POLICJA.PL

Źródło: http://www.policja.pl/pol/zwalczaj-cyberprzestep/83643,Zwalczaj-cyberprzestepczosc.html
Wygenerowano: Wtorek, 20 lutego 2018, 22:14

ZWALCZAJ CYBERPRZESTĘPCZOŚĆ

Polska w ostatnich latach stała się jednym z lepiej nasyconych i rozwijających się w Europie rynków komputerowych. Komputery i urządzenia cyfrowe oraz Internet odgrywają coraz większą rolę w prowadzeniu nielegalnej działalności lub też w znaczny sposób pomagają w jej prowadzeniu, poprzez możliwości, które oferuje, tj: nielegalny handel w sieci, pirackie oprogramowanie, różnego rodzaju oszustwa (aukcje internetowe, ogłoszenia, oferty zarobkowania, usługi medialne) oraz przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych. To wszystko czyni z komputerów i globalnej sieci Internet potężne narzędzie do popełniania przestępstw.

Przestępstwa komputerowe leżą w zainteresowaniu zarówno zorganizowanych grup przestępczych, które wykorzystują Internet i systemy komputerowe jako nowy instrument prowadzenia nielegalnej działalności, jak i pojedynczych cyberprzestępców.

Przestępstwa komputerowe obejmują przestępstwa, w których przetwarzanie danych jest przedmiotem czynności wykonawczych (przestępstwa komputerowe *sensu stricto*) oraz przestępstwa, w których komputer jest jedynie środkiem do jego popełnienia (przestępstwa komputerowe *sensu largo*).

Do przestępstw komputerowych *sensu stricto* zaliczyć możemy m.in. hakerstwo, sabotaż komputerowy, a do przestępstw komputerowych *sensu largo* – oszustwo komputerowe, bądź piractwo komputerowe.

Podstawowym aktem prawnym, na którym opiera się walka z cyberprzestępczością w Polsce jest ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. Nr 88, poz. 553, z późn. zm.), a w szczególności:
Art. 190a § 2 – podszywanie się pod inną osobę, fałszywe profile,
Art. 202 kk – dot. treści pedofilskich,
Art. 256 kk – ekstremizm polityczny – treści faszystowskie,
Art. 267 § 1 kk – nieuprawnione uzyskanie informacji (hacking),
Art. 267 § 2 kk – podsłuch komputerowy (sniffing),
Art. 268 § 2 kk – udaremnienie uzyskania informacji,
Art. 268a kk – udaremnienie dostępu do danych informatycznych,
Art. 269 § 1 i 2 kk – sabotaż komputerowy,
Art. 269a kk – rozpowszechnianie złośliwych programów oraz cracking,
Art. 269b kk – tzw. „narzędzia hacker'skie",
Art. 271 kk – handel fikcyjnymi kosztami,
Art. 286 kk – oszustwo popełniane za pośrednictwem Internetu,
Art. 287 kk – oszustwo komputerowe.

Podstawowym aktem prawnym, na którym opiera się ochrona prawa autorskiego i praw pokrewnych w Polsce, które też w ramach zwalczania przestępczości gospodarczej wchodzą w szeroko rozumianą przestępczość komputerową, jest ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r. Nr 90, poz. 631, z późn. zm.). Pozostałe regulacje, mające charakter pomocniczy, to przede wszystkim:

- ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. Nr 43, poz. 296 z późn. zm.);
- ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503, z późn. zm.);
- ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. Nr 88, poz. 553, z późn. zm.);
- ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. Nr 128, poz. 1402, z późn. zm.);
- ustawia z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (Dz. U. Nr 126, poz. 1068, z późn. zm.);
- ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, z późn. zm.).

Mając na względzie prognozowany wzrost przestępczości popełnianej z wykorzystaniem Internetu i zaawansowanych technologii, a co za tym idzie, potrzebę bezpośredniej i szybkiej wymiany informacji pomiędzy organami ścigania, a społeczeństwem Wydział Wsparcia Zwalczania Cyberprzestępczości Biura Służby Kryminalnej Komendy Głównej Policji dostrzega konieczność funkcjonowania punktu kontaktowego drogą elektroniczną przeznaczonego do przekazywania informacji pomocnych w zwalczaniu cyberprzestępczości.

Informacje, które mogą okazać się przydatne w zwalczaniu cyberprzestępczości należy przesyłać na adres poczty elektronicznej:

Uwaga! Przesłanie informacji na adres email nie jest równoznaczne ze złożeniem zawiadomienia o przestępstwie. Zgodnie z przepisami Kodeksu Postępowania Karnego w celu złożenia zawiadomienia osoba pokrzywdzona/świadek powinna zgłosić się do najbliższej jednostki Policji i złożyć takie zawiadomienie, potwierdzając je własnoręcznym podpisem.

cyber-kgp@policja.gov.pl