CYBERPRZESTĘPCZOŚĆ - DZIAŁALNOŚĆ PRZESTĘPCZA BEZ GRANIC

Opracował JUDr. Ivan Bernátek, Prokurator Prokuratury Powiatowej w Libercu

Wstęp

W 2012 roku Komisja Europejska w związku z utworzeniem Europejskiego Centrum ds. Walki z Cyberprzestępczością w komunikacie z dnia 28.3.2012 r. do Rady i Parlamentu Europejskiego podała, iż internet stanowi integralną część nie tylko społeczeństwa, ale również gospodarki. Podkreśliła, iż z internetowych sieci społecznościowych korzysta celem wzajemnej komunikacji pomiędzy sobą i ze światem prawie 80 % młodych Europejczyków[1], a za pośrednictwem sklepów internetowych co roku na całym świecie zrealizowane zostaną transakcje o wartości 8 billionów USD[2]. I to jest również jedną z przyczyn, dlaczego internet coraz częściej stanowi miejsce popełniania przestępstw. Codziennie na całym świecie ofiarą przestępstwa cybernetycznego pada ponad 1 milion osób. Cyberprzestępczość obecnie przynosi większe dochody aniżeli ogólnoświatowy handel marihuaną, kokainą i heroiną łącznie. Istnieje zgodność co do tego, iż cyberprzestępczość stanowi bardzo dochodową formę działalności przestępczej przy równoczesnym niskim ryzyku, która występuje coraz częściej i która powoduje coraz większe szkody.

Wspólny komunikat Komisji Europejskiej oraz Wysokiej Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa do Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 7. 2. 2013, którym ogłoszono „Strategię bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń“, zawiera następujące stwierdzenie, cytuję: „Technologie informacyjno-komunikacyjne stanowią obecnie fundament wzrostu gospodarczego i są zasobem o krytycznym znaczeniu, na którym opierają się na wszystkie sektory gospodarki. Stanowią one obecnie podstawę złożonych systemów, które napędzają gospodarkę w takich kluczowych sektorach jak finanse, opieka zdrowotna, energetyka i transport; wiele modeli biznesowych opiera się na nieprzerwanej dostępności internetu i na sprawnym funkcjonowaniu systemów informatycznych.

W ostatnich latach można było zauważyć, że chociaż cyfrowy świat przynosi ogromne korzyści, jest również podatny na zagrożenia. Incydenty naruszające bezpieczeństwo cybernetyczne[3], zamierzone bądź przypadkowe, których liczba wzrasta w alarmującym tempie, mogą spowodować zakłócenia w świadczeniu podstawowych usług, które uznajemy za oczywiste, takich jak np. dostawy wody, usługi opieki zdrowotnej, dostawy energii elektrycznej i usługi telefonii komórkowej. Zagrożenia mogą mieć różne źródła – w tym przestępcze, motywowane politycznie, terrorystyczne lub inicjowane przez państwo, jak również mogą być efektem klęsk żywiołowych i niezamierzonych błędów.

[1] „Eurostat, Internet Access and Use z dnia 14. 12. 2010 r.

[2] McKinsey Global Institute, Internet Maatters: the Net´s seeping impact on growth jobs and prosperity

[3] Bezpieczeństwo cybernetyczne ogólnie odnosi się do zabezpieczeń i działań, które mogą być wykorzystywane do ochrony domeny cybernetycznej, zarówno cywilnej, jak i wojskowej, przed tymi zagrożeniami, które dotyczą jej współzależnych sieci i infrastruktury informatycznej oraz które mogą te sieci i tę infrastrukturę uszkodzić. Bezpieczeństwo cybernetyczne polega na działaniach mających na celu zachowanie dostępności i integralności sieci i infrastruktury oraz zachowanie poufności zawartych w nich informacji.

Gospodarka UE pada już ofiarą cyberprzestępstw [4] popełnianych zarówno względem sektora prywatnego, jak i osób fizycznych. Cyberprzestępcy wykorzystują coraz bardziej zaawansowane metody ingerowania w struktury systemów informatycznych, wykradają krytyczne dane i żądają od przedsiębiorstw okupów. Nasilenie szpiegostwa gospodarczego i działań inicjowanych przez państwa w cyberprzestrzeni stanowi nową kategorię zagrożeń dla administracji rządowych i przedsiębiorstw w UE.“ (koniec cytatu)

Głównym instrumentem prawnym do walki z cyberprzestępczością jest Konwencja Rady Europy o Cyberprzestępczości numer 185 z dnia 23 listopada 2001 (Council of Europe Cybercerime Convention ETS 185), znana również pod nazwą Konwencja Budapesztańska. Część powyższej Konwencji stanowi Protokół dodatkowy dotyczący penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych. Aczkolwiek Konwencja Budapesztańska nie definiuje pojęcia cyberprzestępczości, nakłada ona obowiązek na poszczególne państwa ratyfikujące przyjęcia na poziomie krajowym, zarówno w obszarze prawa karnego materialnego, jak i w obszarze prawa karnego procesowego, takich środków, które umożliwią skuteczne zwalczanie cyberprzestępczości.

W imieniu Republiki Czeskiej Konwencja została podpisana w Strasburgu w dniu 9 lutego 2005 roku.
Konwencja została zaaprobowana przez Parlament Republiki Czeskiej a prezydent dokonał jej ratyfikacji. Dokument ratyfikacyjny został złożony u Sekretarza Generalnego Rady Europy, depozytariusza Konwencji, w dniu 22 sierpnia 2013 r.

Przy ratyfikacji Konwencji zostało zgłoszone następujące zastrzeżenie Republiki Czeskiej: „Zgodnie z art. 29 ust. 4 oraz art. 42 Konwencji Republika Czeska zastrzega sobie prawo odmowy wykonania wniosku o zabezpieczenie na podstawie art. 29 Konwencji w przypadkach, gdy ma podstawy, aby sądzić, że warunek podwójnej karalności w odniesieniu do czynów przestępczych innych niż czyny określone w art. 2–11 Konwencji nie może być spełniony w celu udzielenia wzajemnej pomocy w zakresie przeszukania lub podobnego dostępu, zajęcia lub innego zabezpieczenia lub ujawnienia danych.“

Republika Czeska również oświadczyła, iż „w przypadku braku umowy o ekstradycji organem właściwym dla składania lub przyjmowania wniosków o wydanie lub o areszt tymczasowy będzie Ministerstwo Sprawiedliwości Republiki Czeskiej (Vyšehradská 16, 128 10 Praha 2) i że organem centralnym, który jest odpowiedzialny za składanie wniosków i udzielanie odpowiedzi na wnioski, jest Prokuratura Naczelna Republiki Czeskiej w przypadku wniosków pochodzących z postępowania przygotowawczego, a Ministerstwo Sprawiedliwości Republiki Czeskiej w przypadku pozostałych wniosków.

Konwencja weszła w życie na mocy jej artykułu 36 ust. 3 z dniem 1 lipca 2004 r. Dla Republiki Czeskiej weszła ona w życie na mocy ustępu 4 wyżej wymienionego artykułu z dniem 1 grudnia 2013 r.

---

[4] Cyberprzestępczość ogólnie odnosi się do szerokiego wachlarza różnych rodzajów działalności przestępczej, w przypadku której komputery i systemy informatyczne stanowią podstawowe narzędzie przestępcze lub są głównym celem działania przestępczego. Cyberprzestępczość obejmuje tradycyjne przestępstwa (np. nadużycia finansowe, fałszerstwa i kradzież tożsamości), przestępstwa związane z treściami (np. dystrybucja w internecie pornografii dziecięcej lub nawoływanie do nienawiści rasowej) oraz przestępstwa typowe dla komputerów i systemów informatycznych (np. ataki na systemy informatyczne, w tym ataki prowadzące do zablokowania usług/systemów, oraz złośliwe oprogramowanie) („malware“)).

Pojęcie cyberprzestępczości (definicja):

Tytuł mojego referatu brzmi CYBERPRZESTĘPCZOŚĆ - DZIAŁALNOŚĆ PRZESTĘPCZA BEZ GRANIC, powinniśmy więc przedstawić sobie definicję pojęcia cyberprzestępczości.

Konwencja Rady Europy nr 185 o cyberprzestępczości z dnia 23. 11. 2001 r. nie zawiera definicji pojęcia cyberprzestępczości. Wskazuje jedynie środki, które powinny zostać przyjęte na poziomie krajowym w obszarze prawa karnego materialnego oraz formalnego. Środki w obszarze prawa karnego materialnego następnie określają ramy ogólne przestępstw, które można uważać za przestępstwa cybernetyczne.

W 2000 roku Rada Europy wydała definicję przestępczości komputerowej pochodzącą ze Statutu Komisji ekspertów ds. cyberprzestępczości: *„Przestępstwo skierowane przeciwko integralności, dostępności lub poufności systemów komputerowych lub przestępstwo w rozumieniu tradycyjnym, przy popełnianiu którego użyto nowoczesnych technologii informatycznych i komunikacyjnych.“* Decyzja ramowa Rady UE nr 2002/584/JHA w sprawie europejskiego nakazu aresztowania stanowi, że *„computer-related crime“ to takie działanie które skierowane jest przeciwko komputerowi, lub działanie, w którym komputer stanowi środek do popełnienia przestępstwa.* W umowach międzynarodowych dla działalności przestępczej popełnianej przy użyciu środków technologii informatycznych najczęściej używane jest pojęcie „cyberprzestępczość“ (Cyber Crime), a stosowanie tego pojęcia zostało z obszaru normatywnego przejęte również do terminologii stosowanej przez specjalistów.[5]

W uproszczeniu pod pojęciem cyberprzestępczość (w języku angielskim cybercrime) można wyobrazić sobie jakąkolwiek działalność przestępczą popełnianą przy pomocy technologii informatycznych oraz komunikacyjnych). W tym odniesieniu należy jednak podkreślić, iż za cyberprzestępczość można uważać tylko takie działanie, za które może grozić ściganie, względnie jest karalne, jak za przestępstwo.

Dla celów niniejszego referatu będę jednak bazował na definicji Policji Republiki Czeskiej, która cyberprzestępczość określa jako ***działalność przestępczą, która popełniana jest w środowisku technologii informatycznych i komunikacyjnych, w tym sieci komputerowych, kiedy przedmiotem ataku jest sam obszar technologii informatycznych i komunikacyjnych, lub kiedy popełniana jest działalność przestępcza przy wyraźnym wykorzystaniu technologii informatycznych i komunikacyjnych, jako istotnego środka do jej popełniania.***

Penalizacja cyberprzestępczości na podstawie kodeksu karnego (ustawa nr 49/2009 Dz.U., z późniejszymi zmianami)

Republika Czeska przejęła część przepisów materialnoprawnych z kompleksowej Konwencji o cyberprzestępczości (art. 2 do 8) i znamiona przestępstw umyślnych stosownie do § 230 i 231 wprowadziła do części szczególnej kodeksu, ew. dokonała nowych sformułowań *(zob. załącznik numer 2)*. W ten sposób dokonano implementacji zobowiązań Republiki Czeskiej wynikających z wyżej wymienionej Konwencji oraz z Decyzji Ramowej

[5] Cyberprzestępczość (Cybercrime) JUDr. Jan Kolouch, Ph.D. Praha: CZ.NIC, 2016)

Rady UE 2005/222/WSiSW w sprawie ataków na systemy informatyczne. Ponadto, Republika Czeska przyjęła, względnie dokonała nowego sformułowania, również kolejne przepisy prawa karnego materialnego na podstawie kolejnych umów międzynarodowych oraz aktów prawnych Unii Europejskiej, jak na przykład Konwencja Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych oraz Decyzja ramowa Rady 2000/375/JHA w sprawie zwalczania pornografii dziecięcej w Internecie).

Większość przestępstw przeciwko poufności, integralności oraz dostępności danych i systemów informatycznych kierowanych jest ***przeciwko majątkowi***.

Bezprawny podsłuch danych penalizowany jest jako przestępstwo naruszenia poufności przesyłanych wiadomości stosownie do § 182 kodeksu karnego.

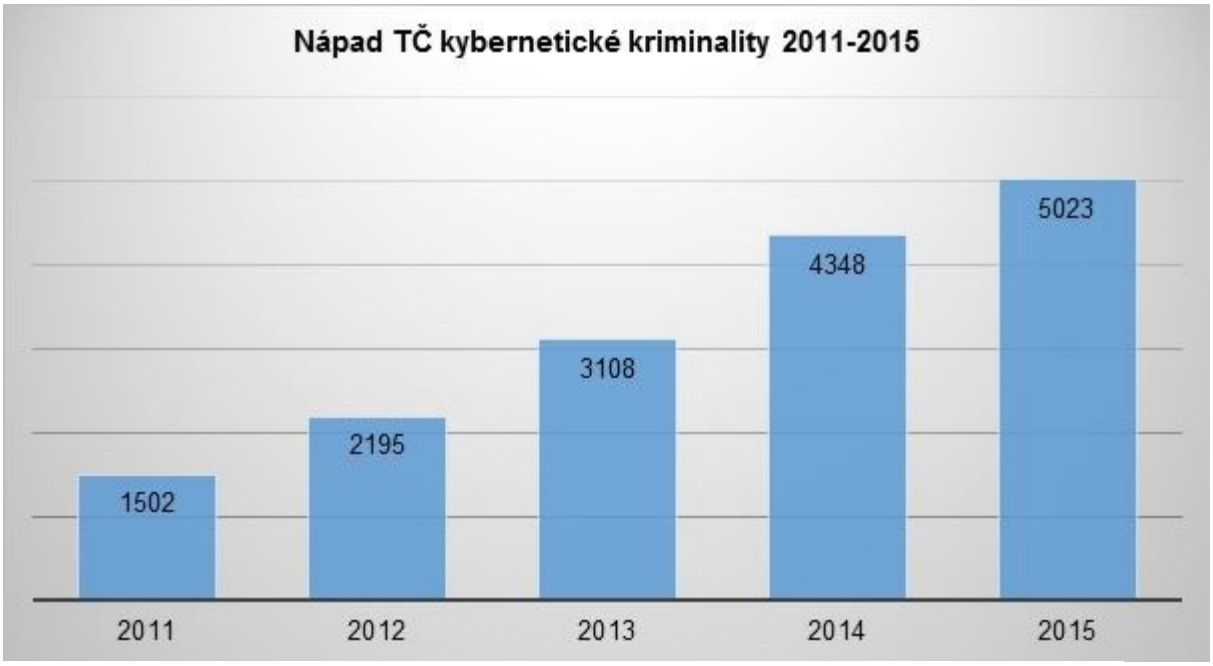
przestępstwa **przeciwko danym (zapisanym informacjom):**

- ***Bezprawny dostęp do systemu komputerowego oraz nośników informacji (§ 230),***
- ***Nabycie oraz przechowywanie urządzenia dostępowego i hasła do systemu komputerowego oraz innych podobnych danych (§ 231),***
- ***Uszkodzenie danych w systemie komputerowym oraz na nośniku informacji oraz ingerencja do wyposażenia komputera przez zaniechanie (§ 232),***

Przestępstwa przeciwko danym (zapisanym informacjom), przy których **komputer stanowi środek do ich popełniania:**

- ***Rozpowszechnianie pornografii (§ 191),***
- ***Produkowanie oraz inne działania związane z pornografią dziecięcą (§ 192),***
- ***Naruszenie praw autorskich, praw pokrewnych oraz praw do bazy danych (§ 270),***
- ***Znieważanie narodu, rasy, grupy etnicznej osób lub innej (§ 355),***
- ***Nawoływanie do nienawiści wobec grupy osób lub ograniczania ich praw i swobód (§ 356),***
- ***Rozpowszechnianie fałszywego komunikatu alarmowego (§ 357),***
- ***Pomówienie (§ 184),***
- ***Szantaż (§ 175),***

Ze statystyk Policji Republiki Czeskiej, która od 2011 roku śledzi ilość przestępstw popełnionych przy użyciu internetu oraz innych sieci komputerowych, wynika, iż od 2011 roku nieustannie rośnie liczba przestępstw cybernetycznych (od 1502 przestępstw w 2011 roku, do 5023 przestępstw w 2015 roku). Liczba przestępstw odnotowanych od 2011 roku do 2015 roku wzrosła o ponad 334%.



Obr.: Statystyki dotyczące przestępczości cybernetycznej 2011-2015

Ze statystyk Policji Republiki Czeskiej wynika, że do grup najczęściej popełnianych przestępstw (rocznie, w setkach przypadków) należą:

Struktura nápadu	2011	2012	2013	2014	2015
podvodná jednání	917	1303	1863	2478	2932
tj. %	*61,05%*	*59,36%*	*59,94%*	*56,99%*	*58,37%*
hacking	66	112	220	555	592
tj. %	*4,39%*	*5,10%*	*7,08%*	*12,76%*	*11,79%*
mravnostní delikty	132	161	261	314	355
tj. %	*8,79%*	*7,33%*	*8,40%*	*7,22%*	*7,07%*
autorskoprávní delikty	155	241	181	262	315
tj. %	*10,32%*	*10,98%*	*5,82%*	*6,03%*	*6,27%*
násilné projevy+hate crime	86	111	155	202	229
tj. %	*5,73%*	*5,06%*	*4,99%*	*4,65%*	*4,56%*
ostatní	146	267	428	537	600
tj. %	*9,72%*	*12,16%*	*13,77%*	*12,35%*	*11,95%*

*Obr.: **struktura przestępstw**, oszustwa, hacking, przestępstwa przeciwko wolności seksualnej i obyczajności, przestępstwa związane z naruszeniem praw autorskich, przejawy przemocy+hate crime, pozostałe*

Oszustwa

Przede wszystkim oszustwo z § 209 kodeksu karnego, kiedy niczym niezwykłym nie jest ani zbieg z bezprawnym dostępem do systemu komputerowego oraz nośnika informacji stosownie do przepisu § 230 kodeksu karnego. Obecnie jest to najliczniej dokumentowane działanie, pod które można subsumować czyny o charakterze nieuczciwych sklepów internetowych, które powstają w celu wyłudzenia środków pieniężnych od klientów, kiedy po krótkim istnieniu taki sklep znika, a środki pieniężne zostają wyprowadzone do zagranicy za

pośrednictwem kilku kolejnych transferów w celu anonimizacji toku środków, często również za pośrednictwem walut wirtualnych. Analogicznie podejmowane są działania w ramach fałszywych ogłoszeń, kolekcji jak i również działania znane jako tzw. oszustwa nigeryjskie. Do danego działania można zaliczyć również jeden z etapów tzw. phishingu, jak i zorganizowane oszustwa w zakresie oferowania sprzedaży samochodów z zagranicy, oszustwa popełniane za pośrednictwem fałszywych wiadomości e-mail, np. legalnej usługi EMKEI.CZ oraz kradzieże z rachunku za pośrednictwem malware, phishingu lub nadużycia środka płatniczego.

- **Hacking**

Bezprawny dostęp do systemu komputerowego oraz nośnika informacji stosownie do przepisu § 230 kodeksu karnego, którego zastosowanie możliwe jest do ścigania większości działań oznaczanych jako tzw. hacking, czyli naruszanie danych, naruszanie systemu, a także nadużywanie urządzeń. Najbardziej typowym, obecnie ściganym przykładem, jest działanie sprawcy, który złamie prawa dostępu do systemu komputerowego, i w ten sposób ma dostęp do danych ofiary, czynnie może pozyskiwać zapisy z aktywności użytkownika, choćby na przykład do danych potrzebnych do dokonywania płatności lub danych, których aktywacji dokona sam sprawca, jak na przykład zapis dźwięku lub obrazu z zaatakowanego urządzenia oraz ich wysyłanie do sprawcy. Elementem danych działań jest między innymi rozpowszechnianie szkodliwych kodów, implementacja tzw. backdoorów do wolnodostępnych oprogramowań itd. Coraz częściej pojawiają się przypadki ataków na skrzynki poczty elektronicznej, konta na portalach społecznościowych – naruszenie prywatności, pozyskiwania informacji, lub ich uszkodzenia czy zniszczenia + możliwa związana z tymi działaniami działalność przestępcza (szantaż, uporczywe nękanie – stalking, kradzieże z kont, oszustwa). Elementem działalności przestępczej tego typu są również ataki cybernetyczne (np. DDoS) czy też szantaż za pośrednictwem ransomware. Kolejną formą może być również przestępstwo naruszenia poufności przesyłanych danych stosownie do § 182 kodeksu karnego, którego najczęściej występującym przejawem jest tzw. sniffing, kiedy sprawca przechwytuje komunikację odbywającą się w sieci, i uzyskuje w ten sposób wrażliwe dane nie tylko o aktywności, lecz również o treści. Dzieje się to często w ramach niezabezpieczonych połączeń wi-fi, po stronie zmanipulowanych serwerów poczty elektronicznej a w ostatnim czasie poprzez ataki na routery domowe. Sprawcy w ten sposób pozyskują wrażliwe dane o charakterze haseł, dane dotyczące płatności czy też wrażliwe treści osobiste lub intymne, które następnie wykorzystują do nacisku celem osiągnięcia korzyści majątkowej lub naruszenia dobrego imienia poszkodowanego.

Blagging

Obecnie za pośrednictwem internetu rozpowszechniane są liczne oszustwa, które wykorzystują między innymi inżynierię społeczną. Na ryzyko narażone są nie tylko poszczególne osoby fizyczne, ale również różne spółki ponadnarodowe. Jednym z wielu rodzajów oszustw w internecie, który korzysta z inżynierii społecznej, jest tzw. CEO – Command Executive Order – pewien rodzaj polecenia osoby uprawnionej do dokonania określonej czynności, w tym przypadku dokonania płatności na rachunek. Oszustwa te polegają np. na przekonywaniu pracownika spółki, aby dokonał on „absolutnie niezbędnego“ przelewu bankowego określonej kwoty na rzecz osoby trzeciej celem wykonania „uprawnionego“ i „zaniechanego“ roszczenia osoby trzeciej – np. dług, prowizja itd. Tego typu oszustwa w większości przypadków stworzone są na podstawie pełnej wiedzy dotyczącej rynku, struktury oraz klientów danej spółki. Pozyskane informacje wykorzystywane są celem przedłożenia wszystkich potrzebnych argumentów w taki sposób, aby ofiary można było łatwiej przekonać i zmanipulować do dokonywania przez nich działań w pożądanym kierunku. Jednym z typowych scenariuszy jest, że po nawiązaniu kontaktu sprawcy podają się np. za dyrektora firmy (np. Prezes, CEO, CFO) lub wiarygodnego

partnera (np. prawnicy, notariusze, rewidenci biegli itd.) spółki. Po takim pretekstem następnie kontaktują się z konkretnym pracownikiem firmy z tym, że skontaktował się z nimi np. dyrektor zarządzający w sprawie terminu płatności określonej wierzytelności lub zawarcia umowy, i w ten sposób przekonają pracownika firmy, że poprzez zapewnienie lub dokonanie płatności działają na korzyść firmy. Umowa może zostać następnie zawarta telefonicznie (naśladują głos) lub za pośrednictwem poczty elektronicznej (naśladowanie adresu poczty elektronicznej). W ten sposób oszuści mogą zażądać niezwłocznego przelewu bankowego środków o dużej wartości na zagraniczny rachunek bankowy. Jeżeli chcą oni być przekonujący, zastosują np. kombinację następujących elementów:

- Tajemnica: „Projekt ten jest nadal poufny a jego sukces uzależniony jest od niniejszej transakcji“,
- Waloryzacja: „Liczymy na Pana/Pani skuteczność i poufność“,
- Nacisk: „Sukces projektu leży na Pana/Pani barkach“.

- **Nieuczciwe sklepy internetowe:**

Popularność zakupów w internecie za pośrednictwem sklepów internetowych nieustannie rośnie. Tendencję rosnącą mają zarówno ilości dokonanych zakupów, jak i wartość utargów sklepów internetowych. Zakupy w internecie są szybkie, często cenowo korzystniejsze aniżeli w zwykłym sklepie z możliwością dostawy na adres podany przez klienta. Pomimo tego kupujący powinni zachować ostrożność w przypadku zakupów w niesprawdzonych sklepach internetowych, przy niezwykle niskich cenach towaru oraz przede wszystkim w przypadku konieczności dokonania zapłaty z góry. W ostatnim czasie, w sprawach nieuczciwych sklepów internetowych pojawiają się przypadki, w których figuruje osoba, której sprawcy oferują pracę o charakterze administracyjnym za pośrednictwem internetowych portali ogłoszeniowych. Osoby te zakładają dla sprawców rachunki bankowe, na które przesyłane są płatności z nieuczciwych sklepów internetowych, a następnie środki te przesyłane są lub w inny sposób przekazywane sprawcom. Jedna osoby zainteresowane pracą o charakterze administracyjnym mogą dopuszczać się prania brudnych pieniędzy pochodzących z przestępstwa, ewentualnie innych przestępstw w formie współudziału.

Przestępstwa przeciwko wolności seksualnej i obyczajności

Zagrażanie wychowaniu dziecka stosownie do § 201 koseksu karnego, rozpowszechnianie pornografii z § 191 kodeksu karnego, produkowanie oraz inne działania związane z pornografią dziecięcą z § 192 kodeksu karnego, wykorzystanie dziecka do produkcji pornografii z § 193 kodeksu karnego, udział w materiale przedstawiającym pornografię stosownie do § 193a kodeksu karnego a także nawiązywanie niedozwolonych kontaktów z dzieckiem stosownie do § 193b kodeksu karnego. Najczęściej jednak ścigane jest działanie, kiedy dochodzi do nawiązania kontaktu z dzieckiem w celu uzyskania jego zdjęć lub filmów intymnych, przy czym najczęściej wykorzystywanym do tego celu środowiskiem są chaty, komunikacja na portalach społecznościowych oraz w grach, kiedy w ten sposób uzyskane materiały są następnie rozpowszechniane lub wymieniane na zamkniętych forach przede wszystkim w sieci onion. Do grupy tej należą również czyny przeciwko osobom pełnoletnim, jak np. zagrażanie obyczajności, stręczycielstwo, przymus seksualny, handel ludźmi.

Przestępstwa związane z naruszaniem praw autorskich

Naruszanie praw autorskich, praw pokrewnych oraz praw do bazy danych stosownie do § 270 kodeksu karnego. Chodzi o rozpowszechnianie utworów muzycznych, filmów oraz oprogramowania z naruszeniem prawa autorskiego w ramach serwerów, które służą jako nośnik danych o dużej pojemności, i są one wyposażone w zaawansowane możliwości wyszukiwania i kategoryzację treści. Jako przykład można przedstawić sprawę postępowania prowadzonego przez Prokuraturę Powiatową w Libercu.

Wyrokiem Sądu Powiatowego w Libercu z dnia *24.11.2011r. skazany został 16 - letni uczeń na karę 5 miesięcy pozbawienia wolności z warunkowym zawieszeniem jej wykonania na okres próby 1 roku, i równocześnie orzeczono* ***środek karny w postaci przepadku przedmiotu****, którym był laptop marki EMACHINES, w tym torby, za popełnienie naruszenia prawa autorskiego, praw pokrewnych oraz prawa do bazy danych stosownie do § 270 ust.1 kodeksu karnego, przy zastosowaniu § 6 ust. 1 ustawy nr 218/2003 Dz.U., o postępowaniu sądowym w sprawach nieletnich, którego dopuścił się tym, że*

„w Libercu w okresie od 10.06.2009r. do 19.04.2010r. przy ulicy Cihlářská nr 666 w miejscu swojego zamieszkania, jako główny administrator prowadził stronę internetową http://www.cinema-world.biz, na której przy użyciu tzw. hostingu z możliwością zapisania danych na serwerze spółki FlyNetwork s.r.o., w przestrzeni przeznaczonej dla swojej strony zamieścił i pozostawił linki, tzw. linki embedded, w wyniku czego udostępnił ogółowi użytkowników co najmniej 2470 różnych bezprawnych kopii dzieł filmowych oraz telewizyjnych zamieszczonych na serwerach zewnętrznych w taki sposób, że każda osoba mogła mieć do nich dostęp za pośrednictwem strony http://www.cinema-world.biz w miejscu i czasie według swojego wyboru w sieci internet, pomimo tego, iż nie posiadał na to zgody posiadaczy praw autorskich i pomimo tego, że listem Czeskiej Unii Antypirackiej, reprezentującej posiadaczy praw autorskich, z dnia 30. 05. 2008 r., został on wezwany do zaniechania takich działań.“

Należy zwrócić uwagę na to, że sąd nie zaakceptował kwalifikacji prawnej wynikającej z aktu oskarżenia, gdyż nie uznał znamiona ustawowego, iż w wyniku popełnionego czynu wyrządzona szkodę o znacznej wielkości (problem obliczenia szkody poniesionej przez posiadacza praw autorskich reprezentowanego przez Czeską Unię Antypiracką, REGON 45768706, Praha 8, Sokolovská 24, która dochodziła naprawienia szkody w wysokości 121.073.265,- CZK, oraz Czeską Telewizję, Kavčí hory, Praha 4, która dochodziła naprawienia szkody w wysokości 1.032.780,-CZK, w wyniku bezprawnego udostępnienia określonych dzieł).

Przejawy przemocy oraz hate crime

Przestępstwa szantażu stosownie do § 175 kodeksu karnego, groźby karalne z § 353 kodeksu karnego, uporczywe nękanie (stalking) z § 354 kodeksu karnego, jak i rozpowszechnianie fałszywego komunikatu alarmowego z § 357 kodeksu karnego. Wszystkie działania ścigane jako wyżej wymienione przestępstwa, dokonane przy użyciu technologii informatycznych, uzyskują większy poziom anonimowości przy pomocy serwerów anonimizacyjnych korzystających z usług proxy, tor, vpn itp. Należą do nich również przejawy ekstremizmu, które mogą być subsumowane pod znamiona czynu zabronionego znieważanie narodu, rasy, grupy etnicznej osób lub innej stosownie do § 355 kodeksu karnego oraz Nawoływanie do nienawiści wobec grupy osób lub ograniczania ich praw i swobód z § 356 kodeksu karnego. Przejawy te następnie w rzeczywistości zamieniają się w formę działań, w ramach których na zagranicznych serwerach tworzone są strony internetowe często o tematyce skrajnie prawicowej lub lewicowej, które nawołują do nienawiści, dyskryminacji a nawet wzywają do stosowania przemocy wobec mniejszościowych grup obywateli czy ugrupowań politycznych. Kolejny przejaw tego typu działań stanowią samodzielne fikcyjne profile na portalach społecznościowych.

WYKORZYSTYWANIE SEKSUALNE DZIECI W INTERNECIE

Wykorzystywanie seksualne dzieci stanowi jeden z poważnych problemów obecnego świata internetowego. Internet zapewnia przede wszystkim anonimowość, i podawanie się za kogoś innego nie jest wcale trudne. Celem wyszukiwania odpowiednich ofiar, sprawcy obecnie

najczęściej nawiązują kontakt z dzieckiem (ofiarą) na portalach społecznościowych. Dzieci w cyberprzestrzeni tracą ograniczenia i nie są świadome wszelkich niebezpieczeństw.

Dzieci nie są w stanie rozpoznać niebezpieczeństw, które zagrażają im w internecie, i z tego wynikają również możliwe negatywne następstwa. Dają się skusić i namówić do wysyłania swoich zdjęć erotycznych. (tzw. SEXTING).

Dzieci same i dobrowolnie udostępniają materiały o charakterze erotycznym, które mogę być przeciwko nim wykorzystane. Często zrobią sobie zdjęcia i nakręcą filmy w seksualnie pobudzających pozycjach, i materiał taki bez głębszej znajomości prawa czeskiego oraz standardowych zasad bezpiecznego zachowania przesyłają za pośrednictwem internetu do drugiej strony, którą w większości przypadków znają właśnie tylko z internetu. Materiały te w znacznej większości przypadków krążą w internecie przez kilka lat, a ich zupełne usunięcie jest praktycznie niemożliwe.

Osoby rozpowszechniające „sexting“ (same dzieci) często stają się sprawcami przestępstwa (rozpowszechnianie pornografii dziecięcej, zagrożenie dla wychowania moralnego dzieci itd.).

Zdjęcia dzieci starają się za pośrednictwem portali społecznościowych poprzez wyspecjalizowane działanie pozyskać sprawcy pełnoletni. W szczególności chodzi o pedofilów, którzy następnie zdjęcia udostępniają kolejnym pedofilom w ramach swoich społeczności lub wykorzystują je do naciskania na ofiarę, celem uzyskania kolejnych zdjęć.

Cyber grooming co prawda nie jest przestępstwem, jednak stanowi przemyślane działanie sprawcy, który najczęściej manipuluje dziecięcą ofiarą w celu umówienia spotkania i wykorzystania seksualnego lub uszkodzenia ciała. Cyber grooming jest jednak ściśle związany z przestępstwem „Nakłanianie do stosunku płciowego“. Sprawcy na portalach społecznościowych, a następnie również w komunikacji prywatnej w ramach programów komunikacyjnych technologii informatycznych przechodzą na prywatny chat, lub do zamkniętych pokojów. Następnie starają się ofiarę namówić do rozbierania przed kamerką internetową, samozaspokajania i następnie również oferują odpłatny stosunek płciowy.

Ogólnie można stwierdzić, iż właśnie portale społecznościowe w ostatnich latach stanowią z punktu widzenia nawiązywania nowych znajomości pewien fenomen. W dużej mierze pomagają one dzieciom z socjalizacją w społeczeństwie. Za pośrednictwem internetu, względnie portali społecznościowych oraz chatów, starają się one nawiązać znajomości z kolejnymi rówieśnikami, i nie są one świadome wszelkich niebezpieczeństw, które im w związku z takimi działaniami zagrażają.

CYBERPRZEMOC. Termin ten często stosowany jest przez media. Cyberprzemoc jest stosunkowo specyficznym rodzajem gnębienia, który jako narzędzie wykorzystuje środki elektroniczne (np. telefon komórkowy, e-mail, portale społecznościowe itd.). Jego celem, tak jak w przypadku klasycznego gnębienia, jest wyrządzenie komuś krzywdy, skrzywdzenie publiczne, ośmieszenie. W większości przypadków jest to wykroczenie lub inny delikt administracyjny (regulaminy szkolne itd.) Czeski kodeks karny pojęcia **Cyberprzemocy** nie zna. W przypadku podejrzenia, iż zostało popełnione przestępstwo, należy pracować z konkretnymi czynami zabronionymi stosownie do okoliczności. Na przykład naruszanie praw innej osoby, pomówienie, groźby karalne, uporczywe nękanie.

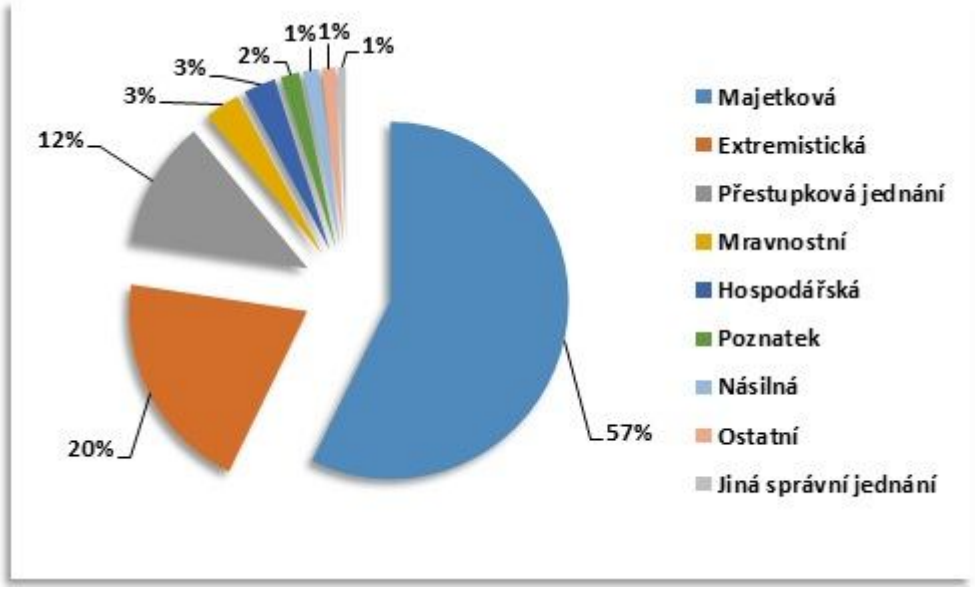
Statystyki odnoszące się do internetu i dzieci (wiek do lat 18-tu)

Spáchané mravnostní tr. činy na dětech 0-18 let prostřednictvím internetu a počít. sítí za r. 2014 a 2015		
paragraf	rok 2014	rok 2015
§ 185-znásilnění	0	1
§ 186-sexuální nátlak	6	35
§ 187-pohlavní zneužívání	1	1
§ 191-šíření pornografie	8	5
§ 192-výroba a jiné nakládání s dětskou pornografií	23	11
§ 193-zneužití dítěte k výrobě pornografie	29	32
	67	85

Przestępstwa przeciwko wolności seksualnej i obyczajności popełnione wobec dzieci w wieku 0-18 lat za pośrednictwem internetu i sieci komputerowych w latach 2014 i 2015		
paragraf	**2014 rok**	**2015 rok**
§ 185 - zgwałcenie	0	1
§ 186 – przymus seksualny	6	35
§ 187 – wykorzystanie seksualne	1	1
§ 191 – rozpowszechnianie pornografii	8	5
§ 192 – produkowanie oraz inne działania związane z pornografią dziecięcą	23	11
§ 193 – wykorzystanie dziecka do produkcji pornografii	29	32
	67	85

W statystykach przedstawiono rozpowszechnianie pornografii dziecięcej, którego sprawcami są oczywiście w znacznej większości przypadków osoby pełnoletnie. Dziecko traktowane jest jako ofiara, aczkolwiek nie jako ofiara (wykorzystanie fizyczne) samego sprawcy – osoby rozpowszechniającej nielegalne zdjęcia lub filmy.

Od 1 sierpnia 2012 roku na stronie internetowej **www.pcr.cz** działa policyjna internetowa linia HotLine, która służy do zgłaszania nielegalnych treści i działań w internecie. W 2015 roku za pośrednictwem formularza – służącego do zgłaszania nielegalnych treści i działań w internecie, przyjęto **łącznie 3 173 zgłoszeń**. Zgłoszenia dotyczą łącznie 9 obszarów, które wskazują na ich możliwą klasyfikacją prawnokarną, w tym wykroczenia. W 2015 roku najliczniejszą grupę stanowił obszar czynów przeciwko mieniu, powodem było przede wszystkim przesunięcie wiadomości mailowych przesyłanych przez oszustów do tego właśnie obszaru, co wynikało z przewidywanej kwalifikacji prawnej takiego działania stosownie do przepisów kodeksu karnego. *Zob. poniższy graf.*



Obr.kolejno: czyny przeciwko mieniu, ekstremistyczne, wykroczenia, przeciwko wolności seksualnej i obyczajności, gospodarcze, powzięcie wiedzy o przestępstwie, przemoc, pozostałe, inne przewinienia administracyjne

Z powyższego grafu wynika, iż najliczniejszą grupę stanowiły zgłoszenia dotyczące czynów przeciwko mieniu. Od połowy 2010 roku do końca 2015 roku odnotowano łącznie 15 202 zgłoszeń HotLine.

Niektóre przykłady cyberprzestępczości w Województwie Libereckim:

1. *Prokuratura Powiatowa w Libercu prowadziła postępowanie karne w sprawie bezprawnego dostępu do systemu komputerowego oraz nośnika informacji, tj. czyn zabroniony z § 230 ustęp 1, ustęp 2, litera a), ustęp 3 kodeksu karnego, naruszenia poufności pism oraz innych dokumentów przechowywanych prywatnie, tj. czyn z § 183 ustęp 1, ustęp 2 kodeksu karnego, oraz występek naruszenia prawa autorskiego, praw pokrewnych oraz praw do bazy danych, tj. czyn z § 270 ust. 1 kodeksu karnego, popełnionych czterokrotnym atakiem* ***DDoS*** *przez nieznanego sprawcę w dniach 6.9.2016r., 8.9.2016r., 2. 10. 2016r. oraz 16.10.2016r. przy użyciu pakietów danych z różnych IP adresów na serwer oraz router spółki C. s.r.o. Serwer został przeciążony a spółka nie mogła świadczyć usług telekomunikacyjnych (internet, telewizja kablowa oraz połączenia telefoniczne VOIP) na rzecze 7.500 swoich klientów. Szkoda 2 x 30.000,--CZK (2 x 1045 €, względnie 2 x 4771 złotych); postępowanie karne zawieszono z powodu nie ustalenia sprawcy.*

2. *w sprawie występków szantażu, tj. czyn z § 175 ust. 1 kodeksu karnego, oraz bezprawnego dostępu do systemu komputerowego oraz nośnika informacji, tj. czyn z § 230 ust. 2, lit., oraz, ust. 3, lit. a) kodeksu karnego, postępowanie prowadzi*

    - *Prokuratura Powiatowa w Semilach w sprawie nieznanego sprawcy, który w dotychczas nie ustalony sposób spowodował aktywację szkodliwego malware (wirusa) szyfrującego typu Ransomware na komputerze roboczym poszkodowanej A. K.F., poprzez zaszyfrowanie plików znajdujących się na dysku twardym, zawierających przede wszystkim księgi rachunkowe, które*

poszkodowana prowadziła dla co najmniej 5 podmiotów gospodarczych. Za odszyfrowanie zakodowanych plików sprawca domaga się 3 bitcoinów (1 bitcoin =ok. 18 727 CZK, tj. 698 € lub 298 PLN).

- *Prokuratura Powiatowa w Libercu w sprawie nieznanego sprawcy, który w 2016 roku przy użyciu przeglądarki internetowej Mozilla Firefox oraz programu SQLMap, dokonał ataku przeciwko zabezpieczonemu serwerowi zawierającemu przeglądarki oraz bazy danych spółki A. s.r.o z siedzibą w Pradze, a po ustaleniu słabego punktu serwera wstąpił do serwera baz danych spółki, z którego pobrał bazę danych wszystkich klientów spółki, a następnie z poczty elektronicznej przesłał na mail serwera spółki znajdującego się na terenie Szwajcarii wiadomość mailową w celu anonimowej zaszyfrowanej komunikacji w sieci internet bez jakiejkolwiek możliwości identyfikacji nadawcy i jego dostępu do usługi, na adres mailowy rostislav.peniska@adrop.cz (prezes zarządu spółki Adrop s. r. o.) o treści: "posiadam kompletną bazę danych .... o ile nie chce Pan, aby została ona opublikowana, proszę przesłać 3 BTC (w przeliczeniu 44.283,522 CZK, czyli 1640 € lub 7044 PLN)) na ... ma Pan 2 dni!" i jako dowód załączył fragment bezprawnie pozyskanej bazy danych. Żądana kwota nie została do chwili obecnej wypłacona.*

3. *w sprawie występków produkowania oraz innych działań związanych z pornografią dziecięcą, tj. czyn z § 192 ust. 1, ust. 2 kodeksu karnego – powtarzalne wchodzenie na strony z pornografią dziecięcą, Prokuratura Powiatowa w Libercu prowadzi postępowanie karne w dwóch sprawach; w jednej sprawie postępowanie prowadzi Prokuratura Powiatowa w Jabloncu nad Nisą. Postępowanie karne nadal trwa, pozyskiwane są dowody, również na drodze pomocy prawnej.*

4. *Prokuratura Powiatowa w Jabloncu nad Nisą prowadzi postępowanie karne w sprawie łącznie 13 ataków w formie **Phishingu**, w ramach których sprawcy, którzy podawali się za spółkę PayPal, pod pretekstem zweryfikowania danych dostępu do kont prowadzonych spółką PayPal, pozyskali do zalogowania, a ponieważ poszkodowani posiadali do swych rachunków zweryfikowane karty płatnicze, sprawcy dokonali następujących bezprawnych płatności: na szkodę pana F.K. w łącznej w kwocie 2.170,00CZK (80€, czyli 345 PLN), pana H.K. w łącznej w kwocie 8.432,00 CZK (300€, czyli 1341 PLN), pani J.P. 2.847 CZK (105 €, czyli 452 PLN), pani Š. M. 1.173,00 CZK (43€, czyli 186 PLN); pani B.M. 1.973 CZK (73 €, czyli 314 PLN); w niektórych przypadkach adresem do doręczeń znajdował się w południowym Libanie; osoby, które miały ustawione przesyłanie kodów za pośrednictwem wiadomości SMS i nie wysłali jej, nie zostali poszkodowani.*

ZAŁĄCZNIK nr 1:

Adresy organów centralnych wskazanych stosownie do przepisu artykułu 27 ust. 2 lit. a) Konwencji o cyberprzestępczości:

Prokuratura Naczelna Republiki Czeskiej, Jezuitská 4, 660 55 Brno, Republika Czeska, Telefon: +420 542 512 330; Fax: +420 542 512 350; E-mail: podatelna@nsz.brn.justice.cz

Ministerstwo Sprawiedliwości Republiki Czeskiej, Vyšehradská 16, 128 10 Praha 2, Republika Czeska, Telefon: +420 221 997 435, Fax: +420 221 997 986, E-mail: mot@msp.justice.cz

Punktem kontaktowym stosownie do artykułu 35 Konwencji o cyberprzestępczości na terenie Republiki Czeskiej jest:

Prezydium Policji Republiki Czeskiej, Sekcja Kryminala i Śledcza, Wydział Przestępczości Komputerowej, Strojnická 27, P.O.Box 62/KPV, 170 89 Praha 7, Republika Czeska,
Kontakt w godzinach pracy (7:30 - 15:30): Telefon: +420 974 834 550; Tel. kom.: +420 603 190 057; Fax: +420 974 834 708; E-mail: contact@mvcr.cz;
Kontakt poza godzinami pracy (czynne 24/7):telefon: +420 974 834 380, Fax: +420 974 834 716, E-mail: contact@mvcr.cz".

ZAŁĄCZNIK nr 2

ZNAMIONA PRZESTĘPSTW „KOMPUTEROWYCH“ W KODEKSIE KARNYM REPUBLIKI CZESKIEJ

§ 230
Bezprawny dostęp do sieci komputerowej oraz nośnika informacji

(1) Kto złamie środek zabezpieczający, i uzyska w ten sposób dostęp do systemu komputerowego lub jego części, podlega karze pozbawienia wolności do lat dwóch, zakazu działalności lub przepadku rzeczy.

(2) Kto uzyska dostęp do systemu komputerowego lub nośnika informacji oraz

a) bezprawnie wykorzysta dane zapisane w systemie komputerowym lub na nośniku informacji,
b) bezprawnie dokona usunięcia lub innego zniszczenia, uszkodzenia, zmiany, zablokowania, obniżenia jakości lub uczyni bezużytecznymi dane zapisane w systemie komputerowym lub na nośniku informacji,
c) fałszuje lub dokona modyfikacji danych zapisanych w systemie komputerowym lub na nośniku informacji w taki sposób, aby uważane były one za autentyczne lub aby na ich podstawie działano w taki sposób, jakby były one autentyczne, bez względu na to, czy dane te są bezpośrednio czytelne i zrozumiałe, lub
d) bezprawnie wprowadzi dane do systemu komputerowego lub na nośnik informacji lub dokona innej ingerencji w wyposażenie programowe lub techniczne komputera lub innego urządzenia technicznego służącego do przetwarzania danych,
podlega karze pozbawienia wolności do lat trzech, zakazu działalności lub przepadku rzeczy.

(3) Karze pozbawienia wolności od sześciu miesięcy do lat czterech, zakazu działalności lub przepadku rzeczy, podlega sprawca, jeżeli czyn określony w ustępie 1 lub 2 popełni

a) z zamiarem wyrządzenia innej osobie szkody lub innego uszczerbku lub z zamiarem osiągnięcia bezprawnej korzyści dla siebie lub na rzecz innej osoby, lub
b) z zamiarem bezprawnego ograniczenia działania systemu komputerowego lub innego urządzenia technicznego służącego do przetwarzania danych.

(4) Karze pozbawienia wolności od jednego roku do lat pięciu lub karze grzywny podlega sprawca,

a) który popełni czyn określony w ustępie 1 lub 2 jako członek zorganizowanej grupy przestępczej,
b) który takim czynem wyrządzi znaczną szkodę,
c) który takim czynem spowoduje poważne naruszenie w działaniu organu administracji rządowej, administracji samorządowej, sądu lub innego organu władztwa publicznego,
d) jeżeli w wyniku popełnienia takiego czynu uzyska dla siebie lub innej osoby znaczną korzyść, lub
e) jeżeli w wyniku popełnienia takiego czynu spowoduje poważne zaburzenie w funkcjonowaniu osoby prawnej lub fizycznej, która jest przedsiębiorcą.

(5) Karze pozbawienia wolności od lat trzech do lat ośmiu sprawca podlega,
a) jeżeli w wyniku popełnienia czynu określonego w ustępie 1 lub 2 wyrządzi szkodę o dużym rozmiarze, lub
b) jeżeli w wyniku popełnienia takiego czynu uzyska dla siebie lub dla innej osoby korzyść o dużym rozmiarze.

§ 231

Środki oraz przechowywanie urządzenia dostępowego oraz hasła do systemu komputerowego ora innych podobnych danych

(1) Kto z zamiarem popełnienia przestępstwa naruszenia poufności przesyłanych danych określonego w § 182 ust. 1 lit. b), c) lub przestępstwa bezprawnego dostępu do systemu komputerowego lub nośnika informacji określonego w § 230 ust. 1, 2 wyprodukuje, wprowadzi na rynek, dokona importu, eksportu, tranzytu, oferuje, umożliwi dostarczenie, sprzeda lub w inny sposób udostępni, dla siebie lub dla innej osoby, dokona nabycia lub przechowania

a) urządzenia lub jego części, procedury, narzędzia lub jakiegokolwiek innego środka, w tym programu komputerowego, utworzonego lub dostosowanego do bezprawnego dostępu do do sieci komunikacji elektronicznych, do systemu komputerowego lub do jego części, lub
b) hasła komputerowego, kodu dostępu, danych, procedury lub jakiegokolwiek innego podobnego środka, przy pomocy którego możliwe jest uzyskanie dostępu do systemu komputerowego lub jego części,

podlega karze pozbawienia wolności do lat dwóch, przepadku rzeczy lub zakazu działalności.

(2) Karze pozbawienia wolności do lat trzech, zakazu działalności lub przepadku rzeczy podlega sprawca,

a) który popełni czyn określony w ustępie 1 jako członek zorganizowanej grupy przestępczej, lub
b) jeżeli w wyniku popełnienia takiego czynu uzyska dla siebie lub dla innej osoby korzyść o dużym rozmiarze.

(3) Karze pozbawienia wolności od sześciu miesięcy do lat pięciu podlega sprawca, który w wyniku popełnienia czynu określonego w ustępie 1 uzyska dla siebie lub dla innej osoby korzyść o dużym rozmiarze.

§ 232

Uszkodzenie zapisu w systemie komputerowym oraz na nośniku informacji i ingerencja w wyposażenie komputera w wyniku niedbalstwa

(1) Kto w wyniku rażącego niedbalstwa poprzez naruszenie obowiązków wynikających ze stosunku pracy, zawodu, stanowiska lub funkcji, lub obowiązków nałożonych przez ustawę lub przejętych na mocy umowy

a) dokona zniszczenia, uszkodzenia, modyfikacji lub uczyni bezużytecznymi dane zapisane w systemie komputerowym lub na nośniku informacji, lub
b) dokona ingerencji w wyposażenie programowe lub techniczne komputera lub innego urządzenia technicznego służącego do przetwarzania danych,

i w wyniku tego wyrządzi na majątku obcej osoby szkodę znacznych rozmiarów, podlega karze pozbawienia wolności do sześciu miesięcy, zakazu działalności lub przepadku rzeczy.

(2) Karze pozbawienia wolności do lat dwóch, zakazu działalności lub przepadku rzeczy podlega sprawca, który w wyniku popełnienia czynu określonego w ustępie 1 wyrządzi szkodę o dużym rozmiarze.