POLSKIE TOWARZYSTWO INFORMATYCZNE
Zarząd Główny, al. Solidarności 82A m. 5, 01-003 Warszawa, tel.: + 48 22 838 47 05, fax: + 48 22 636 89 87, e-mail: pti@pti.org.pl,
www.pti.org.pl
Adres korespondencyjny: ul. Puławska 39 lok. 4, 02-508 Warszawa

L. Dz. W/2040/09

Warszawa, 13 listopada 2009r.

Sz. P. Radosław Chimalski
Zastępca Dyrektora Biura Kryminalnego
Komendy Głównej Policji

Szanowny Panie Dyrektorze,

odpowiadając na pismo z dnia 12 października 2009 (AO-1879/2009) dotyczące propozycji dodania do ust. 6 art. 19 ustawy o Policji kolejnego punktu 4. w brzmieniu:

> *stosowaniu środków elektronicznych umożliwiających niejawne i zdalne uzyskanie dostępu do zapisu na informatycznym nośniku danych, treści przekazów nadawanych i odbieranych oraz ich utrwalenie*

informuję, że przeprowadziliśmy na ten temat szerokie konsultacje wśród członków PTI, specjalizujących się w problematyce bezpieczeństwa danych. W trakcie konsultacji zgłoszono szereg problemów technicznych i prawnych, które podważają sensowność wprowadzenia takiej zmiany.

Zaproponowane sformułowanie jest bardzo szerokie. *Dostęp do danych* może oznaczać nie tylko ich odczytanie, ale także modyfikację, co nie może być zaakceptowane. Należy jednak zwrócić uwagę, że w wielu przypadkach nieujawniony dostęp do danych nie może się odbyć bez zmodyfikowania innych danych (np. systemowych rejestrów dostępu), co zagraża integralności całego systemu i może spowodować ogromne straty po stronie właściciela systemu. Co więcej, poszkodowany mógłby nie wiedzieć, że straty zostały spowodowane przez funkcjonariusza publicznego i że należy mu się odszkodowanie od skarbu państwa. Istnieje też groźba, że Policja włamując się do systemu pozostawi „dziurę", przez którą następnie włamie się ktoś inny – udowodnienie odpowiedzialności i wyegzekwowanie odszkodowania w takim przypadku może być bardzo trudne.

Zdalny dostęp do systemu nie jest możliwy bez przełamania istniejących zabezpieczeń, co obecnie jest zabronione – z proponowanego przepisu nie wynika, w jakim zakresie takie czynności byłyby dozwolone. Ze względów technicznych włamanie do systemu, z którego mają być pozyskane dane, może powodować konieczność włamania się także do innych systemów (np. dostawców Internetu), co może spowodować dalsze uszkodzenia na wielką skalę.

Propozycja jest sprzeczna z art. 269b Kodeksu Karnego:

POLSKIE TOWARZYSTWO INFORMATYCZNE
Zarząd Główny, al. Solidarności 82A m. 5, 01-003 Warszawa, tel.: + 48 22 838 47 05, fax: + 48 22 636 89 87, e-mail: pti@pti.org.pl,
www.pti.org.pl
Adres korespondencyjny: ul. Puławska 39 lok. 4, 02-508 Warszawa

> *Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. [...] a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.*

Nie ma bowiem wątpliwości, że właśnie takie narzędzia musiałyby być użyte w celu niejawnego i zdalnego uzyskania dostępu do komputera. Nie jest także jasne, czy w wyniku przyjęcia proponowanej poprawki Policja miałaby prawo do dokonywania czynności, zakazanych przez art. 268, 268a, 269a Kodeksu Karnego (niszczenie, uszkodzenie, usuwanie lub zmienianie zapisu istotnej informacji lub danych informatycznych; zakłócanie pracy systemu komputerowego lub sieci teleinformatycznej). Uważamy, że spójnej regulacji wymaga całokształt wdrożenia w prawie polskim konwencji o cyberprzestępczości.

Należy też zwrócić uwagę, że sam fakt zdalnego dostępu do danych przez Policję spowoduje ich całkowitą nieprzydatność w przyszłości do celów dowodowych, ponieważ będzie można skutecznie zakwestionować ich wiarygodność (nawet jeśli dostęp polegał wyłącznie na odczycie danych, to nie da się tego udowodnić).

W czasie konsultacji wyrażano obawę o potencjalną odpowiedzialność administratora systemu, który w ramach swoich obowiązków ma uniemożliwiać nieuprawniony dostępu z zewnątrz – czy np. ujawnienie przez niego takiego dostępu nie będzie traktowane jako utrudnianie postępowania i czy Policja będzie mogła zażądać celowego pozostawienia w systemach ochronnych luk, umożliwiających zdalny dostęp. To samo dotyczy producentów oprogramowania obronnego – czy Policja będzie mogła żądać od nich pozostawiania luk.

Nie bez powodu wiele krajów UE nie zdecydowało się na wprowadzenie takiego rozwiązania, nie zdecydowano się także na wprowadzenie go w USA (*Patriot Act*).

Zdaniem PTI proponowana regulacja jest wadliwa, wymaga daleko idącego uściślenia i uszczegółowienia. PTI deklaruje gotowość do współpracy w tym zakresie.

Z poważaniem

SEKRETARZ GENERALNY
Polskiego Towarzystwa Informatycznego
Radosław Bursztynowski