ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI W PRZEDSIĘBIORSTWIE

Andrzej DULBIŃSKI

Streszczenie. W publikacji zostały przedstawione zagadnienia dotyczące bezpieczeństwa i ochrony informacji. Poruszone są kwestie prowadzenia odpowiedniej polityki bezpieczeństwa w organizacji, a także zaprezentowano nowoczesne środki techniczne wykorzystywane w ochronie danych komputerowych.

Abstract. The issues connected with security management and protection of information have been presented in the publication. The issues of appropriate security policy in an organization are touched on as well as modern technological means used in computer data protection.

Słowa kluczowe: informacja, bezpieczeństwo, ochrona, sieć komputerowa, technologia informacyjna.

1. Wprowadzenie

Informacja w dzisiejszych czasach odgrywa coraz ważniejszą rolę w zarządzaniu nowoczesnym przedsiębiorstwem. Stała się czwartym czynnikiem produkcji, kształtującym wartość dochodów i kosztów obok pracy, kapitału i ziemi. Nadrzędnym zadaniem informacji w zarządzaniu przedsiębiorstwem jest zmniejszenie niepewności w procesie podejmowania decyzji. Organizacja powinna gromadzić i przetwarzać dane, aby z kolei na ich podstawie mogła dokonywać analizy i podejmować trafne decyzje. W czasach silnej konkurencji firma powinna funkcjonować i reagować elastycznie na ciągłe zmiany otoczenia. Świadczy to o tym, iż informacja jest czynnikiem diametralnie wpływającym na proces sprawnego i wydajnego zarządzania. Pozyskanie informacji ważnych, strategicznych przez przedsiębiorstwo konkurujące niejednokrotnie może przyczynić się do dużych strat finansowych jak i moralnych. Dlatego też w każdej nowoczesnej organizacji, wykorzystującej określone technologie informacyjne powinny być wdrożone odpowiednie środki zabezpieczeń, zarówno techniczne jak i organizacyjne. Rozwój technologii w bardzo dużym stopniu przyczynił się do zmian w szybkości i łatwości przetwarzania, a także powstania nowoczesnych form przekazu informacji. Jednocześnie z nastaniem procesu digitalizacji informacji powstały nowe zagrożenia związane z technicznymi środkami przekazu. Przechowywanie informacji w postaci cyfrowej, na nośnikach komputerowych, przesyłanie ich na odległość dzięki sieci transmisji danych (Internet, Intranet, Extranet) było przyczyną powstania nowych, dotychczas nie stosowanych form przechwytywania informacji, jak podsłuch, ingerencja zdalna, itp.

2. Rola technologii informacyjnej w organizacji

Potrzeba pozyskiwania informacji, a zarazem wykorzystywanie nowoczesnych technologii informacyjnych stanowi element wpływający na przemiany dzisiejszych organizacji. Wraz z pojawieniem się owego czynnika, pojawiła się nowa dziedzina w nauce: zarządzanie informacją. Obejmuje takie zagadnienia, jak zarządzanie danymi, planowanie systemów informacyjnych, analiza procesów przepływu i obiegu informacji w przedsiębiorstwie. Zarządzanie informacją zazwyczaj traktowane jest jako jedna z funkcji zarządzania o wysokim znaczeniu strategicznym, o czym świadczy charakter informacji i jej rola w procesach zarządzania. Duże znaczenie informacji wynika z cech charakterystycznych dzisiejszych organizacji, jak:

- rozwój sektora usług informacyjnych,
- semantyczny wzrost różnorodności informacji,

- wzrost intensywności strumieni informacyjnych przy jednoczesnym dynamicznym rozwoju różnorodności procesów informacyjnych.

Każda dzisiejsza firma musi konkurować, co jest potrzebą jej funkcjonowania. Jak stwierdził Z. Mikołajczyk zmiana jest warunkiem funkcjonowania i rozwoju organizacji, przy czym szczególnie istotne jest sprzężenie zmian wewnątrz organizacji ze zmianami w jej otoczeniu. Zmiany wewnętrzne, struktury funkcjonowania organizacji powinny być wspierane poprzez wprowadzanie nowoczesnych technologii informacyjnych. Do potrzeb wprowadzania technologii informacyjnej zaliczyć należy następujące cele:

- polepszenie poziomu, szybkości i jakości komunikacji,
- polepszenie kontaktów z kooperantami,
- poprawienie zadań logistycznych,
- poszukiwanie nowych rynków zbytu na własne produkty.

Technologie informacyjne mają również duży wpływ na zarządzanie strategiczne. Przejawia się on w takich celach, jak:

- powiększenie obszaru działalności gospodarczej,
- wprowadzenie nowych metod zarządzania,
- zwiększenie wskaźników efektywności i wydajności firmy,
- wzrost przewagi konkurencyjnej przedsiębiorstwa.

Samo wprowadzenie technologii informacyjnej nie gwarantuje sukcesu gospodarczego. Należy tu pamiętać, iż kontakty międzyludzkie stanowią bardzo ważny czynnik sukcesu. Technologia jest środkiem do lepszego i efektywniejszego zarządzania firmą, a nie celem samym w sobie. Z kolei błędnie podjęte decyzje, dotyczące zakupu technologii czy jej wykorzystania wywołać mogą odmienny skutek, niż zaplanowano, prowadząc do poniesienia znacznych kosztów. Powodzenie zależy w dużej mierze od struktury organizacji, występujących w niej procesów zarządzania. Aby wprowadzenie TI przyniosło spodziewane korzyści, organizacja powinna mieć wyraźnie sprecyzowany cel, do którego musi dążyć. Powinien on być opracowany ze szczególną dokładnością, opierać się na bogatej wiedzy na temat rynku, wyznaczonych zadaniach gospodarczych. Ważnym elementem wpływającym na powodzenie jest czas, moment wdrożenia. Zbyt wczesne rozpoczęcie inwestycji może zagrażać niedopracowaniem technologii, natomiast zbyt późne, to ryzyko, iż zostanie zastosowana przez konkurencyjne przedsiębiorstwa.

2. Zagrożenia dla informacji w przedsiębiorstwie

Mimo, iż liczne organizacje stosują równolegle technologie tradycyjną i elektroniczną jako nośnik informacji, zaobserwować można duże nasilenie prób dotarcia szczególnie do informacji cyfrowej osób trzecich. Próbę ową nazywa się włamaniem. Jest ona ukierunkowana zazwyczaj na system komputerowy w czasie przechowywania informacji lub w momencie jej przesyłania (transmisji). Ataki osoby niepowołanej mogą mieć dwojaki charakter. W pierwszym przypadku następują poprzez ingerencję fizyczną, wymagającą obecności włamywacza przy urządzeniu sieciowym. Druga możliwość, to atak zdalny spoza siedziby firmy z wykorzystaniem technik teleinformatycznych. Do podstawowych metod ataku należy zaliczyć:

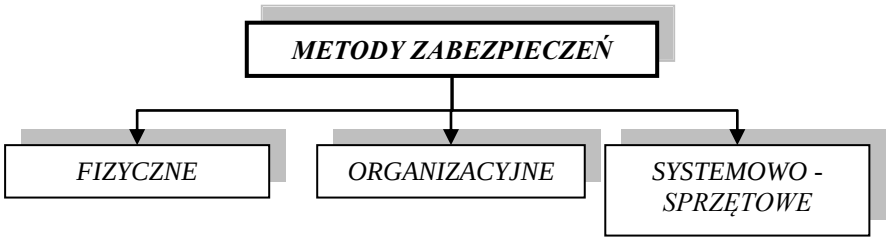
- przechwytywanie w sposób elektroniczny informacji z sieci komputerowych kablowych i bezprzewodowych,
- podsłuch akustyczny,
- przechwytywanie emisji elektromagnetycznej z urządzeń komputerowych,
- obserwacje bezpośrednią.

Praktycznie każda dzisiejsza organizacja oparta jest na przetwarzaniu informacji w postaci cyfrowej. Dane te są gromadzone na nośnikach, takich jak: dyski twarde, nośniki optyczne, pamięci zewnętrzne itp.
Dane zapisane w formie cyfrowej , jak i tradycyjnej są narażone na:

- złe funkcjonowanie sprzętu komputerowego i oprogramowania (przekłamania związane z błędną pracą maszyn, awarie sprzętu i z tego tytułu uszkodzenia informacji źle zapisanej na nośnikach, wirusy komputerowe, destrukcyjna praca oprogramowania itp.),
- zniszczenie (fizyczne uszkodzenie nośnika, uniemożliwiające jego odczytanie),
- zmianą informacji (dokonanie zmian bez uprawnień, szczególnie narażone są tu dokumenty w postaci plików komputerowych, gdyż kolejne wersje plików nie będą zawierały jakichkolwiek śladów ataku),
- powielanie (kopiowanie informacji bez uprawnień, bez dokonywania przy tym zmiany treści),
- ujawnienie zawartości (polega na wtargnięciu osoby postronnej, przeczytaniu i zapamiętaniu dokumentu),
- utratę (pozbawienie firmy nośnika lub informacji przez osobę niepowołaną, która staje się jej właścicielem).

3. Metody zabezpieczeń i ochrony informacji

Formy zabezpieczeń, jakie można zastosować w stosunku do informacji firmowej można podzielić na trzy podstawowe kategorie (rys. 1).



Rys. 1. Metody zabezpieczeń informacji.
Opracowanie własne

Na zabezpieczenia o charakterze fizycznym składa się:

- kontrola prawa dostępu do pomieszczeń i systemów komputerowych, szczególnie do miejsc, w których są przechowywane najcenniejsze informacje, kopie bezpieczeństwa itp.,
- wprowadzenie systemów monitoringu, zabezpieczeń,
- funkcjonowanie systemów przeciwpożarowych,
- ograniczenie nadużyć przez efektywny nadzór,
- wzrost reakcji na nowe zagrożenia pojawiających się w wyniku przemian technologicznych.

Koniecznością jest, aby ochrona fizyczna była skuteczna i w porę wykrywała wszelkie zagrożenia związane z zalaniem, pożarem, włamaniem czy przeciwdziałaniem skutkom nieprzewidzianych przerw w dostawie energii elektrycznej. Zakres ochrony fizycznej obejmuje również zagadnienia dotyczące emisji i transmisji danych. Ograniczenie emisji jest realizowane poprzez zakup certyfikowanego sprzętu komputerowego o obniżonej emisji fal elektromagnetycznych, a także przez zwiększenie granic stref ochronnych. Zabezpieczenia te są realizowane także poprzez:

- wprowadzanie w błąd włamywacza dzięki umieszczeniu urządzeń wysyłających losowo sygnały zakłócające,
- ekranowanie pomieszczeń szczególnie narażonych na ingerencję z zewnątrz,
- zmniejszenie promieniowania przez wyłączanie ekranu monitora,
- wprowadzenie ekranu do kabli przesyłających sygnał w systemie komputerowym,
- instalację sprzętu komputerowego w pomieszczeniach mało narażonych na podsłuch,
- zastosowanie odpowiednich technik szyfrowania, dających należytą gwarancję ochrony w przypadku przewodowych i bezprzewodowych lokalnych sieci transmisji danych IEEE 802.11.

Z terminem ochrona fizyczna związane jest pojęcie strefy bezpieczeństwa. Jest ona wydzielonym obszarem przedsiębiorstwa, w którym są przechowywane informacje, dane i materiały o znaczeniu strategicznym dla funkcjonowania organizacji. Dużą rolę w procesie bezpieczeństwa informacji odgrywają metody organizacyjne. Do zadań ochrony w zakresie organizacyjnym należy zaliczyć:

- opracowywanie określonych procedur dla użytkowników systemu komputerowego,
- wprowadzenie w życie polityki bezpieczeństwa informacji w przedsiębiorstwie,
- politykę zakupów systemów komputerowych pod kątem bezpieczeństwa informacji,
- motywowanie pracowników odpowiedzialnych za dostęp do informacji strategicznych firmy,
- szkolenie pracowników w zakresie prawidłowej obsługi systemów z uwzględnieniem elementów ochrony informacji.

Odpowiednie zarządzanie organizacją i stworzenie efektywnej polityki w zakresie ochrony informacji w przedsiębiorstwie stanowi bardzo ważne ogniwo w tym łańcuchu. Niejednokrotnie to właśnie człowiek jest przyczyną ujawnienia tajnych informacji. Jak podaje literatura przedmiotu blisko 90% ataków, to ataki spowodowane przez pracowników firmy, a tylko 10% przez ingerencję z zewnątrz. Wyrobienie wśród pracowników wysokiego poziomu świadomości w zakresie bezpieczeństwa, to jeden z ważniejszych elementów. Stan ten wymaga przeprowadzenia określonych szkoleń wśród pracowników i uwrażliwiania ich na wartość informacji oraz jej ochrony. Również późniejsze informowanie o sukcesach i przedsięwzięciach w zakresie ochrony powinno być czynnikiem motywującym do zwiększania odpowiedzialności i poczucia własnej wartości w procesie bezpieczeństwa informacji. Wprowadzenie polityki bezpieczeństwa jest poprzedzone sporządzeniem dokumentu, prezentującego koncepcję bezpieczeństwa informacji, strategii, technik i metod, mających na celu osiągnięcie wyznaczonego poziomu bezpieczeństwa. Celem polityki jest także wskazanie wszelkich aspektów i czynników wpływających na zabezpieczenia i procesy związane z przetwarzaniem informacji w organizacji, do których zaliczamy:

- określenie podmiotu chronionego, stopnia niejawności informacji, procedur organizacyjnych i technicznych, przepisy prawne w zakresie ochrony informacji,
- zdefiniowanie zagrożenia; wyznaczenie kierunku, z którego może nastąpić atak,
- dokonanie analizy ryzyka, wyznaczenie metody ochrony,
- przeanalizowanie i przeznaczenie wymaganych środków finansowych,
- określenie procedury w przypadku zagrożenia i awarii,
- wdrożenie w życie planu bezpieczeństwa,
- przeprowadzanie szkoleń w zakresie wprowadzanego planu bezpieczeństwa.

Utrzymanie poziomu bezpieczeństwa w organizacji związane jest z ciągłą kontrolą, nadzorem i obserwacją metod, które zostały wykorzystane oraz ich udoskonalaniem. Organizacja nie może poprzestać na wdrożeniu założonego planu dotyczącego bezpieczeństwa, ale musi koniecznie dokonywać wszelkich przemian posiadanego systemu, wraz z pojawieniem się nowych zagrożeń. Należy nadmienić, iż jedną z metod ochrony jest szybka reakcja na

ewentualne próby ataku. Ma to duże znaczenie, gdyż intruz, który zauważy brak reakcji ze strony przedsiębiorstwa na własne poczynania, czuje się jeszcze bardziej zachęcony do dalszej ingerencji. Wykorzystanie metod organizacyjnych związane jest z opracowywaniem określonych procedur – dokumentów, dotyczących:

- postępowania z nośnikami informacji (już niewykorzystywanymi),
- podjęcia określonych kroków w przypadku ujawnienia informacji firmy,
- procedury zakupu sprzętu teleinformatycznego o należytej jakości,
- metody oznaczania nośników informacji,
- wykonywania kopii bezpieczeństwa ważnych dokumentów,
- zasad użytkowania, instalowania oprogramowania itp.,
- zasad stosowania środków komunikacji.

Ważne jest, aby każda z procedur wyraźnie wskazywała osoby odpowiedzialne za ich wdrażanie, szkolenie pracowników, nadzór i aktualizację.

Kolejnym aspektem organizacyjnym jest odpowiednie dobranie personelu firmy. Z racji wykonywanych funkcji w organizacji zwykle pracownicy mają dostęp do określonej grupy informacji, relatywnie ważnych do stanowiska. Osoby, na których spoczywa tajemnica dochowania informacji powinny być należycie dobierane i weryfikowane. Przed wdrożeniem systemu komputerowego zarząd przedsiębiorstwa ma obowiązek sklasyfikowania swych pracowników pod względem praw do określonych danych. Każdy pracownik, mający dostęp do ważnych informacji powinien być stale weryfikowany pod kątem zaufania. Podczas przydzielania zadań poszczególnym pracownikom powinno wziąć się pod uwagę zasadę:

- dwóch osób (czynniki, które mogą się przyczynić do złamania systemu zabezpieczeń należy rozdzielić pomiędzy dwie osoby; daje to większą gwarancję bezpieczeństwa systemu),
- rotacji obowiązków (najważniejsze zadania w organizacji powinny być przydzielane czasowo i zmiennie w określonej częstotliwości między wybranymi pracownikami),
- wiedzy koniecznej (dany użytkownik systemu ma dostęp wyłącznie do takich danych i informacji, które są one potrzebne, w ramach wykonywanych obowiązków służbowych),
- minimalnego środowiska (pracownikowi należy udostępnić jedynie te pomieszczenia, które są mu naprawdę potrzebne; nie należy dawać prawa wstępu do miejsc zbędnych, co zmniejsza automatycznie poziom bezpieczeństwa),
- motywowania pracowników odpowiedzialnych za zabezpieczenie informacji przez odpowiednie wynagrodzenie.

Ostatnim czynnikiem wpływającym na bezpieczeństwo i ochronę informacji są środki techniczno – sprzętowe i programowe. Firma XXI wieku, to organizacja wyposażona w najnowsze technologie przesyłu informacji, jak: sieci komputerowe przewodowe i bezprzewodowe, Internet, Intranet czy Extranet, technologie zdalnego dostępu do własnych zasobów sieciowych firmy przez pracowników. Dlatego też stanowią one największe zagrożenie dla informacji. Do metod zabezpieczeń związanych z systemami komputerowymi, transmisją danych itp. zalicza się:

- wykorzystywanie kodowania i szyfrowania informacji,
- stosowania podpisów elektronicznych,
- wykorzystywania wirtualnych sieci prywatnych,
- tworzenie kopii bezpieczeństwa,
- instalację systemów operacyjnych umożliwiających przyznawanie praw do poszczególnych folderów czy też plików; identyfikacji; autoryzacji itp.,
- zastosowanie firewall`a,

4. Bezpieczeństwo informacji w sieci korporacyjnej

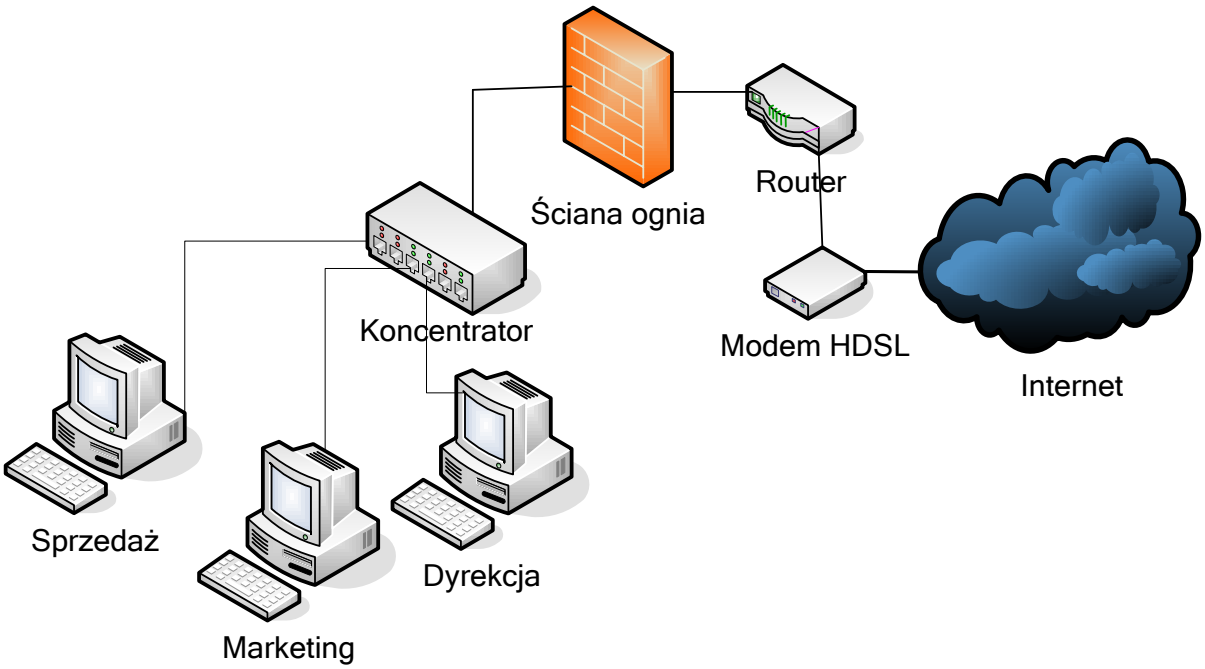
Wykorzystanie Internetu w dzisiejszym przedsiębiorstwie stanowi już powszechność, bez którego trudno sobie wyobrazić prowadzenie działalności gospodarczej. Stosowany jest w takich usługach jak: poczta elektroniczna czy strony www. Z jej strony narażeni jesteśmy również na wszelkie nielegalne próby ingerencji w nasz system sieciowy. Do czynników, zachęcających włamywaczy do ataków należy zaliczyć:

- szpiegostwo, mające na celu zdobycie informacji strategicznych, a zarazem przewagi na rynku,
- odwet, to atak na sieć informacyjną firmy poprzez umieszczenie wirusa komputerowego lub stworzenie sobie „tylniego wejścia" do systemu i późniejszą ingerencję,
- zysk finansowy - są to ataki, których celem jest kradzież środków pieniężnych (banki elektroniczne) lub cennej informacji.

Problemy, jakie stwarza korzystanie z Internetu można powiązać z:

- poufnością (wiele danych przesyłanych przez organizacje należy odpowiednio zabezpieczyć),
- integralnością (uzyskanie całej i niezmienionej przesyłki stanowi podstawowy warunek bezpieczeństwa i możliwości korzystania z tego kanału komunikacyjnego).

Przed atakami poprzez sieć można się zabezpieczyć w prosty sposób stosując firewall. Jest to zespół środków technicznych, sprzętowych i programowych, których zadaniem jest kontrola przepływających informacji pomiędzy dwoma sieciami komputerowymi. Jego naczelnym zadaniem jest ochrona sieci wewnętrznej przedsiębiorstwa przed nieautoryzowaną ingerencją z zewnątrz (rys. 2). Wynika stąd konieczność, aby każda organizacja podłączona do sieci Internet czy też innych sieci rozległych, bezwzględnie stosowała tą technologię. Włączenie do sieci globalnej umożliwia każdej stacji dostęp do usług internetowych, dając jednocześnie szanse ataku ewentualnym włamywaczom do naszych danych. Ograniczenie takiego dostępu realizowane jest najczęściej z wykorzystaniem firewall`a. Poza powyższymi funkcjami firewall może także realizować inne dodatkowe zadania.



Rys. 2. Zastosowanie zapory ogniowej w połączeniu sieci Intranet z siecią rozległą. Opracowanie własne

Wykorzystywane są trzy główne metody pracy zapory sieciowej:

1. Filtrowanie pakietów. Polega na filtrowaniu informacji na poziomie warstwy trzeciej i czwartej modelu referencyjnego OSI. Ma to na celu przepuszczenie i zatrzymanie określonych danych według wskazanych wcześniej wytycznych.
2. Screened-Subnet. Jest zrealizowane poprzez umieszczenie pomiędzy siecią chronią a zewnętrzną komputera-bastionu (będącego pewnego rodzaju „ekranem"), z zainstalowanym oprogramowaniem typu Application-Gateway wraz z jednym lub kilkoma filtrami pakietów. System ochronny musi być tak skonfigurowany, aby cały ruch pomiędzy sieciami odbywał się przez tą maszynę.
3. Dual-home-gateway. To zapora sieciowa zbudowana także z komputera-bastionu, wyposażonego w dwa interfejsy sieciowe oraz oprogramowanie typu Application-Gateway. W tej metodzie możliwe jest filtrowanie przepływającej informacji nie tylko na poziomie nagłówka pakietu, ale także na poziomie zawartości jego pola danych.

Każda informacja od nadawcy do odbiorcy jest przesyłana za pośrednictwem kanału komunikacyjnego. Cechy ich związane są z zastosowaną w nich technologią, sposobami przepływu informacji. Kanały komunikacyjne można w głównej mierze podzielić na analogowe (standardowe) i cyfrowe (komputerowe). Ochrona przed podsłuchem czy też przechwyceniem transmitowanej informacji stanowi ważny czynnik polityki bezpieczeństwa. Włamania są realizowane przeważnie w najsłabszych punktach systemu komputerowego. Aby zapobiec podsłuchowi należy przesyłaną informację szyfrować z wykorzystaniem nowoczesnych algorytmów. Próba włamania może odbywać się z zastosowanie podsłuchu:

- biernego (bez interwencji w przesyłany sygnał; nie podlega żadnym przemianom),
- pasywnego (atak polega na celowym modyfikowaniu przekazywanego sygnału;, np. na usunięciu pewnej ilości informacji, jej duplikowaniu lub uszkodzeniu).

Szyfrowanie przesyłanych informacji to jedna z metod zabezpieczania. Jest ona uważana za jedną z najbardziej skutecznych. Proces szyfrowania polega na przekształceniu informacji w sposób nieczytelny za pomocą funkcji matematycznej, zapewniający tajność dla osób trzecich. Zaleca się używanie szyfrów pomimo wykorzystywania innych technologii związanych z bezpieczeństwem i ochroną informacji. Obecnie wykorzystuje się szyfrowanie z kluczem publicznym i z kluczem prywatnym (rys. 3).

Rys. 3. Metody szyfrowania wykorzystywane w transmisji danych. Opracowanie własne

W metodzie symetrycznej są wykorzystywane następujące algorytmy:

- DES (Data Encryption Standard) – zastosowany został 56 bitowy klucz oraz bity parzystości,
- IDEA (International Data Encryption Algorithm) – algorytm podobny do poprzedniego, ale wykorzystujący klucz 128 bitowy.

W metodzie asymetrycznej są stosowane algorytmy:

- RSA - oparty jest na złożoności problemu rozkładu dużych liczb maturalnych na czynniki pierwsze. Jest to algorytm najbardziej popularny oraz jeden z najbardziej odpornych na wszelkie ataki,
- Elgamal – oparty na obliczeniach algorytmów dyskretnych. Każde szyfrowanie wykorzystuje wygenerowaną losowo wartość liczbową.

Kolejnym środkiem technicznym zwiększającym bezpieczeństwo przesyłanych informacji są wirtualne sieci prywatne VPN (ang. Virtual Private Network). Technologicznie są wydzieloną cząstką ze struktury sieci publicznej. Jest budowana głównie w oparciu o sieć Internet, wykorzystując protokół komunikacyjny TCP/IP.
Istnieją dwa podstawowe tryby pracy sieci VPN:

- tryb tunelowy,
- tryb transportowy.

Tryb szyfrowania tunelowego polega na całkowitym szyfrowaniu pakietu włącznie z jego polami adresu źródłowego i docelowego. Informacja docierająca do punktu docelowego – adresu IP, który jest jednocześnie adresem zapory sieciowej zostaje deszyfrowana, po czym zostaje wysłana do adresata. Przy zastosowaniu trybu transportowego pakiet zostaje zaszyfrowany, ale bez nagłówka, przez co trasa przesyłania nie ulega zmianie. W sieciach VPN do przesyłania danych pomiędzy nadawcą a odbiorcą są wykorzystywane protokoły transmisji:

- L2TP (Layer Two Tunneling Protocol),
- PPTP (Point to Point Tunneling Protocol).

Sieci VPN są usługą skierowaną do przedsiębiorstw posiadających swoje oddziały rozproszone geograficznie.

Podsumowanie

Trudno jest sobie wyobrazić dzisiejsze przedsiębiorstwo funkcjonujące w cięgle zmieniającym się otoczeniu bez wykorzystywania nowoczesnych technologii. To one są środkiem do celu w rozwoju firmy czyli wzrostu konkurencyjności na rynku. Mimo tych szybkich przemian równie szybko powstają nowe zagrożenia związane z bezpieczeństwem informacji, szczególnie w obszarze informatyki. Każda dzisiejsza firma, opiera się na przepływie przetworzonych informacji. Zdobycie ich przez osoby niepowołane stanowi duże zagrożenie dla jej działalności. Skuteczna ochrona jest jednym z elementów właściwie funkcjonującego i działającego przedsiębiorstwa. Wdrożony system ochrony powinien zabezpieczyć przed ich modyfikacją lub utratą w procesie pozyskiwania, gromadzenia (także danych zarchiwizowanych), przetwarzania bądź przesyłania. Dotyczy to zarówno formy tradycyjnej, jak i cyfrowej (komputerowej). Każde z przedsiębiorstw powinno inwestować w miarę ich rozwoju, potrzeb i możliwości finansowych w nowoczesne systemy zabezpieczeń.

Literatura

1. Borowiecki R., Czekaj J.: Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki. Difin, Warszawa 2010.
2. Kiełtyka L.: Komunikacja w zarządzaniu. Techniki, narzędzia i formy przekazu informacji. Agencja Placet, Warszawa, 2002.
3. Kolbusz E.: Informacja jako przedmiot zarządzania. Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 276. US, Szczecin, 1999.

4. Mikołajczyk Z.: Techniki organizatorskie w rozwiązywaniu problemów zarządzania. PWN, Warszawa, 1995.
5. Radziszewski T., Jabłoński M.: Bezpieczeństwo fizyczne i teleinformatyczne informacji niejawnych. Presscom, Warszawa 2012.
6. Roman K.: Zarządzanie informacją. Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2012.