Polityka bezpieczeństwa

Bibliografia

W. Stallings, *Network Security Essentials.* Prentice Hall, 2003
J. Stokłosa, T. Bliski, T. Pankowski, *Bezpieczeństwo danych w systemach informatycznych.* PWN, 2001
N. Ferguson, B. Schneier, *Kryptografia w praktyce.*, Helion, 2004
S. Garfinkel, G. Spafford, *Bezpieczeństwo w Unixie i Internecie.* Wyd. RM, 1997
D. R. Ahmad, Hack Proofing Your Network, Syngress Publ. 2001.
W. R. Cheswick. *Firewalle i bezpieczeństwo w sieci*. Helion, 2003
Zalecenia National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC), 1996, http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
Raport techniczny ISO/IEC 13335TR (PN-I 13335-1- Wytyczne do zarządzania bezpieczeństwem systemów informatycznych: terminologia, związki między pojęciami, podstawowe modele), 2001

Plan wykładu

- Wprowadzenie
- Realizacja polityki bezpieczeństwa
- Zawartość polityki bezpieczeństwa
- Strategie bezpieczeństwa
- Sposoby zabezpieczeń
- Bezpieczeństwo vs. polityka przedsiębiorstwa
- Projektowanie systemu i procedur bezpieczeństwa
- Przykładowe elementy polityki bezpieczeństwa
- Rady dla wdrażających politykę bezpieczeństwa
- Podsumowanie

Wprowadzenie

- **Polityka bezpieczeństwa** (ang. *security policy*) jest zbiorem spójnych, precyzyjnych i zgodnych z obowiązującym prawem przepisów, reguł i procedur, według których dana organizacja buduje, zarządza oraz udostępnia zasoby i systemy informacyjne i informatyczne. Określa ona, które zasoby i w jaki sposób mają być chronione [wikipedia.org]

Zasady

- Polityka bezpieczeństwa (PB) obejmuje swoim zakresem nie tylko sieć komputerową przedsiębiorstwa czy instytucji, ale także **całość zagadnień związanych z bezpieczeństwem** danych będących w dyspozycji firmy
- Polityka bezpieczeństwa organizacji definiuje **poprawne i niepoprawne** - w sensie bezpieczeństwa - sposoby wykorzystywania kont użytkowników i danych przechowywanych w systemie
- PB powinna być dokumentem **spisanym**
- PB należy **przedstawić pracownikom**, tak aby była ona zrozumiana
- PB zazwyczaj jest konkretnym rozwiązaniem specyficznym dla rozważanej firmy, czyli **trudno uogólniać** zasady tworzenia polityki

Polityka bezpieczeństwa

Powinna zawierać:

- Wyjaśnienia, definicje podstawowych pojęć
- Podział odpowiedzialności i kompetencji
- Jasne sformułowania, prosty język
- Opis mechanizmów realizujących PB

NIE powinna zawierać:

- Szczegółów technicznych
- Bezkrytycznych zapożyczeń z innych rozwiązań

Realizacja polityki bezpieczeństwa
Etapy realizacji

- Audyt istniejących zasobów i zagrożeń
- Opracowanie projektu i dokumentacji
- Wdrożenie projektu
- Ciągły nadzór, kontrola i modyfikacja istniejącej polityki

Realizacja polityki bezpieczeństwa

- Przez zmieniające się uwarunkowania pracy firmy, profilu działania, stosowanego sprzętu i oprogramowania polityka bezpieczeństwa wymaga **ciągłych modyfikacji**
- Należy określić co jaki czas mają być **wykonywane** wewnętrzne i zewnętrzne **audyty bezpieczeństwa** oraz **zmiany** w polityce bezpieczeństwa

Model realizacji polityki bezpieczeństwa

Norma PN-ISO/IEC 27001 stosuje „Planuj – Wykonuj – Sprawdzaj – Działaj” (PDCA) dla wdrażania SZBI (Systemu Zarządzania Bezpieczeństwem Informacji)

- **Planuj** - ustanowienie SZBI, celów, zakresu stosowania, procesów i procedur odpowiadających zarządzaniu ryzykiem oraz zwiększających bezpieczeństwo informacji tak, aby uzyskać wyniki zgodne z ogólnymi zasadami i celami instytucji

Model realizacji polityki bezpieczeństwa

- **Wykonuj** - wdrożenie i eksploatacja SZBI - wdrożenie i eksploatacja polityki SZBI, zabezpieczeń, procesów i procedur
- **Sprawdzaj** - monitorowanie i przegląd SZBI - pomiar wydajności procesów w odniesieniu do polityki SZBI, celów i doświadczenia praktycznego oraz dostarczania raportów kierownictwu do przeglądu
- **Działaj** - utrzymanie i doskonalenie SZBI - podejmowanie działań korygujących i zapobiegawczych na podstawie wyników wewnętrznego audytu SZBI i przeglądu realizowanego przez kierownictwo lub innych istotnych informacji, w celu zapewnienia ciągłego doskonalenia SZBI

Zawartość polityki bezpieczeństwa Zasoby chronione w ramach polityki bezpieczeństwa

- **Sprzęt komputerowy**: procesory, zasoby dyskowe, użytkowane połączenia teleinformatyczne, terminale, urządzenia sieciowe
- **Oprogramowanie**: systemy operacyjne, oprogramowanie aplikacyjne, teksty źródłowe programów, programy pomocnicze i komunikacyjne
- **Dane firmy**: transmitowane, dane przechowywane w plikach i w systemach bazodanowych, kopie zapasowe, zapisy zdarzeń (logi), dane przechowywane i przesyłane w wersji papierowej
- **Ludzie**: użytkownicy i administratorzy
- **Dokumentacja sprzętu**, oprogramowania, lokalnych regulaminów i procedur postępowania
- **Inne materialne zasoby**: pomieszczenia, sieć energetyczną, papiery wartościowe

Typowe elementy polityki bezpieczeństwa

- Definicje podstawowych **pojęć**
- Określenie kto za co **odpowiada** w przedsiębiorstwie
- Określenie, kto i jakie może mieć **konto** w systemie
- Określenie, czy wiele osób może korzystać z **jednego konta**
- Określenie, kiedy można **odebrać prawo** do konta, co zrobić z kontem po odejściu pracownika
- Zdefiniowanie wymagań dotyczących **haseł**
- Określenie zasad podłączenia i korzystania z sieci

Typowe elementy polityki bezpieczeństwa

- Określenie zasad podłączenia i korzystania z sieci **Internet**
- Określenie zasad **udostępniania informacji** w Internecie
- **Regulamin użytkownika**
- **Zobligowanie pracowników** do podporządkowania się zaleceniom administratorów systemu w kwestii bezpieczeństwa
- Określenie zasad korzystania z **połączeń modemowych**
- Określenie metod ochrony **krytycznych danych** firmy (finanse, dane osobowe, dane o klientach)

Typowe elementy polityki bezpieczeństwa

- Określenie metod ochrony przed **wirusami**
- Określenie zasad **sporządzania audytów** bezpieczeństwa, kontroli systemu, zapisu historii pracy systemu
- Określenie zasad dokonywania **uaktualnień** oprogramowania
- Określenie zasad korzystania z usługi **outsourcing**
- Określenie zasad **serwisowania** sprzętu

Strategie bezpieczeństwa

Strategie bezpieczeństwa spisane w formie dokumentu tworzą plan ochrony, który jest opracowywany przez osoby opiekujące się systemem informatycznym

Plan ochrony powinien zawierać:

- Opis realizacji metod kontroli dostępu do systemu i zasobów
- Opis metod okresowego lub stałego monitorowania systemu
- Dokładny opis metod reagowania na wykrycie zagrożenia
- Opis metod likwidacji skutków zagrożeń

Koncepcje strategii ochrony

- **Zasada poziomu bezpieczeństwa** – celem projektanta powinno być zapewnienia maksymalnie dostatecznej ochrony i odpowiednio duże zmniejszenie ryzyka wystąpienia zagrożeń, a nie zbudowanie zabezpieczeń idealnych
- **Zasada opłacalnych zabezpieczeń** – mechanizmy zapewniające ochronę systemu informatycznego są opłacalne jedynie w przypadku, gdy koszt ich wdrożenia jest niższy niż koszty związane z wykorzystaniem danego zagrożenia

Koncepcje strategii ochrony

- **Zasada najmniejszych przywilejów** – wymaga, aby użytkownicy końcowi, procesy czy też programy komputerowe miały dostęp jedynie do tych zasobów systemu informatycznego, do których dostęp ten jest wymagany
- **Zasada rozdzielania informacji** – polega na ograniczeniu dostępu do pewnych zasobów jedynie dla tych osób, które powinny ów dostęp posiadać
- **Zasada separacji obowiązków** – określa konieczność pozbawienia pojedynczych osób zdolności do wykonywania krytycznych działań w całości

Koncepcje strategii ochrony

- **Zasada niskiej złożoności systemów** – dla złożonych systemów bezpieczeństwa prawdopodobieństwo wystąpienia w nich błędu jest wprost proporcjonalne do ich złożoności, więc projektowane środki ochrony powinny być proste i skuteczne
- **Zasada najsłabszego ogniwa** – niezbędna jest ochrona nie tylko zasobów strategicznych, lecz także tych mniej znaczących, w myśl zasady, iż system jest tak bezpieczny jak jego najsłabsze ogniwo
- **Zasada ograniczonego zaufania** – odnosi się do konieczności odseparowania od siebie systemów i ograniczenia relacji zaufania między nimi

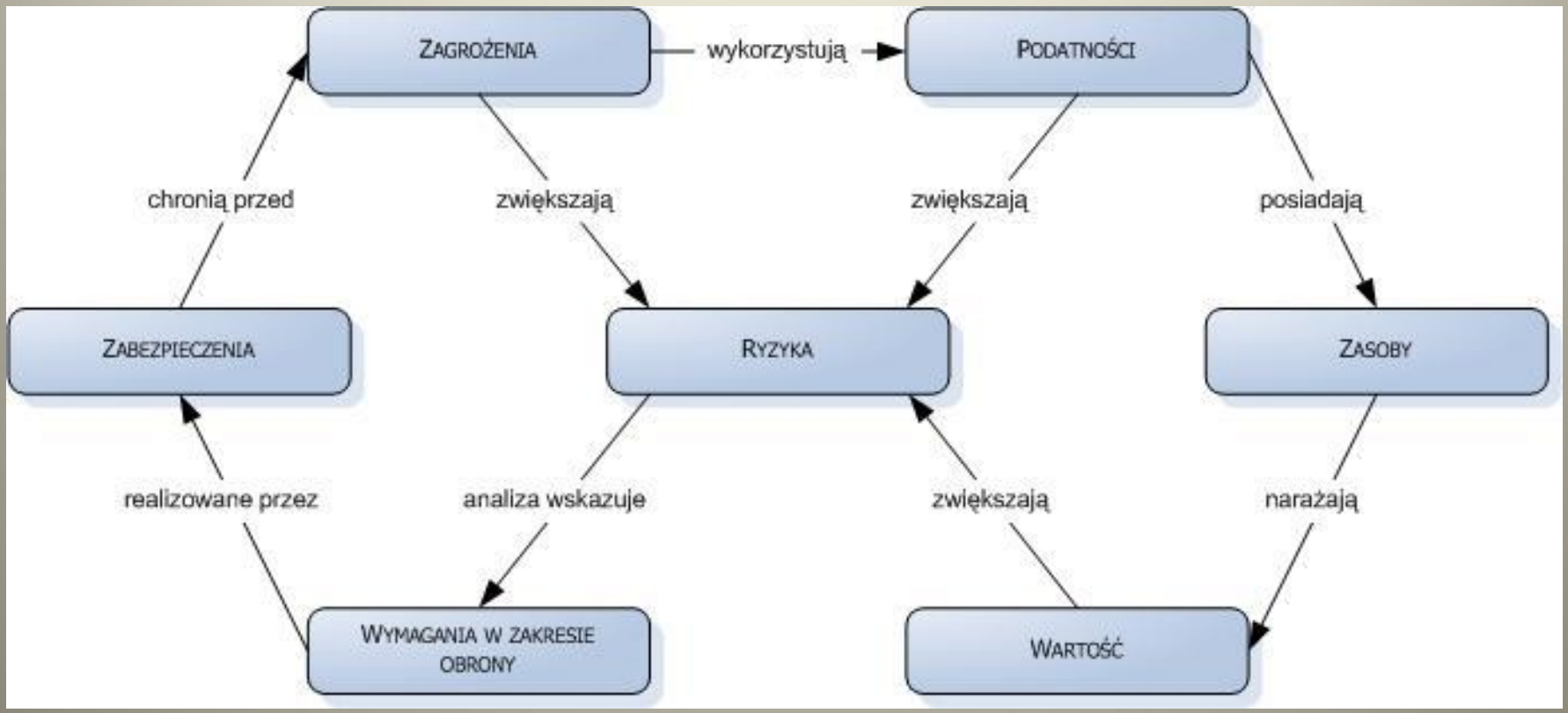
Koncepcje strategii ochrony

- **Zasada wąskiego przejścia** – polega na ograniczeniu liczby możliwych wejść do systemu informatycznego, zmusza to napastnika do używania kanału, który jest odpowiednio dobrze kontrolowany (np. przez zaporę ogniową)
- **Zasada dogłębnej ochrony** – dotyczy tworzenia wielu warstw zabezpieczeń w systemie informatycznym
- **Zasada zróżnicowanej ochrony** – polega na stosowaniu nie tylko dostatecznie dużej ilości warstw mechanizmów obronnych, ale również ich zróżnicowaniu

Analizy ryzyka

- **Ograniczenie ryzyka** – realizowane poprzez stosowanie odpowiednich zabezpieczeń
- **Przeniesienie ryzyka** – odpowiedzialność za ewentualne wykorzystanie podatności przez zagrożenie spoczywa na innej jednostce organizacyjnej
- **Unikanie ryzyka** – realizowane poprzez usunięcie jednego z aktywów, które podatne jest dane zagrożenie, nie są wtedy wymagane żadne mechanizmy bezpieczeństwa
- **Akceptowanie ryzyka** – w przypadku zagrożeń, przed którymi ochrona jest wysoce nieopłacalna oraz prawdopodobieństwo wystąpienia jest znikome, możliwe jest w pełni świadome zaakceptowanie ryzyka

Zarządzanie ryzykiem



Reakcje na próby ataku na system

- Analiza sytuacji
- Zatrzymanie pracy całego lub części systemu, poinformowanie użytkowników
- Analiza zapisu stanu systemu
- Odtworzenie z archiwów ostatniego stanu systemu

Sposoby zabezpieczeń systemu

- Organizacyjne
- Administracyjne
- Fizyczne
- Transmisji
- Emisji
- Programowe

Organizacyjne zabezpieczenia systemu

- Określenie specjalnych **obszarów chronionych**
- Ograniczenie wymiany **dokumentów**
- Opracowanie **regulaminów i procedur** pracy
- Utworzenie **procedur awaryjnych**
- Ograniczenie ryzyka **błędów ludzkich** (wprowadzenie procedur kontrolnych, bilansowanie)
- Opracowanie procedur **przyjmowania urządzeń** (kontrola jakości, gwarancja, serwis, certyfikacja, ochrona zewnętrzna)
- Opracowanie procedur **odbioru i certyfikacji oprogramowania**
- **Szkolenia pracowników**

Administracyjne zabezpieczenia systemu

- Odpowiednie kierowanie wszystkim **procesami**
- **Certyfikacja** sprzętu, oprogramowania, pomieszczeń, osoby
- Zarządzanie **dostępem** do pomieszczeń i obiektów
- Zarządzanie **kluczami** kryptograficznymi
- **Administrowanie systemem** informatycznym

Fizyczne zabezpieczenia systemu

- Fizyczne zabezpieczenie **pomieszczeń**
- **Obszary chronione**
- **Strefy ochronne**
- **Wycofywanie, niszczenie** starych podzespołów komputerowych
- Zapewnienie odpowiednich **źródeł zasilania**
- Bezpieczne **przechowywanie** gotówki, papierów wartościowych
- Stosowanie **sprzętu zapasowego** (awaryjnego)

Zabezpieczenia transmisji

- Określenie **głównych i awaryjnych** dróg transmisji
- Zabezpieczanie **dokumentów elektronicznych**
- Zabezpieczenie **sieci** telekomunikacyjnej i telefonicznej

Zabezpieczenia emisji

- Odpowiedniej **jakości** sprzęt komputerowy
- Strefy **ochronne**
- **Ekranownie**

Programowe zabezpieczenia systemu

- **Kontrola dostępu** do systemu, ochrona plików i bazy danych
- Zastosowania narzędzi **kryptograficznych**
- Użycie mechanizmów **separacj**i (firewall)
- Użycie mechanizmów **wykrywania włamań** (IDS, IPS)
- Użycie programów **antywirusowych**
- Użycie programów do **monitorowania** działań użytkowników systemów informatycznych

Szkolenia pracowników

- Mechanizmy bezpieczeństwa będą skuteczne, jeżeli personel zostanie **prawidłowo przeszkolony** z zakresu bezpieczeństwa
- Na zakończenie szkolenia pracownik powinien **otrzymać i podpisać regulamin użytkownika** opracowany dla danego stanowiska pracy
- **Łamanie** zaleceń regulaminu użytkownika powinno wiązać się **z karami** dla pracownika
- Dotyczy to również wszystkich **nowych pracowników** przyjmowanych do pracy

Bezpieczeństwo vs. polityka przedsiębiorstwa

- **Modele zabezpieczeń**: ochrona wybranych elementów, ochrona całości przedsiębiorstwa
- **Polityka wewnętrzna** powinna zapewniać aktualizacje procedur bezpieczeństwa, analizę zagrożeń oraz ocenę skuteczności stosowanych metod
- **Organizacja firmy** – zaleca się żeby w firmie powstała osobna jednostka organizacyjna zajmująca się bezpieczeństwem i zatrudniająca specjalistów

Bezpieczeństwo vs. polityka przedsiębiorstwa

- **Zatwierdzenie systemu bezpieczeństwa** – zarząd firmy powinien formalnie zatwierdzać najważniejsze dokumenty związane z bezpieczeństwem
- **Kontrola** – specjalna komisja kontroli wewnętrznej systemu bezpieczeństwa powinna systematycznie kontrolować system. Zalecana są także kontrole zewnętrzne
- **Współpraca kierownictwa** – ważne decyzje muszą być podejmowane w porozumieniu z innymi działami i zarządem

Bezpieczeństwo vs. polityka przedsiębiorstwa

- **Odpowiedzialny dobór kadr** na ważne stanowiska związane z bezpieczeństwem
- **Dbałość o pracownika** – pracownik jest najważniejszym i często najsłabszym elementem systemu
- **Współpraca z kontrahentem** wymaga dokładnej kontroli

Projektowanie systemu i procedur bezpieczeństwa

- Etap przygotowania
- Praca nad projektem
- Wyniki projektowania
- Etapy wdrożenia systemu bezpieczeństwa

Etap przygotowania

- **Marketing** – ważne jest poprzez odpowiedni marketing przekonać zarząd i pracowników do konieczności opracowania polityki bezpieczeństwa
- **Różnorodność problemu** – każde przedsiębiorstwo wymaga innych technik i innego podejścia do problemu
- **Opis procesów pracy** zachodzących w przedsiębiorstwie
- **Opracowanie lista obiektów** występujących w firmie wraz z ich dokładnym opisem i ewentualną dokumentacją (np. nieruchomości, obiekty ruchome, narzędzia pracy, pracownicy, dokumenty, itd.)

Praca nad projektem

- **Planowanie**, jaki zakres działalności przedsiębiorstwa będzie chroniony i w jaki sposób
- **Zdefiniowanie źródeł informacji** i drogi jej przekazywania
- **Wybór** różnorodnych **metod zabezpieczeń** (fizycznych, programowych, transmisji, administracyjnych, organizacyjnych) na podstawie aktualnej wiedzy, statystyk, istniejących zabezpieczeń, opinii fachowców, wymogów prawnych
- **Analiza** wprowadzanych **zabezpieczeń i ich wpływu** na procesy pracy. Ewentualna zmiana tych procesów w porozumieniu z kierownictwem poszczególnych jednostek

Wyniki projektowania

- Opis **zakresu** systemu
- Opis przyjętej **polityki bezpieczeństwa**
- Opis **wpływu systemu** ochrony na działanie przedsiębiorstwa
- Lista **obszarów chronionych**
- Lista **procesów i procedur** zdefiniowanych w przedsiębiorstwie
- Opis etapów **wdrażania** systemu
- **Kosztorys** wprowadzenia systemu
- Prezentacja pokazująca **korzyści** wypływające z wdrożenia systemu bezpieczeństwa

Etapy wdrożenia systemu bezpieczeństwa

- Działania **marketingowe** w celu przekonania pracowników i zarządu o potrzebie wdrożenia nowych rozwiązań podnoszących bezpieczeństwo
- Przygotowanie **organizacyjne przedsiębiorstwa** w celu osiągnięcia sytuacji optymalnej dla działania systemu bezpieczeństwa
- **Przeszkolenie kierownictwa** w zakresie: informacji merytorycznych o systemie i wiedzy z zakresu prowadzenia wdrożenia
- **Przygotowanie dokumentacji** (najlepiej dla każdego pracownika)
- **Wprowadzenie podstawowej wersji systemu** bezpieczeństwa obejmującej działania do tej pory już wykonywane, ale nie spisane formalnie

Etapy wdrożenia systemu bezpieczeństwa

- **Wprowadzenie pełnej wersji** pilotażowej systemu bezpieczeństwa w wybranej jednostce organizacyjnej
- **Przeprowadzenie cyklu szkoleń** dla wszystkich pracowników. Zakres szkoleń powinien obejmować: ogólny opis systemu bezpieczeństwa, szczegółowe działanie systemu w poszczególnych jednostkach, szczegółowe omówienie kompetencji i zakresu obowiązków dotyczących każdego stanowiska pracy, przedstawienie wpływu systemu na dotychczas obowiązujące procesy pracy, regulamin pracownika
- **Wprowadzenie systemu** po kolei w każdej jednostce organizacyjnej
- **Zakończenie wdrożenia** i odebranie prac przez kierownictwo

Przykładowe elementy polityki bezpieczeństwa
Przykładowa procedura dla kontroli antywirusowej

Uczestnicy: administrator, operatorzy

Zalecenia:

- Kontrola antywirusowa powinna być przeprowadzana codziennie
- Należy używać dwóch programów antywirusowych
- Komputer powinien być sprawdzany pod względem obecności wirusów po uruchomieniu specjalnej dyskietki bez dostępu do sieci

Kroki:

- Administrator lub operatorzy przeprowadzają kontrolę antywirusową na każdym komputerze
- Po wykrycia wirusa należy natychmiast powiadomić administratora
- Administrator usuwa wirusa i podejmuje korki zaradcze
- Fakt kontroli antywirusowej należy odnotować

Rady dla wdrażających politykę bezpieczeństwa

Rady ekspertów

- Warto zatrudnić **eksperta z zewnątrz** - zwrot z inwestycji jest szybszy, a wdrożony system może oferować oczekiwany poziom bezpieczeństwa i spełniać wymagania prawne i technologiczne
- **Nie** należy **zatrudniać ludzi**, którzy publicznie **chwalą się włamaniami**. Prawdziwi audytorzy przede wszystkim podnoszą poziom bezpieczeństwa, a nie atakują systemu

Rady dla wdrażających politykę bezpieczeństwa

- Członkowie zarządu **powinni uczestniczyć w tworzeniu polityki bezpieczeństwa** i wypełnianiu jej postulatów. Poparcie zarządu pozwala nie tylko uchwalić odpowiedni budżet na bezpieczeństwo, ale też np. wprowadzić wewnętrzne normy i regulaminy oraz wyciągać konsekwencje wobec pracowników, którzy ich nie przestrzegają
- Projekty dotyczące ochrony informacji elektronicznej powinny być oparte na **zarządzaniu ryzykiem**. Najważniejsze jest poprawne określenie zagrożeń i prawdopodobieństwa ich wystąpienia oraz oszacowanie związanego z tym ryzyka. Wynik tych obliczeń należy weryfikować okresowo

Rady dla wdrażających politykę bezpieczeństwa

- Tylko **stałe monitorowanie** działania systemów i realizacji założeń polityki bezpieczeństwa, adaptowanie się do zmian oraz wykorzystanie nowych technologii umożliwia pogodzenie celów biznesowych z bezpieczeństwem IT
- Nieodłącznym elementem bezpieczeństwa są: **audyt i treningi** - wymagają ich międzynarodowe i krajowe normy oraz zalecenia dotyczące bezpieczeństwa informacji elektronicznej. Audyt pozwala na weryfikację obecnego stanu i planowanie dalszych działań biznesowych i technologicznych

Rady dla wdrażających politykę bezpieczeństwa

- Zastosowanie systemu o **prostej architekturze** zwiększa wydajność pracy oraz dostępność, integralność i poufność informacji. System taki można efektywnie kontrolować i łatwiej go rozbudowywać. Jego wdrożenie i eksploatacja jest tańsza niż rozbudowanych rozwiązań
- System zabezpieczeń powinien składać się z **różnych mechanizmów**. Od strony organizacyjnej wprowadza się segregację i podział ról oraz uprawnień dla użytkowników i systemów. Osoba odpowiedzialna za bezpieczeństwo systemu powinna jednak zadbać o zachowanie równowagi między prostotą architektury a liczbą mechanizmów bezpieczeństwa

Rady dla wdrażających politykę bezpieczeństwa

- W stosunku do gotowych produktów należy stosować zasadę **ograniczonego zaufania**. Każde, nawet najlepsze narzędzie może mieć problemy z zagwarantowaniem bezpieczeństwa
- Nawet najprostsze **mechanizmy logujące zdarzenia** mogą okazać się bardzo pomocne w razie incydentu naruszenia bezpieczeństwa

Podsumowanie

- Polityka bezpieczeństwa jest **niezwykle ważnym** dokumentem z punktu widzenia bezpieczeństwa
- Każde przedsiębiorstwo, instytucja **powinno posiadać** taki dokument
- Polityka bezpieczeństwa powinna być **uwzględniana w czasie realizacji** wszystkich **projektów** informatycznych i teleinformatycznych
- Polityka bezpieczeństwa wymaga ciągłych **uaktualnień** wynikających z rozwoju przedsiębiorstwa, instytucji oraz pojawiania się nowych zagrożeń

Dziękuję Państwu za uwagę