z uwagi na błędy np. w procesorach naszych komputerów,

pozwalają przejąć kontrolę nad całą maszyną. Wówczas pozostaje jedynie zmiana procesora na inny (co czasem wymaga wymiany większej liczby podzespołów) lub zainstalowania aktualizacji jeżeli jest dostępna. Niestety stare systemy operacyjne, które nie są już wspierane przez swoich producentów, są narażone na takie ataki. Dlatego, z punktu widzenia bezpieczeństwa danych osobowych, tak ważne jest korzystanie z aktualnego oprogramowania, zarówno komercyjnego, jak i tego, które można używać na licencji open source.

2020-01-31 

- Urząd Ochrony Danych Osobowych
- ul. Stawki 2, 00-193 Warszawa