Szukanie luk bezpieczeństwa będzie karane ostrzej i wciąż niezależnie od intencji

28 lutego 2017

Sejm przyjął przepisy o tzw. konfiskacie rozszerzonej. Niestety posłowie nie zwrócili uwagi na problemowe przepisy dotyczące szukania luk w zabezpieczeniach IT. Ciągle będzie to karalne niezależnie od intencji. Poza tym ustawa wzbudza kontrowersje z powodu rozszerzenia możliwości stosowania podsłuchów.

W ubiegły piątek Sejm uchwalił projekt nowelizacji „Kodeksu karnego" wprowadzający tzw. konfiskatę rozszerzoną. Pod tym pojęciem rozumiemy zabieranie gangsterom majątków, którego dorobili się na przestępstwach. O ile sama idea konfiskaty rozszerzonej jest dobra, o tyle projekt uchwalony w ubiegły piątek jest problemowy z dwóch powodów. Po pierwsze może on narobić dużych problemów tym, którzy szukają luk bezpieczeństwa w dobrej wierze. Poza tym projekt rozszerza możliwości inwigilacji.

Zacznijmy od zagrożeń dla „łowców dziur" i testerów bezpieczeństwa. Już teraz muszą się oni zmagać z tym, że polskie prawo przewiduje karanie zachowań, które są związane z szukaniem luk. Nie jest ważne czy działasz w dobrej wierze czy może chcesz komuś zaszkodzić. Art. 269b „Kodeksu karnego" przewiduję kary za „wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie innym osobom urządzeń lub programów" przystosowanych do popełnienia pewnych przestępstw komputerowych.

Teoretycznie sądy i prokuratury nie powinny ścigać uczciwych badaczy bezpieczeństwa. W praktyce… to się zdarza. W roku 2013 „Niebezpiecznik" opisywał przypadek zatrzymania mężczyzny,

który zgłosił lukę urzędnikowi.

Problem został dostrzeżony przez obecną minister cyfryzacji. W listopadzie ubiegłego roku Anna Streżyńska zaproponowała dodanie do „Kodeksu karnego” tzw. kontratypów przestępstw czyli przepisów wyłączających karalność wytwarzania i posiadania wspomnianych urządzeń lub programów w celach prowadzenia badań naukowych związanych z cyberbezpieczeństwem oraz w celu testowania systemów komputerowych za zgodą ich administratora.

Propozycja została ciepło przyjęta w środowiskach związanych z bezpieczeństwem komputerowym. Niestety jak dotąd jej nie zrealizowano, a tymczasem Ministerstwo Sprawiedliwości postanowiło zaostrzyć karanie przestępstwa określonego w art. 269b. Propozycja tego zaostrzenia pojawiła się właśnie w projekcie o konfiskacie rozszerzonej.

W ubiegły piątek Sejm przyjął projekt, które przewiduje następujące brzmienie art. 269b: „§ 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 lub 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.”

Wcześniej ten przepis przewidywał karę pozbawienia wolności do lat 3. Podniesienie maksymalnej możliwej kary (do lat 5) oznacza nie tylko możliwość wsadzenia na dłużej za kratki. Ten zabieg pozwala również na stosowanie przepadku rozszerzonego wobec sprawców przestępstwa opisanego w art. 269b.

Teraz „łowcy dziur” i pentesterzy mają jeszcze więcej powodów by nie lubić polskiego „Kodeksu karnego”. Oczywiście ten

przepis można jeszcze poprawić dodając do niego kontratypy, ale jeśli najpierw przepis będzie zaostrzony a dopiero później „załatany” to wydaje się… mało bezpiecznym podejściem do sprawy.

Poza opisanym problemem jest jeszcze inny. Przepisy przyjęte w piątek przez Sejm przewidują dodanie w art. 237 „Kodeksu postępowania karnego” paragrafu 3a o następującym brzmieniu: „§ 3a. Kontrola i utrwalanie treści rozmów telefonicznych są dopuszczalne również w celu ujawnienia mienia zagrożonego przepadkiem, o którym mowa w art. 45 § 2 Kodeksu karnego albo art. 33 § 2 „Kodeksu karnego skarbowego”.”

O ewentualnych wadach tej zmiany już pisaliśmy. Zazwyczaj zakładamy, że środek taki jak podsłuch ma służyć wykrywaniu przestępstw w czasie poważnych śledztw. W tym przypadku podsłuch będzie stosowany przy poszukiwaniu rzeczy, które mogły pochodzić z przestępstwa. Teoretycznie więc możliwe będzie podsłuchiwanie osób, które – według prokuratury – mogły mieć jakiś bliżej nieokreślony kontakt z tymi rzeczami.

Wojciech Klicki, ekspert z Fundacji Panoptykon już wcześniej mówił, że jeśli rozszerzamy uprawnienia służb to moglibyśmy wprowadzić pewne przepisy rozszerzające uprawnienia obywateli np. obowiązek informowania o inwigilacji osób, które zostały nią objęte. Oczywiście to prawo miałoby dotyczyć osób, wobec których podsłuch okazał się zbędny.

Niestety w przypadku tej ustawy uwagi dotyczące prywatności nie zostały nawet poważnie przedyskutowane. Teraz ustawa pójdzie do Senatu, a później pozostaje podpis Prezydenta. Jest bardzo mało prawdopodobne, aby na kolejnych etapach wprowadzono potrzebne poprawki. Jak wiadomo prawo w Polsce jest tworzone coraz szybciej, co wcale nie znaczy, że coraz lepiej.

Ustawę uchwaloną przez Sejm znajdziecie TUTAJ.

Autorstwo: Marcin Maj

Źródło: DI.com.pl