Wykrycie i zgłoszenie luki w dobrej wierze nie będzie przestępstwem

15 listopada 2016

Jeśli wykryjesz lukę i zgłosisz ją administratorowi to zawsze ryzykujesz odpowiedzialność karną (sic!). Polskie prawo nie przewiduje, że „haker" może mieć dobre intencje. Na szczęście to się może zmienić bo nowa minister cyfryzacji rozumie problem i nie ignoruje uwag od ekspertów.

Czasem bywa tak, że prawo jest wyraźnie niedostosowane do rzeczywistości i przez lata nikt tego nie zmienia. Po prostu uczymy się żyć z jakimś dziwnym przepisem i liczymy, że sądy lub organy ścigania nie będą nadużywać niedoróbek twórców prawa. Do czasu takie przymykanie oczu może działać, ale może też „niespodziewanie" narobić bałaganu.

Jeden z takich problemów dotyczy polskiego Kodeksu karnego i przepisów o „przestępstwach komputerowych". Chodzi zwłaszcza o art. 269b KK.

„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 § 2 albo art. 269a, 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."

Przepis wydaje się rozsądny, ale nie zawsze „złym facetem" jest ten kto „wytwarza, pozyskuje lub udostępnia innym programy" do popełnienia przestępstw komputerowych. Czasami takie rzeczy robi osoba, która po prostu testuje

bezpieczeństwo. Niestety cytowany wyżej przepis nie przewiduje niekarania jeśli ktoś działał dla dobra publicznego.

Teoretycznie sądy i prokuratury nie powinny się czepiać uczciwych badaczy bezpieczeństwa. W praktyce może być różnie. W roku 2013 Niebezpiecznik opisywał przypadek zatrzymania mężczyzny, który zgłosił lukę urzędnikowi. To był świetny przykład tego jak może zadziałać art. 269b w praktyce.

Już w roku 2013 aktywista Karol Breguła zwracał się w tej sprawie do Rzecznika Praw Obywatelskich oraz do Prokuratora Generalnego. Prokuratura Generalna nawet odpowiedziała, ale jej przedstawiciele skupili się na przekonywaniu Karola Breguły, iż w pewnych sprawach nie ma on racji.

Breguła wrócił do tematu w tym roku. Obecna minister cyfryzacji interesuje się bezpieczeństwem bo wie, że bez niego e-administracja nie ma sensu. Pani minister chce mocniej angażować społeczność ekspertów do szukania i zgłaszania luk w rozwiązaniach informatycznych państwa. We wrześniu Karol Breguła zwrócił się do Ministerstwa Cyfryzacji z pytaniem, czy analizowało ono programy typu bug-bounty w kontekście istniejącego prawa. Wreszcie otrzymał sensowną odpowiedź.

Minister Anna Streżyńska przyjrzała się problemowi i stwierdziła, że nie ma sensu ograniczać się do pustych zapewnień, że badaczom bezpieczeństwa nic nie grozi. Ministerstwo zleciło analizę prawną dotyczącą programów typu Bug Bounty. Z tej analizy wynika, że istnieje możliwość pociągnięcia badaczy do odpowiedzialności jeśli program typu Bug Bounty nie byłby realizowany zgodnie z regulaminem ogłoszonym przez administratora systemu. Ponadto polskie prawo karne wprowadza penalizację nie tylko „dokonania" przestępstwa, lecz także jego „usiłowania".

„Należy też wskazać na art. 9 Kodeksu karnego, zgodnie z którym czyn zabroniony popełniony jest umyślnie, jeżeli sprawca ma zamiar jego popełnienia, to jest chce go popełnić

albo przewidując możliwość jego popełnienia, na to się godzi. Tym samym intencja 7 sprawcy w postaci dokonania przełamania zabezpieczenia lub jego ominięcia a następnie ewentualnego wskazania dysponentowi systemu informatycznego ww. skutków swojej działalności (w dobrej wierze) i w celu poprawienia stanu bezpieczeństwa systemu nie wyłącza odpowiedzialności karnej" – czytamy w analizie Ministerstwa Cyfryzacji.

Pytanie tylko, co Ministerstwo Cyfryzacji może z tym zrobić? Odpowiedzi udzieliła sama minister Streżyńska w czasie dyskusji na „Facebooku". „Po konsultacjach z Ministerstwem Sprawiedliwości dostrzegamy zasadność zmiany art. 269b Kodeksu karnego (…) Po rozmowach z MS czekamy na propozycję ze strony MS w zakresie wprowadzenia do tego przepisu „kontratypów" ww. przestępstw, czyli przepisów wyłączających karalność wytwarzania i posiadania ww. urządzeń lub programów komputerowych w celach prowadzenia badań naukowych związanych z cyberbezpieczeństwem (pierwszy kontratyp) oraz w celu testowania systemów komputerowych za zgodą ich administratora (drugi kontratyp)."

Taka odpowiedź jest dość konkretna. Zawiera nie tylko propozycję rozwiązania problemu, ale też mówi o podjęciu pierwszych prób, jak konsultacje z Ministerstwem Sprawiedliwości.

Oczywiście na radość przyjdzie czas gdy zobaczymy projekt nowelizacji ustawy. Niemniej już teraz warto odnotować, że coś w tej sprawie drgnęło. Tego typu poprawki nie przynoszą wielkiego rozgłosu, natomiast są bardzo potrzebne. Budujące jest to, że Ministerstwo Cyfryzacji ciągle słucha głosu ekspertów.

Kopię analizy prawnej przygotowanej dla Ministerstwa Cyfryzacji i udostępnionej dzięki działaniom Karola Breguły znajdziecie TUTAJ.

Autorstwo: Marcin Maj

Źródło: DI.com.pl