PROTEGERE ET PRODESSE VIII

Tomasz Pączkowski

Słownik cyberbezpieczeństwa

SZKOŁA POLICJI KATOWICE

PROTEGERE ET PRODESSE | VIII

Tomasz Pączkowski

Słownik cyberbezpieczeństwa

Katowice 2017

Tomasz Pączkowski

Słownik cyberbezpieczeństwa

Redakcja:
insp. dr Rafał Kochańczyk
Paweł Mięsiak

Projekt graficzny, skład i przygotowanie do druku:
Paweł Mięsiak

Druk:
Drukarnia Kolumb, Chorzów

Wydawca: Szkoła Policji w Katowicach

ISBN 978-83-934380-5-1

Katowice, 2017 r.

Spis treści

Wprowadzenie

Prawidłowością współczesnych czasów jest to, że coraz więcej elementów ludzkiej działalności przenosi się do sieci komputerowej. Bankowość, handel wymiana informacji oraz wiele innych dziedzin nie są obecnie możliwe bez Internetu. Także przestępcy w dużej mierze przenieśli tam swój proceder.

W codziennej służbie policjanci coraz częściej spotykają się z wirtualną przestępczością, dlatego powinni posiadać odpowiedni zasób wiedzy i umiejętności, aby radzić sobie w takiej sytuacji. Nowoczesny policjant musi odznaczać się nie tylko sprawnością umysłową i fizyczną, musi także sprawnie poruszać się w sieci, wykorzystując jej możliwości i poprawnie identyfikując jej zagrożenia. Bez tego nie będzie w stanie odpowiednio wykonywać swoich obowiązków.

Oczywiście nie każdy funkcjonariusz może od razu zdobyć umiejętności programisty, jednak istnieje pewien podstawowy zakres zagadnień i informacji, który pozwoli mu na wykrycie i zidentyfikowanie działalności kryminalnej w sieci.

W tym celu realizowany jest już w Policji szeroki program adekwatnych szkoleń. Warto jednak pomyśleć również o podręcznej pomocy dla spotykającego się z przestępczością komputerową policjanta.

Trzeba pamiętać również, że stałe podnoszenie kwalifikacji jest istotnym warunkiem awansu zawodowego każdego funkcjonariusza Policji.

Dlatego właśnie autor zgromadził zbiór objaśnień przydatnych terminów związanych z Internetem i cyberprzestępczością. Kompendium to z pewnością nie wyczerpuje wszystkich zagadnień dotyczących wspomnianej tematyki, niemniej powinno pozwolić na lepsze zrozumienie przez policjantów Internetu i przestępczości w nim występującej.

Jeśli czytelnicy napotkają inne terminy, które ich zdaniem powinny się znaleźć w słowniku, bardzo proszę o ich przesyłanie, tak aby uzupełnić jego zawartość i aby mógł być jak najbardziej przydatny w Waszej ciężkiej i odpowiedzialnej służbie.

Co to jest cyberprzestrzeń?

Każdy ludzki wynalazek i każda nowa technologia na przestrzeni wieków bardzo szybko po ich wdrożeniu znajdowały odbiorców, którzy wykorzystywali je niezgodnie z pierwotnym przeznaczeniem lub nawet dla celów przestępczych.

Wraz z pojawieniem się technologii informatycznych i ich udostępnieniem do celów badawczych i obliczeniowych koniec XX i początek XXI wieku były okresami, kiedy upowszechnienie tej technologii, a zwłaszcza budowa sieci (Internetu) doprowadziły do lawinowego wzrostu znaczenia informatyki we wszystkich dziedzinach życia ludzkiego. Współczesny świat podąża w kierunku gospodarki elektronicznej i społeczeństwa informacyjnego. Największe szanse na znalezienie zatrudnienia mają osoby umiejące skutecznie wykorzystać narzędzia dzisiejszej informatyki dla rozwoju firm. Umiejętność korzystania z komunikatorów internetowych dla współczesnej młodzieży określa często ich pozycję w grupie społecznej. Często używane jest strywializowane powiedzenie: kogo nie ma w Internecie, ten nie istnieje.

Określenia „cyberprzestrzeń" (według niepotwierdzonych informacji) jako pierwszy w 1984 roku użył w swojej powieści „Burning Chrome" amerykański pisarz William Gibson. Był to stworzony przez komputer świat wirtualnej rzeczywistości, którą amerykański klasyk cybernetycznych powieści w pierwszym tomie swojej Trylogii – Neuromancer – nazywał też matrycą (*matrix*). [50]

Nawiązanie to nie było zresztą zbyt ścisłe, ponieważ cybernetyka w matematycznej teorii optymalizacji jest teoretycznym studium kontroli i komunikacji w maszynach i żywych organizmach. Teoria ta znajduje zastosowanie w tak różnych dziedzinach, jak teoria sieci nerwowych, teoria komunikacji i percepcji, komputery, serwomechanizmy, zautomatyzowane systemy regulacji.

Pomimo wspomnianych wyżej wątpliwości semantycznych przedrostek „cyber-" dla zagadnień związanych z technologiami informatycznymi upowszechnił się w informacji prasowej i obecnie pod pojęciem cyberzagrożeń rozumie się wszelkie niebezpieczeństwa związane z używaniem Internetu.

Zagrożenia dla komputera i urządzeń mobilnych

We współczesnym świecie istnieje wiele klasyfikacji zagrożeń, obejmujących następujące elementy:

- **wirusy**, czyli programy, które zarażają (uszkadzają) inne programy poprzez dodanie do nich swojego kodu w celu uzyskania dostępu do zawartości komputera przy uruchamianiu zainfekowanego pliku;
- **robaki** – to szkodliwe oprogramowanie, które do rozprzestrzeniania się wykorzystuje zasoby sieci. Klasa ta nazwana została robakami z powodu jej specyficznego działania przypominającego „pełzanie" z komputera na komputer przy korzystaniu z sieci, poczty elektronicznej i innych kanałów informacyjnych. Dzięki temu tempo rozprzestrzeniania się robaków jest bardzo szybkie;
- **konie trojańskie (trojany)** – to programy, które wykonują na zainfekowanych komputerach niekontrolowane przez użytkownika działania, tj. w zależności od warunków mogą usuwać informacje z dysków, powodować stany bezczynności systemu, wykradać prywatne dane itp.;

- **crimeware** – to program szpiegujący gromadzący poufne dane użytkownika komputera, umożliwiające uzyskanie dostępu do rachunków bankowych lub usług finansowych. Celem jest kradzież pieniędzy albo wykonanie niedozwolonych transakcji;
- **bundleware** – sposób dystrybucji oprogramowania przez dołączenie go do innego, popularnego programu. W ten sposób rozpowszechniane są także programy szpiegujące, a nieświadomi użytkownicy sami je instalują.
- **policeware** – określenie na oprogramowanie szpiegujące używane przez organy policyjne państwa lub agencje rządowe mające na celu walkę z przestępczością, np. terroryzmem. Zazwyczaj policeware narusza prywatność komputerów przez zapis wszelkich czynności dokonywanych na danym komputerze lub w danej sieci. Krajami, które podejrzewane są o stosowanie policeware lub je stosują są Izrael, Niemcy i Chiny;
- **snoopware** (ang. *to snoop* – wtykać nos) – oprogramowanie śledzące działania użytkownika komputera, służące szczególnie do monitorowania zachowań pracowników firmy, dzieci w domu itd. Snoopware działa w ukryciu i rejestruje uderzenia w klawisze, a także przechwytuje ekrany, pozwalając osobie kontrolującej sprawdzać, czym się zajmuje użytkownik komputera. Niektóre programy wysyłają także raporty za pomocą poczty elektronicznej. Do snoopware zalicza się keyloggery i cybernianie;
- **spyware** – to oprogramowanie, które pozwala na zbieranie danych na temat konkretnego użytkownika lub organizacji, która nie jest tego świadoma. Ofiara jest całkowicie nieświadoma obecności spyware na komputerze;
- **riskware** – to oprogramowanie, które nie jest wirusem, ale zawiera w sobie potencjalne zagrożenie. W niektórych warunkach obecność riskware na komputerze oznacza zagrożenie dla zapisanych danych;
- **jokes** – to oprogramowanie, które nie szkodzi, ale komputer wyświetla wiadomości, że szkodnik już spowodował uszkodzenie lub je spowoduje. Często ostrzega użytkownika o istniejącym niebezpieczeństwie, np. wyświetla komunikaty o formatowaniu dysku twardego (choć formatowanie nie jest wykonywane), wykrywa wirusy w niezainfekowanych plikach itp.;
- **rootkit** – są to narzędzia wykorzystywane do ukrywania złośliwego działania. Ukrywane są przez złośliwe oprogramowanie, aby uniknąć wykrycia przez aplikacje antywirusowe;
- **spam** – to anonimowa, niepożądana masowa korespondencja pocztowa. Spam jest odbieraną wiadomością polityczną lub propagandową zawierającą prośby o pomoc. Inną kategorią spamu są również wiadomości oferujące wygranie wielkiej sumy pieniędzy, a maile służą do kradzieży haseł i numerów kart kredytowych. [58]

Dodatkowo niebezpieczeństwo związane z wirusami potęguje się poprzez upowszechnienie komunikacji pomiędzy komputerami a urządzeniami przenośnymi (smartfonami, tabletami), gdzie wirusy mogą się rozprzestrzeniać dzięki Wi-Fi lub Bluetooth. Nie należy zapominać także o każdorazowym skanowaniu pamięci pendrive przy podłączaniu jej do komputera. Także w ten sposób można łatwo zainfekować swój komputer.

A

Adres IP

Można stwierdzić, że jest to rodzaj „numeru rejestracyjnego" komputera lub innego urządzenia w sieci. Adres ten nie identyfikuje go jednak jednoznacznie, ponieważ może się zmieniać, np. podczas każdego wejścia do Internetu (adres przydzielany dynamicznie, dynamiczne IP, ang. *dynamic IP*). Kilka urządzeń może występować w sieci pod jednym, publicznym adresem IP (urządzenia te muszą mieć wtedy różne adresy IP wewnątrz sieci).

Adware

Dokuczliwe aplikacje reklamowe, które po zainstalowaniu (świadomym lub nie) zaczynają eksponować na ekranie komputera komunikaty promocyjne. Niestety te reklamy są zwykle bardzo kłopotliwe – potrafią wklejać się w strony internetowe w miejscach, w których ich wcześniej nie było. Często też „towarzyszą" otwieranym zakładkom w przeglądarce. Niektóre adware zmieniają stronę startową, czyli tę, która zawsze otwiera się jako pierwsza po włączeniu programu. Najbardziej fałszywe aplikacje reklamowe umieją modyfikować wyniki wyszukiwania, dodając własne linki. [59] Po kliknięciu w taki odsyłacz może się zdarzyć, że na dysk twardy zacznie się ściągać niebezpieczny wirus.

Anonimizacja

Jest to proces (działanie) uniemożliwiający odkrycie tożsamości użytkownika sieci. W informatyce nazywamy tak postępowanie uniemożliwiające odkrycie tożsamości użytkownika sieci komputerowej. Nazywamy tym pojęciem również proces w informatyce, który ma na celu ukrycie, zaszyfrowanie danych użytkownika sieci.

Archive bomb

Jest to odmiana wirusa. Wygląda jak niewielki plik spakowany archiwizerem (zip, rar itp.), który po rozpakowaniu okazuje się jednym lub kilkoma wielkimi plikami. Prowadzi to do zablokowania wolnego miejsca na dysku, a ponieważ skanowanie takich archiwów przeciw występowaniu w nich wirusa trwa bardzo długo, potencjalnie stanowią one atak DDoS na program antywirusowy, który podejmuje próbę ich skanowania. Dobre programy antywirusowe zawierają niewielki algorytm, który pozwala uniknąć rozpakowywania takich plików. [32]

AstalaVista

Nazwa domeny służącej zwykle jako miejsce gromadzenia i publikacji materiałów związanych z bezpieczeństwem sieci komputerowych. Dwiema najstarszymi (obecnie już niedziałającymi) domenami tego typu były:

- astalavista.box.sk – wyszukiwarka serwisów internetowych dotyczących bezpieczeństwa;

- Astalavista Security Group – serwis internetowy na temat bezpieczeństwa komputerowego wykorzystujący adresy astalavista.com oraz jako portal członkowski astalavista.net.

Jest to również w powszechnej świadomości miejsce pozwalające znaleźć pliki z najnowszymi crackami.

B

Backdoor (ang. tylne drzwi, furtka)

Luka w zabezpieczeniach systemu operacyjnego wykreowana świadomie w celu późniejszego wykorzystania. Backdoor w systemie może być np. pozostawiony przez programistę/autora piszącego program albo crackera, który włamał się przez inną lukę w oprogramowaniu (której przydatność jest ograniczona czasowo do momentu jej usunięcia) bądź poprzez podrzucenie użytkownikowi konia trojańskiego. [20]

Blacklista lub shitlista

Spis nicków czyli pseudonimów (nazw), pod którymi nie można się zarejestrować do programu, choćby był wygenerowany według prawdziwego algorytmu. Autorzy programów wykorzystują tego typu metody, chcąc zabezpieczyć się przed najbardziej znanymi crackerami, udostępniającymi kody rejestrujące program na ich nick. Taką listę zakazanych pseudonimów posiada większość programów. [86]

Backup

Inaczej kopia bezpieczeństwa albo kopia zapasowa plików. Jest ona tworzona na różnych nośnikach danych (tzw. „chmura" – dysk sieciowy, serwery, dyski przenośne, pendrive, płyty CD/DVD itp.) w celu zabezpieczenia danych przed utratą.

Bitcoin

Bitcoin to powstała w Internecie pseudowaluta. Funkcjonuje jako waluta rozproszona, czyli bez centralnej instytucji emisyjnej, niezależna od banków, rządów i instytucji. Wykorzystywany może być między internautami do rozliczeń międzynarodowych, dostępny praktycznie dla każdego mającego dostęp do Internetu (lub telefonu komórkowego). Bitcoin jest walutą, którą można szybko wysłać do dowolnego miejsca na świecie z ominięciem banków i pośredników, a co za tym idzie kosztownych prowizji, limitów i ograniczeń. [5]

Blockchain

Technika określana jako blockchain pozwala na gromadzenie i rozpowszechnianie informacji na temat transakcji zawieranych w Internecie. Transakcje transferowane są w postaci następujących po sobie bloków danych. Każdy z nich zawiera informacje o konkretnie sprecyzowanej liczbie transakcji.

Po wypełnieniu jednego bloku informacjami o transakcjach, tworzony jest kolejny, a za nim następne. W ten sposób powstaje pewnego rodzaju łańcuch (stąd nazwa: *blockchain* – to łańcuch bloków). Nowy blok powstaje średnio co 10 minut. Mogą one zawierać informacje na temat różnych transakcji, np. handlowych, o stanach własności, udziałach, akcjach, wytworzeniu energii elektrycznej oraz kupnie lub sprzedaży walut, w tym kryptowalut, czyli walut elektronicznych. [6]

Blokowanie usług sieciowych oraz komputerów (inaczej spam)

Odbywa się poprzez przesyłanie na wybrany adres setek tysięcy pakietów IP lub listów e-mail. Aby nie pozwolić zablokować pracy naszego komputera masowo przesyłanym wiadomościom, należy przestrzegać w prowadzonej korespondencji wymienionych niżej zasad:

- nie podawajmy bez potrzeby swojego adresu e-mail innym (np. jeśli podajesz swój adres e-mail na stronach internetowych sprawdź jakie obowiązują na nich zasady prywatności, do czego może być on użyty), a także chroń adresy innych;
- zabezpieczaj swój adres e-mail, gdy podajesz go na stronie internetowej przed programami (harvesterami) zbierającymi adresy e-mail, czyli podaj go w postaci niezrozumiałej dla automatów, np. przez: użycie grafiki;
- używaj formularza zamiast adresu e-mail;
- wyposaż się w co najmniej dwa adresy e-mail, jeden „prywatny" (podawany tylko zaufanym osobom), zaś drugi „publiczny" najlepiej na darmowym serwerze;
- nie wysyłaj spamu czy też wiadomości, które mogą być potraktowane jak spam (np. zrezygnuj z przekazywania popularnych listów łańcuszkowych). [11]

Przejawem walki ze spamem w Internecie była uchwalona przez polski Sejm w 2002 roku ustawa o świadczeniu usług drogą elektroniczną. Tym problemem zajął się również Prezes Urzędu Ochrony Konkurencji i Konsumentów. Warto jednak pamiętać, że nigdzie na świecie nie udało się zlikwidować, a nawet zdecydowanie ograniczyć tego zjawiska.

Bluesnarfing

Technika nielegalnego pozyskiwania danych z wykorzystaniem technologii Bluetooth. Najczęściej osoby prowadzące bluesnarfing wykorzystują przenośne urządzenia elektroniczne, tj. laptop, tablet, palmtop, smartfon, telefon komórkowy. Osoba próbująca dostać się do danych w innym urządzeniu wysyła ofierze wiadomość za pośrednictwem technologii Bluetooth, najczęściej w postaci wizytówki w formacie vCard. Odbiorca otrzymuje wiadomość (bez wymaganej zgody na odbiór), a jej tekst zwykle automatycznie pojawia się na ekranie (np. „Problemy z logowaniem. Wpisz pin 1111"). Następnie napastnik włącza odpowiednią aplikację pozwalającą na zdalny dostęp do innego urządzenia wyposażonego w Bluetooth po wpisaniu tego samego PIN-u, który wysłany został w wiadomości. Ofiara, wpisując ten numer, może narazić się na utratę danych. [11]

Bluejacking

Wysyłanie masowych i nieoczekiwanych wiadomości przy pomocy Bluetooth do urządzeń znajdujących się w zasięgu. Bluejacking jest możliwy podczas tzw. parowania urządzeń, ponieważ nazwa urządzenia rozpoczynającego połączenie jest wyświetlana na urządzeniu docelowym w trakcie skanowania i wyszukiwania dostępnych urządzeń. Ponieważ pole z nazwą urządzenia może mieć długość maksymalnie 248 znaków, dlatego za jego pośrednictwem można przesyłać krótkie wiadomości. Można uznać bluejacking za rodzaj spamu rozsyłanego za pośrednictwem Bluetooth. [86]

Bluebugging

Atak przeprowadzony na telefon komórkowy z wykorzystaniem technologii Bluetooth, który umożliwia hakerowi wykonywanie rozmów telefonicznych, wysyłanie wiadomości SMS, odczytywanie i zapisywanie kontaktów w książce adresowej czy też łączenie się z Internetem. [11]

Blue box

Urządzenie wymyślone, zbudowane i stosowane przez pierwszych phreakerów (hackerów telefonicznych) do uzyskiwania darmowych (nielegalnych) połączeń telefonicznych. Działanie blue box odbywa się poprzez generowanie tonów identycznych do stosowanych przez firmy telekomunikacyjne (częstotliwości około 2600 Hz), co pozwala, by phreaker mógł przejąć sterowanie nad centralą telefoniczną i uzyskać połączenie z dowolnym wybranym numerem telefonu na całym świecie. Czasy największej popularności blue box przypadają na lata 70. i początek 80. XX wieku, a dziś ma on już znaczenie raczej zamierzchłe. Nie są potwierdzone przypadki jego wykorzystania w Polsce. Blue box było pierwszym z tego rodzaju urządzeń i zapoczątkowało serię podobnych „kolorowych pudełek": red box, black box, violet box, silver box etc. [8]

BotNet

Potoczna nazwa sieci komputerów-zombie, czyli komputerów pozostających pod kontrolą hakerów z wykorzystaniem wirusów, koni trojańskich itp. Według statystyk ok. 1/3 komputerów w Internecie to sprzęt, nad którym kontrolę przejęli hakerzy. Użytkownik komputera-ofiary zwykle nie ma o tym pojęcia. Komputery wchodzące w skład BotNetu wykorzystywane są najczęściej do przeprowadzania ataków typu DoS lub do wysyłania spamu. Aby uchronić się przed opanowaniem komputera przez hackera i dołączenia do grona członków BotNetu, należy stosować zaktualizowany program antywirusowy i zaporę ogniową (firewall). [63]

Breakpoint lub pułapka

Pułapka zastawiana w debuggerze (programie testującym inne programy w celu wykrywania i usuwania błędów) na konkretną instrukcję, adres kodu lub danych, która polega na wstawieniu przez debugger w zadane miejsce instrukcji CC (INT3). Po wykonaniu tej

instrukcji system zatrzymuje wykonanie programu i oddaje sterowanie debuggerowi, który przywraca oryginalny bajt i czeka na polecenia crackera. W przypadku pułapki na dane debugger z kolei korzysta z atrybutów ochrony fragmentu pamięci przed odczytem lub zapisem, ustawiając je odpowiednio do sytuacji. [11]

Brute-force attack lub metoda siłowa

1. Zaatakowanie systemu komputerowego z wykorzystaniem zasady pełnego przeglądu. Polega na rozwiązywaniu złożonych problemów poprzez poszukiwanie każdego z możliwych wyników. Stanowi próbę ominięcia zabezpieczeń systemu poprzez wielokrotne logowanie się za pomocą każdego dającego się logicznie przewidzieć hasła.
2. Metoda łamania hasła, która polega na wprowadzaniu po kolei każdego znaku i jego kombinacji, np. z literami, cyframi, znakami specjalnymi. Metoda ta trwa bardzo długo, ponieważ sprawdzenie wszystkich możliwych kombinacji znaków wymaga dużej mocy obliczeniowej. Dlatego też do zastosowania tej metody niezbędny jest komputer z dużą mocą obliczeniową. Czas łamania hasła metodą brute force zależy od jego złożoności oraz długości. Mimo długiego czasu uzyskiwania hasła tą metodą ma ona przewagę nad metodą słownikową, polegającą na podstawianiu całych wyrazów ze słownika, ponieważ metoda słownikowa nie sprawdza się w hasłach składających się z przypadkowych cyfr i liter, a brute force – tak. Teoretycznie tą metodą można złamać każde hasło. [18]

Browser hijacker lub porywacz przeglądarek

Złośliwe oprogramowanie, które po kryjomu zmienia ustawienia przeglądarki internetowej użytkownika. Może to prowadzić do zmiany domyślnej strony startowej przeglądarki, przekierowania wyszukiwań na niepożądane strony WWW, dodanie nieproszonych (czasami pornograficznych) zakładek lub generowanie niechcianych okien wyskakujących (pop-up). Do usuwania hijackerów służą programy antywirusowe. Powstały również specjalne programy do usuwania hijackerów. [64]

Browser Helper Object

Wykorzystuje on bibliotekę DLL (lista podprogramów/narzędzi wykorzystywanych przez inne programy), która ładuje się przy każdym uruchomieniu przeglądarki Microsoft® Internet Explorer. Browser Helper Object instalowany jest przez inny program często w sposób niezauważalny (wielu użytkowników nie czyta informacji napisanych małym druczkiem, które wyświetla program freeware w umowie licencyjnej z użytkownikiem końcowym). Ponieważ BHO jest programem, może robić to samo, co inne programy. Poza tym, niełatwo jest wyszczególnić wszystkie programy BHO zainstalowane na komputerze PC. W rezultacie, funkcje BHO mogą zostać wykorzystane do niewłaściwych celów (na przykład powodować wyskakiwanie reklam lub śledzenie sposobów korzystania z przeglądarki). [86]

Buffer Overflow Attack

Jeden z najczęstszych rodzajów ataku sieciowego typu odmowa wykonania usługi (DoS), należący do grupy wykorzystujących, występujący w oprogramowaniu błąd programistyczny. Polega on na wysyłaniu pod dany adres sieciowy większej ilości danych niż przewidziano w programie dla bufora przyjmującego dane. Osoba atakująca może być świadoma tego, że jej cel jest odporny na ten typ ataku, lub próbuje, licząc na łut szczęścia, że atak się uda. [11]

C

Captcha

Technika zabezpieczeń stosowana w formularzach na stronach WWW. Dla zalogowania się lub przesłania danych konieczne jest prawidłowe przepisanie podanego na obrazku tekstu (zazwyczaj losowo dobranych znaków bądź krótkiego wyrazu). Obrazek ten jest prosty do przeczytania przez człowieka, jednakże odczytanie go poprzez komputer jest, przynajmniej w założeniu, prawie niemożliwe. [20] Może mieć również formę wyboru jednego lub kilku spośród obrazków np. „wybierz i zaznacz wszystkie obrazki, na których są znaki drogowe".

Computer forensics – (kryminalistyka informatyczna, skrót ang. CF)

Proces polegający na poszukiwaniu i przedstawianiu elektronicznych środków dowodowych (dowodów w wersji elektronicznej, które zgodnie z naszym prawodawstwem są ekwiwalentne z dowodami w formie materialnej) dotyczących popełnionych przestępstw lub nadużyć. Proces CF obejmuje zebranie, odzyskanie, analizę oraz prezentację w formie specjalistycznego raportu danych elektronicznych znajdujących się na wszystkich rodzajach nośników (dyski twarde komputerów, dyskietki, płyty CD, pamięci przenośne, serwery firmowe itp.). [29]

Cracking

Dyscyplina informatyki poświęcona łamaniu wszelkiego typu zabezpieczeń (oprogramowania i sieciowych). Cracking odbywa się zwykle z naruszeniem praw autorskich, a tym samym nielegalnie. Wykształcił się jednak również rodzaj crackingu, który polega na testowaniu zabezpieczeń na zlecenie producentów oprogramowania oraz użytkowników Internetu (banków, portali, a nawet agencji rządowych).

Zasadniczo wyróżnia się dwa typy crackingu:

- cracking sieciowy, czyli łamanie zabezpieczeń dostępu komputerów w sieciach komputerowych;
- cracking oprogramowania, czyli łamanie zabezpieczeń przed niedozwolonym użytkowaniem programów. [11]

Crackme (ang. crack – łamać)

Programik napisany najczęściej w assemblerze (programie tworzącym kod maszynowy na podstawie kodu źródłowego), nafaszerowany zabezpieczeniami, a adresowany do crackerów w celu skontrolowania ich umiejętności. Crackme stawiają przed crackerami określone zadania, np. wygenerowanie czy napisanie keygena (generatora kodów dostępu/logowania). Cracker, który złamie jako pierwszy trudne crackme zyskuje uznanie w kręgach innych crackerów i programistów. Programiki te są najczęściej tworzone przez istnych fanatyków zabezpieczeń. [86]

Cracker lub reverse engineer

Informatyk zajmujący się poszukiwaniem i usuwaniem zabezpieczeń w oprogramowaniu komputerowym (dotyczy to najczęściej gier komputerowych). W rzadkich przypadkach cracker prowadzi działalność mającą na celu tylko popisanie się i udowodnienie własnych umiejętności. Często crackerzy związani są z nielegalnym rynkiem oprogramowania i czerpią zyski z tego procederu (piractwo komputerowe). Producenci programów zabezpieczają swoje produkty na wiele różnych sposobów, ma to na celu uniemożliwienie lub utrudnienie tworzenia nielegalnych kopii i uruchamianie ich. Najprostszy sposób to podawanie w trakcie instalacji specjalnego kodu/hasła do wprowadzania przed uruchomieniem programu. Bardziej wyszukanym rodzajem zabezpieczeń są specjalne sprzętowe klucze wpinane w jedno ze złącz komputera (najczęściej port USB); ich obecność jest konieczna do uruchomienia oraz poprawnego działania programu. Aplikacje uruchamiane bezpośrednio z czytnika CD-ROM wymagają stałej obecności oryginalnej płyty instalacyjnej w napędzie. Omijanie tego typu lub innych zabezpieczeń jest celem działania crackerów – ludzi doskonale obeznanych z technikami komputerowymi, a także budową wewnętrzną komputera. Programy pozbawione blokad mogą być bez problemu kopiowane i rozprowadzane. Bardzo często wraz z nielegalną kopią dostarczane są niewielkie programy zwane crackami, które przed pierwszym uruchomieniem modyfikują kod programu lub w trakcie działania symulują obecność klucza. Cracker jest pojęciem często wykorzystywanym wymiennie z hakerem, co jest ewidentnym błędem. [75]

Crimeware

Oprogramowanie nielegalnie gromadzące dane na temat użytkownika komputera (loginy, hasła, dane osobowe). Ma to na celu uzyskanie nielegalnego dostępu do rachunków bankowych lub usług finansowych. Ostatecznym celem jest oczywiście kradzież pieniędzy.

CSS

Jest to zbiór pojęć/reguł służących do odwzorowywania szaty zewnętrznej elementów HTML, które po wyświetleniu w oknie przeglądarki internetowej składają się na wygląd strony internetowej. Skrót CSS pochodzi od słów Cascading Style Sheets co oznacza kaskadowy arkusz stylów. [88]

Cybersquatting

Proceder ten polega na rejestrowaniu domen internetowych nawiązujących do znanych marek (jeśli jeszcze nie zostały zastrzeżone) i odsprzedawaniu ich następnie po zawyżonej cenie osobom lub firmom, które mogłyby zarejestrować prawo do nich w ramach prawa o znaku handlowym. Inaczej mówiąc cybersquatter to ktoś podszywający się pod powszechnie znane osoby i firmy.

Cyberstalking

Jest to postępowanie sprawcy mające oddziaływać na psychikę ofiary, poddanie jej prześladowaniu i zastraszaniu. Ogólnie zjawisko to oznacza szykanowanie danej osoby. Może ono być prowadzone bezpośrednio lub wirtualnie. Natarczywe wezwania do komunikacji, przesyłanie gróźb i wyzwisk pod jej adresem, rozsyłanie e-maili w czyimś imieniu, podszywanie się w sieci, rozpowszechnianie nieprawdziwych informacji na czyjś temat to również cyberstalking. Wywołuje to u ofiary poczucie permanentnego zagrożenia i życia pod presją. Aby uniknąć takich prześladowań, należy zadbać o własne bezpieczeństwo i anonimowość w Internecie. W kontaktach online stosować nicki, które nic o nas nie mówią, założyć dodatkowy adres e-mail, tylko na potrzeby uczestnictwa w listach dyskusyjnych itp., unikać uzupełniania formularzy z danymi personalnymi na stronach WWW i nie ufać ślepo sieciowym rozmówcom (patrz także NLP). [26]

Cyfrowa demencja oraz inne formy e-zagrożeń

Cyfrowa demencja to określenie, którego przed kilku laty użyli południowokoreańscy lekarze do opisania symptomów chorobowych – zarówno psychicznych, jak i fizycznych – będących skutkiem niekontrolowanego korzystania z mediów cyfrowych. Renomowany niemiecki psychiatra i neurobiolog Manfred Spitzer daje w swojej książce szczegółowy wgląd w istotę i przyczyny tego zjawiska [97].

Prezentowane przez profesora Spitzera tezy podzieliły zarówno opinię publiczną, jak i kręgi fachowe na dwa antagonistyczne obozy. Zdaniem Spitzera intensywne korzystanie z mediów cyfrowych skutkuje – zwłaszcza u dzieci i młodzieży – zanikiem samodzielnego myślenia, to zaś prowadzi do zakłócenia uwagi i orientacji przestrzennej oraz pogarszania się wyników w nauce. Na płaszczyźnie emocjonalnej ceną za zbyt częste przebywanie w cyfrowym świecie jest samotność, wycofanie się z realnego życia, problemy ze spaniem i koncentracją włącznie z depresją i prawdziwym uzależnieniem od mediów elektronicznych. [61]

Cyberterroryzm

Cyberterroryzm to możliwa do zrealizowania groźba lub ukryty atak nakierowany na system informatyczny bądź zgromadzone dane. Działania takie podejmowane są zwykle w celu zastraszenia czy wymuszenia na osobach, firmach lub organach władzy okupu lub oczekiwanych zachowań. Zakwalifikowanie takich działań jako cyberterroryzm wymaga zwykle, aby stwarzały one istotne zagrożenie lub mogły spowodować poważne (wymierne) straty.

Cyberterroryzm może przybierać trzy zasadnicze formy:

1. włamań – łącznie z nielegalnym pozyskaniem, usuwaniem lub zmianą danych) i blokady serwerów – które podlegają na zmianie lub uszkodzeniu systemów operacyjnych i doprowadzeniu do wielokrotnych połączeń zarówno atakowanego serwera, jak i innych serwerów;
2. wirusów – programów działających wbrew woli użytkownika systemu i na jego szkodę. Najczęściej przeznaczone są do uszkadzania baz danych i systemów operacyjnych.
3. Ataku konwencjonalnego – polegającego na fizycznym uszkodzeniu elementów systemu komputerowego, serwerów, infrastruktury telekomunikacyjnej (lotniska, koleje, itp.) W zależności od sposobu atak tego typu może prowadzić do czasowego paraliżu systemu lub nieodwracalnej utraty danych. [81]

Propagowanie idei nienawiści i rasizmu

Zachowania rasistowskie i szerzenie tej ideologii jest w polskim prawie zakazane. Precyzuje to zwłaszcza art. 256. Kodeksu karnego, który za propagowanie faszyzmu lub totalitaryzmu określa następujące zagrożenia karne:

§ 1. Kto publicznie propaguje faszystowski lub inny totalitarny ustrój państwa lub nawołuje do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto w celu rozpowszechniania produkuje, utrwala lub sprowadza, nabywa, przechowuje, posiada, prezentuje, przewozi lub przesyła druk, nagranie lub inny przedmiot, zawierające treść określoną w § 1 albo będące nośnikiem symboliki faszystowskiej, komunistycznej lub innej totalitarnej. [18]

Internet ze względu na pewną anonimowość wyrażania poglądów oraz utrudniony dostęp do zagranicznych serwerów, gdzie lokują się zwykle portale rozpowszechniające treści tego typu, stanowi bardzo trudne pole do zwalczania tego zjawiska. Do ustawowych zadań Policji należy rozpoznanie organizacji i grup o charakterze rasistowskim i neonazistowskim. W każdej z komend wojewódzkich w pionie prewencji znajdują się komórki odpowiedzialne m.in. za rozpoznawanie potencjalnych zagrożeń ze strony powyższych grup zarówno pod kątem zagrożenia ładu i porządku publicznego, jak i demoralizującego wpływu na małoletnich.

Działania Policji obejmują również prowadzenie współpracy międzynarodowej oraz wymianie informacji, z uwagi na fakt, że grupy neofaszystowskie lub odwołujące się do symboliki faszystowskiej posiadają namiastkę struktur organizacyjnych w wymiarze ponadnarodowym.

Zagrożenie dla funkcjonowania urządzeń i instytucji publicznych

Przewidywane miejsca występowania zagrożeń bezpośrednich krytycznej infrastruktury teleinformatycznej to miejsca lokalizacji kluczowych elementów systemów teleinformatycznych, takich jak:

- centra zarządzania i utrzymania infrastruktury teleinformatycznej: własnych zasobów administracji;
- urzędy, wydziały i biura bezpieczeństwa i zarządzania kryzysowego oraz przedsiębiorcy telekomunikacyjni dostarczający usługi telekomunikacyjne;
- centrale telekomunikacyjne przedsiębiorców telekomunikacyjnych obsługujące instytucje państwowe, urzędy oraz organizacje przewidywane do likwidacji zagrożeń;
- miejsca przebiegu telekomunikacyjnych linii międzycentralowych i podstawowych linii telekomunikacyjnych;
- stacje bazowe i satelitarne;
- inne ważne obiekty telekomunikacyjne (np. wyniesione koncentratory, stacje czołowe, węzły dostępowe itp.). [37]

Sporządzony w 2013 roku „Raport o zagrożeniach bezpieczeństwa narodowego" obejmujący ocenę ryzyka na potrzeby zarządzania kryzysowego określił następujące kluczowe zagrożenia na wypadek ataku cybernetycznego:

- zakłócenia w pracy infrastruktury przesyłowej;
- możliwe zakłócenia zaopatrzenia w energię i paliwa, w żywność oraz wodę pitną;
- możliwe zakłócenia w transporcie i komunikacji;
- możliwe zakłócenia funkcjonowania organów administracji publicznej;
- zakłócenia teleinformatyczne;
- zakłócenia w pracy służb ratowniczych;
- znaczące straty finansowe i gospodarcze oraz skutki społeczne. [65]

Internet jako element łączności terrorystów

Ugrupowania terrorystyczne wykorzystują Internet do propagandy, której w żaden sposób nie można ocenzurować. Tekstowe, wizualne oraz dźwiękowe możliwości przekazu, które Internet im stwarza są niewyobrażalne. Jeszcze kilka lat temu można było o nich jedynie pomarzyć. Szerokim echem odbiło się opublikowanie w Internecie filmów przedstawiających egzekucje zakładników w Iraku. Przykładem może być Abu Musab Al-Zarkawi, który zapoczątkował serię brutalnych porwań kończących się egzekucjami. Właśnie Internet jest miejscem, gdzie każdy może zobaczyć materiały ocenzurowane przez telewizję. A część definicji terroryzmu mówi przecież o popełnianiu aktów przemocy mających na celu wywołanie głębokiego szoku psychologicznego. [74]

Za pomocą poczty elektronicznej terroryści mogą utrzymywać kontakt z agentami rozmieszczonymi na całym świecie. W jednym z wywiadów rzecznik Hezbollahu w Londynie z wielkim zadowoleniem opowiadał o Internecie i jego możliwościach. Umożliwia to chociażby wysłanie fragmentu z Koranu czy wezwanie do dżihadu agentów znajdujących się na innych kontynentach w przeciągu kilku minut. [74]

Zagrożenia dla obronności państwa

Zagrożenia tego typu obejmują najczęściej następujące przypadki:

- naruszenie integralności danych przetwarzanych przez system teleinformatyczny (modyfikacje, dodanie, zniszczenie);
- nieuprawnione skopiowanie danych i wyprowadzenie ich z terenu firmy przez pracownika;
- włamania dokonywane do systemu teleinformatycznego;
- nieuprawniony dostęp do zasobów systemu możliwy dzięki ujawnieniu haseł innych użytkowników;
- niepowołany dostęp do miejsca przetwarzania danych;
- zniszczenie elementów lub całości infrastruktury technicznej systemu teleinformatycznego;
- nieodpowiednie parametry pracy systemu teleinformatycznego (np. wilgotność, temperatura). [52]

Osobnego potraktowania wymaga sprawa zagrożenia dla tajemnicy państwowej i wojskowej. Dotyczy to zwłaszcza prowadzenia tzw. wojny elektronicznej, a poszczególne kraje oficjalnie bądź po cichu, wprowadzają w swoich siłach zbrojnych całe jednostki zajmujące się przygotowaniem i prowadzeniem agresji w sieci.

Wywiady opracowują na własny użytek szczegółowe zasady korzystania z poszczególnych mediów, kanałów radiowych i telewizyjnych. Dokonują analizy wiarygodności poszczególnych gazet i periodyków specjalistycznych, audycji czy też stron WWW, wybierając te najbardziej wiarygodne, a zarazem redagowane przez uznanych w danej dziedzinie dziennikarzy i specjalistów.

Tak więc obecnie powszechność stosowania w gospodarce technologii internetowych oznacza, że każda informacja zyskuje swoją wartość, a umiejętność jej ochrony i właściwego wykorzystania staje się w kontaktach i sporach między państwami bardziej istotna od liczby posiadanej przez nie broni.

Terroryzm państwowy

Finansowanie terroryzmu przez państwo ma długą historię. Pod koniec XIX wieku Rosja wspomagała grupy rewolucyjne na Bałkanach próbujące utworzyć tam państwa słowiańskie. Podczas I wojny światowej Niemcy dostarczali broń nacjonalistom irlandzkim walczącym z władzą brytyjską. Pod koniec XX w. wiele państw wspierało ugrupowania terrorystyczne. Słabsze kraje stwierdziły, że jest to użyteczna metoda uderzenia w przeciwnika, który w konwencjonalnej wojnie miałby nad nimi ogromną przewagę.

Głównymi sponsorami terroryzmu były radykalne państwa Bliskiego Wschodu (szczególnie Iran, Syria, Libia i Irak), Związek Radziecki i inne państwa komunistyczne (w tym kraje bloku wschodniego, Korea Północna i Kuba), a także Republika Południowej Afryki, Stany Zjednoczone i Izrael. Sponsorowanie terroryzmu może mieć charakter od ograniczonego wsparcia, przez pełny sponsoring, aż po całkowitą kontrolę. Państwo może wspierać grupę terrorystyczną poprzez wykorzystywanie swoich mediów do popularyzowania

i popierania konkretnych operacji. Formą ograniczonego wsparcia może być odmowa ekstradycji oskarżonego i ściganego terrorysty. Z drugiej strony, sponsorujące państwo może uczestniczyć w planowaniu i kontrolowaniu akcji terrorystycznych. Wspólną dla wielu państw sponsorujących terroryzm taktyką jest udzielanie wsparcia wojskowego grupom powstańczym, o których wiedzą, że wykorzystują one metody terrorystyczne. [23]

Wśród konkretnych form wsparcia, jakie udzielane jest terrorystom, można wymienić wsparcie wywiadowcze, szkolenie (podstawowe wojskowe oraz specjalistyczne – terrorystyczne) i wykorzystanie placówek dyplomatycznych. Pomoc materialną może stanowić zapewnienie dostępu do nowoczesnej broni i materiałów wybuchowych, pomoc logistyczna i transport. Państwo może też pozwolić terrorystom na korzystanie z własnego terytorium. Ma to szczególne znaczenie w przypadku cyberterroryzmu.

Broń cybernetyczna będąca obecnie w posiadaniu USA nie została jeszcze dostosowana do użycia przeciw systemom niezależnym od Internetu. Na sfinansowanie prac w tym kierunku przeznaczono w zeszłym roku 500 mln dolarów przydzielonych zajmującej się nimi Agencji Zaawansowanych Projektów Badawczych przy Pentagonie. Cały oficjalnie ujawniony budżet na bezpieczeństwo systemów komputerowych i technologie komputerowe, zarówno defensywne, jak i ofensywne, to 3,4 mld dolarów w bieżącym roku podatkowym. [78]

Broń cybernetyczna to wirusy komputerowe różnego rodzaju, które mogą zakłócić działanie komponentów systemów broni nieprzyjaciela. Przykładem jest wirus Stuxnet, który w zeszłym roku uszkodził i zakłócił operacje instalacji nuklearnych w Iranie. Choć strona amerykańska oficjalnie temu zaprzecza, eksperci uważają, że akcja była dziełem służb specjalnych USA.

Chiny znane są z cenzurowania internetowej sieci oraz blokowania witryn, które uznają za niewygodne. Już wkrótce działania te staną się jeszcze intensywniejsze, gdyż tamtejszy rząd opracował specjalne narzędzie zwane Wielkim Działem, które jest w stanie z łatwością wyłączyć dowolną stronę. [12]

Wysoki poziom rozwoju technologicznego przyczynia się do poprawy zarządzania wieloma sferami życia politycznego, społecznego i gospodarczego, ale jednocześnie uzależnia państwo od sprawności i bezpieczeństwa infrastruktury krytycznej.

Atak na jeden z elementów systemu może zakłócić funkcjonowanie pozostałych („efekt domina"), ponieważ są one ściśle ze sobą powiązane.

Najpoważniejszym źródłem zagrożeń dla sieci teleinformatycznych – obok niedoskonałości rozwiązań technicznych – są celowe działania. Mogą przyjmować formę:

- zakłócenia działania systemów;
- nieupoważnionego wprowadzania lub kopiowania danych;
- łamania zabezpieczeń, co pozwala na przejęcie kontroli nad poszczególnymi elementami infrastruktury (np. na wypadek wojny).

Po tę ostatnią metodę mogą sięgać służby specjalne nieprzychylnie nastawionych państw oraz organizacje terrorystyczne. Grupy przestępczości zorganizowanej mogą

być zainteresowane wykradaniem danych lub dokonywaniem nieupoważnionych zmian danych np. w systemach i sieciach instytucji finansowych.

Agencja Bezpieczeństwa Wewnętrznego jest odpowiedzialna za zapewnienie ochrony kluczowych systemów i sieci teleinformatycznych państwa. W tym celu w strukturach ABW powołano Rządowy Zespół Reagowania na Incydenty Komputerowe – cert.gov.pl. [2]

Zagrożenie dla przedsiębiorstw i biznesu

Rozwój technologiczny generuje powstawanie ciasnych specjalizacji wymagających wyspecjalizowanej, hermetycznej wiedzy. Ważnym kierunkiem w rozwoju programowania pozostają tzw. systemy SCADA (Supervisory Control and Data Acquisition) odpowiadające za kierowanie konkretnymi procesami, np. w transporcie publicznym czy energetyce. Obecnie możliwe jest zawirusowanie sterowników do takiego systemu, co powoduje np. błędne odczyty przyrządów w samolocie podchodzącym do lądowania czy systemów sygnalizacji świetlnej w miastach. Przykładem celowego działania przeciwko firmie jest wirus Stuxnet, który doprowadził do uszkodzenia oprogramowania w irańskiej elektrowni atomowej w Bushehr.

W listopadzie 2010 roku prezydent Iranu Mahmud Ahmadineżad potwierdził, iż ofiarą robaka Stuxnet – przenoszonego za pomocą pendrive'ów i atakującego systemy obsługi dużych obiektów przemysłowych – padła elektrownia atomowa w irańskim Bushehr. W styczniu 2011 rosyjski ambasador przy NATO stwierdził, iż Stuxnet mógł wywołać w ten sposób katastrofę ekologiczną podobną do czarnobylskiej. Nakład pracy konieczny do stworzenia tego wirusa każe podejrzewać, że został on zamówiony przez rząd państwa – na razie nie jest pewne którego. Brak jest informacji, które wskazywałyby na wykonanie podobnych ataków na terytorium Polski. [22]

Jednym z podstawowych systemów infrastruktury krytycznej jest system zaopatrzenia w energię, surowce energetyczne i paliwa, który składa się z trzech podsystemów:

- wytwarzania (pozyskiwania) energii;
- przesyłu energii i paliw;
- dystrybucji i dostaw energii i paliw do odbiorców. [85]

W odniesieniu do jednego z podsystemów, jakim są elektrownie, możliwe są następujące formy ataku terrorystycznego:

- bezpośredni atak na system – celem ataku jest jego fizyczna infrastruktura. Mogą zostać zaatakowane stacje elektroenergetyczne lub kluczowe linie w celu wywołania awarii na dużym obszarze sieci;
- atak poprzez system elektroenergetyczny – mogą zostać użyte niektóre instalacje w systemie elektroenergetycznym do zaatakowania innych elementów jego infrastruktury, wywołany silny impuls elektromagnetyczny w sieci w celu uszkodzenia komputerów i infrastruktury telekomunikacyjnej. [85]

Jako przykład ataku terrorystycznego na obiekty systemu energetycznego można przedstawić zamach na elektrownię wodną w Republice Kabardo-Bałkarii na rosyjskim Kaukazie w 2010 r. W wyniku ataku zginęło dwóch strażników oraz uszkodzone zastały dwa z trzech generatorów elektrowni. Atak nie miał istotnego znaczenia ekonomicznego, jednak pokazał, że takie obiekty mogą stanowić cel działania terrorystów. Niezwykle istotnym zagadnieniem bezpieczeństwa obiektów infrastruktury energetycznej jest zagrożenie potencjalnym atakiem elektrowni jądrowych. Obecnie w Europie pracuje około 220 reaktorów. Najbardziej rozbudowane systemy pozyskiwania energii atomowej mają państwa najsilniej zagrożone terroryzmem: Francja, Wielka Brytania, Niemcy i Rosja. [85]

Najlepszy przykład niebezpieczeństwa skażenia radiologicznego środowiska naturalnego, biorąc pod uwagę rozprzestrzenianie się w Europie takiego zagrożenia, stanowi awaria elektrowni jądrowej w Czarnobylu. Elektrownie jądrowe wraz z instalacjami zawsze podlegały szczególnej ochronie ze względu na możliwość przejęcia kontroli nad systemami sterowania pracą reaktorów przez osoby nieupoważnione.

Obecnie najbardziej prawdopodobne zagrożenie dla elektrowni to:

- możliwość przeprowadzenia sabotażu wewnątrz elektrowni przez osobę kierującą się korzyściami materialnymi lub ideologią;
- przejęcie systemu sterowania pracą reaktorów z poziomu sterowni przez uzbrojoną grupę terrorystyczną, która przeprowadziła udany atak i obezwładniła ochronę elektrowni;
- uderzenie dużego samolotu (samolotu pasażerskiego lub transportowego) w reaktor elektrowni. Jest to szczególnie niebezpieczne dla elektrowni starego typu, których reaktory nie zostały zabezpieczone przed taką ewentualnością. [85]

Stan bezpieczeństwa nowoczesnych elektrowni jądrowych nie budzi zastrzeżeń, jednak przeprowadzenie skutecznego ataku terrorystycznego na jedną z elektrowni jądrowych na terenie sąsiednich państw może mieć znaczenie dla bezpieczeństwa i funkcjonowania naszego kraju. Należy mieć nadzieję, że jest to zadanie niezwykle trudne dla terrorystów, ze względu na ochronę i istniejące systemy zabezpieczeń, jednak nie oznacza to, że jest niemożliwe.

Fałszywe alarmy

Stały się one prawdziwym problemem dla służb państwowych. Pojawienie się telefonii komórkowej, w szczególności usługi prepaid oraz powszechny dostęp do Internetu przyczynił się do intensyfikacji tego typu fałszywych zgłoszeń, a zarazem do znacznego utrudnienia w ustaleniu sprawców, którzy często stosują systemy ukrywające tożsamość. W ubiegłych latach autorzy tego typu alarmów najczęściej informowali o zdarzeniu dzwoniąc na telefon alarmowy Policji lub pod ogólnodostępne numery instytucji i urzędów, obecnie wysyłają maile z jednego konta pocztowego jednocześnie do bardzo wielu podmiotów.

Każda informacja o podłożeniu ładunku wybuchowego, nawet gdy zachodzi przypuszczenie, że jest nieprawdziwa, musi zostać sprawdzona. W akcjach, które mają na celu

weryfikację podanej informacji, biorą udział nie tylko grupy policjantów odpowiedzialne za prowadzenie działań saperskich, ale także służby medyczne i inne specjalistyczne służby techniczne. Bardzo często dochodzi do ewakuacji zagrożonych obiektów, co powoduje przerwanie funkcjonowania danej instytucji i zdezorganizowanie jej pracy na kilka godzin. Wszystkie te działania generują oczywiście ogromne koszty. [65]

Ekoterroryści

Na podstawie literatury przedmiotu w zjawisku terroryzmu ekologicznego można wyodrębnić dwa podstawowe nurty:

- obrońców środowiska naturalnego (ugrupowania prośrodowiskowe, enwironmentaliści)
- obrońców praw zwierząt (animaliści).

Ugrupowania prośrodowiskowe (np. Earth First!, Earth Liberation Front) na ogół ograniczają się do nielegalnych aktów sabotażu (tzw. ekotażu), które bezpośrednio nie przynoszą szkody ludziom. Mają one na celu za pomocą taktyki monkeywrenchigu (ang. monkey wrench = klucz nastawny lub francuski) niszczenie maszyn oraz lekkiego sprzętu (np. poprzez podpalenia czy nakłuwanie metalowymi kolcami pni drzew przeznaczonych do wycięcia), a także obalanie billboardów, demontaż znaków ze szlaków narciarskich lub linii wysokiego napięcia itp. Natomiast radykalne ugrupowania animalistyczne (np. Anima Rights Militia, Justice Department) oprócz pośrednich metod działania, często idą znacznie dalej, posuwając się nawet do bezpośrednich aktów terroru wobec ludzi. [15]

Do metod terrorystycznych używanych przez skrajnych animalistów zaliczyć można nie tylko uwalnianie zwierząt poddawanych eksperymentom, ale również podkładanie ładunków wybuchowych w firmach produkujących odzież skórzaną lub w inny sposób użytkujących zwierzęta, atakowanie laboratoriów prowadzących badania naukowe z wykorzystaniem zwierząt. Nie cofają się również przed pobiciami, szantażem, pogróżkami, zatruwaniem produktów w supermarketach, wysyłaniem listów pułapek itp.

Cyberprzemoc

Cyberprzemoc (inaczej agresja elektroniczna) to nic innego jak stosowanie przemocy przez prześladowanie, nękanie, zastraszanie, wyśmiewanie się przy użyciu narzędzi komunikacji elektronicznej takich jak Internet (poczta elektroniczna, portale społecznościowe, fora dyskusyjne) oraz telefon komórkowy (SMS). [90]

Obecnie w Polsce prawo nie przewiduje bezpośrednio odpowiedzialności karnej za tego typu działalność. Nie ma po prostu przepisu, który określałby w prawie karnym przestępstwo cyberprzemocy. Nie oznacza to całkowitej bezkarności osoby, która dopuszcza się takiego czynu. Sądy wykorzystują w takiej sytuacji do pociągnięcia sprawców do odpowiedzialności karnej jeden z następujących przepisów Kodeksu karnego:

- art. 190 (groźba karalna);
- art. 190a (uporczywe nękanie);
- art. 212 (zniesławienie);

- art. 216 (zniewaga);
- art. 265 i nast. (przestępstwa przeciwko ochronie informacji). [18]

Ze względu na powszechność zjawiska cyberprzemocy jej poszczególne formy uzyskały swoje nazwy i tak:

- **stalking** jest uporczywym nękaniem innych za pomocą np. zakładania fikcyjnego profilu w celu ośmieszenia, jego usuwanie i ponownie zakładanie;
- **trollowanie** – to różnego typu nieprzyjazne zachowania wobec innych użytkowników Internetu, które mają na celu rozbicie prowadzonej dyskusji. Zjawisko to jest obecne w miejscach przeznaczonych do wymiany myśli między Internautami, czyli na grupach dyskusyjnych, forach, czatach itp.;
- **flaming** – to celowe zaognianie wymiany zdań między użytkownikami w różnego typu serwisach dyskusyjnych, prowadzące do narastania agresji wypowiedzi;
- **grooming** – to uwodzenie przez Internet (szczególnie dotyczy to nieletnich);
- **phishing** – to wyłudzanie danych osobistych i informacji majątkowych;
- **spoofing** obejmuje szereg technik zmierzających do podszycia się pod kogoś innego w Internecie (patrz hasło IP Spoofing).

D

Dialer

Bardzo niebezpieczny typ wirusa komputerowego, który może wygenerować kolosalne rachunki za połączenie z Internetem. Wirus ten instaluje się na komputerze bez wiedzy i zgody użytkownika i poprzez numer dostępowy nawiązuje płatne połączenia, zwykle z dostawcą usług znajdującym się najczęściej w innym kraju. Zagraża przede wszystkim użytkownikom używającym modemu podłączonego do linii telefonicznej. Efektem działania dialera mogą być ogromne rachunki telefoniczne. Twórcy dialerów zwykle posiadają umowy operatorami telefonicznymi, na mocy których dzielą się z nimi zyskiem. Dialery występują przeważnie na stronach o treści pornograficznej oraz z nielegalnym oprogramowaniem. Aby uniknąć opłat użytkownik przechodzi przez proces „rejestracji", w trakcie którego jednym z kroków jest ukryta instalacja dialera. [36]

DOS (ang. Disk Operating System – Dyskowy System Operacyjny)

DOS to ogólna nazwa systemów operacyjnych stosowanych w komputerach osobistych, które nie posiadały graficznego interfejsu użytkownika lecz używały tekstowego. Najsłynniejszymi systemami typu DOS były: MS-DOS i PC-DOS.

DoS (ang. Denial of Service)

Jest to rodzaj ataku sieciowego powodujący, że atakowany system przestaje działać właściwie. Może to być defekt tylko jednej usługi internetowej (np. e-mail) lub całego serwera. Przy prowadzeniu ataków typu DoS korzysta się z błędów i luk, występujących

już w systemie. Atak ten nie wiąże się nigdy z kradzieżą danych lub ich utratą, ale przynosi on wielkie straty firmom, które przez zablokowanie ich usług ponoszą straty.

DDoS (ang. Distributed Denial of Service)

Odmiana ataku typu DoS stworzona w celu całkowitego uniemożliwienia normalnego działania witryny internetowej, sieci, serwera lub innych zasobów. Atak DDoS różni się od ataku DoS jedynie wykorzystywaną metodą. Atak DdoS prowadzony jest równocześnie przez wiele komputerów. Hakerzy lub twórcy wirusów zazwyczaj używają zaatakowanego komputera jako komputera sterującego („master") oraz koordynują atak za pośrednictwem opanowanych wcześniej tzw. komputerów „zombie." Zarówno komputery zombie, jak i master są atakowane przez wykorzystywanie luki w oprogramowaniu w celu zainstalowania trojana lub innego szkodliwego kodu.

DHA (ang. Directory Harvest Attack)

Jedna z metod stosowanych przez spamerów w celu gromadzenia czynnych adresów e-mail. Adresy te stają się frontalnym celem ataków, które spamerzy prowadzą osobiście albo odsprzedają je chętnym spamerom. Najpierw spamer wybiera domenę (powiedzmy „ofiara_domena.com"), a następnie wysyła spekulacyjne wiadomości e-mail na prawdopodobne adresy w tej domenie (na przykład „jacek@ofiara_domena.com", anna@ofiara_domena.com). Jeśli serwer pocztowy „ofiara_domena.com" nie odrzuci wiadomości, spamer będzie wiedział, że dany adres e-mail jest czynny i może być wykorzystywany jako cel w atakach spamowych. [32]

Dostęp do substancji odurzających i dopingujących

Narkotyki stały się w Internecie takim samym produktem dostępnym i reklamowanym jak pospolite towary. Aby zachęcić do ich używania, stosowanych jest wiele narzędzi przekonywania i manipulacji, od zwykłej informacji poczynając, a kończąc na przedstawianiu udającej logiczną argumentacji. Z pomocą Internetu handlarze i osoby uzależnione nawiązują kontakty i przeprowadzają sprzedaż narkotyków. Internet stanowi też forum „szkolenia" narkomanów na temat skutków przyjmowania oraz wyszukiwania coraz to nowych środków odurzających.

Bardzo powszechne jest w Internecie zjawisko handlu środkami i specyfikami, które mają zwalczać takie dolegliwości jak:

- brak potencji;
- otyłość;
- depresja;
- zwiększenie koncentracji;

Leki lub specyfiki kupowane bez recepty i przyjmowane bez wskazówek i nadzoru lekarza mogą doprowadzić do wielu chorób, a w skrajnych przypadkach nawet do śmierci. W skład wielu z nich wchodzą również substancje uzależniające.

Doxing

Są to działania polegające na ustalaniu tożsamości anonimowej osoby w Internecie, która ukrywa się pod pseudonimem. Często oprócz danych osobowych zdobywa się numer telefonu, dane adresowe czy adresy kont użytkownika w różnych serwisach, gdzie dostępnych może być więcej jego danych. Można również w ramach doxingu wykorzystać metadane zapisane w zdjęciach (np. koordynaty miejsca, gdzie wykonano zdjęcie, tożsamość autora zdjęcia itp.). Doxing wykorzystuje zarówno umiejętności techniczne dotyczące Internetu czy ślady pozostawiane w sieci przez namierzaną osobę, ale również techniki socjotechniczne w celu wyłudzenia od administratorów serwisów danych o poszukiwanym użytkowniku. [70]

Drive-by download

Termin ten odnosi się do procesu instalowania oprogramowania (zazwyczaj szkodliwego) podczas odwiedzania witryn internetowych lub odbierania wiadomości e-mail bez wiedzy użytkownika. Warto stosować zasadę, by bardzo ostrożnie odbierać pocztę od nieznanych użytkowników, a już w żadnym wypadku nie otwierać zawartych w niej załączników albo linków. W przypadku podejrzanych maili od instytucji można również zadzwonić do nich w celu potwierdzenia wiarygodności poczty.

Drive-by pharming

W przypadku tradycyjnego ataku typu „pharming" przestępca stara się przekierować użytkownika odwiedzającego określoną witrynę internetową do strony sfałszowanej. Może to osiągnąć poprzez modyfikacje w komputerze ofiary lub wprowadzając zmiany w systemie DNS (Domain Name System). Z kolei atak „drive-by pharming" to nowy rodzaj zagrożenia polegający na tym, że po odwiedzeniu przez użytkownika destrukcyjnej witryny hacker może zmienić ustawienia DNS na routerze użytkownika lub w punkcie dostępu bezprzewodowego. Zmiana dokonywana jest za pomocą kodu napisanego w języku JavaScript po wejściu na fałszywą witrynę i jest możliwa w sytuacji, gdy router szerokopasmowy nie jest chroniony hasłem lub gdy atakujący jest w stanie je odgadnąć. Dzięki zmianie DNS przestępca komputerowy uzyskuje pełną kontrolę nad tym, które witryny użytkownik odwiedza w Internecie. Użytkownikowi może na przykład wydawać się, że odwiedza stronę swojego banku, gdy w rzeczywistości został przekierowany do spreparowanej witryny. Fałszywe strony są wiernymi kopiami autentycznych witryn, dlatego użytkownik często nie będzie w stanie zauważyć żadnej różnicy. Po przekierowaniu do witryny „banku", wprowadzeniu przez użytkownika nazwy i hasła atakujący metodą „pharming" może wykraść te informacje. Dzięki temu będzie w stanie uzyskać dostęp do konta ofiary w prawdziwej witrynie banku i dokonać przelewu, utworzyć nowe konta lub wypisać czeki. Najprostszym zabezpieczeniem jest zmiana w routerze hasła domyślnego na unikalne. Ponadto zalecane jest korzystanie z oprogramowania zabezpieczającego komputer, czyli antywirusa, zapory ogniowej (firewall), mechanizmów wykrywania włamań i chroniących przed lukami w zabezpieczeniach. [11]

E

Elektroniczne żebractwo

W tym oszustwie wykorzystywane są e-maile, które wyglądają, jakby pochodziły od organizacji charytatywnych lub osób potrzebujących. W rzeczywistości stanowią one zwykłe fałszerstwo lub zawierają kopie stron do prawdziwych stowarzyszeń i fundacji, ale po sfałszowaniu rachunków bankowych wymaganych do dokonania płatności, przez co oszuści sprawiają, że wpłacane darowizny lądują w ich kieszeni.

E-kartki

W okresie świątecznym e-kartki stają się powszechnym sposobem przesyłania życzeń znajomym. Jednakże fałszywe e-kartki mogą zawierać wirusy lub złośliwe oprogramowanie, które może zainfekować komputer. W kartkach czy życzeniach może być link do strony, która sama infekuje – nawet jeśli rzeczywiście znajduje się tam treść świąteczna. Trzeba zachować dużą ostrożność. Bezkrytyczne otwieranie wszelkich załączników lub podążanie za linkami do stron internetowych może się źle skończyć. Dotyczy to zresztą wszystkich wiadomości otrzymywanych w sieci. Dodatkowo świąteczne wygaszacze, muzyka i animacje są prostym sposobem na rozprzestrzenianie się wirusów i złośliwego oprogramowania.

Exploit

Rodzaj ataków na systemy komputerowe, które wykorzystują błąd lub ułomność systemu lub też instrument (np. skrypt, program) wykorzystujący ową lukę do dokonania włamania. Wielu crackerów i hackerów zyskuje poklask z tytułu odnalezienia luki w systemie lub stworzenia skryptu lub programu do hackingu, dlatego też chętnie dzielą się oni tą wiedzą za pośrednictwem Internetu. Następnie liczni tzw. script kiddies (początkujący hackerzy) uruchamiają gotowe programy i atakują strony internetowe lub pojedyncze komputery. Ponieważ programiści popełniali często podobne błędy, exploity dla wielu odmiennych systemów zaczęły stawać się coraz bardziej ujednolicone. Stąd też podzielono je na kilka kategorii. Nazwy exploitów pochodzą najczęściej od nazw luk, które wykorzystują do atakowania systemów:

- buffer overflow;
- backtracking;
- format string attack;
- race condition;
- cross-site scripting;
- defaults (domyślne);
- samples (przykłady);
- Denial of Services (DoS). [86]

Kiedy exploity wykorzystują słabości systemu lub aplikacji, w odpowiedzi na to autorzy systemu lub aplikacji tworzą hot fix lub patch, który ma za zadanie naprawić błąd, który

jest wykorzystywany w ataku. Użytkownicy programów powinni sami zatroszczyć się o zdobycie łatki (np. mogą ściągnąć go z witryny internetowej producenta), aby zabezpieczyć się przed włamaniem. [11]

Exploit zero-day

To program napisany w celu wykorzystywania błędu lub luki w zabezpieczeniach aplikacji lub systemu operacyjnego, który pojawia się natychmiast po wykryciu luki. W rezultacie, producent nie ma czasu na stworzenie łaty, a administratorzy IT na wdrożenie mechanizmów ochrony. [32]

F

Fake mail

Jest to fałszywa wiadomość internetowa. Istnieją portale fejkowe, które nie tylko same są źródłem fałszywych informacji, ale także posiadają i udostępniają mechanizmy (algorytmy, programy) pozwalające wysłać wiadomość z fałszywym adresem nadawcy.

Fałszywe oferty pracy

Fałszywe oferty pracy zawierają propozycję pracy skierowaną do określonej osoby poszukującej odpłatnego zajęcia. Może to być np. zagraniczna firma oferująca bardzo atrakcyjne zarobki przy wykonywaniu prostej czynności, głównie poprzez Internet. Podejrzani „pracodawcy" proszą o dane konta bankowego, aby można było dokonać przelewu za wykonaną pracę. Po jakimś czasie okazuje się, że dane te zostały wykorzystane do zrabowania pieniędzy z kont innych osób, których dane przechwycili cyberprzestępcy. Ofiara myśląc, że pracuje dla określonej firmy, staje się pośrednikiem w kradzieży pieniędzy z innych kont. Dana osoba nieświadomie bierze udział w popełnianiu przestępstwa, udostępniając przestępcom swoje konto i pośrednicząc w przelewaniu środków. [71]

Fałszywe wezwanie do kontaktu lub do zapłaty

Wiadomość wykonana i rozsyłana w sieci przez przestępców przypomina cyfrowe wezwanie przesyłane przez rzeczywistą firmę. W jednym z nich naśladującym Pocztę Polską zgłaszano problem z zagubioną przesyłką. Jednak w treści nie podano numeru przesyłki oraz adresu placówki, pod którym można znaleźć paczkę. Zamiast tego proponowano zajrzeć stronę (specjalnie spreparowaną i przypominającą oryginalną), na której prześledzimy ruch przesyłki wysyłanej przez Pocztę Polską, aby pobrać z niej dokument umożliwiający odbiór paczki.

W dalszej części wiadomości napisano, że w przypadku nieodebrania przesyłki w ciągu 30 dni naliczane będą jakieś kary. Ma to oczywiście wpłynąć na użytkownika, by zajrzał na podstawioną stronę. Warto przy okazji wiedzieć, że awizo na e-mail dostępne jest tylko dla osób, które złożyły żądanie otrzymywania go drogą elektroniczną. Taki formularz

należy złożyć osobiście w placówce pocztowej lub oddać listonoszowi. Nie każdy jednak o tym pamięta, co cyberprzestępcy próbują wykorzystać. [16]

Fast flux

To jedna z technologii funkcjonalna przy popełnianiu przestępstw internetowych np. phishingu. Jest to mechanizm przełączający serwer DNS (Domain Name System – „system nazw domenowych"), który łączy w sobie sieć równorzędną, rozproszone dowodzenie, internetowe równoważenie obciążenia oraz przekierowywanie proxy w celu ukrycia adresu stron, na które przesyłane są wyłudzone dane osobowe. Fast flux przedłuża okres aktywności stron wyłudzających dane osobowe, pozwalając oszukać większą liczbę użytkowników. [11]

G

Gray hat – (z ang. szary kapelusz)

Nazwa stosowana dla hakera lub crackera, który dokonuje włamania do systemu komputerowego lub sieci by nakierować uwagę administratora na wykrytą przez siebie lukę. „Szary kapelusz" działa w dobrych intencjach – pragnie poprawić i udoskonalić zabezpieczenia sieci. Jednakże publikowanie „dziur" umożliwia czasami włamanie się innym hakerom. To odróżnia go od hakera typu „biały kapelusz." Ten drugi zawiadamia administratora o luce, nie publikując jednak informacji o niej w Internecie. Jednym słowem „szary kapelusz" oznacza hakera na granicy dobra i zła, który wykorzystuje swoje umiejętności w pokojowy i przyjazny sposób, nie zrywając jednak z ciemną strona hackingu.

Termin szary kapelusz pochodzi z westernów, gdzie zazwyczaj pozytywni bohaterowie ubrani byli w białe kapelusze, zaś „złe typy" – w czarne. Por. white hat, black hat. [86]

Grooming

Przestępstwo polegające na wprowadzaniu w błąd nieletniego dziecka do lat 15 w celu produkcji materiałów pornograficznych lub składaniu mu propozycji seksualnych przez Internet. Grooming potocznie uważa się za bałamucenie i deprawowanie dzieci przez Internet. Przestępstwo zostało spenalizowane w polskim prawie karnym od 8 czerwca 2010 roku. Grozi za nie kara grzywny oraz od 2 do 3 lat pozbawienia wolności w zależności od okoliczności. Mówi o tym Kodeks karny:

Art. 200a.

§ 1. Kto w celu popełnienia przestępstwa określonego w art. 197 § 3 pkt 2 lub art. 200, jak również produkowania lub utrwalania treści pornograficznych, za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej nawiązuje kontakt z małoletnim poniżej lat 15, zmierzając, za pomocą wprowadzenia go w błąd, wyzyskania błędu lub niezdolności do należytego pojmowania sytuacji albo przy użyciu groźby bezprawnej, do spotkania z nim, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej małoletniemu poniżej lat 15 składa propozycję obcowania płciowego, poddania się lub wykonania innej czynności seksualnej lub udziału w produkowaniu lub utrwalaniu treści pornograficznych, i zmierza do jej realizacji, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2

Art. 200b. Kto publicznie propaguje lub pochwala zachowania o charakterze pedofilskim, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. [18]

H

Hacking

Czynności wykonywane przez hakera (np. włamywanie się na serwer, łamanie haseł, kradzież tożsamości itp.)

Handel w Internecie przedmiotami zabronionymi lub pochodzącymi z przestępstwa (paserstwo)

Przedmiot paserstwa może stanowić rzecz pochodząca z kradzieży lub wręczona w charakterze łapówki, a nawet zapłata za popełnienie przestępstwa na zlecenie. Praktyka policyjna i sądowa wskazuje, że paserstwo zwykle dotyczy handlu skradzionymi przedmiotami. Polskie prawodawstwo mówi o kilku rodzajach paserstwa. W sytuacji, jeśli sprawca chciał lub godził się na popełnienie paserstwa, to jest to równoznaczne z definicją paserstwa umyślnego. Za ten czyn grozi kara pozbawienia wolności od 3 miesięcy do 5 lat więzienia. [11]

Jeśli przedmiot jest mniejszej wagi, to sprawca może zostać ukarany grzywną, karą ograniczenia albo pozbawienia wolności do roku. Jeśli natomiast mienie pochodzące z przestępstwa jest bardzo wartościowe albo ma szczególne znaczenie, np. dla kultury, to sprawca podlega karze pozbawienia wolności od roku nawet do 10 lat.

Kolejną nielegalną plagą jest internetowa sprzedaż alkoholi wysokoprocentowych oraz papierosów z niższą akcyzą niż ta, która aktualnie obowiązuje w kraju (resort finansów nie toleruje konkurencji w tej dziedzinie). W sieci można jednak bez problemu znaleźć i kupić narzędzia i urządzenia do produkcji alkoholu i papierosów.

Naturalnym pozostaje zakaz (oczywiście nie tylko w Internecie) handlu ludźmi, organami oraz zwierzętami. [40]

Hoax (fałszywe ostrzeżenie o wirusie)

Ma zazwyczaj charakter wiadomości e-mail, która ostrzega adresata przed zagrażającym nowym wirusem i proponuje, aby użytkownik przesłał ją dalej. Hoax sam w sobie nie powoduje szkód, jednak rozpowszechniane w dobrej wierze wiadomości tego typu często wywołują przestrach i niepewność. Większość producentów rozwiązań antywirusowych umieszcza na swoich stronach WWW informacje o hoaxach. Zanim więc prześlemy kolejnym osobom wiadomości ostrzegające o zagrożeniach, warto je sprawdzić. [28]

Honeypot
Nazywany tak jest podstęp przeciwko hackerom mający na celu wykrycie prób nieautoryzowanego użycia systemu czy pozyskania danych. W jego skład wchodzą zwykle komputer, dane i wyodrębniony obszar sieci lokalnej, które udają prawdziwą sieć, lecz są odizolowane i odpowiednio zabezpieczone. Wszystko to z zewnątrz wygląda jakby zawierało informacje lub zasób, który mógłby być potencjalnym celem cyberprzestępcy. [87]

HTML
HTML (HyperText Markup Language) jest to język używany do kreowania stron internetowych. Ma on postać języka znaczników, czyli oprócz głównego tekstu dokument zawiera w sobie inne informacje opisujące go. Te dodatkowe informacje implementowane są za pomocą symboli, kiedyś wykorzystywanych w przemyśle wydawniczym. Dzięki językowi HTML możemy dodawać do tekstu akapity, hiperłącza, nagłówki, pliki graficzne lub multimedialne czy formularze. HTML określa także, jak dokument będzie wyglądał w przeglądarce internetowej. [67]

I

IP Spoofing
Termin określający przekłamywanie wyjściowego adresu IP w wysyłanym przez komputer pakiecie sieciowym. Takie działanie może służyć ukryciu tożsamości atakującego (np. w przypadku ataków DoS), stwarzaniu pozorów innego użytkownika sieci i ingerowanie w jego aktywność sieciową lub wykorzystaniu uprawnień posiadanych przez inny adres (atak wykorzystany przez Kevina Mitnicka w celu dostania się do komputera Tsutomu Shimomury). [9]

J

JavaScript
JavaScript jest to język programowania typu skryptowego dla dokumentów internetowych. Skrypty napisane za pomocą JavaScript mogą być umieszczane na stronach WWW. Dzięki temu językowi można przykładowo uzależnić wykonanie jakiejś instrukcji od wykonania odpowiedniej instrukcji przez osobę przeglądającą daną stronę. JavaScript ma też szerokie zastosowanie w kreowaniu formularzy. Umożliwia wnikanie w ich treści i sprawdzanie poprawności wypełnienia poszczególnych pól czy zaznaczenie odpowiednich opcji. Aby uruchomić skrypt napisany w języku JavaScript trzeba posiadać przeglądarkę internetową Netscape Navigator w wersji przynajmniej 2.0 lub Microsoft Internet Explorer w wersji 3.0. [35]

JavaScript injection
Polega to na osadzeniu w treści atakowanej strony kodu (zazwyczaj JavaScript), który po wyświetleniu przez innego użytkownika powoduje wykonanie przez niego niepożądanych akcji. Jedną z takich akcji może być przesłanie pliku cookie atakującemu. [68]

K

Karta kodów jednorazowych
Wykaz haseł służących do potwierdzenia tożsamości w transakcjach internetowych, najczęściej bankowych. Każde z haseł wskazanych na karcie ma swój kolejny numer i może być użyte tylko raz – system prosi o podanie kolejnego hasła.

Keygen – (ang. KEY GENerator)
Program generujący na podstawie danych dowolnego użytkownika odpowiedni kod odblokowujący/uruchamiający dany program. Keygeny są uważane za wskaźnik poziomu wiedzy crackera, gdyż zwykle zawierają one albo odwrócone algorytmy kodujące, albo odkodowane z oryginalnej procedury występującej w rzeczywistym programie.

Keylogger
Jeden z rodzajów oprogramowania typu snoopware przeznaczonego do śledzenia działań użytkownika komputera, np. do kontrolowania zachowań pracowników firmy, dzieci w domu itd. Keylogger działa potajemnie i zapisuje uderzenia w klawisze, a czasem także wygląd ekranu, pozwalając osobie kontrolującej sprawdzać, czym się zajmuje użytkownik komputera. Keyloggery mogą być wykorzystywane również do przejmowania poufnych danych (loginów rejestracyjnych użytkownika, haseł, numerów kart kredytowych, kodów PIN itd.). Wirusy typu backdoor zazwyczaj posiadają wbudowany keylogger. Poufne dane przekazywane są hakerowi, który otrzymuje nieautoryzowany dostęp do zasobów sieci lub firmy. [11]

Koń trojański lub trojan
Niewielki program dołączany zwykle skrycie do załącznika poczty elektronicznej lub jakiegoś programu. Nazwa nawiązuje do konia trojańskiego, w którym ukrywali się żołnierze greccy. Program zawiera ukryty kod umożliwiający hakerowi przejęcie kontroli nad zainfekowanym komputerem i przedostanie się za jego pośrednictwem do zabezpieczonej sieci. Najsłynniejszymi koniami trojańskimi są: Back Orifice i NetBus. W społeczności hakerów używanie koni trojańskich oznacza pójście na łatwiznę, stąd też wszyscy, którzy takich programów używają są wykluczani z ich społeczności i okrzyknięci lamerami. [86]

Kradzież pieniędzy z rachunku

Najczęściej odbywa się to z wykorzystaniem zainstalowanego w komputerze ofiary wirusa, który podgląda i inwigiluje poczynania użytkownika. W trakcie logowania do konta, wirus przejmuje dane (loginy i hasła) logowania. Następnie klient odbiera fałszywy komunikat, aby zwrócił się do banku o przesłanie kodu sms i wpisał go w podanym polu (na sfałszowanej stronie banku lub innej, udającej oficjalną), przez co potwierdza, że zatwierdza inną transakcję, niż planował. Oszukany w ten sposób ustala zmienionego odbiorcę przelewów. Potem hacker ponownie loguje się na konto ofiary, kradnie pieniądze ze wszystkich rachunków i zaczyna wysyłać przelewy na rachunki podstawionych osób (tzw. słupów).

Inny sposób wymaga zdobycia numeru telefonu klienta (np. przesyłając mu komunikat z żądaniem wpisania numeru telefonu na ekranie obserwowanego komputera), a następnie wysłania mu wirusa (pod pozorem aktualizacji programu), który ma zadanie przekierowywać smsy autoryzacyjne do hackera.

Kolejny sposób dotyczy najczęściej komputerów ogólnie dostępnych, z których może korzystać wiele osób (np. kafejki internetowe). Złodziej instaluje w komputerze oprogramowanie, które potrafi zamieniać numer konta w tzw. schowku na komputerze. Jeśli przeklejamy (na zasadzie copy-paste) numer rachunku z jakiegoś dokumentu, żeby go wpisać do druku przelewu, dokonujemy autoryzacji przelewu, ale na zamienione konto. [71]

Pamiętajmy również, że żaden bank nigdy nie poprosi nas sam z siebie o podanie hasła autoryzacyjnego – zwykle przypomina o tym klientowi w trakcie logowania do konta.

Kruegerware lub Kruegerapps

Nazwa złośliwego oprogramowania, które jest trudne do naprawienia. Nazwa pochodzi od Freddy'ego Kruegera, postaci z filmu „Koszmar z ulicy Wiązów" i nawiązuje do zdolności powracania do istnienia. Wirusy takie odtwarzają się nawet po usunięciu z komputera, na przykład przy wykorzystaniu mechanizmu odzyskiwania systemu Windows. Najczęściej to określenie tyczy się wirusów komputerowych, malware i spyware. [86]

Kryptowaluta

Kryptowaluta (inaczej waluta kryptograficzna), to nowy, rozproszony w sieci system ewidencji księgowej gromadzący informacje o stanie posiadania w umownych jednostkach. Główną cechą kryptowaluty jest to, że funkcjonuje ona jak wirtualna waluta. Właściciel takiej kryptowaluty przechowuje ją na swoim komputerze lub w smartfonowej aplikacji w tzw. „portfelu", do którego dostęp ma tylko on. W razie dokonywania transakcji, odbywa się ona drogą elektroniczną, dokładnie pomiędzy nim, a kontrahentem. Każda jednostka kryptowaluty, ma unikalny kod, w którym zawarte są informacje przeciwdziałające jej kopiowaniu czy ponownemu przesłaniu.

Kluczowe dla koncepcji kryptowalut jest także to, że w obrocie nimi nie występuje żaden regulator. Nie ma więc „centralnego banku krypowaluty", który może decydować np. o zwiększeniu podaży kryptowaluty i przez to spadku jej wartości. O tym, ile danej

kryptowaluty znajdzie się w obiegu decyduje jej twórca na etapie tworzenia systemu. Jej wartość znajduje się w rękach wolnego rynku. [21]

L

Likejacking

Rodzaj phishingu polegającego na gromadzeniu fanów poprzez automatyczne „polubienie" danego profilu lub strony na Facebooku. Użytkownik jest wabiony atrakcyjną treścią umieszczoną na wallu swojego znajomego (najczęściej o treści erotycznej), jednak w linku nie kryje się obiecywana zawartość. Po kliknięciu w ten wpis przenoszeni jesteśmy do strony, która powoduje automatyczne „polubienie" jej przez nas bez naszej wiedzy i umieszczenie tej informacji na naszym profilu. Dzięki temu taki spam szybko rozprzestrzenia się wśród kolejnych osób. Zazwyczaj na docelowej stronie znajduje się również szkodliwe oprogramowanie (trojany, wirusy itp.), które dodatkowo narażają użytkownika na niebezpieczeństwa. Ważne jest więc posiadanie programu antywirusowego lub typu Internet Security z aktualną bazą wirusów, który uchroni nas przynajmniej przed infekcją. Najlepiej unikać klikania w podejrzane treści umieszczane teoretycznie przez naszych znajomych, aby uchronić się przed likejackingiem. [86]

Log, wykaz logowań

Log (od nazwy stosowanej w wojsku: dziennik, plik dziennika, rejestr zdarzeń) – chronologiczny zapis informacji o zdarzeniach i działaniach odnoszących się do systemu informatycznego, systemu komputerowego czy komputera. Log budowany jest samoczynnie przez program komputerowy, a sama operacja zapisywania do pliku logu nazywana jest logowaniem – nie jest to tożsame z logowaniem w celu uzyskania uwierzytelnienia.

Logi służą do analizowania pracy systemu informatycznego, np. budowania statystyk, detekcji prób włamań do systemu i metody ich przeprowadzenia oraz wykrywania wszelkich pomyłek i nieprawidłowości działającego oprogramowania.

Typowy wpis w logu zawiera m.in. następujące informacje:

- względny lub bezwzględny czas zdarzenia (np. data i godzina);
- rodzaj zdarzenia, identyfikator (często wykorzystywany do rozdzielania informacji na kilka strumieni danych);
- nazwa użytkownika, programu, procesu generującego wpis;
- dane o pobieranych plikach;
- adres IP jeżeli operacja dotyczy komunikacji przez sieć;
- kwalifikacja zdarzenia (poważny błąd, ostrzeżenie, raport z normalnego przebiegu prac, bardzo szczegółowy);
- tekstowy opis zdarzenia;
- każda informacja potrzebna administratorowi systemu, a możliwa do odczytania w sposób alfanumeryczny. [79]

M

Makrowirus lub wirus makro

Wirusy według firmy zwalczającej wirusy często klasyfikowane są według rodzajów infekowanych obiektów. Makrowirusy dodają swój kod do makr kojarzonych z dokumentami, arkuszami kalkulacyjnymi i innymi plikami danych. Pierwszy makrowirus – Concept – pojawił się w lipcu 1995 roku. W krótkim czasie makrowirusy stały się dominującym typem wirusów. Makrowirusy były pierwszym typem wirusów, które celowo dodawały swój kod do plików danych. Wirusy te były bardzo łatwe do napisania (lub skopiowania) dla potencjalnych autorów. W ten sposób nowy makrowirus dawał początek wielu nowym wariantom. Wreszcie wirusy te wykorzystywały do rozpowszechniania pocztę elektroniczną. Makrowirusy były w ogromnej większości tak skonstruowane, aby mogły rozprzestrzeniać się za pośrednictwem plików tekstowych pakietu Microsoft Office lub innych edytorów tekstów. [32]

Malware – (ang. MALicious softWARE)

Złośliwe oprogramowanie, które powoduje utrudnienia i przeszkody w pracy na komputerze, może mieć również działanie przestępcze (zdobywanie poufnych danych) lub w jakikolwiek sposób szkodzić użytkownikowi. Do malware zaliczamy:

- wirusy komputerowe;
- konie trojańskie
- spyware;
- backdoor;
- exploity;
- rootkity
- dialery i inne. [86]

N

NAT (translacja adresów sieciowych)

NAT to w rozwinięciu „Network Address Translation", czyli konwersja adresów sieciowych. Konwersja umożliwia wielu urządzeniom, zwykle połączonym w sieci lokalnej, na korzystanie ze wspólnego adresu widocznego w Internecie. Również dostawcy internetowi zwykle oferują routery domowe z obsługą NAT. Sprawia to, że dostawca usług może przydzielić nam ze swojej skromnej puli tylko jeden adres IP, a my możemy korzystać z domowego Internetu przy użyciu nieograniczonej (w praktyce ograniczonej, ale bardzo dużej) liczby urządzeń. [43]

Nielegalny handel lekami, anabolikami i sterydami

Ustawa Prawo farmaceutyczne przewiduje za nielegalną sprzedaż leków do 2 lat więzienia. Nie jest to to samo, co handel nielegalnymi narkotykami, który w pewnych okolicznościach jest uznawane za zbrodnie. Kupowanie leków na receptę nigdy nie jest karalne.

Sprzedaż wysyłkowa produktów leczniczych typu OTC (wydawanych bez recepty) przez apteki ogólnodostępne i punkty apteczne jest prawnie dopuszczalna. Jednak sprzedażą detaliczną leków niewymagających recepty mogą zajmować się wyłącznie podmioty uprawnione do wykonywania tej usługi.

Według statystyk Polacy najczęściej kupują leki na receptę. Często jednak te medykamenty są bardzo drogie, dlatego też pacjenci szukają sposobności do zaopatrzenia się w niezbędne środki w innych miejscach, w tym również aptekach internetowych. Apteki internetowe oferują bowiem czasami nawet o 20% niższą cenę od tej w sprzedaży stacjonarnej. Problemem dla pacjentów jednak okazał się brak odpowiedniej regulacji prawnej dotyczącej sprzedaży przez Internet leków na receptę. Brak odpowiedniego przepisu w prawie farmaceutycznym ograniczył dla pacjentów szanse na zakup tańszych leków. [11]

Ostatnie zmiany przepisów sformalizowały definicję sprzedaży wysyłkowej, dzięki czemu nie ma możliwości kupienia tańszych leków przez Internet. Naczelna Izba Aptekarska wsparła tego rodzaju inicjatywę twierdząc, że leki sprzedawane przez Internet mogą zagrażać bezpieczeństwu kupujących. Wszystko to powoduje, że nielegalny handel lekami trwa nadal, a pacjenci, którzy szukają oszczędności, narażając swoje zdrowie – ufając niesprawdzonym ofertom, formułowanym przez oszustów lub osoby bez odpowiednich kwalifikacji.

Dlatego na liście ustawowych zakazów związanych z e-handlem czołową pozycję zajmuje handel lekami oraz innymi środkami farmaceutycznymi (mowa o obrocie środkami, które nie zostały dopuszczone do obrotu, są podróbkami w bardzo podobnych opakowaniach do leków oryginalnych, a także substancje sprzedawane na receptę, nielegalna jest też sprzedaż leków będących w fazie testów). [11]

O

Oszustwa za pomocą kart płatniczych: transakcje w sieci i skimming

Przestępstwa skimmingu mogą być zakwalifikowane łącznie jako przestępstwo: z art. 310 § 1 Kodeksu karnego, czyli podrobienie innego środka płatniczego, którym jest karta wydana przez bank (grozi za nie nawet 25 lat pozbawienia wolności) i z art. 267 § 1 Kodeksu karnego, czyli kradzież informacji zakodowanej w pasku magnetycznym karty (grozi za nie kara do dwóch lat pozbawienia wolności) oraz z art. 278 § 1 Kodeksu karnego, czyli kradzież pieniędzy z konta przypisanego do danej karty (grozi za nie kara do pięciu lat pozbawienia wolności). [18]

Portal Dziennik.pl podaje, że od lipca do grudnia 2014 roku dokonano w Polsce 40 461 oszustw za pomocą kart płatniczych. To wzrost w stosunku do pierwszego półrocza o ok.

11 proc. I najgorszy wynik w historii tych badań w Polsce – wynika z danych Narodowego Banku Polskiego, zawartych w raporcie na temat funkcjonowania polskiego systemu płatniczego w drugiej połowie 2014 r. [54]

Najwięcej, niemal 42 proc, operacji oszukańczych dokonano w kategorii, do której banki zaliczają transakcje internetowe. W stosunku do pierwszej połowy 2014 r. oznacza to wzrost o ponad 6 pkt. proc. Drugą kategorią pod względem liczby fraudów (z angielskiego fraud – oszustwo) były transakcje dokonane kartami skradzionymi, a ich udział wyniósł 29,6 proc. Sfałszowane karty odpowiadają za ponad 18 proc. przestępstw. Reszta to kradzieże za pomocą kart niedoręczonych, zgubionych oraz uzyskanych na podstawie sfałszowanych danych. Raport NBP donosi, że wartość oszustw kartami w drugiej połowie 2014 r. wyniosła 14,6 mln zł, co oznacza wzrost w stosunku do pierwszej połowy roku o niecałe 5 proc. [54]

Mimo dużej dynamiki zarówno liczba, jak i wartość fraudów utrzymuje się na niskim poziomie. Bank centralny wyliczył, że pod względem wartości stanowią one 0,006 proc. całego obrotu dokonanego kartami płatniczymi, co sytuuje nasz rynek w gronie najbezpieczniejszych w Europie.

Zgodnie z ustawą o usługach płatniczych klient nie ponosi odpowiedzialności za transakcje wykonane po zastrzeżeniu karty. W przypadku gdyby doszło do nich nim udało się kartę zastrzec, odpowiedzialność jest ograniczona do równowartości 150 euro. Aby wyeliminować ryzyko strat, można kartę ubezpieczyć. W niektórych bankach polisa taka jest bezpłatna, w innych kosztuje niewiele – kilka złotych miesięcznie. Jednak oprócz przywilejów ustawa nakłada na użytkowników kart obowiązki. Wśród nich jest nakaz starannego chronienia karty i numeru PIN do niej. Klient nie może np. udostępniać swojej karty innym osobom. Mowa tu nie tylko o przyjacielu czy współmałżonku wybierającym się na zakupy, lecz także o sprzedawcy w sklepie. Terminal powinien być tak ustawiony, by użytkownik karty mógł ją samodzielnie zbliżyć lub włożyć do urządzenia bez oddawania karty w ręce sprzedawcy. [54]

Użytkownicy kart zbliżeniowych są dodatkowo chronieni przez rekomendacje NBP. Zgodnie z nimi odpowiedzialność klienta za oszukańcze transakcje bezstykowe kartą zbliżeniową ograniczona jest do równowartości 50 euro. Osoba, która zgubi kartę bezstykową, nie może z tego tytułu ponieść większych strat niż ok. 200 zł. Rekomendacje NBP dają też klientom możliwość rezygnacji z karty bezstykowej. [48]

Oszustwa aukcyjne

Oszustwo, jak i oszustwo komputerowe, zostały określone w Kodeksie karnym (odpowiednio art. 286 i art. 287 k.k.). Istotą oszustwa jest motywowane w celu osiągnięcia konkretnych korzyści majątkowych, doprowadzenie innej osoby do niekorzystnego rozporządzenia mieniem przez wprowadzenie jej w błąd albo wyzyskanie jej błędnej oceny rzeczywistości. Istota tego przestępstwa polega więc na posłużeniu się fałszem jako czynnikiem sprawczym, który ma doprowadzić pokrzywdzonego do podjęcia niekorzystnej decyzji majątkowej. [18]

Na dzień dzisiejszy można mówić o kilku różnych typach zagrożeń związanych z zakupami:

- powszechne wśród oszustów są tzw. aukcje oszukańcze, w których nie wysyłają oni wylicytowanych przedmiotów. Odbywa się to w taki sposób, że po wylicytowaniu przez danego użytkownika towaru, np. odtwarzacza, oszust zamiast tego wysyła mu coś o podobnych gabarytach i wadze, często są to rzeczy o niskiej wartości. Przestępcy podszywają się także pod innych sprzedających. Odbywa się to w taki sposób, że oszust obserwuje aukcję i wysyła do osoby wygrywającej e-maila z prośbą o wpłatę na konto za licytowany przedmiot, cały czas podając się za tamtego sprzedawcę;
- innym niebezpieczeństwem jest kradzież (przejęcie) konta z dużą liczbą pozytywnych komentarzy i za jego pomocą oszukiwanie ludzi, którzy przekonani tymi komentarzami traktują przestępcę jak wiarygodnego sprzedawcę lub kupującego. Sposoby na złamanie hasła są różne i przestępcy często korzystają z wyrafinowanych metod;
- zdarza się, że oszuści zakładają konta w serwisach aukcyjnych za pomocą danych, które wcześniej zostały komuś ukradzione. Pod fałszywą tożsamością zdobywają zaufanie kilku osób, a potem zaczynają realizować aukcje mające na celu oszukanie ludzi;
- z rzadka na aukcjach można kupić towary pochodzące z rabunków, gdyż poprzez aukcje można je szybko sprzedać. Należy więc zawsze sprawdzać numery seryjne danego towaru, o ile nie jesteśmy pewni co do jego pochodzenia.

Opisane wyżej przestępstwa są popełniane przy założeniu, że ze względu na kontakt tylko poprzez sieć zidentyfikowanie sprawcy będzie utrudnione i hackera nie dosięgnie kara. Nie jest to prawdą, bo w przypadku popełnienia przestępstw organy policyjne dysponują bardzo dobrymi środkami do namierzania internetowych złodziei. W przypadku stwierdzenia takiego przestępstwa należy jednak zgromadzić jak najwięcej informacji, które jeszcze prędzej pozwolą Policji na podjęcie właściwych działań:

- informacje na temat sprzedającego (nick z aukcji, dane), numer telefonu, adres e-mail itp.;
- warto posiadać całą korespondencję prowadzoną ze sprzedającym poprzez maila czy portal aukcyjny;
- dowody wpłaty;
- o ile takie miały miejsce, to warto również posiadać zapisy rozmów na komunikatorach, takich jak Skype, GG itp.

Na podstawie zgromadzonych danych organy ściągania mogą podjąć dalsze działania mające na celu zidentyfikowanie oszustwa. Policja korzysta przede wszystkim z danych udostępnionych przez właścicieli portalu aukcyjnego, czyli czasy logowania się przez oszusta oraz numery IP, które pomagają w zlokalizowaniu komputera oszusta.

Także właściciele serwisów aukcyjnych muszą sukcesywnie wprowadzać jak najwięcej technologii, które zmniejszają ryzyko oszukańczych działań. Użytkownicy mogą korzystać choćby z systemu Escrow (jest to transakcja powiernicza, której zadaniem jest zabezpieczenie interesów sprzedawcy i kupującego). Bezpieczeństwo stron uzyskuje się

dzięki uczestnictwu neutralnego powiernika, który nadzoruje realizację umowy oraz rozstrzyga ewentualne spory.

Na podstawie doświadczeń portali aukcyjnych możemy wyróżnić następujące zagrożenia:

- klasyczne oszustwa – czyli ktoś wystawia coś, czego nie ma – to nadal najbardziej powszechna forma popełniania przestępstw poprzez np. serwis Allegro;
- oszustwa związane z wykorzystaniem funkcjonalności serwisu – tutaj królują paczki wysyłane pod zmieniony adres na skutek okazania fałszywych potwierdzeń dokonania płatności;
- kradzieże tożsamości – to najbardziej perspektywiczne z przedsięwzięć i jednocześnie to, które wykorzystuje najbardziej znane metody, w tym phishing i pharming;
- „złote interesy" – przykładowo fałszywe oferty pracy, które za pośrednictwem różnorakich *modus operandi* (łac. sposób działania) doprowadzają do popełnienia przestępstwa;
- naruszenia praw własności intelektualnej – Grupa Allegro posiada program współpracy z właścicielami marek; dzięki temu rozwiązaniu Grupa w ciągu kilkunastu minut udziela odpowiedzi w zgłoszeniach spraw polegających na handlu podróbkami;
- niedostateczna weryfikacja użytkowników przez różne instytucje trzecie, które w połączeniu z anonimowymi (lub pseudo-anonimowymi) środkami płatniczymi oraz siecią TOR ułatwiają dokonywanie przestępstw. [11]

Oszustwo nigeryjskie

Oszustwo nigeryjskie nazywane także 419 Scam (od art. 419 nigeryjskiego Kodeksu karnego, który przewiduje karę za nielegalne przelanie na zagraniczne konta środków pieniężnych), znane jest od XVI wieku. Złodzieje wykorzystują obecnie pocztę elektroniczną i stara metoda ciągle jest skuteczna. Wykorzystuje ona ludzką naiwność i chęć szybkiego wzbogacenia się. Zwykle scenopisy e-maili są różne, jednak opierają się na tym samym szablonie. Do skrzynki pocztowej ofiary wpływa e-mail z informacją, że sympatyczny nieznajomy z Afryki właśnie wygrał na loterii i chętnie się wygraną podzieli. Jednak wcześniej prosi o niewielką pożyczkę z przeznaczeniem na koszty odbioru nagrody, prowizję bankową czy opłatę skarbową.

Ofiara jest na wiele sposobów zapewniana, że otrzyma dużą część pieniędzy, ale najpierw musi wpłacić niewielką kwotę. Jeżeli przekażę oszustom pieniądze, to nigdy więcej ich nie zobaczy. [51]

Oszustwa matrymonialne

Najczęściej mają postać anonsów matrymonialnych dla mężczyzn wysyłanych na przypadkowo pozyskany adres e-mail. Zwykle młodą, atrakcyjną kobietą okazuje się Rosjanka czy Ukrainka, która chce przyjechać do kraju poznanego w sieci partnera. Nie posiada jednak dostatecznych środków na finansowanie podróży. Prosi zatem o pomoc poznaną przez Internet osobę. Jeśli mężczyzna da się na to nabrać, w niedługim czasie okazuje się, że zarówno kontakt, jak i przesłane pieniądze przepadły. [91]

P

Patcher lub crack-maker

Program stworzony w celu ułatwienia pracy crackerom. Tworzy on po prostu cracki (hasła lub pliki dostępowe) poprzez porównanie plików – oryginalnego i odbezpieczonego i wykryciu różnic. Zasadniczo wyróżniamy dwie kategorie crack-makerów (łamaczy haseł): static patcher i generic patcher. Ten pierwszy tworzy patcha, (program odbezpieczający), który modyfikuje podane mu miejsce w pamięci, a więc nadaje się tylko do jednej konkretnej wersji programu ofiary. Drugi działa bardziej „inteligentnie", wyszukuje jakiś ciąg tzw. opkodów (kodów bajtowych) charakterystyczny dla procedury sprawdzającej status programu, a występującej w kilku wersjach danej aplikacji, i tworzy cracka zmieniającego odpowiedni jej fragment, biorąc za podstawę miejsca do odbezpieczenia programu wyszukany strumień bajtów. [86]

Phishing

Phishing polega na wysyłaniu do przypadkowych osób korespondencji e-mailowej, w której odbiorcy pod wymyślonym pretekstem namawiani są do zalogowania się pod fałszywy adres. Zwykle udaje on stronę logowania banku, urzędu lub popularnego portalu. Atakowany ma kliknąć w załączony w e-mailu link. Następuje wtedy przekierowanie na stronę sfałszowaną przez cyberprzestępców. W trakcie logowania nieświadomy klient podaje swój login i hasto przestępcom. Uzyskują oni w ten sposób kontrolę nad rachunkiem lub kontem klienta na portalu internetowym.

Zgodnie z art. 190a Kodeksu karnego, dodanym do kodeksu nowelą 25 lutego 2011 r. w §2 spenalizowany został również phishing (wykorzystanie wizerunku lub innych danych osobowych w celu wyrządzenia szkody majątkowej lub osobistej). [69]

Innym przykładem może być pojawienie się wirusa Zeus. Klient infekuje swój komputer złośliwym oprogramowaniem po otwarciu niebezpiecznego pliku (np. załącznik do maila) lub w trakcie odwiedzania słabo zabezpieczonych stron internetowych (również tych niebudzących podejrzenia; stopień ich zabezpieczenia nie zależy od zamieszczonych treści, ale wyłącznie od profesjonalizmu administratorów). Infekcja nie jest widoczna do chwili zalogowania się na stronie bankowości elektronicznej banku, który znajduje się na liście w pliku konfiguracyjnym trojana (np. Popularny_Bank_Polski_24). Trojan Zeus p2p po zalogowaniu modyfikuje lokalnie na zainfekowanym komputerze klienta wygląd oryginalnej strony banku. W efekcie klient otrzymuje informację (rzekomo z banku) o tym, że w ramach testowania bankowości elektronicznej bank prosi o dokonanie przelewu testowego w kwocie X na rachunek XYZ. Komunikat jest podstawiony przez trojana i nie pochodzi z banku, ale wymusza na kliencie, dzięki ww. socjotechnice, zatwierdzenie oszukańczego przelewu za pomocą używanego przez klienta sposobu autoryzacji. [30]

Pharming lub zatruwanie DNS

Sposób ataku sieciowego wykrytego przez firmę Symantec i Wydział Informatyki na Uniwersytecie Indiana (USA). W tradycyjnym ataku typu „pharming" hacker stara się przekierować użytkownika odwiedzającego witrynę internetową do strony sfałszowanej. Może to osiągnąć, modyfikując plik hosts w komputerze ofiary lub wprowadzając zmiany w systemie DNS (Domain Name System) (patrz również „drive-by pharming"). [11]

PHP

PHP jest językiem skryptowym służącym do rozszerzania potencjałów stron internetowych. Jego składnia jest bardzo podobna do powszechnych języków programowania C/C++, lecz jest wysoce uproszczona – programista PHP zazwyczaj nie musi przejmować się bezbłędnością typów zmiennych, przydzielaniem dla nich pamięci itp. Dodatkowo wbudowana obsługa wielu popularnych baz danych ułatwia twórcy operacje na tych bazach. Dzięki połączeniu z biblioteką GD możliwe jest także dynamiczne tworzenie obrazków GIF (starsze wersje GD) lub PNG (nowsze wersje). [55]

Physical Infrastructure Attack

Jeden z rodzajów ataku sieciowego typu DoS przynależny do grupy exploitów. Jest to jeden z podstawowych sposobów na to, by komputer podłączony do sieci przestał działać. Polega to na fizycznym przerwaniu kabla łączącego komputer z siecią. W przypadku bardziej rozbudowanych sieci komputerowych dane mogą być łatwo kierowane inną trasą. Aby móc w ogóle przystąpić do takiego ataku, niezbędny jest fizyczny dostęp do sprzętu sieciowego (np. wiązki kabli) w pobliżu atakowanego komputera. [11]

Ping flood

Popularny sposób ataku na serwer internetowy polegający na przeciążeniu łącza pakietami ICMP (internetowy protokół komunikatów kontrolnych) generowanymi na przykład przez program ping (ping wysyła komunikat echo request z adresem IP celu, a w zamian dostaje odpowiedź reply jeżeli urządzenie jest dostępne lub komunikat błędu, jeżeli nie). Przeprowadza się go za pomocą komputera posiadającego łącze o przepustowości większej niż przepustowość łącza atakowanej maszyny lub za pomocą wielu niezależnych komputerów. [79]

Piractwo komputerowe

Proceder kopiowania licencjonowanego oprogramowania komputerowego, a następnie nielegalnego rozprowadzania i sprzedawania kopii po zaniżonych cenach (wobec cen programów oryginalnych). Ze względu na stosowanie przez producentów oprogramowania zabezpieczeń sprzętowych i programowych, piractwo komputerowe związane jest z działalnością osób nazywanych crackerami i hakerami. Obecnie komputerowe bazy danych stały się produktem handlowym, posiadającym określoną, wymierną cenę. Pojęcie piractwa komputerowego rozciągnięte zostało więc także na wszelkiego rodzaju ingerencje

w zgromadzone dane – kopiowanie poufnych informacji, zmiany oraz kasowanie danych lub grożenie ich skasowaniem. W Polsce – ze względu na relatywnie wysokie ceny zarówno sprzętu, jak i oprogramowania – „piratowanie" programów jest bardzo popularne.

Poachware – (ang. to poach – kłusować, nielegalnie polować)

Rodzaj oprogramowania szpiegowskiego, nastawionego głównie na zdobywanie wrażliwych informacji typu nazwy użytkownika czy hasła.

Polimorfizm – (z gr. – wiele form)

Polimorfizm to jedna z cech niektórych wirusów, która utrudnia ich rozpoznanie i usunięcie. Wirusy polimorficzne są zmiennie szyfrowane. Są trudne do wykrycia ponieważ zmieniają własną „formę" wraz z każdą infekcją, co uniemożliwia programom antywirusowym ich zwalczanie poprzez poszukiwanie stałej sekwencji bajtów. W efekcie programy antywirusowe muszą używać skomplikowanych technik do identyfikowania i usuwania wirusów polimorficznych, łącznie z emulacją kodu lub specjalistycznymi algorytmami matematycznymi. [32]

Pornografia dziecięca w Internecie

Zgodnie z art. 202 Kodeksu karnego „kto publicznie prezentuje treści pornograficzne w taki sposób, że może to narzucić ich odbiór osobie, która tego sobie nie życzy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". Kolejne paragrafy 3 i 4 koncentrują się szczególnie na pornografii dziecięcej i tak za rozpowszechnianie produkcję, utrwalanie lub sprowadzanie, przechowywanie lub posiadanie albo rozpowszechnianie lub prezentowanie treści pornograficznych z udziałem małoletniego (...) podlega karze pozbawienia wolności od lat 2 do 12. Za utrwalanie treści pornograficznych z udziałem małoletniego grozi kara pozbawienia wolności od roku do lat 10. Także ten, kto dla zaspokojenia seksualnego uczestniczy w prezentacji treści pornograficznych z udziałem małoletniego podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. [18]

W kwietniu 2014 r. weszła w życie nowelizacja Kodeksu karnego prezentowana przez Ministerstwo Sprawiedliwości jako wprowadzająca większą ochronę małoletnich przed pornografią. Tworzy ona klasę zakazanych treści, dla których samo obejrzenie na terenie Rzeczpospolitej wiąże się z sankcją karną. Do tej pory prokuratura ścigała tych, którzy rozpowszechniali i posiadali materiały pornograficzne z udziałem małoletnich, teraz karane będzie także uzyskanie do nich dostępu. Zmieniono również definicję pornografii dziecięcej – są to teraz materiały z udziałem małoletnich poniżej 18. roku życia, a nie jak dotychczas, poniżej 15. roku życia. [24]

Według raportu z badania gemiusReport przeprowadzonego na zlecenie Fundacji Dzieci Niczyje świadomość zagrożeń związanych z tym zjawiskiem, a zwłaszcza odpowiedzialności karnej za upowszechnianie pornografii, pozostaje w Polsce w dalszym ciągu ograniczona. Zdaniem co trzeciego użytkownika sieci (34%) za pornografię dziecięcą polskie

prawo uznaje materiały pornograficzne z udziałem dzieci/młodzieży do 18. roku życia. Co czwarty badany sądzi, że pornografia dziecięca to treści i materiały pornograficzne, w których uczestniczą dzieci do 16. roku życia. Jedynie co piąta badana osoba uważa, że cenzus wyznacza 15. rok życia.

W opinii co dziesiątego internauty samo przeglądanie czy zapisanie na dysku pornografii dziecięcej nikogo nie krzywdzi, więc nie powinno być karane. Opinię taką częściej wygłaszają mężczyźni (14%) niż kobiety (10%). Zdecydowana większość użytkowników sieci (80%) jest przeciwnego zdania (84% kobiet oraz 76% mężczyzn), a 8% nie ma poglądu na ten temat.

Zdecydowana większość badanych (77%) uważa, że dostawcy Internetu powinni „automatycznie, obowiązkowo i bezwarunkowo" blokować dostęp internautów do treści pornograficznych z udziałem dzieci. Co ciekawe, pogląd ten podziela większy odsetek kobiet (84%) niż mężczyzn (70%). Pięć razy więcej mężczyzn (10%) niż kobiet (2%) sądzi natomiast, że automatyczne blokowanie tego typu treści jest ingerencją w wolność Internetu (pornografia dziecięca w Internecie raport z badania gemiusReport przeprowadzonego na zlecenie Fundacji Dzieci Niczyje). [60]

Niebezpiecznym problemem jest stale rosnąca liczba osób małoletnich pokrzywdzonych przez zjawisko pornografii. Warto pamiętać, że liczba ujawnionych przypadków stanowi tylko wierzchołek góry lodowej, gdyż wiele przypadków pozostaje nieujawnionych.

Portfel kryptowalutowy, adres kryptowalutowy

Według informacji portalu bitcoin.pl portfele takie dzielimy na 5 grup:

1) portfele w postaci aplikacji na komputer. Portfeli tych możemy używać wyłącznie na komputerze, na którym są zainstalowane, więc ich mobilność jest niska. Oczywiście możemy taki portfel zainstalować na kluczu USB (pendrive) i korzystać z niego na niemal każdym komputerze, jednak mobilność nadal pozostaje mało satysfakcjonująca. Portfele te dzielą się na:
   a) pełne. Przechowywujące cały łańcuch bloków (Blockchain). Długi czas synchronizacji,
   b) lekkie. Łańcuch bloków przechowywany jest na serwerach, a nie na komputerze jak w przypadku portfeli pełnych. Cechują się szybką synchronizacją z siecią;
2) portfele offline (bez kontaktu z Internetem). Służące jako sejf do przechowywania bitcoiów. Mobilność bardzo niska z wyjątkiem Paper Walleta, który umożliwia np. wydruk banknotu o dowolnym nominale. Portfele: Paper Wallet;
3) portfele przeglądarkowe – udostępniane przez serwis świadczący tego typu usługi. Do korzystania z portfela potrzebujemy jedynie przeglądarki na dowolnym komputerze/telefonie/tablecie. Duża mobilność kosztem mniejszego bezpieczeństwa, gdyż bezpieczeństwo naszych środków zależy już od osób trzecich;
4) portfele mobilne – Portfel jako aplikacja na telefony/tablety. Jak sama nazwa wskazuje portfele te cechują się bardzo dużą mobilnością. Umożliwiają np. błyskawiczną zapłatę w restauracji lub w dowolnym miejscu/serwisie internetowym przez zeskanowanie kodu QR;

5) portfele sprzętowe – w postaci klucza USB. Bardzo bezpieczne lecz z ograniczoną mobilnością. Możemy używać na dowolnym komputerze z wolnym gniazdem USB. [5],[7]

Public domain

Według portalu kompinf.cba.pl. jest to licencja dobroczynna czyniąca z oprogramowania własność ogółu, w myśl której autor lub autorzy oprogramowania zrzekają się praw autorskich lub prawa te wygasły. Czas ich trwania określa prawo. Są one ważne:

- przez cały czas życia twórcy i 70 lat po jego śmierci;
- jeżeli twórca nie jest znany – 70 lat liczy się od daty pierwszego rozpowszechnienia programu;
- jeżeli z mocy ustawy autorskie prawa majątkowe przysługują innej osobie niż twórca – 70 lat liczy się od daty pierwszego rozpowszechnienia programu;
- jeżeli program nie został rozpowszechniony – 70 lat liczy się od daty jego ukończenia.

Wówczas oprogramowanie takie staje się wolnym dla ogółu społeczeństwa i może być wykorzystywane bezpłatnie przez każdego. [36]

Prawa autorskie w Internecie

Zasady korzystania z cudzych utworów uregulowane są ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. 1994 nr 24 poz. 83), zwaną prawem autorskim. Zgodnie z art. 1 przedmiotem prawa autorskiego jest każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia. Jest to definicja uniwersalna dla wszystkich dzieł twórczych. Tak rozumiany utwór podlega ochronie prawnej, niejako automatycznie, już od chwili jego ustalenia. Jako przykład wskazać należy teksty publikowane w Internecie, filmy, nagrania muzyczne, programy komputerowe, itp. Ich autorom przysługuje ochrona, a tym samym możliwość egzekwowania odpowiedzialności cywilnej i karnej. [28]

Odpowiedzialność karna w tym zakresie określają szczegółowo art. 115 do 119 ustawy o prawie autorskim (Dz. U. 1994, nr 24, poz. 83). Odpowiedzialność ta może, w zależności od rodzaju wyszczególnionego w ustawie przestępstwa, dotyczyć kar, poczynając od grzywny, nawet do pozbawienia wolności na okres od roku do lat 5.

Naruszanie praw autorskich jest coraz powszechniejsze. Szczególnie dotyczy to fotografii, gdy często pisząc artykuły bądź zakładając blogi używamy pasujących do tematu obrazów. Często nieświadomie naruszamy przy tym prawa autorskie. Samo ściąganie (czyli pobieranie, kopiowanie) utworu już opublikowanego w sieci, nie stanowi naruszenia prawa. Stanowi ono tzw. dozwolony użytek osobisty. Oznacza nieodpłatne korzystanie z już dostępnego w sieci wytworu. Nie wymaga to wyrażenia zgody ze strony twórcy. Nieistotne jest, czy plik jest ściągany na dysk komputera, czy tylko oglądamy w przeglądarce internetowej. Takie korzystanie może dotyczyć m.in. książki lub filmu albo sporządzenia pojedynczej kopii utworu. Dozwolony użytek osobisty nie może naruszać normalnego korzystania z utworu ani godzić w interesy twórcy. Udostępnianie takich plików jest już przestępstwem.

Do rozpowszechniania i często nielegalnej sprzedaży plików audiowizualnych stosowane są narzędzia takie jak:

- peer-to-mail (w skrócie P2M) – technologię wymiany plików opierającą się o wykorzystanie kont pocztowych w charakterze miejsca ich przechowywania;
- peer-to-peer (w skrócie P2P) – model komunikacji w sieci komputerowej, zapewniający wszystkim hostom te same uprawnienia, w odróżnieniu od architektury klient-serwer. [11]

Według Małej sieciowej encyklopedii P2P, czyli peer-to-peer (z ang. każdy z każdym) jest siecią komputerową, która umożliwia komunikację swoich użytkowników na równorzędnych zasadach. Każdy korzystający z tego rodzaju internetowej aplikacji może w dowolnej chwili zainicjować połączenie. Struktura P2P jest płynna, czyli zależna od liczby zalogowanych osób i nie posiada centralnego serwera. Technologia ta służy do bezpośredniej wymiany plików pomiędzy użytkownikami, dzięki uzyskanemu dostępowi do zawartości ich twardych dysków. [44]

Przekręt z Xi'anu

Ten sposób oszustwa popełniany przez chińskich przestępców wobec firm z Europy Wschodniej był stosowany już w latach 90., ale wówczas ofiarami padały głównie firmy z USA. Ten osobliwy rodzaj wyłudzeń jest nazywany przez pracowników WPHI (Wydziały Promocji Handlu i Inwestycji przy ambasadach i Konsulatach Generalnych RP) przekrętem z Xi'anu, ponieważ wszystkie firmy, które go stosują, pochodzą właśnie z tego starożytnego miasta, słynącego z Terakotowej Armii cesarza Cin Shi Huanga. Szwindel jest na tyle popularny, że ponad 40 proc. firm znajdujących się na czarnej liście prowadzonej przez WPHI to firmy z Xi'anu. [76]

Przekręt polega na tym, że nieznany oferent z terenu Azji kontaktuje się z firmą przez Internet i składa duże zamówienie na jej produkty. Przeważnie wartość takiego zamówienia waha się pomiędzy 500 tys. a nawet milionem euro. Prosi jedynie o pokrycie przez stronę polską połowy kosztów manipulacyjnych umowy. Opłata wydaje się niewielka wobec sumy, na jaką ma opiewać umowa.

Zdarzają się nawet przypadki zaproszenia polskiej firmy do wizyty w danym kraju, by uroczyście podpisać korzystny dla niej kontrakt. Wówczas „opłaty manipulacyjne" wyłudzane są na miejscu, w gotówce. Zdarza się też scenariusz z „wymianą prezentów". Przestępcy wręczają Polakom upominki opatrzone metkami z wysokimi cenami, a następnie sugerują, że strona polska powinna się odwdzięczyć podarkami o podobnej wartości. Proponują jednocześnie konkretne sklepy, gdzie takie prezenty można nabyć. [13]

R

Ransomware – (ang. ransom – okup)

Rodzaj oprogramowania używanego w przestępczości internetowej. Działanie tego typu polega na przeniknięciu wirusa do wnętrza atakowanego komputera i zaszyfrowaniu dysku należącego do użytkownika. Potem wirus umieszcza w komputerze notatkę. Hacker

pisze w niej, co musi zrobić właściciel cennych plików, aby je odzyskać. Zwykle domaga się przelania pieniędzy na konto w banku elektronicznym i obiecuje, że w zamian wyśle klucz oraz instrukcje jak odszyfrować dane.

Odpowiada to sytuacji, gdy ktoś przyjdzie do twojego domu zamknie twoje rzeczy w sejfie i nie poda ci kombinacji – stwierdził Oliver Friedrichs dyrektor do spraw bezpieczeństwa w korporacji Symantec. [77]

Są sposoby, żeby bronić się przed zaszyfrowaniem cennych danych. Najważniejszy z nich to robienie kopii bezpieczeństwa cennych plików. Jeżeli ktoś tego nie robi regularnie, to nie potrzeba internetowego przestępcy, żeby np. jego dysk twardy sam uległ awarii.

Dane zaszyfrowane przez program w małej liczbie wypadków są szyfrowane na tyle prostym szyfrem, że da się je złamać. Złamanie większości algorytmów szyfrujących wysokiej klasy jest zadaniem wyjątkowo trudnym, praktycznie niemożliwym bez dostępu do systemów komputerowych o bardzo wysokiej mocy obliczeniowej. [92]

Rootkit

Zbiór programów wykorzystywanych przez hakerów dla uniknięcia wykrycia w trakcie włamywania się do atakowanego komputera. Haker może to osiągnąć poprzez zamianę plików lub bibliotek systemowych lub zainstalowanie modułu jądra. Haker instaluje rootkita dzięki uzyskaniu dostępu do atakowanego systemu na poziomie użytkownika: najczęściej łamie stosowane hasło lub wykorzystuje lukę w zabezpieczeniach oprogramowania. Termin „rootkit" wywodzi się ze środowiska oprogramowania w języku Unix, jednak obecnie najczęściej stosowany jest w odniesieniu do technik wykorzystywanych przez autorów trojanów przeznaczonych dla systemów MS Windows w celu ukrywania obecności i aktywności szkodliwego kodu. Ze względu na to, że wielu użytkowników systemów MS Windows pracuje z prawami administracyjnymi rootkity coraz bardziej zyskują na popularności. [11]

S

Samobójstwa z inspiracji sieci

Internet bywa miejscem, w którym ludzie nawiązują przyjaźnie, ale kiedy osoby z samobójczymi skłonnościami doradzają sobie nawzajem bez nadzoru specjalistów, staje się niebezpieczny. Mamy tu do czynienia z dwoma zasadniczymi przypadkami:

- osoba trzecia udziela poprzez sieć osobie zdesperowanej z różnych pobudek wskazówek i pomocy w popełnieniu samobójstwa oraz
- dwie lub więcej osób, opanowanych depresją, umawiają się poprzez sieć w celu jednoczesnego popełnienia samobójstwa.

Należy pamiętać, że Kodeks karny zawiera w art. 151 zagrożenie karne za pomoc udzielaną w samobójstwie: „kto namową lub przez udzielenie pomocy doprowadza człowieka do targnięcia się na własne życie, podlega karze pozbawienia wolności od 3 miesięcy do lat 5". [18]

Scam

Działanie, którego celem jest wprowadzeniu kogoś w błąd, sugerując jakoby był właścicielem (posiadaczem) określonego dobra, zwykle finansowego (np. wygranej na loterii, gadżetu promocyjnego). Celem tego działania jest przeprowadzenie trudnego do udowodnienia oszustwa. Najpopularniejszą formą scamu jest korespondencja w formie tradycyjnej lub elektronicznej – odmiana spamu.

Script kiddie (ang. skryptowy dzieciak)

W żargonie komputerowym negatywne określenie dla niedoświadczonych crackerów, którzy używają programów i skryptów napisanych przez innych bez wiedzy o zasadach ich działania w celu uzyskania nieuprawnionego dostępu do komputerowych kont lub plików, a także aby przeprowadzać ataki na całe systemy komputerowe (zobacz: DoS). Na ogół crackerzy ci nie potrafią sami napisać takich programów. Zazwyczaj nie atakują oni konkretnego celu, lecz skanują tysiące komputerów w sieci w poszukiwaniu celów podatnych na ataki. [20]

Seksting

Według materiałów opublikowanych na stronie Fundacji Dzieci Niczyje w artykule M. A. Moreno, Y. Reid Chassiakos, C. Crossa, dotyczących korzystania z mediów przez dzieci i młodzież w wieku szkolnym przytoczono, że w USA obecnie 76% nastolatków korzysta z co najmniej jednego z mediów społecznościowych. Choć Facebook pozostaje najpopularniejszym serwisem społecznościowym, nastolatki zazwyczaj nie angażują się tylko w jedną społeczną platformę mediów. Ponad 70% utrzymuje swoje medialne portfolio na kilku wybranych witrynach, w tym Facebooku, Twitterze i Instagramie. Aplikacje mobilne zapewniają szeroką gamę funkcji, takich jak udostępnianie zdjęć, gry i rozmowy wideo. Autorzy artykułu szacują, że około 12% młodzieży w wieku od 10 do 19 lat co najmniej raz przesłało zdjęcie seksualne do kogoś innego. [24]

Typologie zjawiska sekstingu przedstawili J. Wolak, D. Finkelhor oraz K. J. Mitchell na podstawie przeprowadzonych badań. Przypadki sekstingu podzielili na:

1. **Kwalifikowane** **67%**
   a. o podłożu romantycznym 10%
   b. mające na celu zwrócenie uwagi 19%
   c. spowodowane przez inne motywy 4%
2. **Wynikające z eksperymentowania** **33%**
   a. z udziałem osób dorosłych 36%
   b. wyłącznie z udziałem młodzieży 31%
      – w celu skrzywdzenia 12%
      – bez złych intencji 19%.

W ostatnich latach również w Polsce, zwłaszcza wśród młodzieży, upowszechniła się moda na przesyłanie za pomocą Internetu lub komórki nagich zdjęć i filmów. Z badań przeprowadzonych na zlecenie Fundacji Dzieci Niczyje wynika, że co dziewiątemu nastolatkowi w Polsce w wieku 15-18 lat zdarzyło się wysłać swoje rozbierane fotki.

Jak koszmarne skutki może wywołać seksting pokazuje jeden z przypadków opisany w polskiej prasie w 2006 r. Gdy w szkole nauczyciel wyszedł z sali, dwóch chłopców zaatakowało dziewczynkę. Rozebrali ją i dotykali. Trzeci za pomocą telefonu komórkowego sfilmował zajście, którego świadkami byli inni uczniowie. Następnego dnia 14-latka powiesiła się.

Działalność opisana wyżej jest spenalizowana – nawet osoba poniżej 17. roku życia może za to odpowiedzieć przed sądem rodzinnym. Dorosła osoba za rozsyłanie tego typu materiałów może zostać objęta karą do 12 lat więzienia. [24]

Sekty w sieci

Osoby reprezentujące różnego rodzaju sekty religijne, wykorzystując do tego celu sieć, mają ułatwione zadanie przy nawiązywaniu nowych kontaktów. Możliwość nieskrępowanego publikowania w sieci materiałów o dowolnej treści, a nawet bezpośredniej rozmowy przez Skype'a z potencjalnym kandydatem na członka sekty, idealnie nadaje się do pozyskiwania innych do swojej ideologii i zdobywania kolejnych członków. Zauważalny jest wzrost liczby stron WWW, na których wyżej wymienione zagadnienia podane są w sposób bardzo subtelny i zakamuflowany. Czytając tekst, dziecko-ofiara nawet nie zauważa kiedy zaczyna myśleć kategoriami zgodnymi z założeniami sekty, co często jest pierwszym krokiem do konfliktu i izolacji od jego dotychczasowego środowiska. [93]

Session hijacking (przechwytywanie sesji)

Nazywamy tak ataki, w których hacker próbuje uzyskać dostęp do istniejącej sesji użytkownika, tzn. takich gdzie identyfikator został mu już wcześniej przydzielony. Polega to na uzyskiwaniu nielegalnego dostępu do systemów komputerowych na skutek przechwycenia sesji legalnego użytkownika. Opiera się na przesyłaniu w sesji np. adresu IP komputera wraz z nazwą przeglądarki, spod których została ona utworzona, aby następnie porównywać je przy kolejnych wizytach z danymi dostarczonymi przez serwer. [17]

Słownikowa metoda łamania hasła

Określamy tak łamanie hasła za pomocą metody słownikowej polegającej na odczytaniu wybranej listy słów, zakodowaniu ich i sprawdzaniu po kolei przyrównując je do źródła. Program, który korzysta z tej metody odczytuje plik haseł, następnie odczytuje listę słów w pliku, którą podajemy jako słownik, koduje słowa używając tego samego algorytmu co łamany program i sprawdza czy słowo zakodowane z naszego słownika pasuje do zakodowanej wersji hasła. W przypadku łamania słownikowego nie ma 100% pewności, że hasło zostanie odgadnięte ponieważ ta metoda nie sprawdza się w przypadku haseł typu „t9J30nM" czyli będących zbitką przypadkowych liter i cyfr – wtedy lepszym wyjściem jest metoda brute force. Najlepiej używać programu do łamania haseł, który posiada obsługę filtru mutacji słów. Dzięki takiemu zastosowaniu ów filtr dodatkowo sprawdza mutacje słowa np.: „underground" sprawdza też „?„ă3RgRě?„ă" i inne, tak by wydobyć wszystkie kombinacje ze słowa. [86]

Smurf Attack

Jeden z rodzajów ataku sieciowego typu DoS, należący do grupy exploitów. Atakujący wysyła zapytanie ping do dużej liczby hostów (odbiorców). Zanim jednak to zrobi, zmienia nagłówek pakietu danych, modyfikując adres hosta (nadawcy), z którego ping został wysłany (takie działanie nazywamy spoofingiem). Adresem tym jest adres ofiary. Gdy hosty otrzymają zapytanie, odpowiadają na nie do hosta, którego adres był w nagłówku (czyli ten zmieniony). W przypadku bardzo dużej liczby odpowiedzi na zapytania, host--ofiara nie jest w stanie poradzić sobie z napływem dużej ilości danych i zawiesza się, przez co staje się niedostępny. [86]

SMiShing lub SMS phishing

Rodzaj ataku socjotechnicznego podobnego do phishingu. Polega on na rozsyłaniu SMS-ów, które mają skłonić ofiarę do podjęcia określonego (zwykle niekorzystnego) działania. Pierwsze ofiary smishingu na Islandii i Australii otrzymywały SMS-y z potwierdzeniem rzekomego członkostwa w serwisie randkowym oraz informacją o związanej z tym opłacie w wysokości paru dolarów dziennie. Opłaty można było uniknąć anulując członkostwo na wskazanej stronie internetowej. W rzeczywistości otwarcie strony powodowało zainstalowanie na komputerze ofiary trojana otwierającego „tylne wejście" do komputera PC. [79]

Sniffing

Podsłuchiwanie wiadomości w sieci, które nie są adresowane do nas. Jest to możliwe w sieciach LAN. Pakiety od komputera A do komputera B wysyłane siecią lokalną są ignorowane przez wszystkie maszyny po drodze. Tak więc wystarczy tylko znaleźć program, który zainteresuje się owymi danymi i je pokaże. Program taki nazywa się sniffierką, np. Sniffit. Oferuje on dwa tryby pracy – interaktywny i nieinteraktywny. Pierwszy daje nam możliwość na bieżąco oglądania odebranych danych, drugi loguje wszystko do plików. Sniffierki dają nam możliwość filtrowania danych i odbierania tylko tych nas interesujących, np. z danego komputera do innego lub wszystkie połączenia na dany port itd. [63]

Snoopware – (ang. to snoop – wtykać nos)

Oprogramowanie śledzące działania użytkownika komputera, służące szczególnie do kontrolowania zachowań pracowników firmy, dzieci w domu itd. Snoopware działa potajemnie i rejestruje naciśnięcia klawiszy, a także przechwytuje zawartość ekranu, pozwalając osobie kontrolującej inspekcjonować, czym się zajmuje użytkownik komputera – niektóre programy wysyłają także raporty za pomocą poczty elektronicznej. Do snoopware zalicza się keyloggery, cybernianie. [11]

Snort

Snort (ang. niuchacz – sieciowy system wykrywania ataków) to oprogramowanie do wykrywania ataków na komputery poprzez sieci, dostępne na licencji wolnego oprogramowania.

Socjotechnika (social engineering – inżynieria społeczna)

Psychologia społeczna nastawiona jest na zdobywanie informacji o atakowanym systemie od osób pracujących z tym systemem, czyli jest to forma ataku opierająca się na atakowaniu umysłów ludzi, którzy są w stanie dzięki technikom socjologicznym zapewnić nam dostęp do danych, na których nam zależy.

Takim atakiem może być mail/telefon od osoby, która podaje się za administratora systemu, a w rzeczywistości nim nie jest. Socjotechnika to wywieranie wpływu na ludzi i stosowanie perswazji w celu oszukaniu ich tak, aby uwierzyli, że używający socjotechnik jest osobą o sugerowanej przez siebie, a stworzonej na potrzeby manipulacji, tożsamości. Dzięki temu jest on w stanie wykorzystać swoich rozmówców przy dodatkowym (lub nie) użyciu środków technologicznych, do zdobycia poszukiwanych informacji. Ponieważ od dawna wiadomo, że nawet najbardziej zabezpieczony system ma poważną lukę, czyli beztroskiego użytkownika, dlatego ważne jest zatem wcześniejsze przeszkolenie go oraz uświadomienie [26].

Socjotechnika zwrotna

Atak socjotechniczny, gdy hacker kreuje sytuację, w której użytkownik sieci zauważa jakiś problem i kontaktuje się z napastnikiem, prosząc o pomoc. Inna forma socjotechniki zwrotnej polega na odwróceniu ról. Ofiara orientuje się, że została zaatakowana i korzystając z wiedzy psychologicznej, i wywierając wpływ na napastnika stara się wyciągnąć od niego jak najwięcej informacji, w celu ochrony firmy. [26]

Spam – niechciana korespondencja

Według publikacji na portalu Interia.pl eksperci w dziedzinie cyberbezpieczeństwa przeprowadzili analizę spamu w 2014 r. Wynika z niej, że czwarty rok z rzędu programy stworzone w celu kradzieży loginów użytkownika, haseł oraz innych informacji poufnych utrzymują się na szczycie listy najbardziej rozprzestrzenianych szkodliwych programów dystrybuowanych za pośrednictwem poczty e-mail. [49]

Coraz większą popularnością wśród cyberprzestępców cieszą się wysyłki spamowe podszywające się pod e-maile wysyłane z urządzeń mobilnych. Wiadomości te pojawiły się w kilku językach, a ich celem byli użytkownicy iPadów, iPhone'ów, smartfonów Samsunga i innych urządzeń mobilnych. Wiadomości te mają jedną cechę wspólną – bardzo krótką treść (lub jej brak) oraz podpis „Wysłano z mojego iPhone'a". Zwykle zawierają również odsyłacze do szkodliwych załączników.

Niechciane wysyłki masowe często podszywały się pod powiadomienia z różnych aplikacji mobilnych, takich jak WhatsApp czy Viber. [49]

Również przesyłanie niechcianych komunikatów na telefony komórkowe stanowi naruszenie prawa do prywatności i można dochodzić przed sądem zadośćuczynienia.

Spoofing

„Spoofing", czyli fałszowanie adresów IP mające na celu udawanie innego serwera w istniejącym połączeniu sieciowym. Technika ta ma na celu uniknięcie zabezpieczeń jakie wprowadzają na danym serwerze administratorzy sieci wewnętrznej oraz „podszycie" się pod użytkownika sieci, co umożliwia atakującemu przechwytywanie wszystkich danych, które miały trafić do prawdziwego komputera. „Hijacking" jest to metoda polegająca na przechwytywaniu transmisji odbywającej się między dwoma systemami. Metoda ta jest bardzo skuteczna, gdy próbujemy uzyskać dostęp do szczególnie chronionych programów Denial of service. [11]

SQL (Structured Query Language)

Jest najbardziej znanym i rozpowszechnionym strukturalnym językiem zapytań, który służy do tworzenia, modyfikacji oraz zarządzania bazami danych. SQL należy do języków deklaratywnych. Oznacza to, że jest on oparty na paradygmatach programowania nieopartych na programowaniu imperatywnym, które opisuje procesy wykonywania jako sekwencję instrukcji zmieniających stan programu. Sposób przechowywania i pobierania danych jest zależny od decyzji systemu zarządzania bazą danych (Database Management System, DBMS). [67]

SQL injection

Zapytanie SQL to żądanie wykonania jakiejś czynności w bazie danych, zwykle jest to zapytanie ze strony internetowej pytającej o nazwę użytkownika i hasło. Ponieważ jednak większość stron nie wymaga podania żadnych danych poza nazwami użytkownika i hasłami, haker może wykorzystać pola formularzy do wysyłania własnych żądań, tzn. wprowadzania kodu SQL do bazy danych. Tym sposobem hakerzy mogą tworzyć, odczytywać, aktualizować, modyfikować i usuwać dane przechowywane w bazach danych, zwykle w celu pozyskania poufnych informacji, takich jak nr PESEL lub karty kredytowej czy inne dane finansowe. [4]

Spyware lub oprogramowanie szpiegujące

Program, który bez wiedzy i zgody użytkownika ewidencjonuje jego zachowanie w Internecie. Uzyskane w ten sposób dane przekazywane są z reguły do producenta programu, przechowywane w bazie danych, przetwarzane i ewentualnie przekazywane osobom trzecim. Spyware może się zainstalować na komputerze użytkownika poprzez konia trojańskiego, odwiedziny strony internetowej z zainstalowanym oprogramowaniem spyware lub podczas instalacji ściągniętego z Internetu oprogramowania. W celu uchronienia się przed oprogramowaniem typu spyware używaj uaktualnionego programu antywirusowego. Do usuwania spyware służą następujące programy: Ad-Aware, Spybot Search & Destroy i Spy Sweeper. [11]

Stalking

Uporczywe nękanie lub napastowanie innej osoby za pomocą telefonów, SMS-ów, Internetu (przez e-mail, komunikator, czat, serwis społecznościowy itp.) lub inne działanie,

które może doprowadzać do utraty poczucia bezpieczeństwa. Za stalking można więc uznać wielokrotne telefony, SMS-y czy nawet wysyłanie prezentów dla zastraszanej osoby, zamawianie w jej imieniu usług, wykorzystywanie czyjegoś wizerunku lub danych do tworzenia fikcyjnych kont w serwisach społecznościowych itp. Zgodnie z ustawą z dnia 25 lutego 2011 r. o zmianie ustawy Kodeks karny, która weszła w życie 6 czerwca 2011 roku, za stalking grozi kara do 3 lat pozbawienia wolności, a jeśli nękanie doprowadzi pokrzywdzoną osobę do próby samobójczej, to kara ta wydłuża się do lat 10. Ściganie sprawców stalkingu ma następować na wniosek pokrzywdzonego. [69],[86]

Sygnatura ataku

Sekwencja danych wykorzystywana do rozpoznania ataku sieciowego, przeprowadzanego zazwyczaj za pośrednictwem luk w systemie operacyjnym lub aplikacjach. Sygnatury takie są wykorzystywane przez system wykrywania włamań (IDS) lub zaporę sieciową w celu oznaczania szkodliwych działań w systemie. [86]

Sygnatura przeglądarki (ang. fingerprint – odcisk palca)

Są to takie cechy jak wersja, rozdzielczość, zainstalowane dodatki i wtyczki. Sprawiają one, że przeglądarka nabiera unikalnych cech. Jeśli nikt inny nie ma takiej konfiguracji przeglądarki jak my, strony internetowe są w stanie śledzić ruchy danej osoby w Internecie, łatwo odróżniając jej kliknięcia od innych. [30]

Sygnatura wirusa lub definicja wirusa

Według definicji firmy zwalczającej wirusy komputerowe są to unikatowe sekwencje bajtów wykorzystywane przez program antywirusowy do identyfikowania szkodliwego kodu, np. wirusa. Analiza sygnatur jest jedną z kluczowych metod wykorzystywanych do wykrywania i usuwania szkodliwego kodu. [32]

SYN Attack

Jest to jeden z rodzajów ataku sieciowego typu DoS, należący do grupy exploitów. Podczas inicjacji sesji między klientem a siecią używany jest bardzo mały bufor dla informacji potrzebnych do porozumienia się komputerów i zapoczątkowania sesji. Pakiet z tymi informacjami zawiera pole SYN, które identyfikuje hierarchię wymiany informacji. Osoba atakująca może przesłać dużą liczbę zapytań w celu nawiązania połączenia w krótkim czasie, przez co serwer nie potrafi odpowiedzieć na wszystkie zadane zapytania. W buforze pozostaje pierwszy pakiet, przez co kolejne zapytanie o połączenie nie może być przyjęte. Mimo tego, że pakiet bez odpowiedzi jest po jakimś czasie usuwany, efektem wysłania dużej liczby zapytań jest niemożność zainicjowania sesji przez legalnego użytkownika przez pewien czas. [86] To, czy atak typu SYN powiedzie się, zależy od systemu operacyjnego, wielkości bufora oraz ustawień czasu, po jakim pakiet bez odpowiedzi jest usuwany. Za prawidłowe ustawienie dwóch ostatnich parametrów odpowiedzialny jest administrator. [86]

T

Tabnapping (ang. tab kidnapping – porywanie zakładek)

Według definicji firmy Kaspersky Lab jest to rodzaj ataku sieciowego typu phishing, który polega na wykorzystywaniu faktu otwierania stron w wielu zakładkach przeglądarki internetowej. Tabnapping polega na tym, że witryna atakująca podmienia zawartość innej strony znajdującej się w innej zakładce przeglądarki. Jeśli podmienioną w tle stroną jest np. strona banku, użytkownik może przypadkowo próbować się zalogować na podszywającą się pod prawdziwą witrynę banku spreparowaną stronę, która zdobędzie hasło do naszego konta bankowego. Podmieniana może być również strona logowania serwisu aukcyjnego lub systemu pocztowego (webmail). [32]

Teardrop IP Attack

Atak tego typu odbywa się przy wykorzystaniu błędu protokołu IP, który wymaga od zbyt dużego pakietu danych, który nie może być przesłany przez następny router, podzielenia go na części. Fragment pakietu rozpoznaje miejsce, w którym zaczyna się pierwsza część pakietu i uruchamia proces łączenia wszystkich fragmentów w całość. W przypadku ataku typu Teardrop IP, osoba atakująca zmienia fragment odpowiedzialny za odnalezienie początku pakietu i rozpoczęcie procesu scalania, przez co system ma problemy z poskładaniem pakietu w całość i przesłaniem go dalej. To najczęściej doprowadza do zawieszenia systemu, jeśli system nie ma odpowiedniego przepisu na rozwiązanie tego problemu. [86]

Tempest (ang. burza)

Każda elektroniczna transmisja danych, sygnału wizyjnego z karty graficznej do monitora, danych przesyłanych taśmą dysku twardego, sygnału naciśniętych klawiszy klawiatury, da się podsłuchać. Ochrona sprzętu komputerowego przed wyciekiem informacji (tzw. emisją ujawniającą) jest bardzo trudna. Dlatego Tempest jest bardzo rzadką metodą przechwytywania haseł i innych informacji z komputera na podstawie przechwytywania emitowanych fal elektromagnetycznych, emitowanych w dużej ilości przez podzespoły komputera. Za pomocą specjalistycznego, drogiego sprzętu można dostroić go do promieniowania z klawiatury czy z monitora i uzyskać dane pochodzące z tych urządzeń. Przeciętny użytkownik raczej nie stanie się ofiarą takiego ataku, chyba że interesują się nim służby specjalne. Jednakże firmy, dla których poufność danych jest krytyczna (np. instytucje finansowe) czy agencje rządowe, których pracą może interesować się obcy wywiad, muszą brać pod uwagę takie zagrożenie. Jedyną ochroną przed takim atakiem jest stworzenie osłony, która nie przepuszcza na zewnątrz żadnego promieniowania elektromagnetycznego. [17],[26] Osłony te obejmują specjalnie ekranowane przed podsłuchem pomieszczenia w ambasadach, niektórych urzędach i wielkich firmach. Prowadzone tam są utajnione spotkania i narady.

TOR (The Onion Router)

Wirtualna sieć komputerowa implementująca trasowanie cebulowe drugiej generacji. Sieć zapobiega analizie ruchu sieciowego i w konsekwencji zapewnia użytkownikom prawie anonimowy dostęp do zasobów Internetu. TOR może być wykorzystywany w celu ominięcia mechanizmów filtrowania treści, cenzury i innych ograniczeń komunikacyjnych. [79]

Treści niebezpieczne dla dzieci

To treści, które ze względu na swoją zawartość np.: pornografia, hazard, brutalna przemoc, itp. mogą wywołać niepożądane oddziaływanie na psychikę dzieci. [98]

Trojan dropper

Rodzaj wirusa typu trojan, którego celem jest zainstalowanie złośliwego kodu na komputerze ofiary. Wirusy te instalują na komputerze inny złośliwy program lub nową wersję wcześniej zainstalowanego wirusa.

Trojan dropper często służy do przenoszenia na komputer kilku całkowicie niezwiązanych ze sobą złośliwych programów, które mogą różnić się zachowaniem lub nawet zostać stworzone przez różnych koderów. W rezultacie stanowią one pewnego rodzaju archiwum złośliwych programów zawierające wiele różnych typów złośliwego kodu. Mogą one obejmować również żarty lub fałszywe alarmy, których celem jest odwrócenie uwagi użytkowników od rzeczywistego przeznaczenia droppera lub programy adware czy „pornware".

Droppery często wykorzystywane są do przenoszenia znanych trojanów, ponieważ znacznie łatwiej jest napisać droppera niż zupełnie nowego trojana, którego program antywirusowy nie będzie w stanie wykryć. Większość dropperów pisanych jest przy użyciu języka VBS lub JavaScript, dlatego są one łatwe do stworzenia i mogą być wykorzystywane do wykonywania licznych zadań. [32]

Trojan clicker

Rodzaj trojana, którego celem jest według Kaspersky Lab informowanie autora lub „osoby, która je kontroluje", że złośliwy kod został zainstalowany na komputerze ofiary oraz przekazanie informacji o adresie IP, otwartych portach, adresach email itd. Wchodzi zazwyczaj w skład „pakietu" zawierającego inne złośliwe programy. [32]

Trojan downloader

Jest to kolejny rodzaj trojana służącego do instalowania złośliwego kodu na komputerze ofiary, podobnie jak trojan dropper, jest jednak bardziej użyteczny dla twórców złośliwego oprogramowania. Po pierwsze, trojan downloader jest znacznie mniejszy niż trojan dropper. Po drugie, może być wykorzystany do pobrania nieskończonej liczby nowych wersji złośliwego kodu, programów adware lub „pornware". Podobnie jak trojan dropper, trojan downloader pisany jest zazwyczaj w językach skryptowych, takich jak VBS czy JavaScript. Często wykorzystuje również luki w przeglądarce Microsoft Internet Explorer. [32]

Trojan proxy

Rodzaj trojana, który śledzi aktywność użytkownika, zapisuje zebrane informacje na dysku twardym użytkownika, a następnie przesyła je autorowi szkodnika lub „osobie, która go kontroluje". Rejestrowane informacje obejmują uderzenia klawiszy i zrzuty ekranu, które wykorzystywane są do kradzieży danych bankowych lub pomagają w przeprowadzaniu oszustw internetowych. [86]

Trojan backdoor

Rodzaj trojana, który pozwala jego autorowi lub osobie, która go kontroluje, na zdalne zarządzanie komputerami ofiar. W przeciwieństwie do legalnych narzędzi zdalnej administracji, trojany te instalują się, uruchamiają i działają w ukryciu, bez wiedzy czy zgody użytkownika. Po zainstalowaniu trojan backdoor może otrzymać instrukcje, aby wyszukiwać, wysyłać, otrzymywać, wykonywać i usuwać pliki, zapisywać w dzienniku czynności wykonywane na komputerze i przeprowadzać wiele innych czynności. [86]

U

Utrata prywatności (danych osobowych i wrażliwych)

Udostępnianie danych osobowych budzi coraz więcej pytań i kontrowersji. Obecnie wiele instytucji (urzędy, banki) gromadzi informacje na nasz temat. Często również podajemy nasze dane biorąc udział w konkursach lub też imprezach promocyjnych. Podobnie przy zakupach w sklepach stacjonarnych lub internetowych często nieświadomie udostępniamy swoje dane.

W Polsce niestety nie ma przepisów, które zobowiązywałyby przedsiębiorcę czy instytucję publiczną do poinformowania klienta o tym, że jego dane wydostały się do sieci. Pierwszy postęp, który został zrobiony w tym zakresie, dotyczy prawa telekomunikacyjnego. Od kwietnia 2013 roku taki obowiązek spoczywa na operatorach telekomunikacyjnych. [99]

W Polsce według raportu przygotowanego w 2012 roku przez Dynamics Markets Limite UK średnia strata wynosiła 35 000 zł. 27% ofiar kradzieży tożsamości zostało posiadaczami nowych kart kredytowych, 27% respondentów musiało zapłacić za usługi i towary, z których nigdy nie korzystali, a 26% ofiar kradzieży tożsamości weszła w posiadanie nowych nieruchomości. Aż 38% ofiar kradzieży dowiedziało się, że ktoś żyje na ich konto. Bez uszczerbku z sytuacji kradzieży tożsamości wyszło tylko 29% ofiar. Tak wiec należy zawsze sprawdzać, czy dane, o które nas proszą, są rzeczywiście potrzebne i wymagane, a najlepiej ograniczać maksymalnie ich udostępnianie. Szczególnie dotyczy to danych zawartych w dowodzie osobistym. [39]

Osobnym problemem pozostaje ochrona medycznych danych osobowych w postaci cyfrowej. Są one szczególnym przypadkiem danych osobowych i szczególnym rodzajem dokumentacji elektronicznej, a co za tym idzie podlegają regułom przetwarzania i ochrony obowiązującym dla tych danych. Występuje tu problem szczególnej wrażliwości osób,

których dane medyczne mogą zostać upublicznione oraz na przykład sytuacji, gdy dostęp do takich danych uzyskuje pracodawca. Należy zatem zapewnić w wystarczającym stopniu bezpieczeństwo tych danych – chronić je przed niepowołanym dostępem i utratą, czy to w postaci elektronicznej czy fizycznej i należy chronić ich poufność i prywatność. [100]

Uzależnienie od sieci i gier komputerowych

Osobami najczęściej uzależniającymi się od gier komputerowych są te, które mają wysokie poczucie wartości, są bardzo ekspresyjne, agresywne, nadpobudliwe, nie liczą się z innymi, czują potrzebę kontroli i wygrywania z innymi, nie liczą się z uczuciami osób trzecich, a ponadto są przekonane o swojej doskonałości. Z drugiej zaś strony mogą to być osoby lękliwe, zagubione, niemające znajomych oraz przyjaciół, o niskim poczuciu własnej wartości, odrzucone i nieakceptowane. [31]

Obecnie wyróżniamy dwa rodzaje uzależnień od gier komputerowych: wtórne (gdy gra komputerowa stanowi ucieczkę od codzienności) oraz pierwotne (gdy gracz koncentruje się na posiadanym sprzęcie oraz grach).

Osoba uzależniona zaczyna żyć światem wirtualnym, odcina się od rzeczywistości, potrafi spędzać przed komputerem godziny, dni, a nawet tygodnie (traci poczucie czasu), zapomina o codziennych obowiązkach, higienie osobistej, spożywaniu pokarmów oraz odpoczynku. Zaczyna mieć problemy w każdej dziedzinie życia, które cały czas się pogłębiają. Sytuacja, w której nie może zagrać w grę powoduje u niej lęk, niepokój, a także agresję i wybuchowość. [101]

Infoholizm to uzależnienie od związków wirtualnych, czasami tłumaczone jako socjomania internetowa (cyber-relationship addiction) – jest to uzależnienie od internetowych kontaktów społecznych, nadmierne zaangażowanie w związki w sieci (wirtualne). Wyraża się poprzez udział w listach dyskusyjnych, IRC (Internet Relay Chat) oraz kontaktach przy pomocy poczty elektronicznej. Osoba chora nawiązuje nowe kontakty tylko i wyłącznie poprzez sieć, ma zachwiane relacje człowiek-człowiek w kontaktach poza siecią. Ludzie tacy potrafią godzinami „rozmawiać" z innymi użytkownikami Internetu, lecz mają trudności przy kontaktach osobistych, następuje też u takich osób zanik komunikacji niewerbalnej, nie potrafią odczytywać informacji nadawanych w tej płaszczyźnie lub odczytują je błędnie. Osoby z tym zaburzeniem spotyka się głównie w tych formach kontaktu, które zapewniają synchroniczną komunikację. [94]

Formą infoholizmu jest również uzależnienie od komputera (computer addiction) – osoba chora nie musi w tym wypadku „być" w sieci, wystarczy, iż spędza czas przy komputerze. Nie jest dla niej ważne to, co robi, czy pisze ważną pracę czy gra w pasjansa. Liczy się tylko to, że komputer jest włączony, a ona spędza przy nim czas. Najczęściej przejawia się w obsesyjnym graniu w gry komputerowe.

Kolejną formą jest uzależnienie od sieci (net compulsions) – jest ono bardzo podobne do uzależnienia od komputera, lecz polega na pobycie w Internecie. Osoby takie są cały czas zalogowane do sieci i obserwują, co się tam dzieje. Obsesyjnie grają w sieci, uczestniczą w aukcjach etc. Uzależnienie to łączy w sobie wszystkie inne formy IAD. [94]

Przeciążenie informacyjne lub przeładowanie informacjami (information overload) – nałogowe surfowanie w sieci lub przeglądanie baz danych. Występuje przy natłoku informacji, na przykład przebywanie w wielu pokojach rozmów jednocześnie lub udział w wielu listach dyskusyjnych. [57]

V

Viber

Viber to bezpłatna aplikacja umożliwiająca łączność z osobami na całym świecie. Komunikator ułatwia wysyłanie pomiędzy odbiorcami wiadomości tekstowych, udostępnianie zdjęć, a także prowadzenie rozmów głosowych. W aplikacji Viber numer telefonu jest jednocześnie identyfikatorem użytkownika. Aplikacja na smartfon synchronizuje się z listą kontaktów zapisaną w telefonie i automatycznie wykrywa numery, które także korzystają z komunikatora. Program wzbogacony o powiadomienia push gwarantuje, że nigdy nie przegapimy żadnej wiadomości. Dotrą one do nas nawet wtedy, gdy aplikacja będzie wyłączona. [84]

Vishing

Nowa metoda oszustwa, mająca swoje podstawy w phishingu, polegająca na tym że oszuści wykorzystujący telefonię internetową starają się podszywać przede wszystkim pod instytucje finansowe. Jedną z praktykowanych przez nich metod jest rozesłanie spamu, w którym podawany jest numer 0-800, pod którym odbiorca e-maila powinien zaktualizować swoje dane konta bankowego. Po wykręceniu podanego numeru włącza się automat, który prosi ofiarę o podanie konkretnych danych dostępowych do konta. [86]

Niektórzy hackerzy posiłkują się sposobami pozwalającymi na ominięcie pośrednictwa e-maila w oszustwie. Używają programów, które automatycznie telefonują przez VoIP pod zadaną im listę numerów telefonicznych. W momencie odebrania przez kogoś takiego telefonu automatycznie odtwarzana jest informacja o próbie nieautoryzowanego wykorzystania karty kredytowej danej osoby oraz prośba o dokonanie procedury weryfikacyjnej, w której należy podać numer karty oraz dane jej właściciela. [3]

VPN (Virtual Private Network)

Wirtualna sieć prywatna – słowo wirtualna, określa w tym przypadku przeciwieństwo słowa fizyczna, a co za tym idzie, że nie istnieją żadne kable, które umożliwiają połączenia wewnątrz niej. Wszystko to dzieje się w przestrzeni. Termin prywatna odnosi się do faktu, iż dostęp do takiej sieci jest ograniczony i moderowany. Ma to na celu zwiększenie bezpieczeństwa takiej sieci. Jej użytkownicy, mają czuć się chronieni podczas wymiany plików czy wspólnej pracy. VPN można opisać jako tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. [95]

W

Wabbit

Jest programem rezydentnym (uruchamiającym się w tle) typu malware, niepowielającym się przez sieć. Wynikiem jego działania jest jedna określona operacja np. powielanie tego samego pliku aż do wyczerpania zasobów pamięci komputera. [86]

Wardriving

Polega na jeżdżeniu po mieście w celu wyszukiwania bezprzewodowych punktów dostępowych, tzw. hot spotów w celu zdobycia nieautoryzowanego dostępu do niezabezpieczonych sieci bezprzewodowych. [86]

Wirus komputerowy

Program komputerowy zawierający zestawy krótkich samopowielających się sekwencji poleceń, które powodują jego samoczynne rozprzestrzenianie się w oprogramowaniu i rozmnażanie w systemach operacyjnych sterujących pracą komputera. Zasadę działania wirusa można łatwo porównać do sposobu rozprzestrzeniania się w żywym organizmie wirusów biologicznych. Wirus zmienia kod genetyczny komórki, wirus komputerowy zaś zmienia sekwencje układów elektronicznych. Poza rozmnażaniem się wirusy mogą mieć złośliwe, destrukcyjne działanie. [11]

Szkodliwa działalność wirusa przybiera rożne formy, wśród których najczęściej spotykanymi są: zmuszanie komputera do wykonywania niepotrzebnych operacji, blokowanie niektórych operacji, zaciemnianie ekranu, podmiana rozkazów, zniekształcanie danych, wprowadzanie chaosu w magazyny pamięci komputera, kasowanie danych itp.; zanotowano także przypadek destrukcji materialnej – na skutek działalności wirusa monitor spłonął. Wirus komputerowy wprowadzany zostaje do wyizolowanych (niewłączonych do sieci) komputerów poprzez zarażone dyskietki, a do sieci komputerowych – rożnymi metodami – przez hakerów. Taka szkodliwa działalność miewa rożne rozmiary. Zdarza się, iż wirus kontynuuje ją długo, co jest kolejną analogią pomiędzy epidemią biologiczną a komputerową. Pojawienie się wirusa w sieciach komputerowych może wywołać groźne skutki społeczne. Przy tak obecnie rozbudowanej sieci powiązań miedzy rożnymi instytucjami zagrożenie może stanowić dosłownie każdy przyjmowany przez sieć materiał. W takiej sytuacji nie jest wykluczone uruchomienie np. wyrzutni rakietowych przez zarażony komputer służący do celów militarnych, chociaż wojskowe sieci należą do najlepiej zabezpieczanych pod każdym względem. W przypadku innych sieci, np. powiązań miedzy bankami, systematyczne odejmowanie lub dodawanie określonych sum do wybranych lub wszystkich kont może spowodować konsekwencje finansowe na skalę globalną. Znane są przypadki szantażowania czy grożenia wprowadzeniem wirusów paraliżujących komunikację miedzy poszczególnymi instytucjami, co z kolei powodowało panikę podtrzymywaną przez media. [11]

Wirusy typu multipartite

Wirusy, które stosują wiele różnych metod ataku. Wirusy polimorficzne próbują unikać wykrycia, zmieniając własny kod wraz z każdą infekcją. Programy antywirusowe nie mogą więc poszukiwać stałej sekwencji bajtów. Niektóre wirusy polimorficzne używają również różnych technik szyfrowania przy każdej infekcji. Obecnie twórcy szkodliwego oprogramowania wciąż stosują polimorfizm. Częściej w połączeniu z robakami i spamem, coraz rzadziej natomiast z klasycznymi wirusami.

Wirus sektora startowego

Wwirus który infekuje poprzez zmianę kodu w sektorze startowym dyskietki (czasami dysku twardego) na własny kod. W rezultacie, przy każdej próbie rozruchu z zainfekowanej dyskietki wirus zostanie załadowany przed systemem operacyjnym. [32]

Wirusy towarzyszące

Rodzaj klasycznych wirusów plikowych, które nie zmieniają atakowanego pliku. Zamiast tego tworzą jego kopię zawierającą wirusa. Podczas uruchamiania zainfekowanego pliku, pierwsza aktywowana zostanie kopia zawierająca wirusa. Przykładowo wirus może zmienić nazwę pliku notepad.exe na notepad.exd i dopisać swój własny kod do pliku z oryginalną nazwą. Przy każdym uruchomieniu pliku notepad.exe przez użytkownika najpierw aktywowany będzie kod wirusa, a dopiero potem oryginalny plik Notatnika – notepad.exd. [33]

Wirus – odsyłacz

Typ wirusa, który nie dodaje swojego kodu bezpośrednio do zainfekowanych plików. Rozprzestrzenia się poprzez manipulowanie sposobem dostępu do plików w systemie plików FAT. W momencie uruchamiania zainfekowanego pliku wirus przenika do pamięci oraz zapisuje (zazwyczaj ukryty) plik na dysku: ten plik zawiera kod wirusa. Następnie wirus modyfikuje system plików FAT tak, aby inne pliki były przekierowywane do sektora dysku zawierającego kod wirusa. W rezultacie, zawsze po uruchomieniu zainfekowanego pliku system przeskakuje najpierw do kodu wirusa i uruchamia go. Przekierowanie może zostać wykryte po uruchomieniu programu CHKDSK, jednak jeżeli wirus jest aktywny w pamięci (komputer nie został uruchomiony z niezainfekowanego nośnika startowego), może on użyć technologii ukrywania się w celu zamaskowania zmian. [33]

Wirus nadpisujący

Wirus całkowicie zastępuje kod w zainfekowanym pliku własnym kodem. Naturalnie oryginalny program przestanie działać, co będzie oznaczać, że komputer został zainfekowany. Z tego powodu, wirusy nadpisujące nigdy nie rozprzestrzeniały się skutecznie na wolności. [33]

Wirus ukrywający się

Taki wirus próbuje uniknąć skanerów antywirusowych przedstawiając po zapytaniu produktu antywirusowego czyste dane. Niektóre z tych wirusów podczas skanowania ukazują

czystą wersję zainfekowanego pliku. Inne ukrywają nowy rozmiar zainfekowanego pliku i wyświetlają rozmiar sprzed infekcji. [86]

White hat (z ang. – biały kapelusz)

Określenie opisujące hakera lub crackera, który włamuje się do systemu komputerowego lub sieci w dobrych intencjach. Chodzi mu o to, by ujawnić słabe strony testowanego systemu, następnie przekazać je administratorowi, w celu usunięcia niedociągnięć i zabezpieczyć przed kolejnymi atakami. „Białe kapelusze" często traktują swoją działalność jako hobby, są jednak tacy, którzy świadczą swoje usługi za określoną opłatą. Zdarza się również, że wynajmowani są przez firmy jako tymczasowi konsultanci lub stali pracownicy strzegący bezpieczeństwa sieci. [86]

Włamania do skrzynek pocztowych i zagrożenia z tym związane

Włamanie do skrzynki mailowej to nieuprawniona ingerencja w dobra osobiste. W prawo do prywatności oraz tajemnicę korespondencji. Obydwa dobra podlegają zasadniczej ochronie konstytucyjnoprawnej, cywilnoprawnej oraz karnoprawnej. [11]

Podstawę ochrony dóbr osobistych stanowi art. 49 Konstytucji: „zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony". Natomiast art. 47 konstytucji jasno stwierdza: „każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym". Z wymienionego powyżej przepisu art. 49 wynika generalny zakaz stosowania podsłuchu telefonicznego czy wchodzenia w inny sposób w krąg wiadomości dotyczących życia, interesów i działań innych osób.

Art. 23 Kodeksu cywilnego (Dz.U. z 1998 r. Nr 21, poz. 94) również stanowczo broni prawa do prywatności: dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego, niezależnie od ochrony przewidzianej w innych przepisach. W sytuacji naruszenia tego paragrafu, sąd może przyznać temu, czyje dobro osobiste zostało naruszone, odpowiednią sumę tytułem zadośćuczynienia pieniężnego za doznaną krzywdę lub na jego żądanie zasądzić odpowiednią sumę pieniężną na wskazany przez niego cel społeczny, niezależnie od innych środków potrzebnych do usunięcia skutków naruszenia.

Zgodnie z Kodeksem karnym (art. 267) osoba, która w sposób nieuprawniony uzyskuje dostęp do informacji dla niej nieprzeznaczonej (np. poprzez otwarcie zamkniętego pisma, a w analizowanym przypadku internetowym – przełamując jej zabezpieczenie) podlega karze grzywny, ograniczenia, a nawet pozbawienia wolności do lat 2. Nieco inna sytuacja jest w momencie, gdy sprawca dostał się do naszej poczty, a następnie dokonał np. różnego typu zmian, wysyłki maili, uszkodzenia danych itp. (art. 268 Kodeksu karnego). Za takie działanie Kodeks karny przewiduje karę pozbawienia wolności nawet do 3 lat. Jeśli

natomiast dokonane zmiany spowodowały straty finansowe (majątkowe), sprawcy grozi kara pozbawienia wolności od 3 miesięcy aż do 5 lat. [18]

Przestępstwo włamania się na czyjeś konto internetowe jest ścigane na wniosek pokrzywdzonego. W przypadku zauważenia takiej sytuacji należy poinformować Policję, która będzie poszukiwać przestępcy.

Współcześni cyberprzestępcy lekceważą przepisy i zdarza im się dokonać włamania na wybraną skrzynkę poczty elektronicznej. W sytuacji przekazania zdobytych informacji dalej czyn nabiera znamiona jeszcze innego przestępstwa, tj. zniesławienia.

Włamanie do poczty internetowej stwarza dla poszkodowanej osoby liczne zagrożenia. Po pierwsze nasz wizerunek może zostać skopiowany, a później bezprawnie wykorzystany do celów komercyjnych albo prywatnych przez obce nam osoby. Problem dotyczy także upowszechniania twórczości własnej, mogą to być pliki grafiki, profesjonalne zdjęcia oraz muzyka)

Poza tym dane uzyskane w tym jednym miejscu mogą posłużyć do wykrycia informacji zamieszczonych gdzie indziej. W ten sposób przestępcy tworzą kompletny obraz danej osoby, która nie ma pojęcia jak wiele wiedzą o niej osoby, z którymi nigdy nie miała styczności. Pozyskane w ten nielegalny sposób (naruszający szereg polskich przepisów prawa) prywatne informacje, które zostawiamy na swój temat na przeróżnych portalach stworzą internetowym oszustom kompletny obraz naszej osoby, na który będzie się składał nasz wizerunek, nasze zainteresowania i przemyślenia, pasje i poglądy. A tego rodzaju wiedza jest bardzo przydatna dla specjalistów branży marketingowej. [11]

Worm lub robak

Nazywamy tak rodzaj samoreplikującego się wirusa komputerowego, który nie zmienia zawartości plików, ale rezyduje w pamięci komputera, ciągle mnożąc się. Worm używa części systemu operacyjnego, dzięki czemu działa samoczynnie i jest zazwyczaj niewidoczny dla użytkownika. Najczęściej worm jest zauważany, gdy niekontrolowanie zwiększy się liczba jego kopii tak, że zużywa zbyt dużo zasobów komputera, zwalnia jego pracę lub go zawiesza. [86]

Z

Zagrożenia zdrowotne związane z używaniem komputera i Internetu

Osoby dorosłe wskazują przede wszystkim na takie medyczne negatywne skutki obcowania z komputerem jak wady postawy i pogorszenie wzroku.

Jak podają oficjalne statystyki amerykańskie ok. 30% użytkowników komputerów cierpi na różnego rodzaju dolegliwości nabyte w związku z wykonywaną pracą. Najbardziej narażone części ciała na problemy zdrowotne to: nadwyrężanie mięśni nadgarstka, naprężony kark, bóle dolnych części kręgosłupa, oczy – niewłaściwe oświetlenie powoduje męczenie się wzroku, bóle głowy i ogólne zmęczenie organizmu. Wykrzywianie kręgosłupa nadwyręża naturalne więzadła kręgów. Dzieci i młodzież w okresie intensywnego rozwoju fizycznego

są szczególnie narażeni na niebezpieczeństwo utraty zdrowia: wady wzroku, skrzywienia kręgosłupa. Należy dbać o higienę pracy przy komputerze, zapewnić bezpieczne warunki pracy, właściwy sprzęt, oświetlenie, uczyć prawidłowej postawy podczas pracy na komputerze, uczyć relaksu i zmuszać do czynienia przerw rekreacyjnych podczas pracy. [96]

Zapobieganie cyberzagrożeniom

Marian Żuber z Wyższej Szkoły Oficerskiej Wojsk Lądowych podzielił całe zagadnienie zapobiegania cyberzagrożeniom na trzy poziomy.

Poziom pierwszy dotyczy zagrożeń w skali całego państwa. Podejmowane na tym poziomie działania zapobiegawcze powinny dotyczyć:
- budowy i stałego unowocześniania zabezpieczeń technicznych sieci informatycznych;
- wprowadzania i egzekwowania procedur bezpieczeństwa dostępu do sieci;

zwalczania prób infiltrowania systemów telekomunikacyjnych;
- międzynarodowej współpracy w zwalczaniu ponadnarodowej cyberprzestępczości;
- wspierania produkcji oprogramowania do celów zabezpieczeń;
- opracowywania programów i planów na wypadek zagrożeń.

Poziom drugi dotyczy zagrożeń w skali organizacji i przedsiębiorstw. Podejmowane na tym poziomie działania powinny dotyczyć:
- budowy i przestrzegania systemów zabezpieczeń;
- przestrzegania dyscypliny dostępu do danych;
- regularnego używania oprogramowania antywirusowego;
- szkolenia pracowników w zakresie bezpieczeństwa korzystania z Internetu.

Poziom trzeci dotyczy zagrożeń dla indywidualnych obywateli Podejmowane na tym poziomie działania powinny dotyczyć:
- regularnego używania oprogramowania antywirusowego;
- odwiedzania tylko zaufanych stron i portali;
- dokładnego weryfikowania źródeł przychodzącej korespondencji;
- natychmiastowego sygnalizowania Policji wszelkich zjawisk związanych z cyberprzemocą;
- przestrzegania zasad prawidłowego prowadzenia korespondencji przyjętych w sieci;
- szkoleń chętnych z zakresu bezpieczeństwa w Internecie, pomocy państwa dla organizacji zajmujących się szerzeniem tego typu wiedzy. [85]

Zapora sieciowa (ang. firewall – ściana/zapora)

Jeden ze sposobów zabezpieczania sieci i systemów przed hackerami. Termin ten może odnosić się zarówno do dedykowanego sprzętu komputerowego wraz ze specjalnym oprogramowaniem, jak i do samego oprogramowania blokującego niepowołany dostęp do komputera, którego strzeże. [79]

Zatruwanie DNS – (z ang. cache poisoning)

Technika phishingu polegająca na wysłaniu do serwera DNS fałszywego rekordu kojarzącego nazwę domeny z adresem IP. Serwer DNS zapamiętuje go na pewien czas (do kilku godzin) i zwraca klientom zapamiętany adres IP, czego skutkiem jest przeniesienie na fałszywą stronę. [3]

Zombie (komputer-zombie)

Komputer przyłączony do Internetu, na którym bez wiedzy jego posiadacza został zainstalowany program nadzorowany z zewnątrz przez kogoś innego. Celem takiego działania jest zazwyczaj wykorzystanie komputera do działań sprzecznych z prawem, jak ataki DDoS. Czasami bywają również wykorzystywane do uzyskania dostępu do dużej mocy obliczeniowej. Nazwa wirusa wzięła się od postaci zombie w horrorach, które również były tam pozbawione świadomości i kierowane przez kogoś innego.

Literatura

1. A new European network to exchange and transfer knowledge and expertise in the field of treatment programs for perpetrators of sexual harassments and violence against children and young people. European Commission Dg Justice, Freedom And Security (tłumaczenie własne).
2. Agencja Bezpieczeństwa Wewnętrznego, https://www.abw.gov.pl/pl/zadania/zwalczanie-terroryzmu/cyberterroryzm/306,Cyberterroryzm.html
3. Ataki na serwery DNS, http://docplayer.pl/7926258-Ataki-na-serwery-dns-ponizej--prezentuje-kilka-typow-atakow-na.html
4. Avast.co.pl, https://www.avast.com/pl-pl/c-sql-injection
5. Bitcoin.pl, http://bitcoin.pl/o-bitcoinie/co-to-jest-bitcoin
6. Biedrzycki N., Blockchain – wszystko, co warto o nim wiedzieć, https://businessinsider.com.pl/technologie/blockchain/blockchain-co-to-jest/vlfytn4
7. Bitcoin.p,l http://bitcoin.pl/poradniki/portfele/382-jaki-portfel-bitcoin-wybrac
8. Blogmobility.pl, http://blogmobility.pl
9. Bezpieczeństwo w sieci, http://ostanskaconsulting.pl/bezpieczenstwo-w-sieci/
10. Beznienawiści.pl, http://beznienawisci.pl/koalicja/
11. Cyberprzestępczość.info, http://www.cyberprzestepczosc.info
12. Chiny mają potężną broń internetową – Technowinki, http://webcache.googleusercontent.com/search?q=cache:4XFLRRzP7xQJ:technowinki.onet.pl/internet-i-sieci/chiny-maja-potezna-bron-internetowa/q3czk3+&cd=1&hl=pl&ct=clnk&gl=pl&client=opera
13. Chińscy hakerzy celują w Europę Wschodnią, https://www.forbes.pl/wiadomosci/chinscy-hakerzy-celuja-w-europe-wschodnia/qnnny2m
14. Co grozi za włamanie na skrzynkę e-mail, FB, GG?, http://teczka.pl/prawo/co-grozi--za-wlamanie-na-skrzynke-e-mail-fb-gg
15. Ciszek M., *Ekoterroryzm zagrożeniem dla polityki zrównoważonego rozwoju,* INS UPH Siedlce, s. 109.
16. Cyberprzestępcy podszywają się pod Pocztę Polską, http://pclab.pl/news63023.html
17. Dbi.cba.pl, http://www.dbi.cba.pl/bezpieczenstwo.html

18. Dz.U.2016.0.1137 t.j. – Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny.
19. Dz.U.1997.88.553 – Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny.
20. Encyklopedia hackingu, http://hack.pl/baza-wiedzy/encyklopedia-hackingu.html
21. Ergokantor.pl, https://ergokantor.pl/co-to-sa-kryptowaluty.html
22. Ewolucja wirusów w ciągu ostatnich 25 lat, http://www.web-news.pl/ewolucja-wirusow-w-ciagu-ostatnich-25-lat/
23. Florczak A., Lisowska A., *Organizacje międzynarodowe w działaniu*, OTO Agencja Reklamowa, Wrocław 2014.
24. Fundacja Dajemy Dzieciom Siłę (dawniej Dzieci Niczyje), http://seksting.fdn.pl
25. Grosset R., *Zabić tysiące, przestraszyć miliony*, WSZiP im. Heleny Chodkowskiej, Warszawa 2009.
26. Hackme.pl, Rodzaje i klasyfikacja włamań oraz ataków internetowych, http://hackme.pl/print.html?type=A&item_id=247
27. Handel przedmiotami, których posiadanie jest zabronione lub pochodzącymi z przestępstwa, Cyberprzestępczość.info, http://www.cyberprzestepczosc.info/handel_przedmiotami.html
28. infor.pl, http://mojafirma.infor.pl/e-firma/slownik/692586,H-jak-Hoax.html
29. Informacja niejawna, http://www.iniejawna.pl
30. Jak działa Zeus, https://niebezpiecznik.pl/post/jak-dziala-zeus/
31. Kacperska M., *Czy można się uzależnić od gier komputerowych?*, Portal Psychiatria.pl
32. Kaspersky Lab Polska Sp. z o.o., http://securelist.pl/glossary/A.html
33. Kaspersky Lab, http://support.kaspersky.com/pl/viruses/general/614
34. Klienci banków zagrożeni. Internetowe konta pod ostrzałem hakerów Forsal.pl – Biznes, Gospodarka, Świat.
35. Kurs Javascript, http://javascript.blox.pl/2010/03/Krok-1-Co-to-jest-JavaScript.html
36. kompinf.cba.pl by dark24, http://kompinf.cba.pl/kompendium/oprogramowanie/rodzaje-wirusow/dialer.html
37. Kowalewski J., Kowalewski M., Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa, http://www.wnp.pl/tech/cyberterroryzm-szczegolnym-zagrozeniem-bezpieczenstwa-panstwa,235632_1_0_0.html
38. Kozłowski A., Cyberterroryzm w amerykańskiej wojnie z terroryzmem w XXI wieku, http://www.academia.edu/7673885/Cyberterroryzm_w_amerykańskiej_wojnie_z_terroryzmem_w_XXI_wieku
39. Kradzież tożsamości naraża nas na poważne straty finansowe, http://www.rp.pl/artykul/941370-Kradziez-tozsamosci-naraza-nas-na-powazne-straty-finansowe.html
40. Kwiatkowski K., Wystąpienie pokontrolne NIK, http://www.mf.gov.pl/documents/764034/12765096/2015_02_05_Ujednolicony_+tekst_+WP_NIK.pdf
41. Lichocki E., Cyberterroryzm państwowy i niepaństwowy – początki, skutki i formy, http://www.csikgw.aon.edu.pl/index.php/pl/pobieranie/Publikacje/Cyberterroryzm-pa%C5%84stwowy-i-niepa%C5%84stwowy—-pocz%C4%85tki-skutki-i-formy-Uniwersytet-Gda%C5%84ski-Gda%C5%84sk-2009

42. Lidwa W., Krzeszewski W., Więcek W., *Zarządzanie w sytuacjach kryzysowych,* Akademia Obrony Narodowej, 2010.
43. Mam.komputer.info, http://www.mamkomputer.info/nat-translacja-adresow-sieciowych/
44. Mała sieciowa encyklopedia, http://munitus.pl/co-to-jest-p2p.html
45. Mazur K. Relacja z Ataków Sieciowych, http://cyberprzestepczosc.pl/2015/relacja-z-atakow-sieciowych-2015/
46. Mazurkiewicz M., Seksting. Groźna zabawa nastolatków, Nto.pl, http://www.nto.pl/apps/pbcs.dll/article?AID=/20141004/REGION/141009779
47. Moreno M. A., Reid Chassiakos Y., Cross C., *Wykorzystanie mediów przez dzieci i młodzież w wieku szkolnym*, American Academy of Pediatrics Volume 138, nr 5/2016 (tłumaczenie własne).
48. Najczęstsze oszustwa na kartach płatniczych: transakcje w sieci i skimming, http://serwisy.gazetaprawna.pl/finanse-osobiste/artykuly/863214,najczestsze-oszustwa-na-kartach-platniczych-transakcje-w-sieci-i-skimming.html
49. Najgroźniejsze programy rozsyłane w spamie, http://nt.interia.pl/news-najgroznie jsze-programy-rozsylane-w-spamie,nId,1697774#utm_source=paste&utm_medium=paste&utm_campaign=chrome
50. Nowak A., *Cyberprzestrzeń jako nowa jakość zagrożeń*, Zeszyty Naukowe AON nr 3(92) 2013.
51. Nowe metody oszustw nigeryjskich. Celem są prawnicy, http://prawo.gazetaprawna.pl/artykuly/680294,nowe-metody-oszustw-nigeryjskich-celem-sa-prawnicy.html
52. Ochrona informacji niejawnych. Materiał szkoleniowy, http://archiwalna.polsl.pl/adc/obrona/docs/OchrInf.pdf
53. Ochrona praw autorskich w Internecie, INFOR, http://www.infor.pl/prawo/prawo-karne/ciekawostki/325443,Ochrona-praw-autorskich-w-Internecie.html
54. Oszustwa za pomocą kart płatniczych, http://gospodarka.dziennik.pl/finanse/artykuly/486932,oszustwa-za-pomoca-kart-platniczych-skimming-falszerstwo-kradziez.html,komentarze-popularne,1
55. PHP Kurs, http://phpkurs.pl/podstawy/
56. Platforma WP Tech: Jak chronimy swoje dane osobowe i ile tracimy na ich kradzieży?, http://tech.wp.pl/kat,1009785,wid,15008505,wiadomosc.html?title=Jak%20chronimy%20swoje%20dane%20osobowe%20i%20ile%20tracimy%20na%20ich%20kradzie%BFy%3F%20
57. Poprawa R., W pułapce Internetu, http://siecioholizm.eu/mid.php?sel=w_pulapce_internetu
58. Portal Kaspersky Lab, https://support.kaspersky.com/pl/viruses/general/614
59. Poradnik przedsiębiorcy, https://poradnikprzedsiebiorcy.pl/-jak-pozbyc-sie-adware-i-spyware
60. Pornografia dziecięca w Internecie – raport z badania gemiusReport przeprowadzonego na zlecenie Fundacji Dzieci Niczyje.

61. PCWorld, https://www.pcworld.pl
62. Prawa autorskie w Internecie, Portal Cyberprzestępczość.info http://www.cyberprzestepczosc.info/prawa_autorskie_w_internecie.html
63. Programista-it.pl, http://programista-it.pl/internetowy
64. Programki.pl, https://www.programki.pl
65. RCB Centrum Operacyjno-Analityczne, http://rcb.gov.pl/wp-content/uploads/9.pdf
66. Słowiak A. Cyberzagrożenia, https://prezi.com/gjvphakxemp6/cyberzagrozenia/ 2014
67. Strony malowane, http://stronymalowane.pl/html/
68. Socha Ł., http://lukasz-socha.pl/php/niebezpieczny-kod-xss/
69. Stalking i phishing w Polsce zagrożone karą do trzech lat pozbawienia wolności, http://prawo.vagla.pl/node/9454
70. Szalony Pecet, http://szalonypecet.pl
71. Tak internetowi złodzieje kradną nam pieniądze, http://samcik.blox.pl/2014/02/Tak-internetowi-zlodzieje-kradna-nasze-pieniadze.html
72. TVN24.pl, http://www.wiadomosci24.pl/artykul/po_koszmarze_w_szkole_ania_popelnila_samobojstwo_9862.html
73. TVN24.pl, https://www.tvn24.pl/wiadomosci-ze-swiata,2/2-5-roku-wiezienia-za-ujawnienie-danych-agenta-cia,284905.html
74. TVN24.pl, http://www.wiadomosci24.pl/artykul/internet_bron_w_rekach_terrorystow_20523.html
75. UW-Team.org Forum, http://www.uw-team.org/forum
76. UE: Chińczycy dobrali się do naszych firm, PAP, http://biznes.interia.pl/firma/news/chinczycy-dobrali-sie-do-naszych-firm,2114604,1852?utm_source=paste&utm_medium=paste&utm_campaign=chrome
77. Uważaj na tego wirusa. Hakerzy żądają pieniędzy, http://tvn24bis.pl/tech,80/ransomware-hakerzy-zarabiaja-miliony,631475.html
78. USA szykują cyberbroń przyszłości, http://www.newsweek.pl/swiat/usa-szykuja-cyberbron-przyszlosci,89716,1,1.html
79. Wikipedia, https://pl.wikipedia.org/wiki/Log_(informatyka)
80. Wiśniewska A., *Cyberprzemoc a odpowiedzialność prawna*, INFOR, http://www.infor.pl/prawo/prawo-karne/ciekawostki/298808,Cyberprzemoc-a-odpowiedzialnosc-prawna.html
81. Wpływ terroryzmu na bezpieczeństwo krajów Unii Europejskiej i Polski, http://cojawiem.pl/pl/articles/6292-wplywy-terroryzmu-na-bezpieczenstwo-krajow-unii-europejskiej-i-polski/page/6
82. Wojtowicz W., *Bezpieczeństwo infrastruktury krytycznej*, MON, Warszawa 2006.
83. Wolak J., Finkelhor D., MitchellJ K. *Jak często nastolatki są aresztowane za seksting? Dane z krajowego rejestru spraw policyjnych*, American Academy of Pediatrics Volume 129, nr 1/2012 (tłumaczenie własne).

84. Viber – co to za aplikacja? Jak działa Viber?, http://www.fokus.tv/news/viber-co-to--za-aplikacja-jak-dziala-viber/1376
85. Żuber M., Infrastruktura krytyczna państwa jako obszar potencjalnego oddziaływania terrorystycznego, http://www.rocznikbezpieczenstwa.dsw.edu.pl/fileadmin/user_upload/wydawnictwo/RBM/RBM_artykuly/2014_8_11.pdf
86. http://www.i-slownik.pl
87. Polska Szerokopasmowa. Honeypot, czyli skuteczna pułapka na Cyberprzestępców, Źródło: NASK.
88. http://webkod.pl/kurs-css/lekcje/dzial-1/css-co-to-takiego
89. http://jegostrona.pl/news/artykuly/383951,cybernetyczna-bron-drugiej-generacji--zniszczy-cel-bez-pomocy-internetu.html
90. Wiśniewska A., Cyberprzemoc a odpowiedzialność prawna, www.infor.pl
91. http://www.telewizjapolska24.pl/PL-H23/3/1962/uwaga-na-niebezpieczenstwa--w-internecie.html
92. http://www.nowemedia.org.pl
93. http://www.powiatrawicki.home.pl/
94. http://www.psychologiainternetu.pl/zui/
95. http://reset.ath.bielsko.pl
96. www.profesor.pl
97. Zob. więcej Spitzer M., *Cyfrowa demencja*, Wyd. Dobra Literatura, Słupsk 2013.
98. Zob. więcej Kozak S., *Patologie komunikowania w Internecie. Zagrożenia i skutki dla dzieci i młodzieży*, Difin, Warszawa 2011.
99. Raport: firmy coraz lepiej chronią dane wrażliwe, http://www.lex.pl/czytaj/-/artykul/raport-firmy-coraz-lepiej-chronia-dane-wrazliwe?refererPlid=2285075
100. https://www.csioz.gov.pl/fileadmin/user_upload/rekomendacje_bezpieczenstwo_projekt_kwiecien2017_58f615848ab44.pdf
101. http://misjagabriela.pl/gry-komputerowe/

Prawidłowością współczesnych czasów jest to, że coraz więcej elementów ludzkiej działalności przenosi się do sieci komputerowej. Bankowość, handel wymiana informacji oraz wiele innych dziedzin nie są obecnie możliwe bez Internetu. Także przestępcy w dużej mierze przenieśli tam swój proceder.

W codziennej służbie policjanci coraz częściej spotykają się z wirtualną przestępczością, dlatego powinni posiadać odpowiedni zasób wiedzy i umiejętności, aby radzić sobie w takiej sytuacji. Nowoczesny policjant musi odznaczać się nie tylko sprawnością umysłową i fizyczną, musi także sprawnie poruszać się w sieci, wykorzystując jej możliwości i poprawnie identyfikując jej zagrożenia. Bez tego nie będzie w stanie odpowiednio wykonywać swoich obowiązków.

ISBN 978-83-934380-5-1