PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
Technika, Informatyka, Inżynieria Bezpieczeństwa 2013, t. I

Michał Pałęga, Dorota Wojtyto, Mariusz Salwierak, Wiesław Kulma, Marcin Knapiński
Politechnika Częstochowska
Al. Armii Krajowej 36, 42-200 Częstochowa, e-mail: mpalega@wip.pcz.pl

BEZPIECZEŃSTWO TELEINFORMATYCZNE JAKO ELEMENT KOMPLEKSOWEJ OCHRONY INFORMACJI

Streszczenie. W artykule przedstawiono kluczowe zagadnienia związane z bezpieczeństwem informacji przetwarzanej i przechowywanej w systemach oraz sieciach teleinformatycznych. Dokonano kategoryzacji incydentów bezpieczeństwa teleinformatycznego oraz wskazano główne źródła ich powstawania. Ponadto w niniejszym opracowaniu podkreślono znaczącą rolę analizy ryzyka w procesie przeciwdziałania zagrożeniom bezpieczeństwa teleinformatycznego.

Słowa kluczowe: bezpieczeństwo informacji, bezpieczeństwo teleinformatyczne, szacowanie ryzyka, zarządzanie ryzkiem.

Wprowadzenie

W dzisiejszym świecie informacja to majątek każdej nowoczesnej organizacji, która podobnie jak inne ważne składniki kapitału stanowi klucz do jej działania, rozwoju i sukcesu na rynku. Dlatego też wymaga ona odpowiedniego zabezpieczenia. W poszukiwaniu właściwych instrumentów ochrony danych niezmiernie istotne jest uświadomienie sobie, iż strategiczne znaczenie informacji pociągnęło za sobą wzrost zagrożeń dla jej bezpieczeństwa, natomiast rozwój technologii komputerowej oraz powszechna informatyzacja generują coraz to nowsze, niezidentyfikowane dotąd niebezpieczeństwa. Informacje przetwarzane i przechowywane w sieciach i systemach komputerowych należą do najbardziej narażonych, gdyż źródło niebezpieczeństwa czyha na nie z każdej strony, począwszy od wandalizmu, pożaru lub powodzi, a skończywszy na szpiegostwie, sabotażu czy innego rodzaju przestępstwach z użyciem sprzętu komputerowego. Codziennością niemal są incydenty związane z wyciekiem nieodpowiednio chronionej informacji, mogące nieść katastrofalne skutki dla

przedsiębiorców oraz konsekwencje i restrykcje prawne. Główną siłą sprawczą utraty informacji są najczęściej złośliwe kody, włamania komputerowe, ataki typu „odmowa dostępu". Doświadczenia życia codziennego wskazują na ogromną rolę bezpieczeństwa informacyjnego, którego kluczowym elementem jest bezpieczeństwo teleinformatyczne, stanowiące przedmiot rozważań niniejszego opracowania.

Celem artykułu jest zwrócenie uwagi czytelnika na problematykę bezpieczeństwa informacji jako całości, ze szczególnym uwzględnieniem ochrony zasobów informatycznych. Przedstawiono w nim klasyfikację zagrożeń, dostępne mechanizmy ochrony i przeciwdziałania niebezpieczeństwom. Wskazano również na wiodącą rolę analizy ryzyka w procesie zapobiegania niszczenia i utraty danych informatycznych oraz zapewniania ciągłości działania organizacji gospodarczej.

Bezpieczeństwo informacyjne

Bezpieczeństwo i ochrona informacji jest zagadnieniem bardzo szerokim, a dostępna literatura przedmiotu prezentuje liczne jej definicje. Zdaniem autorów niniejszego opracowania najbardziej trafne jest stwierdzenie określające bezpieczeństwo informacji jako: „poziom ochrony informacji i narzędzi służących do opracowania, przechowywania i transmisji przed losowymi lub celowymi zniekształceniami sztucznego lub naturalnego pochodzenia, które mogą przynieść szkodę właścicielom lub użytkownikom informacji i narzędzi" [18]. Bezpieczeństwo informacji można także utożsamiać z ochroną informacyjną, „[…] która polega na uniemożliwieniu i utrudnieniu zdobywania danych o fizycznej naturze aktualnego i planowanego stanu rzeczy i zjawisk we własnej przestrzeni funkcjonowania oraz utrudnienia wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do nośników danych" [3].

Bezpieczeństwo informacyjne stanowi całokształt przedsięwzięć ukierunkowanych na ochronę zasobów informacyjnych przed gamą różnorodnych zagrożeń, takich jak: nieuprawnione ujawnienie, zmiana, zniszczenie lub utrata w przypadkach: dostępu do informacji, jej transmisji oraz przechowywania. Wobec powyższego, bezpieczeństwo informacji wiąże się z zapewnieniem odpowiedniego poziomu [19]:

- integralności – oznacza, że informacja jest adekwatna i precyzyjna, chroniona przed zniszczeniem oraz nieautoryzowaną zmianą;
- dostępności – właściwe przygotowanie informacji do wykorzystania jej zawsze, gdy zaistnieje taka potrzeba;
- poufności – powinna być dostępna wyłącznie określonym użytkownikom.

Ponadto P. Tyrała uważa, że bezpieczeństwo informacji nakłada konieczność uwzględniania atrybutów informacji, które dostarczane są jego użytkowni-

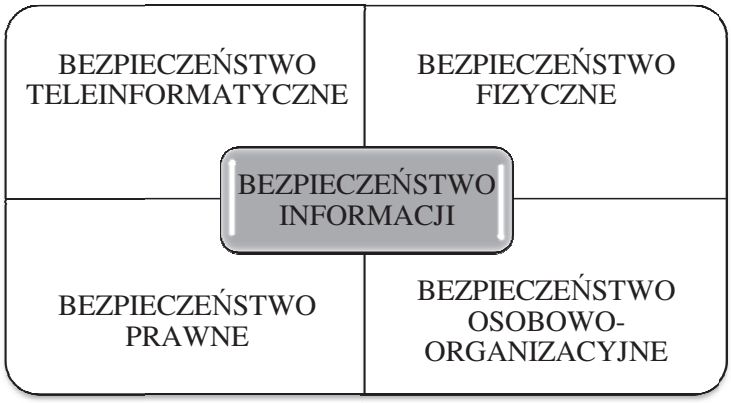
kom: aktualność, dokładność, elastyczność, jednoznaczność, rzetelność, wartość, wystarczalność [17].

Zagwarantowanie bezpiecznych warunków do przechowywania, przetwarzania oraz transmisji danych wymaga zaangażowania właściwych metod, sił i środków zdefiniowanych w polityce bezpieczeństwa informacji. Dostępna literatura wskazuje na szereg wielorodzajowych rozwiązań, do których należą m.in. uregulowania prawne (akty prawnicze i normatywne, standardy itp.), rozwiązania organizacyjno-administracyjne (reguły i inne działania w zakresie bezpieczeństwa informacji) i proceduralne (konkretne środki bezpieczeństwa stosowane w stosunku do ludzi), a także zespół metod i środków programistyczno-technicznych (specjalistyczne oprogramowania, narzędzia elektroniczne) [14].

W oparciu o prezentowane przez P. Bączka treści dotyczące bezpieczeństwa informacyjnego państwa autorzy opracowania definiują pojęcie bezpieczeństwa informacji jako stan wewnętrzny i zewnętrzny, w którym [1]:

- istnieje brak zagrożenia zasobów informacyjnych;
- decyzje podejmowane na podstawie prawdziwych, aktualnych i rzetelnych danych, natomiast ich wymiana odbywa się w sposób nieprzerwany;
- bezpieczeństwo teleinformatyczne oraz system bezpieczeństwa informacji kształtowane są w oparciu o przepisy prawa.

Literatura przedmiotu wskazuje na bezpieczeństwo informacyjne jako zespół działań, metod i systemów, które koncentrują się na zabezpieczaniu informacji gromadzonych, przetwarzanych, przekazywanych oraz przechowywanych w sieciach i systemach teleinformatycznych [1]. J. Łuczak w swojej publikacji natomiast podkreśla, iż bezpieczeństwo informacyjne to wypadkowa bezpieczeństwa fizycznego, prawnego, osobowo-organizacyjnego oraz teleinformatycznego [13]. Składowe bezpieczeństwa informacji prezentuje rys.1.



Rys. 1. Składowe bezpieczeństwa informacji.
Źródło: [13].

Bezpieczeństwo fizyczne ma swoje odzwierciedlenie w dokładnie przeprowadzonej analizie ryzyka, poprzedzonej identyfikacją zagrożeń oraz w zastosowaniu właściwych środków ochrony fizycznej sklasyfikowanych jako środki ochrony budowlano- mechanicznej (bramy, kraty, sejfy, szafy ogniotrwałe itp.), środki ochrony elektronicznej (system sygnalizacji włamania i napadu, system telewizji dozorowej, system sygnalizacji przeciwpożarowej) oraz środki ochrony czynnej (portierzy, pracownicy pionu ochrony, patrole interwencyjne). *Bezpieczeństwo prawne* wynika z obowiązujących przepisów i uregulowań prawnych. Wszystkie podmioty gospodarcze zobligowane są przechowywać, przetwarzać oraz wymieniać informacje zgodnie z wytycznymi zawartymi w podstawowych aktach prawnych: ustawa o ochronie danych osobowych, ustawa o ochronie informacji niejawnych, ustawa o dostępnie do informacji publicznych, ustawa o prawie autorskim i prawach pokrewnych. *Bezpieczeństwo osobowo-organizacyjne* wiąże się z opracowaniem właściwej polityki bezpieczeństwa informacji, w której zostaną zdefiniowane jasno i klarownie zasady oraz procedury postępowania z informacjami chronionymi. Ponadto opracowanie skutecznego systemu bezpieczeństwa informacji wymaga określenia kompetencji pracowników oraz ich wzajemnych zależności, a także wyznaczenia osób, które mają dostęp do pomieszczeń znajdujących się w tzw. strefie ochronnej. Bardzo ważną kwestią organizacyjną jest także przygotowanie procedury dostępu do każdego pomieszczenia osobom postronnym (np. sprzątaczce) oraz w przypadku wystąpienia sytuacji awaryjnej (np. strażakom podczas pożaru). Niebagatelne znaczenie ma również szkolenie pracowników oraz budowanie wśród nich poczucia świadomości odpowiedzialności za bezpieczeństwo danych w firmie.

Bezpieczeństwo teleinformatyczne najprościej można zdefiniować jako ochronę informacji przetwarzanej, przechowywanej i przesyłanej przy użyciu systemów teleinformatycznych przed przypadkowym bądź celowym ujawnieniem, zmianą, zniszczeniem czy też uniemożliwieniem jej przetwarzania i wykonywania na niej operacji. Problematyka bezpieczeństwa teleinformatycznego zostanie przedstawiona w szerszym kontekście w dalszej części niniejszego opracowania.

Bezpieczeństwo informacji w sieci komputerowej

Zachodzący w zawrotnym tempie proces informatyzacji społeczeństwa spowodował, iż współcześnie informacja jest jednym z kluczowych zasobów gospodarczych, kulturalnych czy naukowych. Poszukiwanie, przetwarzanie oraz transmisja informacji może być efektywnie realizowana dzięki zastosowaniu nowoczesnych technologii komputerowych oraz rozbudowanej sieci teleinformatycznej. Należy jednak mieć na uwadze, iż obok ich pozytywnych aspektów,

do których możemy zaliczyć choćby łatwość komunikowania się, istnieje szereg zagrożeń i niebezpieczeństw. Wobec powyższego ważnym czynnikiem funkcjonowania sieci i systemów teleinformatycznych jest zapewnienie właściwego poziomu bezpieczeństwa informacji, co wymaga skrupulatnej analizy zagrożeń oraz opracowania możliwych sposobów przeciwdziałania.

Bezpieczeństwo systemów teleinformatycznych determinowane jest spełnieniem kilku podstawowych warunków, które można sklasyfikować w dwóch płaszczyznach – wewnętrznej i zewnętrznej.

W wymiarze wewnętrznym wiąże się z zachowaniem poufności, integralności i autentyczności [4]. Pojęcia te zostały zdefiniowane w rozdziale 1. niniejszego artykułu. Przykładowe czynniki mogące doprowadzić do utraty wyżej wymienionych parametrów bezpieczeństwa przedstawiono w tab. 1.

Tab. 1. Czynniki wpływające negatywnie na bezpieczeństwo teleinformatyczne

Zagrożenie	**Przykładowe czynniki**
1	**2**
Utrata poufności	- pokonanie zabezpieczeń fizycznych i programowych - niekontrolowana obecność w obszarze chronionym osób nieupoważnionych - nieroztropność osób uprawnionych - wynoszenie poza strefę ochronną wydruków, przenośnych komputerów oraz elektronicznych nośników danych - naprawy oraz konserwacje przez osoby nieuprawnione - podgląd i podsłuch - elektromagnetyczna emisja ujawniająca
Utrata integralności	- przypadkowe lub celowe spowodowanie awarii systemu operacyjnego lub urządzeń systemu sieciowego - przypadkowe lub celowe uszkodzenie, zniszczenie czy też nieautoryzowana zmiana danych - celowe bądź przypadkowe uszkodzenie oprogramowania aplikacyjnego i użytkowego - wirusy komputerowe - sytuacje kryzysowe: powódź, pożar, huragan itp. - ataki terrorystyczne
1	**2**
Utrata dostępności	- defektywnie działający sprzęt oraz programy - awaria zasilania - wirusy komputerowe - klęski żywiołowe - ataki terrorystyczne - błędy organizacyjne

Źródło: [4]

Ponadto pod uwagę brane mogą być również inne własności, takie jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Autentyczność należy rozumieć jako zgodność istniejącego podmiotu bądź zasobu (użytkownicy, procesy, systemy, instytucje) z deklarowanym; rozliczalność – zagwarantowanie, że działalność podmiotu (użytkownika) przypisana jest jednoznacznie tylko jemu; niezawodność – oznacza, że zachowanie i skutki działania (elementów lub urządzeń systemu) są zgodne z zamierzonymi [14].

W aspekcie zewnętrznym natomiast bezpieczeństwo odnosi się do zdarzeń i sytuacji, które w wyniku nieprawidłowego funkcjonowania systemu informatycznego negatywnie oddziałują na otoczenie fizyczne. Najczęstszą przyczyną jego zakłóceń są nieprawidłowe rozwiązania technologiczne przyjęte na etapie analizy lub sporządzanie systemu [4].

W kolejnych podrozdziałach niniejszego opracowania szczegółowo zostaną scharakteryzowane elementarne zagrożenia determinujące utratę poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności danych przechowywanych i przetwarzanych w systemie komputerowym oraz mechanizmy ochrony i przeciwdziałania przed szerokiego spektrum niebezpieczeństwami.

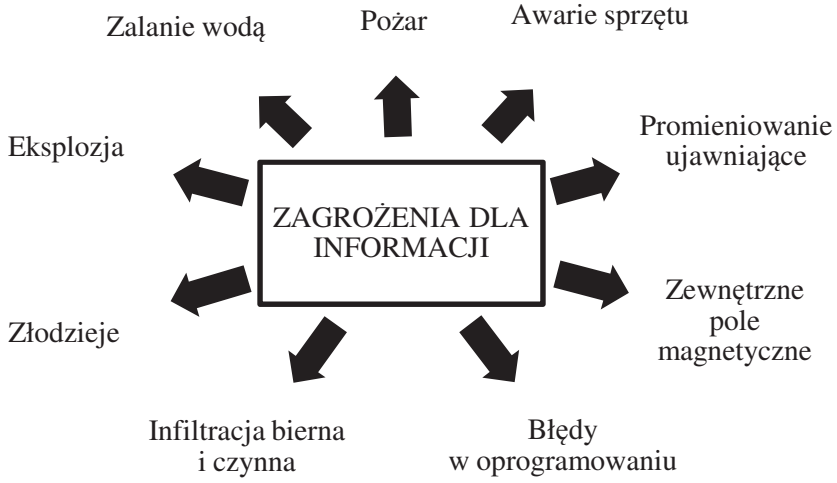
Klasyfikacja zagrożeń bezpieczeństwa teleinformatycznego

Zaprojektowanie oraz wdrożenie skutecznych mechanizmów ochrony zasobów informatycznych wymaga przede wszystkim precyzyjnej identyfikacji zagrożeń, z uwzględnieniem ich wielorodzajowości oraz źródeł powstawania.

Rozważania dotyczące problematyki klasyfikacji zagrożeń, zdaniem autorów, należy rozpocząć od określenia, czym w ogóle jest zagrożenie. Dostępna literatura przedmiotu przedstawia to zagadnienie z różnych perspektyw. *Słownik języka polskiego PWN* podaje, że „zagrożenie to sytuacja bądź stan, który które komuś czymś zagrażają lub, w którym ktoś czuje się zagrożony" [16]. W naukach humanistycznych pojęcie zagrożenia utożsamiane jest z wyzwaniami, o czym mówi niniejsza definicja, „[…] wyzwania, które są właściwie rozpoznane i podejmowane, stanowią szanse, zaś wyzwania nie podejmowane lub podejmowane za późno mogą przekształcić się w zagrożenia" [1].

Zagrożenia dla bezpieczeństwa teleinformatycznego to zdarzenia (np. pożar, powódź) bądź przyczyny zdarzeń (np. skopiowanie danych), które mogą generować straty dla przedsiębiorstwa, szczególnie o charakterze finansowym. W najprostszy sposób zagrożenia bezpieczeństwa zasobów informatycznych można klasyfikować jako zagrożenia: losowe (zewnętrzne, wewnętrzne) oraz intencjonalne. Do zagrożeń losowych zewnętrznych zalicza się temperaturę, wilgotność, wyładowania atmosferyczne, zanieczyszczenie powietrza, awarie systemu zasilania, klimatyzacji, instalacji wodociągowej, a ponadto kataklizmy i katastrofy budowlane. Z kolei zagrożenia losowe wewnętrzne tworzą błędy

użytkowników, przypadkowe zniszczenie bądź uszkodzenie danych, błędne działania administratora bazy danych czy administratora systemu operacyjnego, nieprawidłowa konfiguracja systemu, wadliwy sprzęt i oprogramowanie. Drugą grupę stanowią zagrożenia związane z intencjonalną działalnością człowieka. Tego typu zagrożenia można podzielić na pasywne oraz aktywne. Do pasywnych zalicza się monitorowanie sieci, podgląd oraz analizę ruchu w sieci. Natomiast do zagrożeń aktywnych należy zaliczyć: nieuprawioną zmianę, ujawnienie lub usunięcie informacji, oszustwa (np. bankomatowe, fałszownie kart magnetycznych), powielanie programów komputerowych, przechowywanie nielegalnych zbiorów, zakup oraz sprzedaż nielegalnymi kanałami sprzętu i oprogramowania, zakłócenie pracy serwera lub urządzeń zabezpieczających, korzystanie ze służbowego sprzętu komputerowego w celach prywatnych lub jego kradzież [15, 20]. Na rys. 2 przedstawiono kilka przykładowych zagrożeń dla bezpieczeństwa informacji przetwarzanej i przechowywanej w systemie komputerowym.



Rys 2. Zagrożenia dla informacji przetwarzanej i przechowywanej w systemach komputerowych
Źródło: [11].

Z punktu widzenia bezpieczeństwa informacji szczególną grupę zagrożeń stanowią wirusy komputerowe oraz złośliwe oprogramowanie.

Wirus komputerowy to samoreplikujący się złośliwy program, którego kod wykonywalny zaszyty jest w innym programie użytkowym lub w inny sposób jest z nim powiązany. Infekuje inne programy i pliki po zmodyfikowaniu ich do przyjęcia. Wirusy mają za zadanie umieścić własny kod w określonym miejscu na dysku lub w programie, a tym samym zniszczenie zapisanej na dys-

kach informacji. Bardzo często towarzyszy temu generowanie dziwnych melodii i komunikatów oraz zakłócanie wyświetlania wszelkiego rodzaju informacji na ekranie [13]. Podział wirusów ze względu na sposób infekowania wraz z ogólną ich charakterystyką został zaprezentowany w tab. 2.

Tabela 2. Charakterystyka wirusów komputerowych

Rodzaje wirusów	Charakterystyka
1	**2**
▪ Wirus dyskowy	umiejscawia się w sektorach zawierających informacje na temat struktury dysku twardego; dysk zostaje zainfekowany wirusem tylko wtedy, gdy użytkownik uruchomi system z zainfekowanego nośnika
▪ Wirus plikowy	przenosi się wraz z plikami wykonalnymi (COM, EXE, SYS i in.); integruje się z plikiem, pozostawiając nienaruszoną większą część jego kodu
▪ Wirus towarzyszący	rozprzestrzenia się tak, że w przypadku dwóch programów o tej samej nazwie system operacyjny wykonuje plik z rozszerzeniem *.COM przed plikiem *.EXE; wirus towarzyszący tworzy plik z rozszerzeniem *.COM i umieszcza w nim swój własny kod wykonywalny, a nazwa pliku jest taka sama jak plik z rozszerzeniem *.EXE
▪ Wirus sprzęgający	nie modyfikuje plików, ale mimo to mnoży się bardzo szybko
▪ Wirus hybrydowy	jest krzyżówką wyżej wymienionych wirusów łączący w sobie ich metody działania
▪ Wirus rezydentny	zaraża w chwili wywołania przerwania systemowego
▪ Wirus nierezydentny	zaraża w chwili działania programu-nosiciela
1	**2**
▪ Wirus mieszany	początkowo działa jak wirus nierezydentny, a po uzyskaniu pełnej kontroli pozostawia w pamięci rezydentny fragment swojego kodu

Źródło [2].

Obok wirusów komputerowych wykorzystywane są inne różnorodne formy programów (tzw. złośliwe oprogramowanie), które w skuteczny sposób zagrażają stabilności systemu oraz zgromadzonych w nim danych i informacji. Dostępna literatura przedmiotu wskazuje na następujące [11, 13, 19]:
– koń trojański,
– bomba logiczna,
– bomba czasowa,

- królik,
- robak,
- muł trojański,
- łańcuch szczęścia,
- makrowirusy,
- ukryte narzędzia zdalnej administracji,
- programy kradnące hasła i inne poufne informacje,
- programy w przyszłości mające być wirusami,
- zestawy do konstruowania wirusów i generatory polimorficzne.

Koń trojański to program, który zawiera ukryte funkcje przeznaczone najczęściej do ułatwienia przejęcia kontroli nad komputerem bez wiedzy właściciela. Konie trojańskie najczęściej niszczą dane na dyskach lub zawieszają pracę systemu w zależności od pewnych okoliczności lub przy pierwszym uruchomieniu. Najczęściej ukryte są w programach „udających" inne pożyteczne programy czy narzędzia [13].

Bomba logiczna. W programie znajduje się złośliwy kod bomby logicznej, który uaktywnia się wtedy, gdy zostaną spełnione konkretne warunki, np. określona liczba uruchomień.

Bomba czasowa. Jest to bomba logiczna, która uruchamia się po upływie określonego czasu.

Królik. Program wykorzystujący w pełni określone zasoby systemu, a na skutek błyskawicznego i niekontrolowanego powielania się zapełnia system.

Robak. Funkcjonuje bardzo podobnie do wirusa. Działa w sieci przesyłając kopie do innych systemów. Jego działanie sprowadza się do tworzenia własnych duplikatów [5, 19].

Muł trojański. Pobudza fałszywe komunikaty, które naśladują dialog z komputerem.

Łańcuch szczęścia. Replika komunikatu wysyłanego pocztą elektroniczną.

Makrowirusy. Wirusy działające i rozmnażające się w środowisku pojedynczej aplikacji, bądź nawet jej konkretnej wersji, przenoszone za pośrednictwem makropoleceń programu [11, 13].

Identyfikacja technik ataku

Specyficznym rodzajem zagrożeń dla poufności, integralności i dostępności informacji są ataki na system teleinformatyczny, wyczerpujące znamiona działalności przestępczej. Ataki na system komputerowy można podzielić w następujący sposób [11]:

- ataki lokalne – intruz posiada fizyczny dostęp do atakowanego komputera;

- ataki wewnętrzne – atak jest prowadzony z komputera, który jest włączony do tej samej sieci lokalnej;
- ataki zewnętrzne (zdalne) – wykonywane z sieci publicznej.

Do najważniejszych technik ataku na system teleinformatyczny autorzy niniejszego opracowania zaliczają: hacking, spyware, crimeware, eksploit, atak słownikowy, back door, skanowanie portów, phishing, sniffing, pharming, spoofing, Denial of Service, rootkit. W oparciu o analizę literatury przedmiotu poniżej dokonano ich ogólnej charakterystyki.

Hacking – włamanie komputerowe, próba uzyskania dostępu do systemu komputerowego z pominięciem uwierzytelniania. Ataki przeprowadzane są przez kanały komunikacji komputera z Internetem. Sprawców tego przestępstwa nazywa się *hackerami*. Można ich podzielić na pięć kategorii [19]:

- nowicjuszy – ich działania są nieprzewidywalne, a cel, który chcą osiągnąć może w każdej chwili się zmienić;
- analityków lub badaczy – dla nich głównym celem nie jest powodowanie szkód i niszczenie, a poznawanie innego rodzaju komputerów;
- turystów – traktują systemy komputerowe jak pewnego rodzaju zagadki i łamigłówki;
- wandali – ich celem jest spowodowanie jak największych szkód;
- złodziei – najczęściej działają na rzecz konkurencji.

Spyware, crimeware – są to programy szpiegowskie, których zadaniem jest zbieranie i wysyłanie informacji o komputerze bez wyraźnej zgody właściciela.

Eksploit – atak, wykorzystujący błąd lub lukę w aplikacji bądź systemie operacyjnym. Celem jest tu przede wszystkim przepełnianie buforów i umieszczanie podprogramów w losowych miejscach w pamięci normalnie zabronionych przez użytkownika. W skutek takiego ataku intruz może uzyskać pełny dostęp do atakowanego komputera [13].

Atak słownikowy – polega na próbie zalogowania się do systemu z wykorzystaniem dużej listy słów, które znajdują się w określonym pliku.

Back door – „tylne drzwi", zainstalowanie oprogramowania, które umożliwia intruzowi na dostanie się do systemu w inny sposób niż poprzez logowanie.

Skanowanie portów – czynność, która poprzedza zdalny atak na system teleinformatyczny. Dzięki skanowaniu potencjalny intruz posiada informacje o aktywnych portach i udostępnionych usługach [13]. Wyróżnia się skanowanie otwarte, półotwarte oraz skryte.

Phishing – bardzo poważna i groźna odmiana spamu, która polega na tworzeniu fałszywych wiadomości e-mail i stron WWW, głównie finansowych, wyglądających identycznie jak serwisy internetowe firm o znanej marce lub

banków. Te atrapy stron mają za zadanie nakłonić klientów do podania numeru karty kredytowej, hasła logowania, informacji o koncie bankowym.

Sniffing – podsłuchiwanie przesyłanych przez sieć pakietów. Za pomocą tzw. sniffera można przechwycić dane przesyłane niekodowanym kanałem.

Pharming – wykorzystywanie oprogramowania wymuszającego na przeglądarce internetowej przekierowanie wysyłanych danych do serwera atakującego, zamiast do serwera banku.

Spoofing – podszywanie się pod inny komputer w sieci. Metoda ta opiera się na umieszczaniu w sieci preparowanych, modyfikowanych lub uszkodzonych pakietów danych. Następuje to przez przechwytywanie przesyłanych pakietów w celu ich modyfikacji i odesłania sfałszowanych do komputera docelowego. W efekcie „legalny" użytkownik zostaje rozłączony, a włamywacz kontynuuje połączenie z pełnymi prawami dostępu, np. do konta w banku [19]. Najpopularniejsze techniki oparte na spoofingu to:

- IP spoofing,
- E-mail spoofing

Denial of Service (DoS) – odmowa wykonania usługi. Atak ten bazuje na takim wykorzystaniu zasobów komputera, że nie jest on w stanie zagwarantować poprawnej realizacji usług, jakie oferuje. Jednym ze sposobów na zastosowanie ataku typu DoS jest tzw. *flooding*, polegający na wysyłaniu do atakowanego komputera takiej liczby zapytań, by odwołania rzeczywistych użytkowników do serwera nie mogły zostać obsłużone. Sprawcę ataku DoS jest względnie łatwo namierzyć, gdyż jest on przeprowadzany z jednej, konkretnej maszyny w sieci. Pakiety agresora są wysyłane ze sfałszowanym (*spoofing*) adresem sieci, aby utrudnić wyśledzenie nadawcy. Inną odmianą ataku DoS jest *ping of death*, polegający na wysyłaniu do atakowanego komputera pakietów ping o złej długości, który może spowodować awarię systemu docelowego (zawieszenie się lub restart komputera), jeżeli jest on podatny na ten atak. Zmodyfikowaną wersją DoS jest *Distributet Denial of Service* (DDoS), która wprowadza kilka istotnych innowacji, znacznie zwiększających jego skuteczność i utrudniających jego zablokowanie. Atak przeprowadzany jest w sposób skoordynowany z kilku komputerów jednocześnie, natomiast maszyna, z której uruchamiany jest atak, w ogóle w nim nie uczestniczy, co utrudnia jej namierzenie.

Rootkit – trojany, wirusy, a także programy typu spyware stosują różne metody ukrywania się przed skanerami. Te sposoby i metody nazywamy rootkitami. Mogą to również być różnego rodzaju narzędzia lub programy, których głównym zadaniem jest skuteczne ukrycie jakiejkolwiek próby uzyskania uprawnień administratora czy włamania. Intruz, chcąc włamać się do systemu, najczęściej wykorzystuje do tego celu dziurę w systemie i instaluje rootkit. W skład rootkitu bardzo często wchodzą proste narzędzia do przesyłania haseł oraz do monitorowania ruchu w sieci. Program typu spyware jest podstawą

działania rootkitu, gromadzi informacje o użytkownikach, a następnie przesyła je do bazy atakującego, dając mu tym samym pełen dostęp do systemu [11].

Socjotechnika – uzyskiwanie informacji na temat systemu od jego legalnych użytkowników. Jest to bardzo skuteczna technika, jeśli chodzi o dostęp do danych wrażliwych, np. odbiorców, haseł systemowych itp. Napastnik wzbudza zaufanie ofiary stopniowo, za pomocą odpowiedniego połączenia informacji o systemie i technik manipulacyjnych. Ofiara w rezultacie ujawnia więcej dodatkowych informacji, które zostaną wykorzystane przez napastnika do kontynuacji ataku [13]. Atak z wykorzystaniem socjotechniki może przynieść napastnikowi wiele korzyści, takich jak uzyskanie dostępu fizycznego, uzyskanie danych uwierzytelniających do dostępu zdalnego, zdobycie informacji, naruszenie innych mechanizmów kontroli bezpieczeństwa.

Ataki socjotechniczne można podzielić na aktywne, podczas których wskazuje się obiekty ataku i oczekuje się od nich reakcji oraz ataki pasywne, w przypadku których najpierw pozostając w ukryciu, gromadzi się informacje (najczęściej jest to podsłuchiwanie, obserwowanie i prowadzenie analiz).

Jedną z najstarszych technik stanowiących bardzo duże zagrożenie i mającą na celu wykradzenie danych z przedsiębiorstwa jest zbieranie przez konkurencję informacji o przedsiębiorstwie poprzez przeszukiwanie śmieci. Często ta metoda jest bagatelizowana. Jest to jednak sposób bardzo popularny, a decyduje o tym nie tylko łatwość, z jaką można zdobyć takie dane, ale również bezkarność w przypadku zatrzymania.

Przeciwdziałanie zagrożeniom

Procedury ochronne stosowane są w celu zabezpieczenia systemów komputerowych przed niepowołanym dostępem osób nieupoważnionych. W obecnych czasach istnieje bardzo wiele systemów zabezpieczania, mimo tego niestety nie ma idealnego mechanizmu przeciwdziałania zagrożeniom. Duży wybór metod zabezpieczeń, które stanowią ograniczenie przed uzyskaniem dostępu przez użytkowników nieupoważnionych do korzystania z danego systemu, jest poważnym problemem. Szczególnie trudnym przedsięwzięciem jest zidentyfikowanie użytkowników mających dostęp do danego systemu, którzy działają szkodliwie na część bądź cały system. Procedury zarządzania pracą oraz rozwiązania technologiczne stanowią istotną podstawę skutecznego zabezpieczenia systemów informacyjnych [7].

Zaleca się, aby systemy mające kluczowe znaczenie dla funkcjonowania organizacji były kopiowane i przechowywane w osobnym miejscu. W momencie, gdy awarii ulegnie system podstawowy, to system dodatkowy ma za zadanie w jak najkrótszym czasie przejąć obowiązki systemu podstawowego. W celu uchronienia systemu awaryjnego przed katastrofą należy go umieścić jak najdalej od źródła zagrożenia. Do zastąpienia systemu głównego podczas

katastrofy niezbędna jest nadmiarowość sprzętu, danych oraz personelu. Niezbędną rzeczą, którą należy sporządzić, a następnie wdrożyć, jest procedura bezpieczeństwa mająca na celu wyeliminowanie jak największej liczby zdarzeń i sytuacji mogących powstać podczas katastrofy naturalnej [7].

Czynnik ludzki stanowi istotne zagrożenie dla bezpieczeństwa informacji przetwarzanej i przechowywanej w systemach i sieciach informatycznych. Każde działanie jednostki społecznej obarczone jest ryzykiem popełnienia błędu. Nie ma ludzi nieomylnych, więc nie da się całkowicie wyeliminować błędu ludzkiego, można go jedynie starać się ograniczać i zmniejszać. W celu minimalizacji częstotliwości popełnienia pomyłki skuteczne są różnego rodzaju szkolenia, uświadamianie, jakie są konsekwencje złych działań i zaniedbań, ograniczenia zakresu obowiązków, a także uprawnień do zasobów informacyjnych.

Jeśli mowa o uszkodzeniach sprzętu, oprogramowania i infrastruktury, to w celu ochrony tego rodzaju zasobów najczęściej stosuje się nadmiarowość urządzeń. Jedną z najlepszych i najczęściej stosowanych metod zabezpieczenia przed utratą danych jest utworzenie kopii zapasowej, zwanej także kopią bezpieczeństwa. Istnieją także zautomatyzowane systemy monitorujące poprawność działania sprzętu oraz oprogramowania, mające na celu naprawienia powstałej usterki bądź przejmujące zadania uszkodzonego elementu podczas powstania awarii. Niezbędne jest ponadto szczegółowe sprawdzanie poprawności działania programów przede wszystkim pod względem bezpieczeństwa.

Szczególnym rodzajem zagrożenia są intencjonalne działania człowieka, który w sposób negatywny oddziałuje na sieć komputerową (np. za pomocą złośliwego oprogramowania) przedsiębiorstwa lub instytucji, powodując modyfikację, utratę bądź nieupoważniony dostęp do wrażliwych danych. W celu zapewnienia właściwej ochrony przed tego rodzaju zagrożeniami bardzo skuteczne okazują się szkolenia pracowników firmy z zakresu bezpiecznego korzystania z zewnętrznych programów, sieci oraz instalacji elementów ochronnych. W dążeniu do zmniejszenia zagrożeń wynikających ze świadomego działania ludzi powinno się uszczelnić procedury bezpieczeństwa i uświadomić pracowników o potencjalnych zagrożeniach. Ponadto firma może nawiązać wzajemną współpracę z sąsiednimi firmami bądź partnerami działającymi w podobnym segmencie rynku w celu budowy wspólnych systemów antyawaryjnych. Nie można jednoznacznie określić zakresu działania, ponieważ zagrożenia zależne są od branży firmy, rodzaju przedsiębiorstwa oraz skali wykorzystywania technik teleinformatycznych [7, 13].

Analiza ryzyka

Głównym zadaniem współczesnych systemów teleinformatycznych jest przetwarzanie, przechowywanie oraz przesyłanie informacji. Funkcjonują one w otoczeniu skrywającym w sobie różnego rodzaju zagrożenia i niebezpieczeństwa. Dlatego też podstawowym elementem zarządzania bezpieczeństwem systemów teleinformatycznych jest zarządzanie ryzykiem bezpieczeństwa informacji.

Podejmując problematykę zarządzania ryzykiem, w węższym wymiarze analizy ryzyka w pierwszej kolejności, należy dokonać interpretacji pojęcia ryzyko. Termin ten wywodzi się z włoskiego słowa risico. *Słownik języka polskiego PWN* definiuje ryzyko „jako możliwość, że coś się nie uda; przedsięwzięcie, którego wynik jest niepewny" [16]. Według *Polskiego podręcznika procesu zarządzania ryzykiem* wydanego przez Ministerstwo Finansów Rzeczypospolitej Polskiej ryzyko to „niepewność związana ze zdarzeniem lub działaniem, które wpłynie na zdolność organizacji do realizacji celów jej działalności. Może mieć charakter negatywnego zagrożenia lub też pozytywnej możliwości". Najbardziej adekwatną definicją dla potrzeb bezpieczeństwa informacji w systemach teleinformatycznych jest ta zawarta w normie IEC 61508, według której ryzyko oznacza „[…] miarę stopnia zagrożenia dla tajności, integralności i dostępności informacji wyrażoną jako iloczyn prawdopodobieństwa wystąpienia sytuacji stwarzającej takie zagrożenie i stopnia szkodliwości jej skutków" [11]. Z kolei za najbardziej powszechną definicję analizy ryzyka dla potrzeb bezpieczeństwa teleinformatycznego można uznać następującą: „analiza ryzyka […] jest procesem identyfikacji (jakościowej i ilościowej) ryzyka utraty bezpieczeństwa teleinformatycznego" [11].

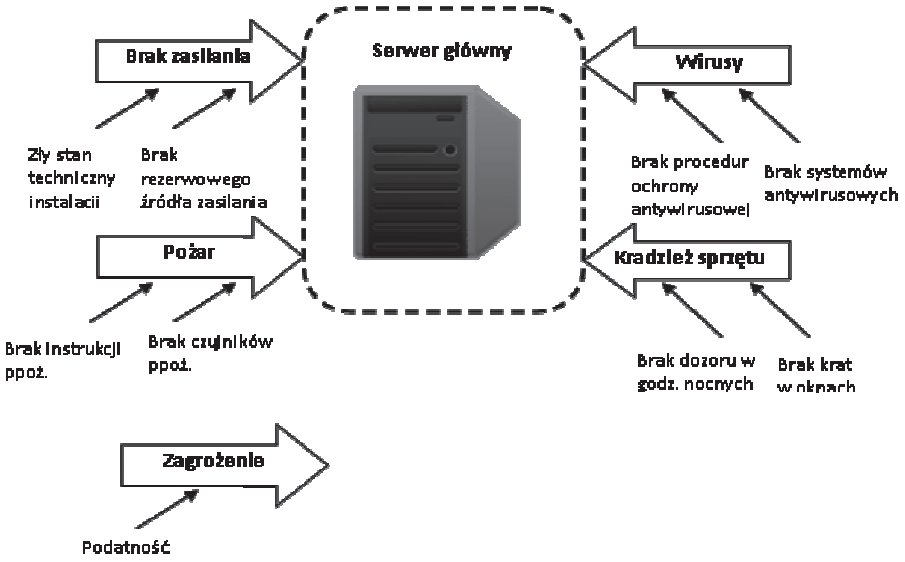
K. Liderman w swojej pracy wskazuje na następujące czynności tworzące proces analizy ryzyka bezpieczeństwa teleinformatycznego [11]:

- identyfikacja zagrożeń oraz jakościowe/ilościowe określenie narażonych na utratę dóbr materialnych oraz informacji;
- wyznaczenie wartości dóbr materialnych (np. sprzętu komputerowego);
- określenie wartości informacji w sytuacji jej utraty, ujawnienia, zmiany czy niedostępności;
- wyznaczenie zagrożeń (oraz ich stopnia) dla bezpieczeństwa teleinformatycznego;
- zdefiniowanie elementów systemów teleinformatycznych podatnych na owe zagrożenia (i ich stopnia podatności);
- przeprowadzenie analizy ryzyka cząstkowego;
- akceptacja ryzyka cząstkowego.

Warunkiem koniecznym do przeprowadzenia analizy ryzyka jest identyfikacja wszystkich narażonych na niebezpieczeństwo zasobów. W przypadku

systemu teleinformatycznego będą to: zasoby fizyczne (komputery, nośniki danych), oprogramowanie, zasoby ludzkie (użytkownicy, projektanci, programiści, administratorzy) oraz informacja [15]. Niezbędne jest także oszacowanie wpływu utraty poufności, integralności i dostępności poszczególnych aktywów na funkcjonowanie jednostki gospodarczej oraz na realizowane przez nią cele biznesowe. Do tego celu można wykorzystać 4-stopnią skalę ważności (1 – niski wpływ, 2 – średni, 3 – wysoki, 4 – bardzo wysoki, maksymalny). W zależności od rodzaju narażonych aktywów ich wyceny dokonuje się wyłącznie w oparciu o wartość księgową bądź wartość księgowa stanowi jedynie podstawę do jej wyceny [6]. Jako przykład może posłużyć zdarzenie losowe, jakim jest pożar, w wyniku którego zniszczeniu ulega sprzęt komputerowy przechowywany w magazynie i niewykorzystywany do codziennej pracy o wartości księgowej 120 000 zł oraz główny serwer firmy, którego wartość księgowa również wynosi 120 000 zł. Zniszczenie zarówno jednego, jak i drugiego zasobu organizacji powoduje straty o tej samej wartości księgowej, lecz niesie zupełnie odmienne skutki dla przedsiębiorstwa. Dokonując wyceny sprzętu komputerowego niewykorzystywanego do realizacji żadnych zadań biznesowych przyjąć należy tylko jego wartość księgową. Całkiem inaczej sytuacja wygląda w przypadku wyceny wartości serwera firmy. Wówczas oprócz wartości księgowej należy wziąć pod uwagę koszty związane z przestojem firmy, a przede wszystkim wartość przechowywanych danych. Utrata strategicznych informacji może okazać się przysłowiowym „gwoździem do trumny" i doprowadzić do upadłości firmy [8].

Drugi etap analizy ryzyka koncentruje się na identyfikacji zagrożeń dla bezpieczeństwa informacji przetwarzanej i przechowywanej w systemie teleinformatycznym przedsiębiorstwa. Do uprzednio zdefiniowanych zasobów należy przypisać konkretne zagrożenia oddziałujące na nie w negatywny sposób. Ważne jest, aby proces identyfikacji zagrożeń prowadzony był z należytą starannością i skrupulatnością, uwzględniając nie tylko aktualne, ale także przyszłe niebezpieczeństwa. Etap identyfikacji i szacowania ryzyka musi odbywać się w oparciu o różnego typu informacje dotyczące występowania zagrożeń, zarówno gromadzone przez samą jednostkę gospodarczą, jak również dane statystyczne publikowane przez rozmaite instytucje i organizacje, jak np. Główny Urząd Statystyczny czy też Komendę Główną Policji (w zakresie przestępstw komputerowych), a skończywszy na wszelkich opracowaniach dotyczących awarii wydawanych przez producentów sprzętu i oprogramowania komputerowego. Po zidentyfikowaniu i oszacowaniu zagrożeń równie ważne jest zdefiniowanie podatności odnoszących się do konkretnych zagrożeń. Podatność, czyli „[…] słabość, luka, brak zabezpieczeń przed występującymi zagrożeniami wobec aktywów organizacji" [9]. Wzajemne relacje pomiędzy zasobami, zagrożeniami oraz podatnościami zobrazowano na rys. 3.



Rys. 3. Relacje między zasobem, zagrożeniem a podatnością
Źródło: opracowanie własne.

Zasadniczym etapem analizy ryzyka jest oszacowanie jego wartości. W praktyce gospodarczej wyróżnia się dwie podstawowe grupy metod dokonywania analizy ryzyka bezpieczeństwa informacji. Pierwszą z nich stanowią metody ilościowe określane również jako kwantyfikatywne. Polegają na zastosowaniu matematycznych obliczeń w celu wyznaczenia wpływu zagrożeń na bezpieczeństwo systemu oraz określenia prawdopodobieństwa ich wystąpienia. Bazują one głównie na danych liczbowych – do wykonywania obliczeń brane są pod uwagę przeważnie dane statystyczne oraz dane archiwalne, natomiast wynik oszacowania ryzyka wyrażany jest w formie kwotowej (pieniężnej) bądź też procentowej. Drugą grupę tworzą metody jakościowe (kwalifikatywne), charakteryzujące się dość dużym subiektywizmem z uwagi na fakt, iż w procesie analizy ryzyka wykorzystuje się wiedzę i doświadczenie specjalistów. Ryzyko określane jest w formie opisowej, posiadającej liczbowe odpowiedniki (ryzyko małe – 1, ryzyko maksymalne – 4) [6].

W niniejszym artykule przyjęto, że na ogólną wartość ryzyka składa się przewidywana łączna suma strat wszystkich aktywów systemu spowodowana określonym zagrożeniem oraz podatnością w ustalonym czasie [9].
Niniejsze założenie można opisać wzorem:

$$R = F \times V \times W \text{ oraz } F \times V = P \quad (1)$$

gdzie:
R – wartość ryzyka;
F – częstotliwość wystąpienia zagrożenia;
V – podatność systemu informatycznego (lub jego elementu) na zagrożenie (zgodnie z PN-I-13335–1:1999 jest to miara prawdopodobieństwa wykorzystania określonej podatności przez dane zagrożenie);
W – wartość straty – przewidywana średnia utrata wartości aktywów w wyniku wystąpienia pojedynczego incydentu;
P – prawdopodobieństwo wystąpienia zdarzenia powodującego utratę wartości aktywów w przyjętym okresie.

W oparciu o powyższe rozważania autorzy niniejszego opracowania proponują ogólną wartość ryzyka utraty bezpieczeństwa teleinformatycznego opisać poniższym założeniem:

$$R = F \times V \times W, \text{ gdzie } W = W_1 + W_2 + \ldots W_n \quad (2)$$

gdzie:
W_1 – wartość księgowa aktywów;
W_2 – wartość przetwarzanych i przechowywanych informacji w systemie teleinformatycznym;
W_n – wartość pozostałych strat.

Posłużmy się w niniejszym opracowaniu ponownie przykładem przedstawiającym zniszczenie głównego serwera firmy w wyniku pożaru. Dla potrzeb oszacowania ryzyka przedsiębiorstwo przyjmuje, że jego wartość księgowa równa się 120 000 zł, wartość zgromadzonych na nim informacji, niezbędnych w realizacji podstawowych funkcji biznesowych, oszacowano na kwotę równą 200 000 zł, natomiast wartość strat poniesionych w wyniku przestoju w funkcjonowaniu firmy oraz przywracania sprawności funkcjonowania systemu oszacowano na 90 000 zł; częstotliwość zajścia tego zdarzenia szacowana jest na 0, 001 w okresie 1 roku, podatność systemu natomiast oszacowana została na 5%. Oczekiwana wartość straty (ryzyko utraty informacji) wyniesie, zatem: *(120 000 zł + 200 000 + 900 000) x 0, 001 x 5% = 45 zł.*

Omawiany przypadek pokazuje, iż wartość ryzyka utraty poufności, dostępności, integralności, rozliczalności, autentyczności i niezawodności informacji przetwarzanej, przechowywanej i przesyłanej przez systemy i sieci teleinformatyczne na skutek wystąpienia pożaru jest relatywnie niska [9]. Wynika to przede wszystkim z niskiej wartości oszacowanej podatności systemu oraz częstotliwości wystąpienia tego rodzaju zagrożenia. Istniejący stan rzeczy jest zapewne rezultatem wdrożenia kompleksowego systemu przeciwpożarowego, który obok fizycznych środków wykrywania źródła zagrożenia obejmuje swym

zakresem liczne działania organizacyjne, takie jak regulaminy i instrukcje ppoż. połączone ze szkoleniem pracowników.

Podsumowanie

Jedną z podstawowych funkcji współczesnego przedsiębiorstwa bądź instytucji publicznej jest zarządzanie zasobami informatycznymi, z których strategiczną wartość stanowią aktywa informacyjne. Wykorzystywane są one w procesie podejmowania decyzji, dlatego też muszą charakteryzować się podstawowymi atrybutami bezpieczeństwa, czyli optymalnym poziomem poufności, integralności i dostępności, a w przypadku informacji przetwarzanej, przechowywanej i przesyłanej w systemach i sieciach komputerowych dodatkowo autentycznością, rozliczalnością, niezaprzeczalnością oraz niezawodnością.

Prowadzenie aktywności gospodarczej w środowisku zdominowanym przez technikę informatyczną stanowi pewnego rodzaju wyzwanie dla utworzenia i utrzymania bezpiecznych warunków przetwarzania i przesyłania informacji [15].

Wobec powyższego wywodu główną potrzebą staje się ciągłe identyfikowanie zagrożeń dla bezpieczeństwa teleinformatycznego, z uwzględnieniem różnorodnych kryterium podziału. Należy mieć również na uwadze fakt, iż postęp w dziedzinie technologii informatycznej, oprócz pozytywnych walorów, generuje coraz to nowsze, niezidentyfikowane dotąd niebezpieczeństwa i zagrożenia. Doświadczenia życia codziennego pokazują, iż praktycznie każdego dnia dochodzi do prób włamania do systemu komputerowego, a administratorzy sieci udaremniają nieuprawnione wejścia do systemu. Równocześnie w środkach masowego przekazu pojawiają się komunikaty o kolejnej luce w systemie operacyjnym lub szkodliwym oprogramowaniu [14]. Niezbędne jest zatem opracowywanie oraz implementacja różnorodnych mechanizmów przeciwdziałania.

Z uwagi na złożoność podejmowanej w niniejszym artykule problematyki przedstawiono w nim jedynie wycinek z całego katalogu zagrożeń i niebezpieczeństw oraz możliwych do zastosowania technik przeciwdziałania.

Podstawowym przedsięwzięciem w ochronie i zabezpieczaniu systemów jest analiza ryzyka identyfikująca ryzyko, które powinno być kontrolowane bądź zostać zaakceptowane. Z perspektywy bezpieczeństwa teleinformatycznego na analizę ryzyka składają się: analiza wartości, zasobów, zagrożeń oraz podatności. Rezultatem analizy ryzyka jest określenie stopnia prawdopodobieństwa wystąpienia niebezpieczeństwa. Skrupulatnie przeprowadzona analiza ryzyka pozwala jednocześnie na redukcję negatywnych skutków lub uniemożliwienie wystąpienia incydentu.

Literatura

[1] Bączek P., Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Wydawnictwo Adam Marszałek, Toruń 2006.
[2] Błaszczyk A., Wirusy – pisanie wirusów i antywirusów, Oficyna Wydawnicza Read me, Warszawa 1998.
[3] Ciborowski L., Walka informacyjna, Wydawnictwo Adam Marszałek, Toruń 1999.
[4] Drogoń W., Mąka D., Skawina M., Jak chronić tajemnice? Ochrona informacji w instytucjach państwowych i przedsiębiorstwach prywatnych, Wydawnictwo Bellona, Warszawa 2004.
[5] Fischer B., Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne, Kraków 2000.
[6] http://www.computerworld.pl/artykuly/318160/Zarzadzanie.ryzykiem.bezpieczenstwa.informacji.w.systemach.TI.html (06.05.2013)
[7] http://www.egospodarka.pl/25690,Bezpieczenstwo-systemow-informatycznych-rodzaje-zagrozen,1,20,2.html (4.05.2013).
[8] http://www.mrf.pl/index.php?mod=m_artykuly&cid=89&id=3&p (6.05.2013).
[9] http://www.mrf.pl/index.php?mod=m_artykuly&cid=89&id (6.05.2013)
[10] Jóźwiak I.J., Szleszyńska A., Rola analizy ryzyka i specyfikacji wymagań bezpieczeństwa w procesie tworzenia systemu zarządzania bezpieczeństwem informacji, Zeszyty Naukowe Politechniki Śląskiej, Gliwice 2010.
[11] Liderman K., Bezpieczeństwo teleinformatyczne, Wydawnictwo WSISiZ, Warszawa 2002.
[12] Liedel K., Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego, Wydawnictwo Adam Marszałek, Toruń 2006.
[13] Łuczek J. (red.), Zarządzanie bezpieczeństwem informacji, Wydawnictwo Oficyna Współczesna, Poznań 2004.
[14] Nowak A., Scheffs W., Zarządzanie bezpieczeństwem informacyjnym, Wydawnictwo AON, Warszawa 2010.
[15] Pańkowska M., Zarządzanie zasobami informatycznymi, Wydawnictwo Difin, Warszawa 2001.
[16] Doroszewski W. (red.), Słownik języka polskiego, Wydawnictwo PWN, www.sjp.pwn.pl.
[17] Tyrała P., Zarządzanie kryzysowe. Ryzyko – bezpieczeństwo – obronność, Wydawnictwo Adam Marszałek, Toruń 2001.
[18] Urbanowicz P. (red.), Ochrona informacji w sieciach komputerowych, Wydawnictwo KUL, Lublin 2004.

[19] Wrzosek M., Nowak A., Identyfikacja zagrożeń determinujących zmiany w systemie bezpieczeństwa społeczeństwa informacyjnego, Wydawnictwo AON, Warszawa 2009.
[20] Żebrowski A., Kwiatkowski M., Bezpieczeństwo informacji III Rzeczypospolitej, Oficyna Wydawnicza Abrys, Kraków 2000.

Michał Pałęga, Dorota Wojtyto, Mariusz Salwierak, Wiesław Kulma, Marcin Knapiński
Politechnika Częstochowska

TELECOMMUNICATION SECURITY AS AN ELEMENT OF THE COMPLEX INFORMATION PROTECTION

Abstract

In the article the pivotal issues related to information security which it is processed and stored in the ICT systems and network was presented. The categorization of incidents of the telecommunication security was elaborated and their main causes of occurrence was indicated. Besides in this article the significant role of the risk analysis in the process to prevent threats of information security was pointed.

Keywords: information security, telecommunication security, risk assessment, risk management.