

Inspektor ochrony danych osobowych zlustruje bezpieczeństwo w UPC

Telekomunikacja

Jakub Styczyński
jakub.styczynski@infor.pl

Pracownicy operatora internetu mogą mieć dostęp do haseł skrzynek pocztowych założonych w domenie usługi. GIODO zapowiada kontrolę.

Sprawę nagłośnił jeden z internautów. Podczas wizyty technika UPC w związku z przedłużeniem umowy i wymianą dekodera zauważył, że monter ma na zleceniu usługi wydrukowany login i hasło do prywatnej e-poczty abonenta, założonej w domenie UPC. Nie było to hasło „fabryczne”,

lecz to, które ustanowił użytkownik.

Doktor Paweł Litwiński z Instytutu Allerhanda podkreśla, że to niedopuszczalne.

– Monter lub inni pracownicy firmy mogą zgubić hasło, celowo udostępnić lub używać w nieokreślonych celach. Dane mogą być też wykradzione przez hakerów – mówi.

Generalny inspektor ochrony danych osobowych deklaruje, że zajmie się sprawą i wyjaśni jej okoliczności. Co do zasady bowiem hasła użytkowników przechowywane w bazie systemu operatora powinny być tam zakodowane, co gwarantuje zapewnienie ich poufno-

ści. Firma UPC zarzeka się, że odpowiedzialność za błąd ponosi system, który tylko w pojedynczym przypadku zachował się nieprawidłowo. Podjęto też kroki, aby ta sytuacja już się nie powtórzyła. Jednak nie otrzymaliśmy odpowiedzi, czy sprawa została rozwiązana indywidualnie, czy zmieniła się cała architektura systemu.

To ważne, bowiem GIODO informuje, że jeśli hasła użytkowników wciąż są udostępniane nieuprawnionym, to doszło do naruszenia przepisów ustawy o ochronie danych osobowych (t.j. Dz.U. z 2014 r. poz. 1182 ze zm., dalej: u.o.d.o.) i ustawy – Prawo telekomuni-

kacyjne (t.j. Dz.U. z 2014 r. poz. 243 ze zm., dalej: p.t.). Zgodnie z art. 36 ust. 1 u.o.d.o. administrator danych (w tym przypadku spółka UPC Polska) musi zastosować środki techniczne i organizacyjne zapewniające ochronę przed przetwarzaniem danych osobowych, a w szczególności przed ich udostępnieniem nieupoważnionym. Zgodnie z art. 51 tej ustawy sankcją za nieumyślne złamanie przepisu jest grzywna, kara ograniczenia bądź pozbawienia wolności do roku – a lat dwóch w przypadku jego umyślnego nieprzestrzegania.

A to nie wszystko. Tego typu praktyki łamią również

tajemnicę telekomunikacyjną (art. 159 ust. 3 p.t.). Za ujawnianie poufnych danych grozi kara pieniężna (art. 209 ust. 1 pkt 24). Eksperci wskazują również sankcje za bezprawne przetwarzanie danych osobowych. Zgodnie z art. 49 ust. 1 u.o.d.o. grozi za to grzywna, kara ograniczania lub pozbawienia wolności do lat dwóch.

Doktor Paweł Litwiński twierdzi także, że działanie może łamać zbiorowe interesy konsumentów i pod tym kątem zostać zakwestionowane przez Urząd Ochrony Konkurencji i Konsumentów.

– Prezes urzędu może nałożyć karę finansową oraz naka-

zać poczynienie rekompensaty publicznej dla poszkodowanych – twierdzi prawnik.

To nie pierwsza tego typu sprawa. W 2010 r. wyszło na jaw, że serwis aukcyjny Allegro przechowywał nieszyfrowane hasła i w wyniku błędu systemu przez godzinę można było poznać hasła dostępu do wolnego użytkownika serwisu, o ile brał on udział w aukcji 90 dni przed incydemem. Również platforma udostępniająca sklepy internetowe IAI-Shop przechowywała jawne hasła i argumentowała, że to dla wygody użytkowników: by mogli szybciej zmieniać hasło ustawione domyślnie. ☹☹