Bezpieczeństwo
Sieci Komputerowych

Część 1.

Zapoznanie z planem i programem zajęć.
Aspekty prawne oraz podstawowe zagadnienia teoretyczne z zakresu bezpieczeństwa sieci i systemów teleinformatycznych.

Praktyczny Pedagog

Bezpieczeństwo Sieci Komputerowych

PLAN ZAJĘĆ

3 spotkania w dniach **18.09, 16.10, 30.10** tj.
20h lekcyjnych = 10 bloków 1,5h (2+4+4).

W trakcie zajęć oraz/lub po każdym bloku

- wykłady teoretyczne na podstawie prezentacji
- dyskusje (debata, burza mózgów)
- wymiana wiadomości, doświadczeń z zakresu omawianego materiału.
- materiały filmowe, pokazy praktyczne oraz ćwiczenia laboratoryjne obejmujące wybrane zagadnienia.

Na ostatnim spotkaniu quiz moodle –
test samosprawdzający (zaliczenie przedmiotu z oceną).

Praktyczny Pedagog

Bezpieczeństwo Sieci Komputerowych

PROGRAM ZAJĘĆ cz. 1

Zapoznanie z planem i programem zajęć.
Terminologia: system teleinformatyczny, sieć teleinformatyczna, zabezpieczenie danych
w systemie informatycznym.
Czym jest bezpieczeństwo w sieciach i systemach teleinformatycznych i dlaczego jest takie ważne?
Główne filary bezpieczeństwa: poufność, integralność, dostępność oraz bezpieczeństwo fizyczne oraz bezpieczeństwo logiczne.
Zasada równowagi przy projektowaniu systemu teleinformatycznego.
Zarządzanie ryzykiem.
Klasyfikacja przechowywanych informacji.

Praktyczny Pedagog

Bezpieczeństwo Sieci Komputerowych

PROGRAM ZAJĘĆ cz. 1 c.d.

Obowiązki administratora systemu informatycznego, administratora sieci.
Ochrona danych osobowych – jakie dane podlegają ochronie, obowiązki spoczywające na instytucjach przetwarzających dane osobowe, obowiązki administratora danych osobowych.
Standardy.
Organizacje.
Certyfikaty.
Statystyki.
Internetowe źródła informacji.

System teleinformatyczny*

Zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego.

*Termin prawniczy, którego definicja zawarta jest w ustawie z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną.

Sieć teleinformatyczna*

Organizacyjne i techniczne połączenie systemów teleinformatycznych.

art.2 pkt.9. ustawy z dn. 22.01.1999 o ochronie informacji niejawnych

Zabezpieczenie danych w systemie informatycznym*

Rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

*art.7 pkt.2b. Ustawy z 29.08.1997 r. o ochronie danych osobowych.

Czym jest bezpieczeństwo w sieciach/systemach komputerowych?

Bezpieczeństwo systemów komputerowych to ogół działań mających na celu zabezpieczać dane przechowywane w komputerze, tak by nie mogły zostać wykorzystane przez niepowołane osoby czy też narażone na trwałą utratę.

Większość użytkowników bezgranicznie ufa swoim systemom, powątpiewając, że ich dane osobiste mogą kiedykolwiek zostać wykradzione i dostać się w niepowołane ręce, **gdyż nie są świadomi zagrożeń** czyhających nad ich komputerami.

Główne filary bezpieczeństwa systemu informatycznego

- **poufność** (ang. confidentiality)
- **integralność** (ang. integrity)
- **dostępność** (ang. availability)

Poufność to zapewnienie, że informacja jest dostępna jedynie osobom upoważnionym.

Integralność to ochrona przed nieautoryzowaną modyfikacją informacji.

Dostępność to zapewnienie, że osoby upoważnione mają możliwość wykorzystania informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne.

Główne filary bezpieczeństwa systemu informatycznego

Rozważając różne aspekty bezpieczeństwa systemu informatycznego można wyróżnić:

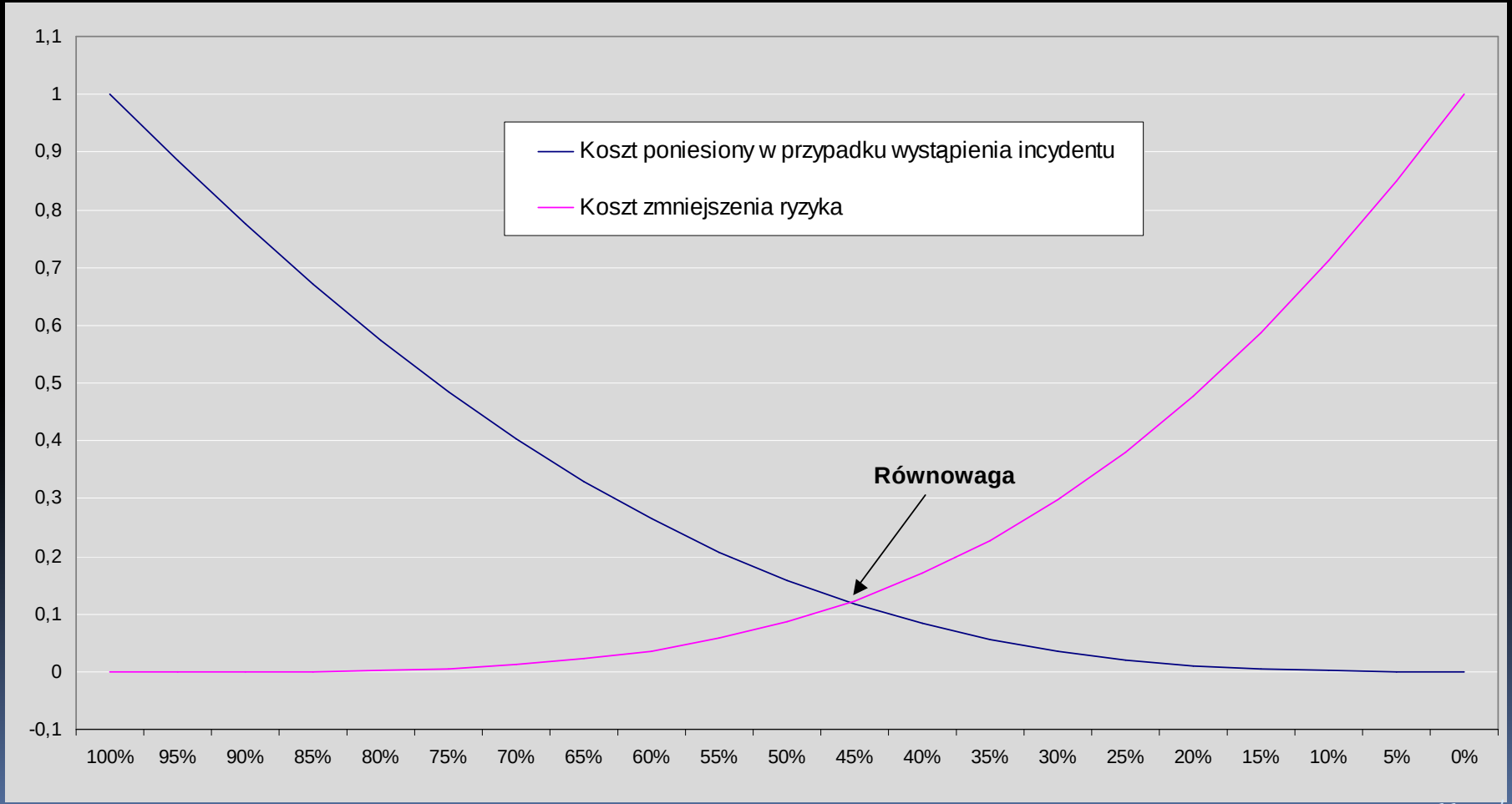
· **bezpieczeństwo fizyczne (ang. physical security)**

Określa sposób, w jaki obiekty systemu informacyjnego oraz jego użytkownicy są chronieni przed zagrożeniem fizycznym (np. przed kradzieżą dysków twardych) i bezpośrednią obserwacją (np. podsłuchem). W zakres bezpieczeństwa fizycznego wchodzą także procedury sprawdzające tożsamość personelu korzystającego z systemu.

· **bezpieczeństwo logiczne (ang. logical security) oraz bezpieczeństwo komunikacyjne (ang. communication security)**

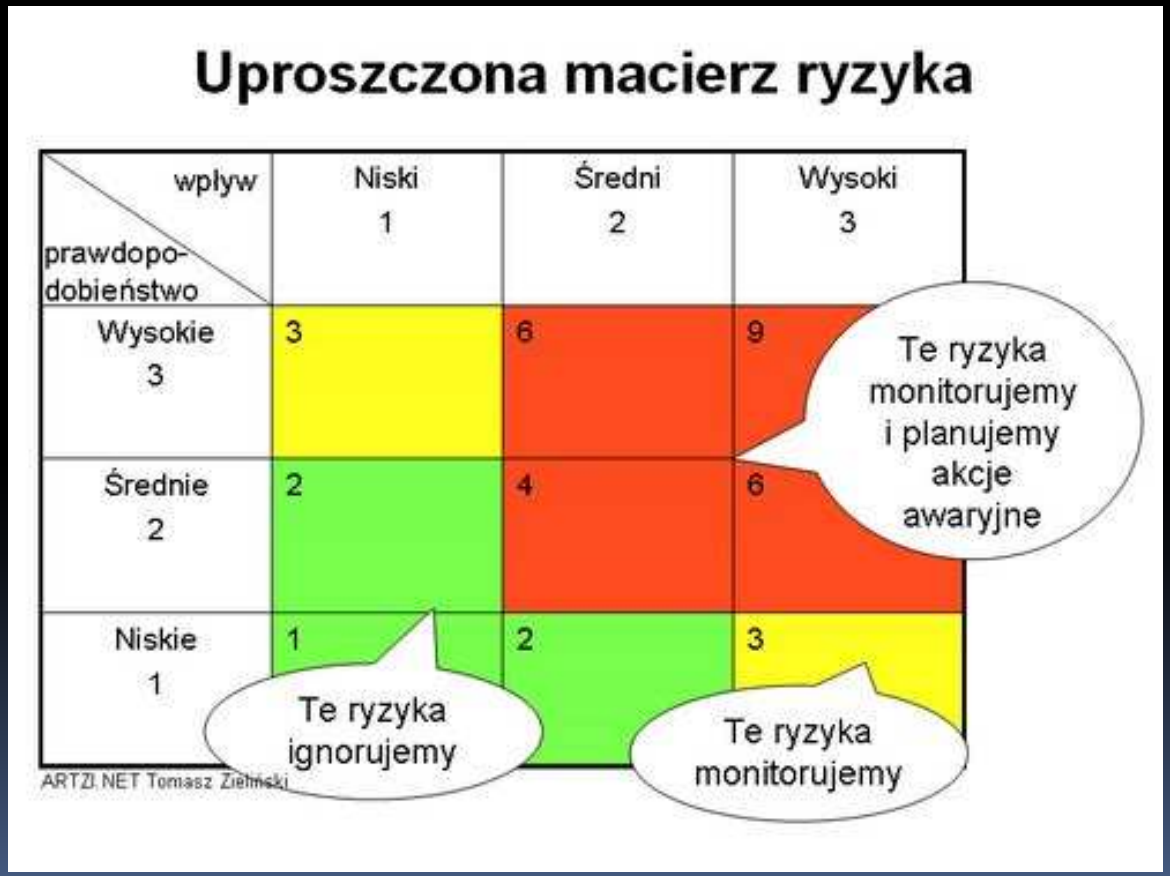
Polega na zapewnieniu poprawności przesyłania danych, uniemożliwienie ich podsłuchania oraz zmianie czy też zniszczeniu podczas transmisji. Jest to ochrona informacji przed nieuprawnioną zmianą oraz jej pozyskaniem czy zniszczeniem.

Projektując zarówno system informatyczny, jak i jego zasady bezpieczeństwa, trzeba uwzględnić jego środowisko (otoczenie), w którym będzie funkcjonował



Zarządzanie ryzykiem

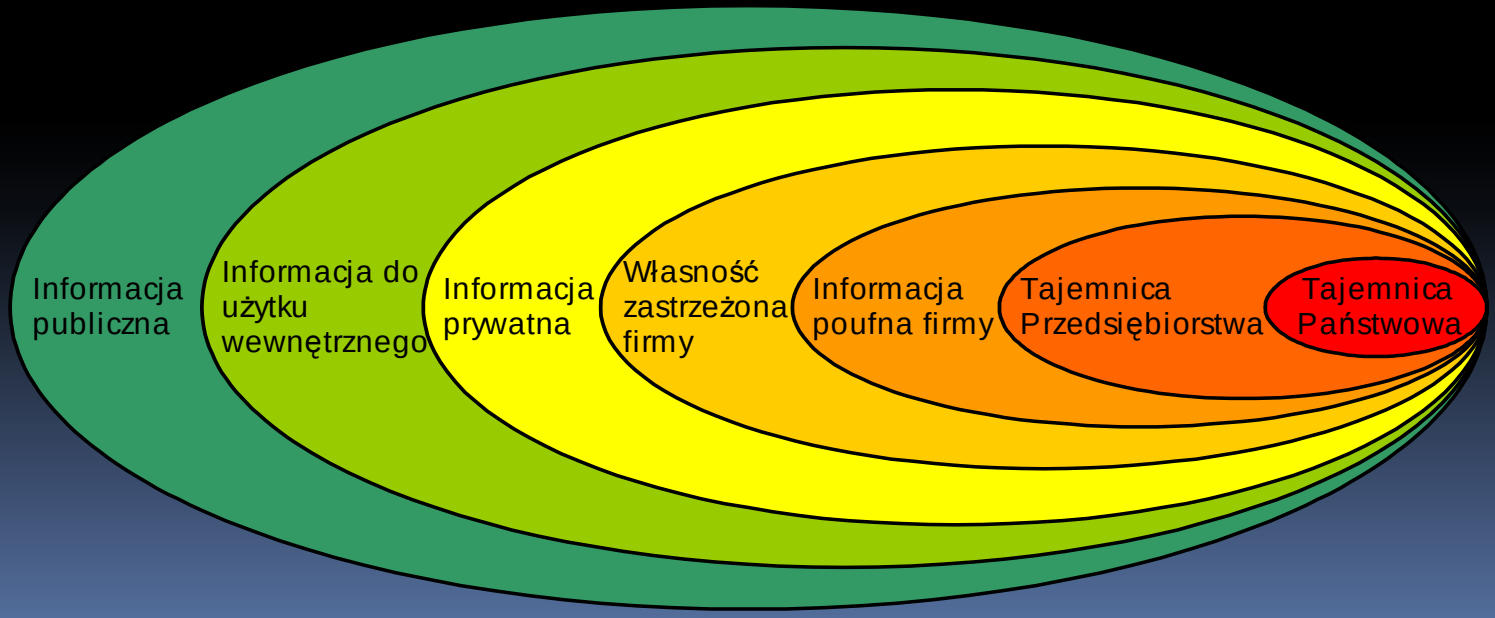
Całkowity proces postępowania z ryzykiem, obejmujący m.in. identyfikację zagrożeń i podatności, określenie i wdrożenie zabezpieczeń oraz monitorowanie ryzyka.



Źródło: Tomasz Zieliński, http://www.artzi.net

Klasyfikacja przechowywanych informacji

- **zasoby strategiczne** - decydują o strategii przedsiębiorstwa. Wymagania ochronne bardzo wysokie,
- **zasoby krytyczne** – mają wpływ na bieżące funkcjonowanie przedsiębiorstwa. Wymagania ochronne wysokie,
- **zasoby autoryzowane** – podlegają ochronie na podstawie ogólnie obowiązujących przepisów. Wymagania ochronne umiarkowane,
- **zasoby powszechnie dostępne** – ogólnie dostępne. Wymagania ochronne – brak.



Administrator systemu

Administrator (potocznie *admin*) – informatyk zajmujący się zarządzaniem systemem informatycznym i odpowiadający za jego sprawne działanie. Wyróżnia się administratorów:

- systemów operacyjnych
- baz danych
- serwerów
- sieci
- poszczególnych usług typu fora dyskusyjne, czaty itp., gdzie rola administratora sprowadza się przede wszystkim do moderowania.

Administrator systemu

Do zadań administratora należy nadzorowanie pracy serwerów, dodawanie, ewentualna edycja danych, i kasowanie kont ich użytkowników, konfiguracja komputerów, instalowanie oprogramowania, dbanie o bezpieczeństwo systemu i opcjonalnie samych danych, nadzorowanie, wykrywanie i eliminowanie nieprawidłowości, asystowanie i współpraca z zewnętrznymi specjalistami przy pracach instalacyjnych, konfiguracyjnych i naprawczych, dbanie o porządek (dotyczy w szczególności forów internetowych) itp.

Ze względu na zakres obowiązków, specjalistyczna wiedza typowego administratora czasem wykracza poza znajomość administracji powierzonego mu oprogramowania lub sieci, i dotyczyć pogranicza takich kategorii jak m.in.: elektronika, znajomość wielu różnych języków programowania, kryptografia i kryptoanaliza, etyka.

Administrator sieci

Administrator sieci informatycznej zarządza siecią komputerową w przedsiębiorstwach przemysłowych, handlowych, administracyjnych i innych. Do jego zadań może należeć:

- Archiwizowanie konfiguracji urządzeń;
- Informowanie o dostępnych usługach i ich możliwościach;
- Instalowanie nowych wersji oprogramowania;
- Instalowanie systemu rozliczenia użytkowników za wykorzystane zasoby sieci;
- Konfigurowanie interfejsów sieciowych komputerów;
- Kontrola poprawności działania sieci poprzez reagowanie na wszelkie zakłócenia i nieprawidłowości;
- Nadzorowanie innych pracowników;
- Nadzór nad prawidłową pracą urządzeń wspomagających;
- Prowadzenie szkoleń pracowników w zakresie korzystania z sieci;

Administrator sieci

Administrator sieci informatycznej zarządza siecią komputerową w przedsiębiorstwach przemysłowych, handlowych, administracyjnych i innych. Do jego zadań może należeć:

- Przestrzeganie zasad ochrony haseł;
- Reagowanie w przypadku stwierdzenia nieprawidłowego korzystania z sieci przez jej użytkowników;
- Tworzenie systemu haseł dostępu do urządzeń,
- Wskazywanie konieczności zainstalowania odpowiednich mechanizmów ochrony i wykrywania szpiegów;
- Wskazywanie niezbędnych danych administratorowi systemu komputerowego
- Zapewnienie bezawaryjnej pracy sprzętu w sieci,
- Zapewnienie ochrony haseł i dostęp do sieci
- Zarządzanie adresacją sieci,
- Zarządzanie siecią i jej eksploatacja.
- Zmiany w konfiguracja urządzeń i systemów sieciowych oraz ich dokumentowanie na bieżąco;

Ochrona danych osobowych

Za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Ochrona danych osobowych jest bardzo młodą dziedziną prawa.

Źródło jej wprowadzenia tkwi w koncepcji prawa do prywatności, którą
w skrócie można by określić jako ochronę możliwości decydowania przez dana osobę fizyczna o tym, jakie informacje o niej mogą być pozyskiwane
i udostępniane innym osobom.

Ochrona danych osobowych

Podstawy prawne:

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78 poz. 483 z późniejszymi zmianami)
Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. 2002 nr 101 poz. 926 z późn. zm.)
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. 2004 nr 94 poz. 923)
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004 nr 100 poz. 1024)
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. 2008 nr 229 poz. 1536)
Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 nr 144 poz. 1204).

Obowiązki Administratora Danych Osobowych

Administrator Danych jest zobowiązany przez ustawę o ochronie danych osobowych do:*

- zabezpieczenia przetwarzanych danych osobowych przed ich udostępnieniem osobom nieupoważnionym oraz zabraniem przez osobę nieuprawnioną,
- przetwarzania danych zgodnie z wymogami ustawy
- chronienia danych przed zmianą, utratą, uszkodzeniem lub zniszczeniem

*wg imagin.com.pl

Obowiązki Administratora Danych Osobowych

Zadania te powinny zostać zrealizowane poprzez:

- opracowanie dokumentacji
- monitorowanie czynności wykonywanych na zbiorze danych
- zapewnienie technicznych środków bezpieczeństwa

Jeśli Administrator Danych sam nie wykonuje powyższych czynności, powinien wyznaczyć Administratora Bezpieczeństwa Informacji (ABI), który będzie nadzorował przestrzeganie zasad ochrony. W efekcie ma on możliwość kontrolowania systemów informatycznych oraz wydawania zaleceń wszystkim użytkownikom.

Szeroki zakres zadań Administratora Bezpieczeństwa Informacji i duża odpowiedzialność sprawia, że powinno to być stanowisko podporządkowane w strukturze firmy bezpośrednio Administratorowi Danych (przedsiębiorcy, zarządowi firmy).

Obowiązki Administratora Danych Osobowych

Rozporządzenie wykonawcze zobowiązuje Administratora Danych do opracowania przynajmniej dwóch dokumentów:

- Polityki Bezpieczeństwa Danych Osobowych
- Instrukcji Zarządzania Systemem Informatycznym

Obowiązki Administratora Danych Osobowych

Polityka Bezpieczeństwa Danych Osobowych powinna zawierać między innymi:

- wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych
- opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi
- sposób przepływu danych pomiędzy poszczególnymi systemami
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Obowiązki Administratora Danych Osobowych

Instrukcja Zarządzania Systemem Informatycznym powinna omawiać następujące aspekty:

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności
- stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem
- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

Obowiązki Administratora Danych Osobowych

Instrukcja Zarządzania Systemem Informatycznym powinna omawiać następujące aspekty (c.d.):

- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania
- sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych
- sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego
- sposób odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia,
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

Obowiązki Administratora Danych Osobowych

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym muszą zostać odnotowane następujące informacje:

- data pierwszego wprowadzenia danych do systemu
- identyfikator użytkownika wprowadzającego dane osobowe do systemu
- źródło danych, w przypadku zbierania danych, nie od osoby, której one dotyczą
- informacja o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych
- fakt wniesienia sprzeciwu wobec przetwarzania danych, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania danych osobowych innemu administratorowi danych
- **Możliwe musi być sporządzenie i wydrukowanie raportu zawierającego wymienione powyżej informacje.**

Obowiązki Administratora Danych Osobowych

W zależności od rodzaju przetwarzanych danych osobowych oraz faktu czy system informatyczny jest podłączony do sieci publicznej (Internetu), Administrator Danych musi zapewnić środki bezpieczeństwa na jednym z poziomów:

- poziom podstawowy
- poziom podwyższony
- poziom wysoki

Obowiązki Administratora Danych Osobowych

Poziom podstawowy

Wymagania:

- system informatyczny musi zapewniać mechanizmy kontroli dostępu do danych
- jeżeli dostęp do danych posiadają co najmniej dwie osoby, to każda z musi posiadać odrębny identyfikator, a dostęp powinien zostać przyznany dopiero po dokonaniu uwierzytelnienia
- system informatyczny musi zostać zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego
- system informatyczny powinien zostać zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej
- identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych nie może zostać przyznany innej osobie

Obowiązki Administratora Danych Osobowych

Poziom podstawowy

Wymagania (c.d.):

- jeśli do uwierzytelniania użytkowników używa się hasła, to jego zmiana następuje nie rzadziej niż co 30 dni, a hasło składa się z co najmniej 6 znaków
- przetwarzane dane osobowe zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych
- kopie zapasowe powinny być przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem

Obowiązki Administratora Danych Osobowych

Poziom podstawowy

Wymagania (c.d.):

- niezwłocznie po tym jak kopie zapasowe tracą swoją użyteczność powinny zostać zniszczone
- osoba korzystająca z komputera przenośnego zawierającego dane osobowe powinna zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem w którym w normalnej sytuacji przetwarza się dane osobowe oraz stosować środki ochrony kryptograficznej wobec przetwarzanych danych
- przed likwidacją, przekazaniem lub naprawą urządzeń, dysków lub innych elektronicznych nośników informacji zawierających dane osobowe należy usunąć zapis tych danych w sposób uniemożliwiający ich odczytanie i odzyskanie

Obowiązki Administratora Danych Osobowych

Poziom podwyższony

Wymagania takie jak na poziomie podstawowym oraz:

- jeśli do uwierzytelniania użytkowników używa się hasła, to powinno składać się z co najmniej 8 znaków oraz zawierać małe i wielkie litery, cyfry lub znaki specjalne
- urządzenia i nośniki zawierające dane osobowe i przekazywane poza obszar w którym w normalnej sytuacji przetwarza się dane powinny zostać zabezpieczone w sposób zapewniający poufność i integralność tych danych

Obowiązki Administratora Danych Osobowych

Poziom wysoki

Wymagania takie jak na poziomie podwyższonym oraz:

- system informatyczny powinien być chroniony przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem (firewall)
- zapewniona powinna zostać kontrola przepływu informacji między systemem informatycznym a siecią publiczną
- działania inicjowane z sieci publicznej i systemu Administratora Danych powinny być kontrolowane
- należy zastosować środki kryptograficznej ochrony danych wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej (w praktyce zaleca się szyfrowanie całej transmisji)

Obowiązki Administratora Danych Osobowych

Wszystkie zbiory danych osobowych należy zgłosić do Generalnego Inspektora Ochrony Danych Osobowych (art. 40 ustawy). Z tego obowiązku zwolnieni są administratorzy następujących danych osobowych (art. 43 ustawy, ust. 1):

- przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się,
- dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta,
- przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,
- powszechnie dostępnych,
- przetwarzanych w zakresie drobnych bieżących spraw życia codziennego,
- ... i inne, szczegółowe informacje w art. 43 ustawy, ust. 1.

Zwolnienie z obowiązku zgłoszenia zbioru danych do rejestracji nie zwalnia z obowiązku przestrzegania innych obowiązków wynikających z przepisów ustawy o ochronie danych osobowych. Administrator danych jest zobowiązany między innymi do przestrzegania wymogów w zakresie zabezpieczeń technicznych i organizacyjnych.

Obowiązki Administratora Danych Osobowych

Zgodnie z art. 27 ust. 1 ustawy o ochronie danych osobowych, dane osobowe szczególnie chronione (wrażliwe) to:

- dane ujawniające:
  - pochodzenie rasowe lub etniczne,
  - poglądy polityczne,
  - przekonania religijne lub filozoficzne,
  - przynależność wyznaniową, partyjną lub związkową,
- dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym,
- dane dotyczące:
  - skazań, orzeczeń o ukaraniu i mandatów karnych
  - innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
- Przetwarzanie danych wrażliwych podlega szczególnym rygorom.

Obowiązki Administratora Danych Osobowych

Administrator Danych (przedsiębiorca, zarząd firmy), który nie wypełnia obowiązków nałożonych na niego przez ustawę i rozporządzenia, między innymi w zakresie rejestracji zbioru danych osobowych, legalności przetwarzania informacji oraz zabezpieczeń technicznych i organizacyjnych **może zostać pociągnięty do odpowiedzialności**:

- **karnej** — grzywna, ograniczenie lub pozbawienie wolności do lat 3
- **administracyjnej** — wymóg poprawienia błędów, a nawet usunięcia zgromadzonych danych
- **dyscyplinarnej** — dotyczy pracowników i może doprowadzić do zwolnienia dyscyplinarnego
- **odszkodowawczej** — odszkodowanie w przypadku naruszenia praw osoby lub wyrządzenia szkody majątkowej lub krzywdy

Standardy

Przykłady norm definiujących zagadnienia związane z ochroną danych. *

ISO/IEC 20000:2005
Międzynarodowa norma ISO 20000 określa wymagania i wskazuje wytyczne w zakresie ustanowienia, wdrożenia, eksploatacji, monitorowania i doskonalenia Systemu Zarządzania Usługami Informatycznymi w organizacji.

ISO/IEC 27001:2005
Międzynarodowa norma ISO 27001 określa wymagania związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji.

PN-I-02000:2002 – Technika informatyczna – Zabezpieczenia w systemach informatycznych – Terminologia
Norma ta stanowi opracowanie mające na celu unormowanie terminologii polskiej dotyczącej bezpieczeństwa systemów informatycznych i ochrony informacji.

*wg http://www.centrum.bezpieczenstwa.pl/content/blogcategory/0/46/

Organizacje

W Polsce prowadzi działalność wiele organizacji propagujących zagadnienia związane z bezpieczeństwem danych cyfrowych. Na ich serwisach internetowych można znaleźć wiele informacji m.in. nt. aktualnych zagrożeń, wykrytych luk i sposobów na poprawienie bezpieczeństwa. Większość z tych organizacji oferuje certyfikowane szkolenia.*

CERT(Computer Emergency Response Team) Polska jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet. CERT Polska działa od 1996 roku (do końca roku 2000 pod nazwą CERT NASK), a od roku 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams). W ramach tej organizacji współpracuje z podobnymi zespołami na całym świecie. Zespół CERT Polska działa w strukturach Naukowej i Akademickiej Sieci Komputerowej. Działalność zespołu jest finansowana przez NASK.

Strona WWW: www.cert.pl

*wg http://www.centrum.bezpieczenstwa.pl/content/blogsection/7/80/

Organizacje

Założona w 1969 roku ISACA liczy ponad 50 000 członków z ponad 140 państw. ISACA od 1978 administruje nadawaniem certyfikatów Certified Information Systems Auditor (CISA), który posiada już ponad 44 000 profesjonalistów. ISACA nadaje również certyfikaty Certified Information Security Manager (CISM), który w przeciągu pierwszych 3 lat otrzymało 5 500 profesjonalistów.

ISACA jest sponsorem międzynarodowych konferencji, wydaje Information Systems Control Journal oraz rozwija międzynarodowe standardy audytu i kontroli. Jej oddział badawczy IT Governance Institute, utworzony w 1998 roku, opublikował COBIT - rozpoznawany na całym świecie zbiór wytycznych wspomagający utrzymywanie ładu korporacyjnego.

Strona WWW: www.isaca.org.pl

Organizacje

Celem "ISSA Polska - Stowarzyszenie do spraw Bezpieczeństwa Systemów Informacyjnych" jest krzewienie wiedzy na temat bezpieczeństwa systemów informacyjnych oraz promowanie zasad i praktyk, które zapewniają poufność, integralność, niezaprzeczalność i dostępność zasobów informacyjnych, a także promowanie i rozwój swoich członków poprzez podnoszenie ich umiejętności zawodowych związanych z ochroną systemów informacyjnych.
Strona WWW: www.issa.org.pl

Organizacje

Stowarzyszenie Biegłych ds. Przestępstw i Nadużyć Gospodarczych ACFE Polska jest organizacją non-profit zrzeszającą osoby zawodowo zajmujące się zapobieganiem i wykrywaniem oszustw gospodarczych. ACFE Polska jest uznanym przez ACFE w Stanach Zjednoczonych Oddziałem ACFE nr 114. Członkowie Stowarzyszenia podlegają Kodeksowi Etyki.
Celem organizacji jest działalność edukacyjna służąca podnoszeniu kwalifikacji członków w zakresie prowadzenia badań oraz świadczenia usług doradczych w dziedzinie zapobiegania i wykrywania przestępstw i nadużyć gospodarczych.
Strona WWW: www.acfe.pl

Organizacje

Krajowe Stowarzyszenie Ochrony Informacji Niejawnych (KSOIN), jest apolitycznym, dobrowolnym, samorządnym zrzeszeniem pracowników pionów ochrony informacji niejawnych oraz osób zainteresowanych wspieraniem jego celów statutowych.
Strona WWW: www.ksoin.com.pl

Organizacje

Ogólnopolskie Stowarzyszenie Pełnomocników Informacji Niejawnych powstało w październiku 2000 r. z inicjatywy osób zainteresowanych propagowaniem zasad ochrony informacji niejawnej w myśl ustawy z dnia 22 stycznia 1999 r.
Stowarzyszenie skupia wokół siebie grupę osób zajmujących się zawodowo ochroną informacji niejawnej w różnych instytucjach zarówno państwowych i firmach komercyjnych.
Aktywna współpraca w tym zakresie z prawnymi instytucjami powołanymi do ochrony bezpieczeństwa państwa, pozwala na wniesienie aktualnej wiedzy oraz praktycznego rozwiązywania codziennych problemów na jakie napotykają w praktyce zawodowej Pełnomocnicy Ochrony Informacji Niejawnej. Realizacji tych celów służą organizowane przez Stowarzyszenie różne formy szkoleń, seminaria i konferencja, ale także kontakty interpersonalne.
Strona WWW: www.zgospoin.com.pl

Organizacje

Stowarzyszenie Audytorów Wewnętrznych IIA-Polska skupia audytorów wewnętrznych oraz osoby zainteresowane tą profesją. IIA zajmuje się opracowywaniem standardów, zasad etycznych, certyfikatów, programów kształcenia oraz rozwiązań metodycznych i technicznych w zakresie audytu wewnętrznego.
Strona WWW: www.iia.org.pl

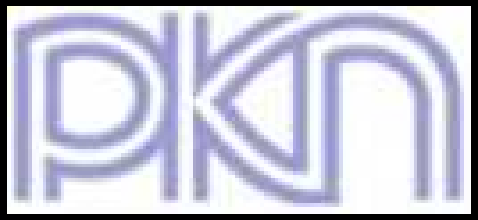
Organizacje

Z inicjatywy Edmunda Saundersa oraz Brytyjskiego Funduszu Know How (BKHF) powstała w 1998 specjalistyczna organizacja, Polski Instytut Kontroli Wewnętrznej (PIKW), która przygotowuje kadry do oceny systemów kontroli wewnętrznej i profesjonalnego wykonywania zawodu audytora wewnętrznego.
Strona WWW: www.pikw.pl

Organizacje

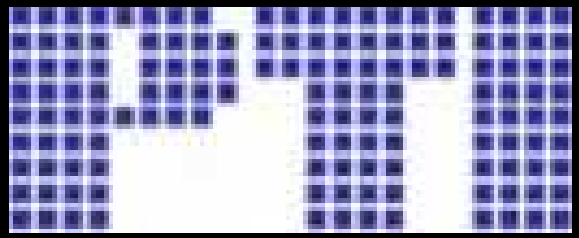
Stowarzyszenie Zarządzania Ryzykiem (POLRISK) ma ambicję stać się ogólnopolską organizacją konsolidującą i aktywnie reprezentującą interesy polskich risk managerów.
Strona WWW: www.polrisk.pl

Organizacje



Polski Komitet Normalizacyjny (PKN) jest krajową jednostkę normalizacyjną i jednocześnie państwową budżetową jednostką organizacyjną. Polski Komitet Normalizacyjny ma wyłączne prawo używania skrótu "PKN" i zastrzeżonego znaku graficznego.
Strona WWW: www.pkn.pl

Organizacje



Cele i środki działania Polskiego Towarzystwa Informatycznego:
popieranie działalności naukowej i naukowo-technicznej we wszystkich dziedzinach informatyki i doskonalenia metod jej efektywnego wykorzystania w gospodarce narodowej, podnoszenie poziomu wiedzy i etyki zawodowej oraz kwalifikacji członków, a także oddziaływanie w tym kierunku na inne osoby zajmujące się informatyką, ułatwianie wymiany informacji w środowisku zawodowym; popularyzacja w społeczeństwie zagadnień informatyki i jej zastosowań, reprezentowanie członków Towarzystwa, ich opinii, potrzeb, interesów i uprawnień wobec społeczeństwa, władz oraz stowarzyszeń w kraju i za granicą.
Strona WWW: www.pti.org.pl

Organizacje

Polska Izba Informatyki i Telekomunikacji (PIIT) istnieje od stycznia 1993 roku i brała udział w pracach nad ustawami i przepisami podatkowymi, celnymi, certyfikacyjnymi, prawem autorskim oraz prawem zamówień publicznych i telekomunikacyjnych.
Strona WWW: www.piit.org.pl

Organizacje

W 1991 r. NASK podłączył Polskę do Internetu. W swej obecnej formie organizacyjnej, jako jednostka badawczo-rozwojowa, działa od grudnia 1993 r. Działalność naukowa jest skoncentrowana w Pionie Naukowym. Badania prowadzone w Pionie Naukowym mają na celu opracowanie mechanizmów i algorytmów pozwalających na zwiększenie efektywności i niezawodności nowoczesnych sieci teleinformatycznych. Podstawowe miejsce zajmują zagadnienia związane z zapewnieniem jakości usług (QoS), optymalną wyceną usług, oraz zwiększaniem bezpieczeństwa zarówno sieci jak i usług sieciowych. Szczególny nacisk położony jest na badania dotyczące metod biometrycznych w bezpieczeństwie usług.
Strona WWW: www.nask.pl

Organizacje

Fundacja Wspierania Edukacji Informatycznej "PROIDEA" jest niezależną, samofinansującą się organizacją typu non-profit. Powstała w odpowiedzi na rosnące zapotrzebowanie na organizacje przekazujące w sposób kompetentny wiedzę z zakresu teleinformatyki. Fundacja wypełnia swoje cele statutowe wspierając edukację oraz promując inicjatywy służące popularyzowaniu informatyki w szkołach.
Strona WWW: www.proidea.org.pl

Certyfikaty

Przykładowe certyfikaty poświadczające wiedzę z szeroko pojętego zakresu bezpieczeństwa systemów informatycznych.*

Certyfikat Certified Information Systems Security Professional (CISSP) jest potwierdzeniem doświadczenia i kompetencji w temacie szeroko pojętego bezpieczeństwa systemów informatycznych. Certyfikacja CISSP jako pierwsza w branży IT została uznana przez International Organization for Standardization/International Electrotechnical Commission za spełniającą wymagania normy ISO/IEC 17024.

Certyfikat SSCP (Systems Security Certified Practitioner) potwierdza posiadanie wiedzy z obszaru bezpieczeństwa informacji. Certyfikaty SSCP przyznawane są przez firmę ISC.

*wg http://www.centrum.bezpieczenstwa.pl/content/blogcategory/0/93/

Certyfikaty

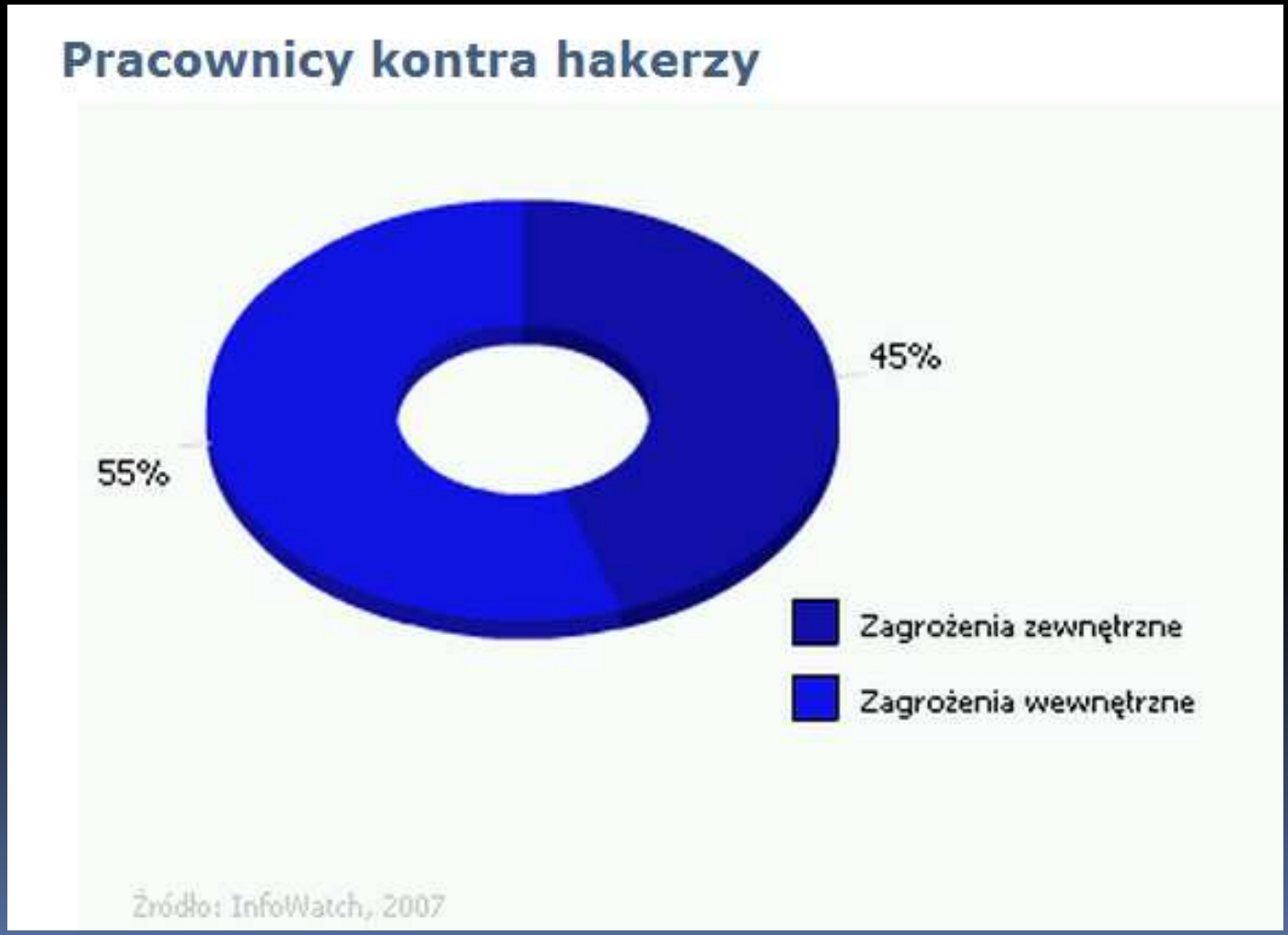
Przykładowe certyfikaty poświadczające wiedzę z szeroko pojętego zakresu bezpieczeństwa systemów informatycznych.

Posiadanie certyfikatu CISA daje wiele korzyści zawodowych i organizacyjnych. Poświadcza wiedzę w zakresie audytu systemów informatycznych oraz intencję służenia organizacji w profesjonalny sposób. Ci, którzy zostają CISA, dołączają się do światowej grupy uznanych profesjonalistów.

Program CISM (Certified Information Security Manager / Certyfikowany Menedżer Bezpieczeństwa Informacji) został przygotowany przez ISACA w 2003 roku specjalnie na potrzeby doświadczonej kadry zarządzającej bezpieczeństwem systemów informacji. Jest nakierowany na osoby, które zarządzają, projektują i oceniają systemy bezpieczeństwa informacji w przedsiębiorstwach.

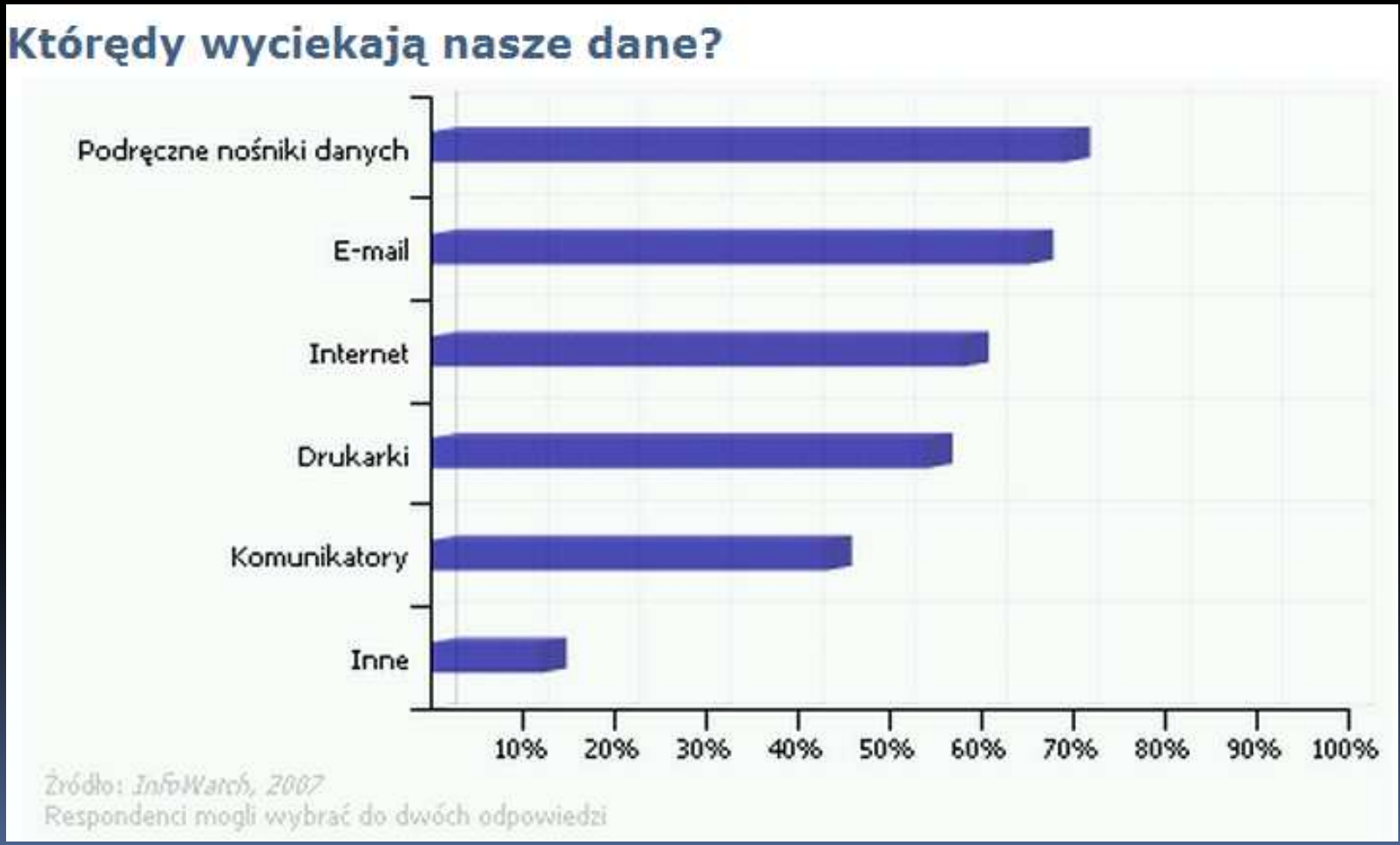
Statystyki

Kilka interesujących wyników badań z zakresu bezpieczeństwa i ochrony danych.



Statystyki

Kilka interesujących wyników badań z zakresu bezpieczeństwa i ochrony danych.

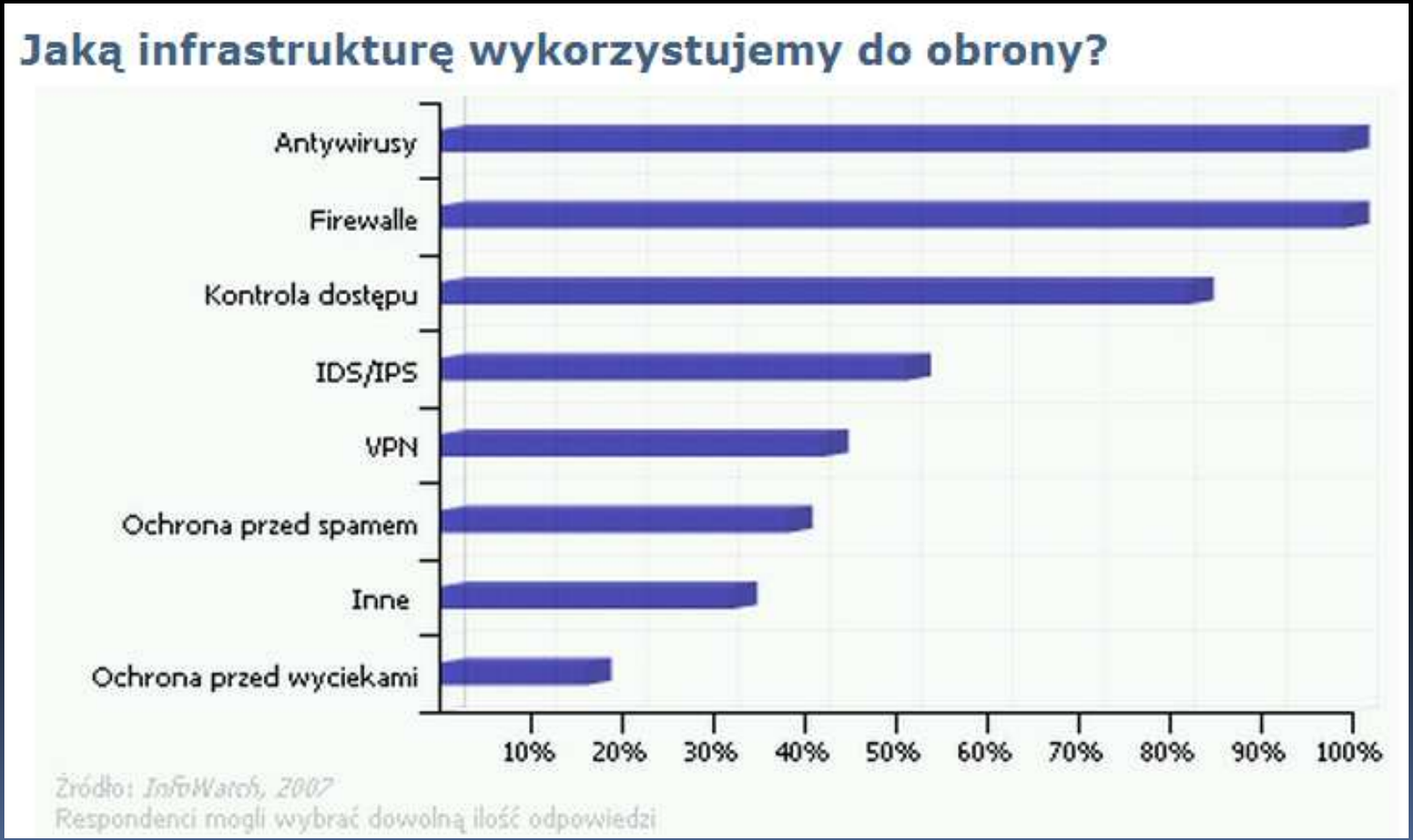


Statystyki

Kilka interesujących wyników badań z zakresu bezpieczeństwa i ochrony danych.

Statystyki

Kilka interesujących wyników badań z zakresu bezpieczeństwa i ochrony danych.



Statystyki

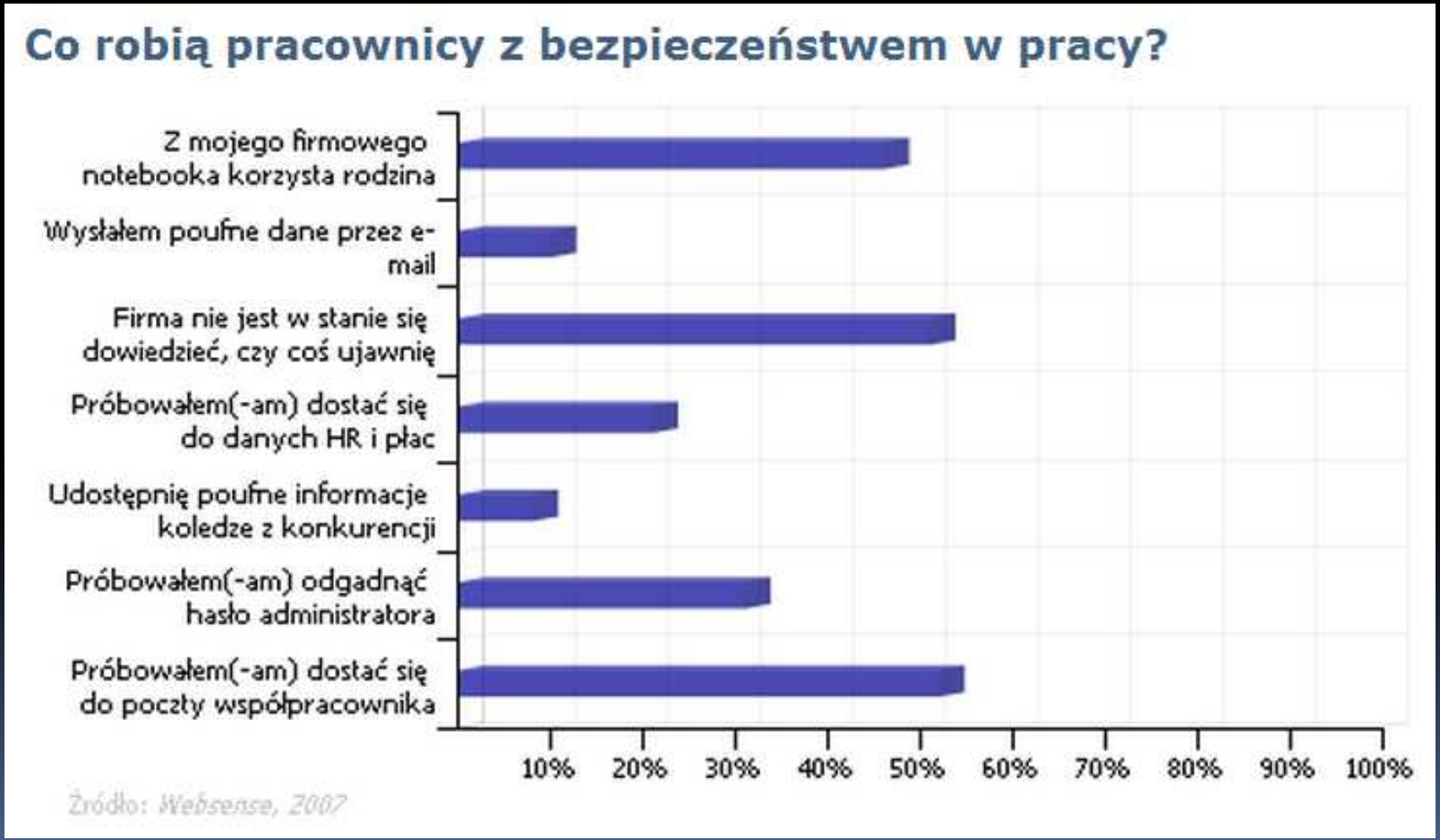
Kilka interesujących wyników badań z zakresu bezpieczeństwa i ochrony danych.

Statystyki

Kilka interesujących wyników badań z zakresu bezpieczeństwa i ochrony danych.

Statystyki

Kilka interesujących wyników badań z zakresu bezpieczeństwa i ochrony danych.



Internetowe źródła informacji

Skąd pozyskać aktualne informacje na temat bezpieczeństwa, zagrożeń i ochrony danych w sieciach?

http://hacking.pl/
http://hack.pl/
http://niebezpiecznik.pl/
http://www.centrum.bezpieczenstwa.pl
http://www.viruslist.pl
http://www.hcsl.pl/
http://www.e-ochronadanych.pl/
http://securityinfo.pl
Strony internetowe wymienionych organizacji
Fora dyskusyjne, blogi, twitter, facebook

Koniec części 1.