Estera Pietras

Modelowanie zagrożeń w bezpieczeństwie informacji

JEL: R41 DOI: 10.24136/atest.2018.383
Data zgłoszenia: 19.11.2018 Data akceptacji: 15.12.2018

Obecnie zapewnienie bezpieczeństwa informacji jest jednym z najważniejszych aspektów prowadzenia działalności. Dzięki nowym technologiom jest to dużo bardziej możliwe i dostępne, niż jeszcze kilka lat temu. Należy jednak pamiętać, że nowe technologie, które są do dyspozycji w przedsiębiorstwie posiadają także osoby, którym zależy na kradzieży danych. Dlatego tak ważne jest uświadamianie personelu przedsiębiorstwa o wartości i cenie informacji a jednocześnie o sposobach jej ochrony. W artykule przedstawiono istotę bezpieczeństwa informacji i jego znaczenie dla przedsiębiorstwa. Ponadto wskazano przykładowe metody wyłudzenia i wycieku danych.

Słowa kluczowe: zagrożenia bezpieczeństwa informacji.

Wstęp

Jedną z głównych potrzeb człowieka, tą pierwotną i zasadniczą jest poczucie bezpieczeństwa. Odgrywa ono szczególną rolę w życiu każde jednostki. Pozwala żyć w spokoju, dobrobycie i umożliwia osiąganie założonych celów życiowych przez człowieka. Nie byłoby to możliwe bez określonych informacji, dzięki którym można uzyskać znaczącą wiedzę o wpływie bezpieczeństwa na życie ludzkie.

Wielu uczonych twierdzi, że informacja jest podstawą funkcjonowania społeczności, a w szczególności tej w zakładach pracy, w których organizuje się jej ochronę wszelkimi możliwymi środkami, zabezpieczając organizację przed wyciekiem ważnych strategicznych informacji. Analizując obszar działalności przedsiębiorstwa jest ona majątkiem i kluczem do pełnego sukcesu na rynku.

Celem bezpieczeństwa informacji jest niedopuszczenie do ujawniania tajemnic posiadanych przez organizację. Ich utrata może spowodować straty finansowe dla przedsiębiorstwa, a co za tym idzie utratę konkurencyjności. W praktyce gospodarczej można zaobserwować, iż informacja pełni wymowną rolę w przeliczeniu na wartość za którą można nabyć aktywa. Wobec tego jednym z podstawowych zagrożeń może być szpiegostwo gospodarcze, którego celem jest m.in. zdobycie informacji od konkurencji, a następnie wyeliminowanie tego podmiotu z rynku. Codziennością stały się również incydenty związane z podejrzeniem informacji, nieuprawnionym kopiowaniem danych, świadomym umyślnym przekształceniem danych, fałszerstwami, oszustwami komputerowymi, sabotażem komputerowym, czy podsłuch. Wszystkie te zagrożenia są wszechobecne i mogą doprowadzić do utraty bezpieczeństwa informacji. Ponadto w wielu organizacjach możemy zaobserwować incydenty, które w skutek braku świadomości pracowników doprowadzają do ujawnienia kluczowych informacji. Sytuacje takie niosą katastrofalne skutki dla przedsiębiorców.

Z pomocą dla organizacji świadomych znaczącej roli bezpieczeństwa i ochrony informacji w procesach realizacji misji i celów, odpowiedniej obsługi klienta, przychodzi międzynawowy standard EN ISO/IEC 27001:2017 stanowiący zbiór zaleceń, wymagań oraz dobrych praktyk, których zaimplementowanie do systemu bezpieczeństwa informacji gwarantuje jego niezawodność dla klientów, dostawców i osób trzecich. Nietrudno dostrzec, że dużą zaletą tej normy jest kompleksowe podejście do bezpieczeństwa informacji. Należy jednak podkreślić, że wyniki analizy certyfikacji ISO/IEC 27001:2017 w sektorze przemysłu wskazują, że jest jeszcze wiele do zrobienia w tym obszarze. Przedsiębiorstwa coraz częściej decydują się na wdrażanie certyfikowanych systemów zarządzania bezpieczeństwa informacji [20].

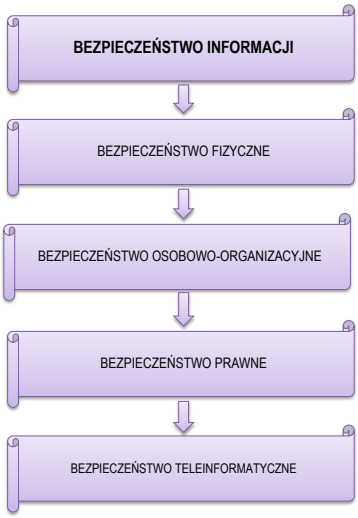
Artykuł omawia wybrane zagrożenia bezpieczeństwa informacji.Za pomocą modeli zagrożeń w sposób graficzny zaprezentowano pewien scenariusz wydarzeń, który przypuszczalnie może się zdarzyć w każdej jednostce organizacyjnej.

1.Bezpieczeństwo informacji

W ocenie Jana Luberadzkiego przedsiębiorstwo, które kieruje się zasadami otwartości informacyjnej, ignorując zasady bezpieczeństwa może narazić się na poważne straty. Dotyczy to ochrony własnych zasobów, jak i pozyskiwania informacji, niezbędnej do prawidłowego zarządzania. W ocenie autora, pozyskiwanie informacji jak i ich ochrona, to dwie strony tego samego medalu, którym nazywamy bezpieczeństwo informacji [1].

Jak słusznie wskazuje inna pozycja literaturowa, bezpieczeństwo informacji można zdefiniować jako „poziom ochrony informacji i narzędzi służących do jej opracowania, przechowywania i transmisji przed losowymi zniekształceniami, które mogą przynieść szkodę właścicielom lub użytkownikom informacji" [2]. Zgodnie z prezentowanymi w piśmiennictwie treściami informację uznaje się za bezpieczną, wówczas gdy zagwarantowane są wszystkie atrybuty jej bezpieczeństwa: poufność, spójność, dostępność, rozliczalność, autentyczność, niezaprzeczalność i niezawodność [3,5]. Wobec powyższego bezpieczeństwo informacji należy rozmieć wielowymiarowo, uwzględniając nie tylko wielkość atrybutów informacji, podlegających ochronie, ale także różnorodność form ich występowania np. w postaci pliku danych, wydruku, zapisu w formie elektronicznej i tradycyjnej, rekordu w bazie danych czy wiadomości przekazywanej ustnie.

Na całokształt bezpieczeństwa informacji składają składowe: bezpieczeństwa fizycznego, osobowo-organizacyjnego, prawnego oraz teleinformatycznego. Przedstawia to w następujący sposób rysunek 1.



Rys.1 Składowe bezpieczeństwa informacji [4].

Rys. 1 obrazuje podstawowe komponenty wchodzące w skład bezpieczeństwa informacji. Bezpieczeństwo to obejmuje część systemu informatycznego, bezpieczeństwo danych, sieciowe, komputerowe czy telekomunikacyjne. Wszystkie obszary związane z technologią podlegają pod bezpieczeństwo informacyjne.

Ochrona systemów informatycznych to tylko jeden z czterech obszarów, o które powinno zadbać przedsiębiorstwo zainteresowane pomyślnością ekonomiczną na rynku.

Wykrywanie niebezpieczeństw jest bardzo ważnym aspektem, gdyż daje szanse na przeciwdziałanie niepożądanym konsekwencjom. Podstawą do wykrywania zagrożeń wpływających na zachowanie odpowiedniego poziomu bezpieczeństwa jest identyfikowanie zmian zachodzących w systemie.

Ze względu na obszary powstawania zagrożeń, można wyróżnić [8]:

1. Zagrożenia losowe – do tego obszaru można zaliczyć wypadki, klęski żywiołowe wpływające na stan organizacji i bezpieczeństwo jej przepływu informacji np.; pożar budynku w którym znajdują się nośniki danych.
2. Tradycyjne zagrożenie informacyjne, – do których zaliczyć można działalność sabotażową bądź dywersyjną, a także szpiegostwo gospodarcze ukierunkowane na zdobycie informacji.
3. Zagrożenia technologiczne – związane są z gromadzeniem, przetwarzaniem, przekazywaniem i przechowywaniem informacji w sieciach i systemach teleinformatycznych np.: przestępstwa komputerowe.

Kolejnym kryterium podziału zagrożeń informacyjnych jest źródło ich występowania. Wówczas można wyróżnić [5]:

1. Zagrożenia wewnętrzne, te powstają wewnątrz organizacji, a w których skład wchodzą:

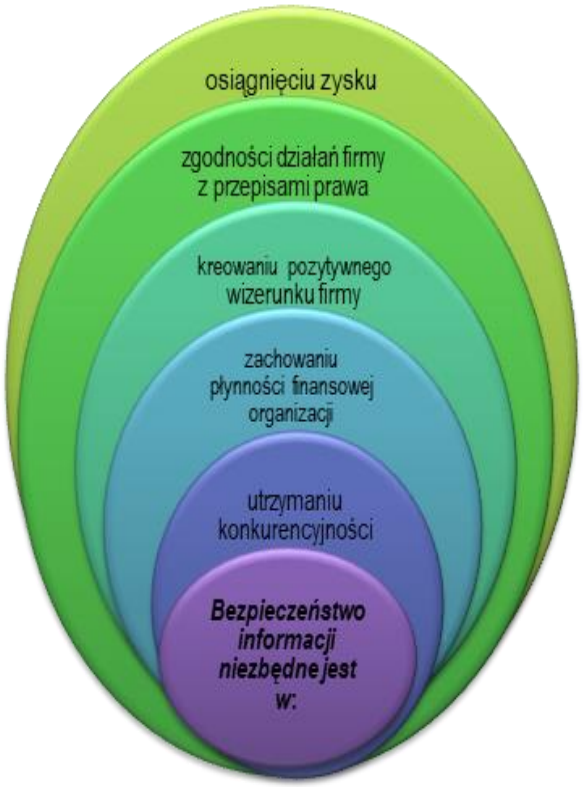
a) uszkodzenie bądź utrata danych lub całkowity brak możliwości obsługi z przyczyn błędu lub przypadku;
b) uszkodzenie bądź utrata danych spowodowane celowym działaniem niepożądanych osób, bądź celowym działaniem nieuczciwych pracowników.

2. Zagrożenia zewnętrzne, generowane poza instytucją, do których należy zaliczyć uszkodzenie lub utratę danych, ingerencję osób trzecich. Mogą one powodować brak możliwości obsługi systemu bądź sieci teleinformatycznej.
3. Zagrożenia fizyczne, w których pozbawienie możliwości obsługi, uszkodzenie lub utrata danych nastąpiło z powodu katastrofy, awarii bądź wystąpienia innego niepożądanego zdarzenia wpływającego na bezpieczeństwo informacyjne danej organizacji.

Dokładne i rzetelne zdefiniowanie zagrożeń jest podstawą do zapewnienia odpowiedniego stanu bezpieczeństwa informacji w przedsiębiorstwie. Te zagrożenia, które są za późno wykryte lub w ogóle są ignorowane mogą w znacznym stopniu przyczynić się do realnego zagrożenia bezpieczeństwa informacji.

Niezależnie od postaci informacji oraz form ich zabezpieczenia duża część informacji znajduje się w umysłach pracowników. W związku z ogromnymi możliwościami ludzkiej pamięci zaleca się dzielenie informacji i nie ujawnianie wszystkich danych jednej osobie. W przedsiębiorstwach, w których informacja ma ogromne znaczenie zaleca się podział informacji. Służą do tego narzędzia takie jak: klucze kryptograficzne, hasła. W celu uzyskania dostępu konieczne jest podanie dwóch połówek klucza lub hasła przez dwie osoby. Takie rozwiązania bezpieczne są dla osób, które z racji zajmowanych stanowisk znają hasła i klucze dostępu. W takiej sytuacji ryzyko próby wyłudzenia jest znacznie niższe.

Obszary które wspomagają zachowanie atrybutów bezpieczeństwa informacji wpływają na całe przedsiębiorstwo. Wpływ zachowania odpowiedniego poziomu bezpieczeństwa przedstawiono na rysunku



Rys.2 Dominujące korzyści wynikające z bezpieczeństwa informacji [4].

2.Ataki na systemy komputerowe

Rozwój sieci komputerowych, rozproszone przetwarzanie danych, korzystanie z usług sieci publicznych takich jak Internet wywołują powstawanie licznych zagrożeń. W tego rodzaju systemach np.; komunikacyjno-informacyjnych pojawiają się problemy z zachowaniem odpowiedniego poziomu bezpieczeństwa, wynikające z technologii czy też z faktu przekraczającego granice samego przedsiębiorstwa [6].

Według raportu PwC „Ochrona biznesu w cyfrowej transformacji", przygotowanego na podstawie 4 edycji dorocznego badania „Stan bezpieczeństwa informacji w Polsce" *aż w 96% średnich i dużych przedsiębiorstw istniejących aktywnie w Polsce w ostatnich 12 miesiącach doszło do ponad 50 cyberataków. Najczęściej wykorzystywaną metodą był atak phishingowy. Jednocześnie, aż 41%*

firm przemysłowych, obawia się, że w wyniku ataku hakerskiego może dojść do uszkodzenia infrastruktury „[7].

W przypadku ataków na systemy komputerowe można wyróżnić:
- przypadkowe
- celowe

Jest to najłatwiejsza droga do pozyskania informacji, całkowicie opracowana przez internet.

Do najczęściej stosowanych ataków komputerowych należą:
- wirusy-które mogą nawet doprowadzić do unieruchomienia tysięcy komputerów,
- wirusy są one uśpione w komputerze i działają jak hakerzy, których atak nie musi być kontrolowany. Podczas korzystania z poczty elektronicznej lub popularnych stron infekuje on system poprzez instalowanie się na innych komputerach,
- bomba logiczna- często może pozostawać nieaktywna jednak obecność niektórych plików może ją uaktywnić.

1.1. Oszustwa komputerowe

Informatyzacja systemów bankowych, elektroniczny przepływ pieniądza, skomputeryzowane systemy księgowe istnieją już w każdym przedsiębiorstwie. Dziś zintegrowane systemy łączą ze sobą dział księgowo-finansowy z magazynem, produkcją czy kadrami.

W zakresie zagrożeń bezpieczeństwa informacji stwarzają niebezpieczeństwo trzy rodzaje manipulacji:
- danymi- polega ona na wprowadzeniu nieprawidłowych informacji do bazy danych, dzięki takim działaniom można zmodyfikować stany magazynowe, nieprawnie udzielić koncesji, czy fałszować bilans roczny.
- wynikiem- polega na działaniu w publicznie dostępnych urządzeniach elektronicznych, wykorzystując np.: terminale .
- programami- polega na przekształceniu komend lub pisaniu nowych, które powodują, że program sam wykonuje operacje, na które użytkownik nie ma wypływu. Ten rodzaj manipulacji jest trudny do wykrycia [3, 12].

Pierwszym państwem które masowo zostało dotknięte manipulacjami była Japonia, gdyż przodowała w sferze automatyzacji operacji bankowych, później Stany Zjednoczone i kraje europejskie. Pojedynczo takie nadużycia nie powodują strat finansowych, aczkolwiek statystycznie są to najczęściej dokonywane działania [8,13, 19].

1.2. Włamania do systemu komputerowego

Na podstawie dostępnych informacji rozróżniamy dwie kategorie włamań:
- celowe,
- przypadkowe.

Znaczną grupę stanowią włamania celowe. Sprawcami tych działań mogą być osoby, które działają w ramach wywiadu gospodarczego, przestępczości zorganizowanej czy organizacji konkurencyjnych, lub pracownicy poszkodowanej firmy. Osoby te mogą działać w ramach zemsty na pracodawcy To tylko nieliczne powody dla których następuje nieuprawnione wejście do systemów. Za sprawców tych działań uznaje się hakerów, którzy mogą działać na zlecenie firmy konkurencyjnej bądź wywiadu gospodarczego. Pojęcie „haker" tłumaczy się jako" poskramiacz komputerów", „rozprawacz komputerów". Definicja niestety nie może być jednoznaczna. Na przełomie lat siedemdziesiątych i osiemdziesiątych kogoś takiego nazwalibyśmy fascynatem komputerowym, rozpracowujący technologiczne przeszkody, udoskonalający komputer. W latach osiemdziesiątych –dziewięćdziesiątych nastąpiło przewartościowanie pojęcia na włamywacz pokonujący zabezpieczenia. Natomiast obecnie hakerem można nazwać kogoś kto jest obsesyjnie zaangażowany w wyszukiwanie i wykorzystywanie luk w oprogramowaniu komputerowym [9]. Hakerów można podzielić na pięć kategorii:
- nowicjuszy-działają nieprzewidywalnie, ważne jest dla nich wejście do bazy danych,
- analityków-osoby które, chcą zapoznać się z różnego rodzajami komputerami, bez wyrządzania szczególnych szkód,
- turystów-system komputerowy jest dla nich dość skomplikowany, jak łamigłówka,
- złodziei-najczęściej wynajmowane osoby przez podmioty konkurencyjne, które chcą zdobyć informacje o produkcie, czy procesie produkcji,
- wandali.

W przeszłości takiemu włamaniu hackerskiemu nie przypisywano żadnego szpiegostwa a jedynie osiągnięcie satysfakcji z pokonania zapory w postaci zabezpieczeń technicznych. Jednak z czasem zostało to zweryfikowane do gry ambicji aż po terroryzm. Hakerzy działają w sieciach zamkniętych, ale i też otwarcie w internecie. Jedni działają żywiołowo, przeskakując z systemu do systemu inni kreują całą metodykę postepowania, dokumenty kartoteki [8,13].

Do dodatkowego zagrożenia należałoby zaliczyć używanie nielicencjonowanego oprogramowania. Zdecydowanie ułatwia to działanie hakerów.

3.Modelowanie zagrożeń informacyjnych

Aby z góry przewidzieć prawdopodobieństwa wystąpienia różnych zagrożeń związanych z bezpieczeństwem informacji kluczowym wydaje się zastosowanie metod opartych na strukturach drzewiastych. Literatura przedmiotu szeroko omawia metody drzewa błędów, metodę drzewa zdarzeń, czy też analizę przyczynowo skutkową. Przegląd wybranych metod zawiera tabela nr.1

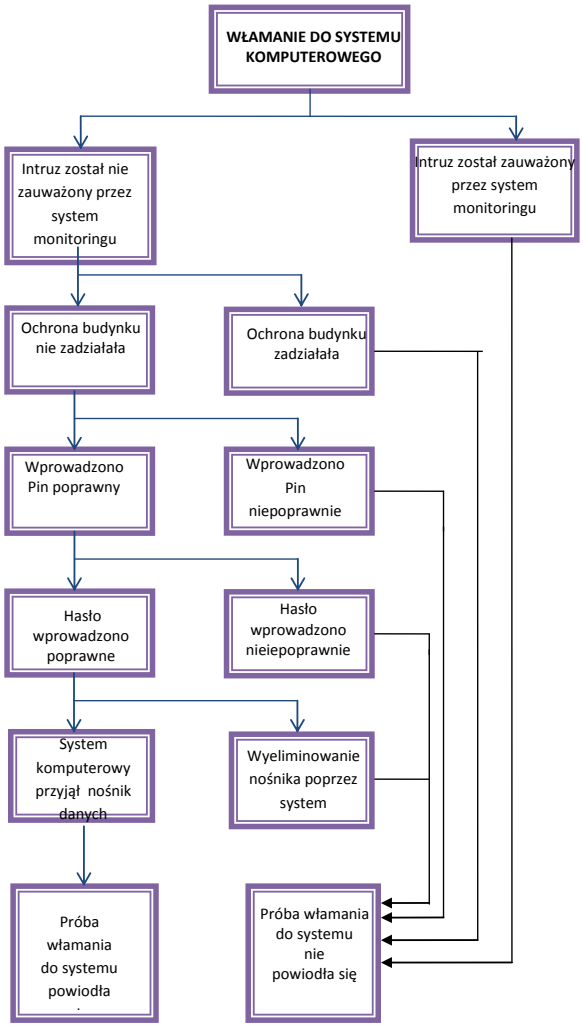
Tab. 1. Metody wykorzystujące struktury drzewiaste [10].

NAZWA METODY	METODY JAKOŚCIOWE OCENY RYZYKA
Metodę drzewa błędów (Fault Tree Analysis)	Metodę drzewa błędów opracowano w latach sześćdziesiątych podczas prac nad międzykontynentalnymi pociskami balistycznymi. W metodzie FTA (Fault Tree Analysis) na podstawie skutków zdarzeń szuka się dedukcyjnie przyczynę danego zdarzenia, natomiast drzewo błędów to diagram logiczny dzięki któremu widzimy zależności błędnego stanu w systemie począwszy od błędnych stanów komponentów, z których system jest zbudowany.
Metoda drzewa zdarzeń (Event Tree Analysis)	Metoda drzewa zdarzeń (Event Tree Analysis) ma charakter indukcyjny,co oznacza że na podstawie danego zdarzenia cząstkowego wnioskuje się o większości jego skutkach. Analizę wykonuje się od zdarzenia inicjującego. Takimi zdarzeniami inicjującymi mogą być na przykład: pojawienie się osoby obcej w pomieszczeniach serwera, czy też kradzież komputera przenośnego użytkowanego przez właściciela firmy.
Metoda analizy przyczynowo- skutkowa (CCA Cause Conseguence Analysis)	Metoda analizy przyczynowo- skutkowej (CCA Cause Conseguence Analysis) została opracowana w Danii, podczas prac dotyczących bezpieczeństwa elektrowni jądrowych. Metoda ta łączy w sobie idee obu wcześniejszych metod. Celem metody jest zidentyfikowanie łańcuchów zdarzeń ukierunkowanych do niepożądanych skutków. Prawdopodobieństwo wystąpienia uciążliwych konsekwencji jest obliczane na zasadzie prawdopodobieństw zdarzeń i przyczyn ich wywołujących.

4.Modelowanie zagrożeń bezpieczeństwa informacji

Metoda drzewa zdarzeń jest graficznym modelem zależności przyczynowo skutkowych występującym podczas zaistnienia problemu. Zakłada się że określony skutek jest wynikiem zaistniałego wcześniej zdarzenia. Zdarzenie inicjujące jest początkiem ciągów zdarzeń, które są już tylko następstwami zdarzenia inicjującego. Poniżej zaprezentowano kilka prawdopodobnych sytuacji utraty bezpieczeństwa informacji.

Model włamania do systemu komputerowego.

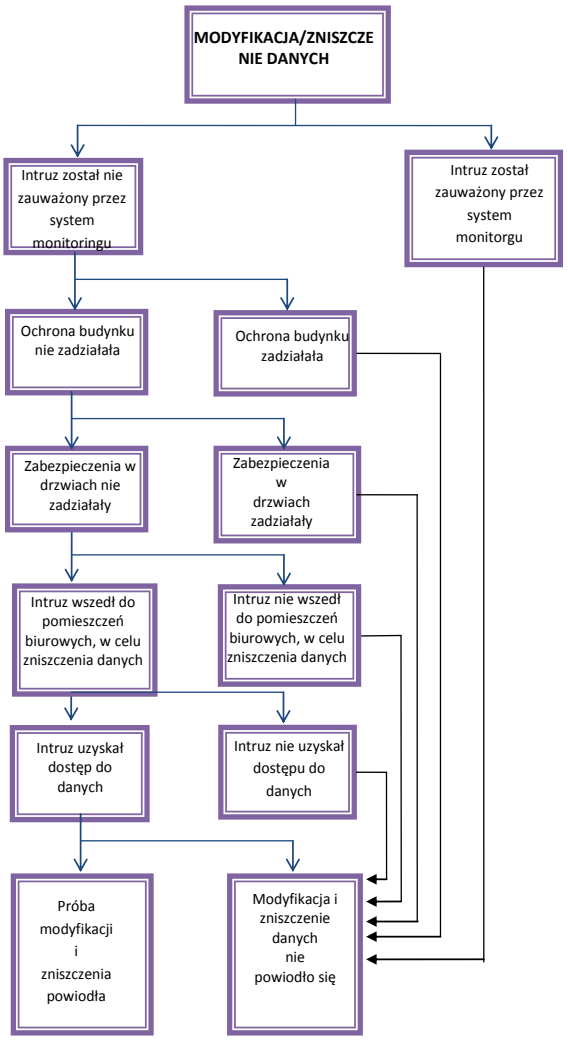


Rys.3 Model włamania do systemu komputerowego.
Źródło :opracowanie własne na podstawie [10].

Prezentowany model włamania do systemu komputerowego pokazuje jakie podatności mogą wystąpić przy tym zagrożeniu.

Jedną z nich jest uzyskanie hasła i kodu PIN przez osobę nieupoważnioną. Można wyciągnąć kolejne wnioski iż brak odpowiednich procedur weryfikujących tożsamość osób spoza kadry pracowników przyczynia się do włamania do systemu. Lekceważenie obowiązku wylegitymowania osób postronnych powinno wynikać ze świadomości wcześniej nabytej w wyniku np.: szkoleń. Ponadto na schemacie można zauważyć podatność, jaką jest brak odpowiedniej kontroli dostępu. Jednocześnie nie zadawalający jest fakt, że nie we wszystkich pomieszczeniach znajdują się czujki systemu alarmowego. Zauważono iż używa się przestarzałych i wyeksploatowanych systemów niezgodnych z obecnymi wymogami.

Model modyfikacji danych.



Rys.4 Model niszczenia danych.
Źródło :opracowanie własne na podstawie [10].

Rysunek 4. prezentuje zagrożenie i podatność która ma wpływ na nieautoryzowaną modyfikację danych. Mianowicie intruz nie został zweryfikowany. Na skutek braku świadomości pionu ochrony, intruz może swobodnie wejść na teren organizacji. Procedury identyfikacyjne, obowiązujące pracowników są nie zrozumiałe, albo nie jasno sprecyzowane. Sytuacja taka mogła nastąpić w wyniku braku ostrożności pracowników ochrony lub mogła być spowodowana chwilową nieobecnością ochroniarza. Zakłada się że, z powodu opuszczenia miejsca pracy i nieostrożności pracowników ochrony nie zostanie przeprowadzona weryfikacji osoby, i nie eskortuje się gościa na terenie organizacji. System kontroli dostęp może zawierać luki i błędy powodujące np.: kradzież karty dostępu do pomieszczeń. Nieprawidłowe zabezpieczenie systemów komputerowych to następna podatność przedstawiona na modelu. Na skutek pozostawienia sprzętu komputerowego, nie zabezpieczonego, w pomieszczeniu otwartym można dokonać modyfikacji danych. Ponadto pozostawienie dokumentacji w łatwo dostępnym miejscu lub nie przestrzeganie zasad czystego biurka również może z potęgować podatność.

W toku analizy można dojść do kolejnych wniosków że szafy do przechowywania dokumentów mogą zostać nieodpowiednio zabezpieczone. Podatnością również będzie wgranie przez nieuprawnioną osobę, wirusa który przenoszony jest z danymi na nośnikach.

Użycie tego nośnika może spowodować rozprzestrzenienie się wirusa po całym systemie.

5.Działania redukujące zagrożenia

Wysoka świadomość zagrożeń i stopień wiedzy z zakresu bezpieczeństwa są kluczowymi elementami skutecznych, przemyślanych działań. Natomiast brak świadomości znacznie redukuje skuteczność zabezpieczeń poziomu bezpieczeństwa. Personel traktowany jako zagrożenie wewnętrzne stanowi najsłabsze ogniwo w zabezpieczeniach. Dlatego też zaleca się okresowe szkolenia nie tylko personelu lecz również dostawców czy też partnerów w zakresie bezpieczeństwa informacji. Taki program uświadamiania w obszarze bezpieczeństwa należałoby wdrożyć na wszystkich poziomach przedsiębiorstwa, począwszy od dyrektorów po osoby odpowiedzialne za zwykłe codzienne czynności [11,12, 15, 16, 17].

W przedsiębiorstwach zdarza się również podglądanie informacji przesyłanych internetem. W tym celu tworzone są systemy monitorujące przesył danych przepływające przez łącza dostawcy internetu. [6].Propozycje zabezpieczeń których celem jest zminimalizowanie ryzyka wystąpienia zagrożeń zaprezentowano w tabeli 2.

Tab.2. Zabezpieczenia redukujące poziom ryzyka.

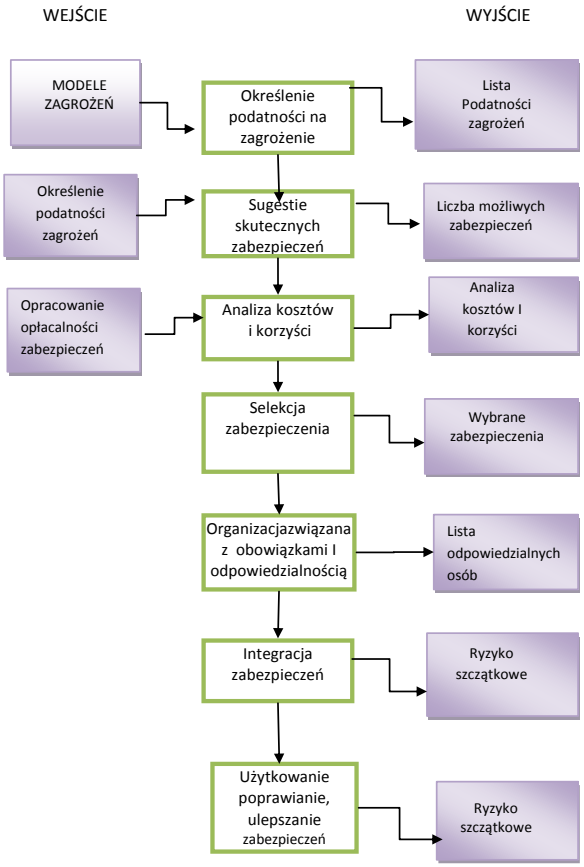
Zagrożenie	Proponowany opis zabezpieczenia
Niszczenie danych	Pomocne może się okazać wyznaczenie obszarów ochronnych w przedsiębiorstwie. Należy wprowadzić zapis w umowach zawartych z pracownikami dotyczących zwolnień dyscyplinarnych w przypadku celowego zniszczenia danych.
Modyfikacja danych	W celu ochrony przed tego typu zagrożeniem wprowadza się regularne szkolenia dla osób upoważnionych do przetwarzania informacji. Zaleca się szyfrowanie danych, i zapory ogniowe, oraz korzystanie z oprogramowania posiadającego licencję.
Włamanie do systemu komputerowego	Zaleca się szyfrowanie danych. Wyznaczenie gdzie w budynku g przechowywane są ważne informacje, lub wyznaczenie obszarów ochronionych. Należy również chronić komputery, przed programami szpiegowskimi czy hackerskimi nadając uprawnienia określonym osobom do tego upoważnionym.

Proponowane zabezpieczenia są dość uniwersalne i ogólnodostępne w związku z czym mogą zostać zastosowane w wielu przedsiębiorstwach i jednostkach organizacyjnych zdecydowanie minimalizując prawdopodobieństwo wystąpienia zagrożenia. Ponadto autor proponuje wdrożenie zabezpieczeń technicznych. Można do tej grupy zaliczyć :niszczarkę dokumentów, sejf, rolety antywłamaniowe, szlaban na parkingu, dodatkowy moduł GSM który umożliwia przekazanie sygnału wizyjnego bezpośrednio do portierni czy też system kontroli dostępu.

6.Algorytm wdrażania zabezpieczeń

Proces przykładowego algorytmu wdrażania zabezpieczeń przedstawia się następująco:

1. Na podstawie listy zidentyfikowanych zagrożeń, ustala się podatności
2. Opracowanie propozycji efektywnych zabezpieczeń
3. Ocena opłacalności rozwiązań jest podstawą do zastosowania rozwiązania.
4. Podjęcie decyzji o wyborze zabezpieczenia, które zapewni bezpieczeństwo organizacji
5. Ustalenie obowiązków i zasad odpowiedzialności personelu.
6. Wdrożenie zabezpieczenia-jako wynik badań
7. Bieżące doskonalenie wdrożonych zabezpieczeń. Akceptacja ryzyka szczątkowego.



Rys.6 Algorytm wdrożenia zabezpieczeń.
Źródło :opracowanie własne na podstawie [10].

Podsumowanie

Zagwarantowanie właściwego poziomu bezpieczeństwa informacji jest w obecnych czasach dużym problemem niemal wszystkich organizacji. Przedsiębiorstwa często skupiają się na produkcji i pomnażaniu środków finansowych zupełnie zapominając, że jedno zdarzenie związane z nieuprawnionym ujawnieniem informacji może spowodować ogromnie straty finansowe. Informacja przedstawia określoną miarodajną wartość. Dlatego wymaga się, aby była odpowiednio chroniona. Szybkość rozwoju nowych technologii dostarcza wiele możliwości, ale i jeszcze więcej zagrożeń. Można ich oczekiwać ze strony wewnętrznej jak i zewnętrznej przedsiębiorstwa jednak najsłabszym ogniwem w systemie bezpieczeństwa informacji jest i będzie człowiek.

Identyfikacja potencjalnych zagrożeń bezpieczeństwa informacji ukazuje jak ogromna jest różnorodność i wieloaspektowość tego problemu. Jedynie rzetelna przeprowadzona analiza ryzyka w pełni pozwoli na uświadomienie groźby utraty cennych informacji i danych. Niedopuszczalne jest bagatelizowanie jakichkolwiek zagrożeń, nawet tych pozornie błahych. W wielu organizacjach panuje

przekonanie, że inwestycje w system bezpieczeństwa są za nader kosztowne. Poza tym małe przedsiębiorstwa, uważają, że zagrożenie utraty informacji jest niewielkie i może wydaje im się, że system bezpieczeństwa informacji nie jest im potrzebny. W takim przypadku należałoby się jednak zastanowić na czym przedsiębiorstwa skupiają swoje działania - na produkcji czy na zabezpieczeniu informacji o posiadanych technologiach czy innowacjach?

Bibliografia:

1. Luberadzki J., *Wywiad i szpiegostwo gospodarcze w konkurencji rynkowej* w: Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały VII Kongresu Katowice.
2. Urbanowicz P.(red.), *Ochrona informacji w sieciach komputerowych*, Wydawnictwo KUL, Lublin 2004.
3. Nowak A., Scheffs W., *Zarządzanie bezpieczeństwem informacyjnym*, Wyd. AON, Warszawa 2010.
4. Łuczak J.(red), Zarządzanie bezpieczeństwem informacji. Praca zbiorowa Wydawca "Oficyna Wsółczesna" Poznań 2004
5. Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej,* Oficyna Wydawnicza Abrys, Kraków 2000.
6. Borowiecki R. Romanowska M. System informacji strategicznej. Wywiad gospodarczy
7. www.pwc.pl dostęp 26.10.2018
8. Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2009.
9. *Encyklopedia Popularna* ,PWN, Warszawa 1982.
10. Białas A. Bezpieczeństwo informacji i usług w nowoczesnej firmie. Wydanie Naukowo-Techniczne, Warszawa 2007.
11. Pod red.Małachowski A., Internet w zarzadzaniu przedsiębiorstwem.Wydawnictwo Akademii Ekonomicznej im.Oskara Langego we Wrocławiu, Wrocław 2003
12. Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego,* Wyd. Adam Marszałek, Toruń 2006.
13. Wrzosek M., Nowak A., *Identyfikacja zagrożeń determinujących zmiany w systemie bezpieczeństwa społeczeństwa informacyjnego*, Wydawnictwo AON, Warszawa 2009.
14. Hamrol A. Zarzadzanie jakością z przykładami. Wydawnictwo naukowe PWN warszawa, 2005.
15. Muliński T.: Zagrożenia bezpieczeństwa Dla Systemów Informatycznych E-Administracji, Wydanie I. Wydawnictwo CeDeWu, Warszawa 2015.
16. Kura A.: Zagrażenia Dla Bezpieczeństwa Informacyjnego Państwa u progu XXI wieku. Wydawnictwo Sztafeta, Stalowa Wola 2016.
17. Liedel K., Piasecka P., Aleksandrowicz T.R.: Sieciocentryczne Bezpieczeństwo Wojna, Pokój i Terroryzm w Epoce Informacji. Wydawnictwo Difin, Warszawa 2014.
18. Red.Naukowa Staniec,I., Zawiła-Niedzwiec ki J.:Ryzyko operacyjne w naukach o zarządzaniu. Wydawnictwo C.H.Beck, Warszawa 2015.
19. Liderman K.: Bezpieczeństwo Informacyjne Nowe Wyzwania Wydawnictwo Naukowe PWN SA, Warszawa 2017.
20. EN ISO/IEC 27001:2017 Technika informatyczna -Technika bezpieczeństwa-Systemy zarządzania bezpieczeństwem informacji-Wymagania.

Modeling threats in safety information

In the information society, ensuring information security in an enterprise is one of the most important aspects of running a business. Thanks to new technologies, it is much more possible and available than a few years ago. However, it should be remembered that new technologies that are available in the enterprise also have people who care about the theft of data. That is why it is so important to make the company's staff aware of the value of information and at the same time how to protect it.

Keywords: information security threats.

Autorzy:

Estera Pietras mgr inż. Politechnika Częstochowska Zakład Bezpieczeństwa i Ergonomii