

## **ODPOWIEDZIALNOŚĆ PRAWNA HAKERÓW – PRAWO KARNE**

### **I. Czy polskie prawo zabrania blokowania stron internetowych? Jaka grozi za to odpowiedzialność?**

W polskim kodeksie karnym znalazły się przepisy dotyczące tzw. cyberprzestępczości. Przepisy te zostały włączone do kodeksu w ślad za podpisaniem przez Polskę Konwencji Rady Europy o cyberprzestępczości. Według tej Konwencji oraz polskich przepisów karnych ochrona prawna przysługuje każdemu (zarówno administratorowi jak i użytkownikowi systemu teleinformatycznego), jeśli dojdzie do zakłócenia działania tego systemu wskutek umyślnego ataku na ów system lub też na urządzenia, które pracują/współpracują z takim systemem.

### **II. Czy legalne jest blokowanie stron internetowych?**

Zgodnie z art. 268a § 1 kodeksu karnego (dalej jako kk) kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3. Utrudnienie dostępu do danych informatycznych to utrudnienie ścieżki dotarcia do katalogów, plików na których znajdują się informacje. Przepis ten mówi o dostępie do danych – co zawiera w sobie również dostęp do stron internetowych. Dotyczy to więc tzw. blokowania stron internetowych i to zarówno komercyjnych jak i nie komercyjnych.

W przypadku dokonania takiego czynu kodeks karny przewiduje karę pozbawienia wolności do lat trzech, jednak w przypadku gdy poprzez tego typu działania zostanie wyrządzona znaczna szkoda majątkowa sprawca podlega karze pozbawienia wolności od 3 miesięcy do lat 5 (tak art. 268 a § 2 kk). Aby jednak organy ścigania mogły rozpocząć swoją pracę ofiara takiego ataku musi złożyć tzw. wniosek o ściganie. Bez takiego wniosku Policja lub/i Prokuratura nie może wszcząć postępowania.

### **III. Czy kodeks rozróżnia blokowanie/ zakłócanie działania stron komercyjnych i niekomercyjnych np. rządowych.**

Według obecnego brzmienia kodeksu karnego (art. 269 kk) karze pozbawienia wolności od 6 miesięcy do 8 lat podlega każdy, kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o tzw. szczególnym znaczeniu. Za takie dane uznano dane szczególnie istotne dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego). W praktyce - takich danych nie można odtworzyć lub uniemożliwiony jest ich odczyt, ale nie tylko. Niszczenie danych to bowiem unicestwienie tego typu danych (np. zniszczenie dokumentów, programów itp.)

Takiej samej karze (od 6 miesięcy do 8 lat) podlega sprawca, który zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie tzw. danych szczególnych. Sprawca nie musi czynić trwałych szkód (nie niszczy, nie usuwa, nie zmienia danych), niemniej jednak poprzez jego działanie czasowo spowolnieniu może ulec i ulega proces automatycznego przetwarzania czy gromadzenia danych

Atak na strony zawierające dane informatyczne o szczególnym znaczeniu może polegać na niszczeniu lub wymianie informatycznego nośnika danych czy też na uszkodzeniu urządzenia służącego do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych. W takich wypadkach sprawca także może zostać pociągnięty do odpowiedzialności, zaś wymierzona mu kara może oscylować między karą pozbawienia wolności od 6 miesięcy do 8 lat. Tutaj Policja lub/i Prokuratura podejmują postępowanie z urzędu, bez konieczności składania wniosku od pokrzywdzonego.

W piśmiennictwie prawniczym, przestępstwo o jakim mowa w art. 269 nazywane jest „sabotażem informatycznym”.

Za najsłynniejszy atak z rodzaju „sabotażu informatycznego” uznaje się atak na strony rządowe w Estonii w 2007 r. (atak typu Ddos). Do dziś nie wykryto sprawców ataku.

#### IV. Jak wygląda od strony prawa karnego przeprowadzenie ataku? Do którego momentu działania są legalne a od którego momentu stają się nielegalne?

Przeprowadzenie ataku, z którym najprawdopodobniej mieliśmy do czynienia, tj. ataku typu Ddos jest działaniem składającym się z kilku etapów tj:

1. Napisanie skryptu/aplikacji (tzw. aplikacja złośliwa)
2. Przesłanie skryptu/aplikacji na strony skąd zostanie pobrany lub bezpośrednio do komputerów (komputery zombie)
3. „Odpalenie” skryptu w określonym czasie na komputerach zombie
4. Komputery zombie generują ruch (wysyłają zapytania na atakowany serwer)

Więc po kolei:

#### V. Czy napisanie skryptu, który posłużył do przestępstwa jest nielegalne?

Samo napisanie skryptu czy aplikacji, nie musi być nielegalne. Ale tutaj mamy dwie „ciekawostki prawne”. Pierwsza: kodeks wskazuje, że w pewnych sytuacjach samo stworzenie aplikacji, która **przystosowana jest do popełnienia przestępstwa jest nielegalne** (w art. 269b wymienione są te kategorie przestępstw i tylko w takim przypadku można pociągnąć autora skryptu do odpowiedzialności). Czyli polski kodeks uznaje, że wytworzenie tzw. narzędzia hakierskiego (programu, który jest przystosowany do popełnienia wymienionego w kodeksie przestępstwa) już samo w sobie jest działaniem nielegalnym. Co to oznacza? Nawet jeśli nie popełniono przestępstwa z użyciem tego skryptu, ale sama aplikacja jest przystosowana do popełnienia przestępstwa określonego w art. 269b kk, to wówczas autor aplikacji podlega karze pozbawienia wolności do lat. 3.

Tylko, że wiele programów będzie miało „podwójny charakter”. Mogą być użyte zarówno w celu zbadania poziomu zabezpieczeń danej strony/serwera jak również mogą być użyte w celu ataku na daną stronę internetową czy serwer.

I druga ciekawostka prawna w kontekście ostatnich wydarzeń ataku na strony rządowe. Nie poniesie (na mocy art. 269b kk) odpowiedzialności karnej piszący skrypt w celu popełnienia

przestępstwa zakłócenia automatycznego przetwarzania danych informatycznych o szczególnym znaczeniu (tj. blokowania stron rządowych), jeśli zakłócenia **nie dokonano**

- niszcząc albo wymieniając informatyczny nośnik danych lub
- niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych,

**ale dokonano w inny sposób.**

Ustawa wskazuje bowiem, że tylko wytworzenie takiej aplikacji, która wpływa na zakłócenia automatycznego przetwarzanie danych o szczególnym znaczeniu, ale zakłócenie owo nastąpi wskutek określonych działań (albo poprzez niszczenie/wymianę wymiany informatycznego nośnika danych, albo poprzez niszczenie/uszkodzenie urządzenia służącego do automatycznego przetwarzania, gromadzenia lub przekazywania danych) podlega karze pozbawienia wolności do lat 3.

Tajemnicą ustawodawcy pozostanie dlaczego nie ponosi odpowiedzialności osoba, która pisze skrypt (aplikację) w celu zakłócenia automatycznego przetwarzania (np. blokowania rządowych stron internetowych), ale nie niszcząc przy tym ani nie wymieniając informatycznego nośnika danych.

## **VI. Czy przesłanie skryptu do twz. komputerów zombie lub na strony internetowe skąd skrypty zostaną pobrane przez komputery użytkowników jest nielegalne?**

Tutaj sprawa nie jest tak oczywista. Pojawia się bowiem pewien problem, gdyż nie do końca można znaleźć przepis, który penalizowałby takie działanie (czyli uznawał, że takie działanie jest nielegalne). Mamy co prawda art. 267 § 3 kk, który przewiduje karę pozbawienia wolności do lat 2 dla osoby, która posługuje się oprogramowaniem, ale w celu pozyskania informacji (np. kradzieży haseł). Jeśli więc nasz haker wysłał konia trojańskiego, ale nie w celu uzyskania informacji, to nie będzie go można pociągnąć do odpowiedzialności z tytułu art. 267 § 3 kk.

Odpowiedzią na tego typu działania może być jednak art. 267 § 1 kk który stanowi, iż karze grzywny, karze ograniczenia wolności lub pozbawienia wolności do lat 2 podlega każdy, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

## **VII. Czy jeśli haker pozmięnia stronę rządową (np. na parodiującą stronę właściwą) to poniesie odpowiedzialność?**

Tu w doktrynie zdania są podzielone. Według niektórych prawników, w takiej sytuacji możemy mówić jedynie o postępowaniu cywilnym, zaś działanie takie nie jest skodyfikowane jako nielegalne w kodeksie karnym.

Jeśli jednak spróbować pociągnąć sprawcę do odpowiedzialności karnej to wydaje się, że najważniejsze byłoby wskazanie art. 268 § 1 kk lub art. 269 § 1 kk. Zgodnie z art. 268 § 1 kk kto, nie będąc do tego uprawnionym, (...) zmienia zapis istotnej informacji podlega karze wolności do lat dwóch, przy czym jeśli dotyczy to zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3 (tak art. 268 § 2 kk). Można by wskazać również art. 269 § 1 kk, zgodnie z którym zmiana danych informatycznych o szczególnym znaczeniu polega karze pozbawienia wolności do lat 8.

## **VIII. Czy jeśli haker skopuje informacje zawarte na stronie internetowej będzie ponosił odpowiedzialność i jaką?**

„Kradzież informacji” uregulowane jest w art. 267 § 1 kk, zgodnie z którym kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przelamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

## **IX. Czy użytkownicy komputerów zombie poniosą odpowiedzialność za sztuczne generowanie przez ich komputery ruchu?**

Nie, przestępstwa internetowe może popełnić tylko z tzw. winy umyślnej (tj. chcąc popełnić to przestępstwo lub godząc się na jego popełnienie). Użytkownik komputera zombie nie jest świadomy, że jego komputer uczestniczy w procederze ataku.

## X. Jak dotrzeć do sprawców ataków?

To jest bardzo skomplikowany i żmudny proces. Jest to tzw. śledztwo komputerowe (informatyczne), które niestety często nie przyniesie efektów. W przypadku ataku typu Ddos w zasadzie można uznać, że dotarcie do tych sprawców może nastąpić w trzech sytuacjach:

- zaangażowania dużej liczby ekspertów/biegłych, zaangażowaniu środków oraz czasu
- przyznanie się sprawców
- wykrycie sprawców, przy okazji wykrycia innych przestępstw.

Często osoby dokonujące tego typu zamachów internetowych pozostaną bezkarne, gdyż organy ścigania musiałby przebadać (gruntownie) komputer zombie. Jeśli tych komputerów jest kilkadziesiąt tysięcy, zaś skrypt automatycznie się odinstalował i nie pozostawił śladu – wówczas znalezienie faktycznego sprawcy może okazać się niemożliwe.

Warto tutaj dodać, że nawet jeśli wykryjemy adres IP faktycznego sprawcy, to nie oznacza to, że znaleźliśmy sprawcę zamach. Przestępcy potrafią bowiem „zacierać ślady” np. poprzez podszywanie się pod adres IP.

### **Podsumowując:**

#### **Karalne jest m.in.:**

1. Tworzenie narzędzi hakerskich przystosowanych do popełnienia pewnego rodzaju przestępstw, wymienionych w art. 269b kk (i tylko do tych przestępstw, nie zaś tworzenie wszelkiego rodzaju „złośliwego oprogramowania”)
2. Utrudnianie dostępu do danych informatycznych jak i zakłócanie czy uniemożliwianie automatycznego przetwarzania danych informatycznych (potocznie zwanych blokowaniem strony np. atakami typu Dos czy też DDos)

3. „Sabotaż informatyczny” – dotyczy to danych informatycznych o tzw. szczególnym znaczeniu
4. Dostęp do całości lub części systemu informatycznego bez uprawnienia
5. Posługiwanie się programami komputerowymi w celu uzyskania informacji
6. „Kradzież informacji” czyli uzyskanie dostępu do informacji bez uprawnienia
7. Uszkodzenie, usuwanie, niszczenie, zmiana zapisu istotnej informacji



**Adwokat Monika Brzozowska** – Dyrektor Departamentu Prawa Własności Intelektualnej w kancelarii Pasieka, Derlikowski, Brzozowska i Partnerzy. Kontakt: [monika.brzozowska@pdbllegal.pl](mailto:monika.brzozowska@pdbllegal.pl), tel.: +48 12 431-08-50, + 48 502 27 58 23.

*Niniejszy tekst przeznaczony jest do dowolnego wykorzystania, bez dokonywania zmian, z podaniem autorstwa.*