enterprise europe network

Wsparcie dla biznesu w zasięgu ręki

RCI LTT

REGIONALNE CENTRUM INNOWACJI i TRANSFERU TECHNOLOGII

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Komisja Europejska

BEZPIECZEŃSTWO **informatyczne**

W dzisiejszych czasach, większość procesów biznesowych wspomaganych jest przez różnego rodzaju systemy informatyczne, które ułatwiają dostęp do ogromu danych i przyczyniają się do podejmowania kluczowych decyzji, dlatego też bezpieczeństwo teleinformatyczne stanowi ważny aspekt w każdym przedsiębiorstwie. Informacje niejawne, które są bezpośrednio powiązane z bezpieczeństwem teleinformatycznym wymagają szczególnej ochrony przed nieuprawnionym dostępem, niepożądanym ujawnieniem, modyfikacją bądź zniszczeniem. Ponieważ pojęcie absolutnego bezpieczeństwa układu jest tylko teorią, nadrzędną cechą dobrze zaprojektowanego systemu informatycznego jest skuteczna ochrona danych wprost proporcjonalna do wartości przechowywanych informacji, przy możliwie jak najprostszym sposobie użytkowania.

I. Standard bezpieczeństwa PN-ISO/IEC 27001:2005.

Dla przedsiębiorstw, które chcą świadomie chronić swoje aktywa, powstała międzynarodowa norma ISO/IEC 27001: 2005 opisująca wymagania stawiane przed Systemami Zarządzania Bezpieczeństwem Informacji (SZBI). Norma ta została przetłumaczona na język polski i wydana przez Polski Komitet Normalizacyjny, jako PN-ISO/IEC 27001: 2007. Standard ten składa się z części podstawowej oraz załączników. Część podstawowa definiuje wszelkie aspekty związane między innymi z: ustanowieniem, zarządzaniem, dokumentacją, odpowiedzialnością, ulepszaniem oraz przeglądami SZBI.

Wszystkie założenia znajdujące się w części podstawowej powinny być spełnione. W normie ISO/IEC 27001: 2005 wyróżniono 11 obszarów mających wpływ na bezpieczeństwo:

- polityka bezpieczeństwa;

Kluczowe fakty i liczby

- Dla przedsiębiorstw, które chcą świadomie chronić swoje aktywa, powstała międzynarodowa norma ISO/IEC 27001: 2005 opisująca wymagania stawiane przed Systemami Zarządzania Bezpieczeństwem Informacji (SZBI).
- Norma ISO 27001 oparta jest na podejściu procesowym i wykorzystuje model: Planuj-Wykonuj-Sprawdzaj-Działaj (PDCA tj. Plan Do Check Act)
- W 2010 roku, ustalono, że likwidacja skutków ataków cyber przestępczości i poniesionych w związku z tym strat przez firmę lub instytucję może sięgać od 237 tysięcy do 52 milionów $.
- Organizacje uczestniczące w badaniu Instytutu Ponemon wskazały, że na przestrzeni roku odbyło się około 205 ataków mocno zagrażających firmie, ale skutki ich działania dostrzegalne były średnio dopiero po czterech tygodniach.

- organizacja bezpieczeństwa informacji;
- zarządzanie aktywami;
- bezpieczeństwo zasobów ludzkich;
- bezpieczeństwo fizyczne i środowiskowe;
- zarządzanie systemami i sieciami;
- kontrola dostępu;
- zarządzanie ciągłością działania;
- pozyskiwanie, rozwój i utrzymanie systemów informatycznych;
- zarządzanie incydentami związanymi z bezpieczeństwem informacji;
- zgodność z wymaganiami prawnymi i własnymi standardami.

Bezpieczeństwo informacji jest sprawą priorytetową i niewątpliwie zaletą standardu jest kompleksowe podejście do tego zagadnienia w zakresie ochrony bezpieczeństwa fizycznego, osobowego, teleinformatycznego oraz prawnego. Norma wskazuje nam te elementy, które należy skonkretyzować w oparciu o analizę ryzyka i pozwala nam na dobranie sposobu zabezpieczenia tych obszarów. Dzięki kompleksowemu podejściu do bezpieczeństwa informacji oraz uogólnionemu charakterowi wymagań, norma może zostać wykorzystana do budowy SZBI zarówno w małych organizacjach, jak i w wielkich koncernach oraz może zostać wykorzystana w różnych sektorach branżowych. Zgodność z wymogami ISO/EIC 27001: 2005 można potwierdzić odpowiednimi certyfikatami.

II. Bezpieczeństwo jako proces

Norma ISO 27001 oparta jest na podejściu procesowym i wykorzystuje model Planuj – Wykonuj – Sprawdzaj – Działaj (PDCA tj. Plan – Do – Check – Act), który jest stosowany dla całej struktury procesów SZBI. Znaczna część obowiązków określonych w procesie zarządzania bezpieczeństwem informacji leży po stronie osób zarządzających infrastrukturą IT, czyli administratorów sieci. Nie wszystkie jednak zadania powinny być wykonywane przez te osoby. Wymagania normy PN-ISO/IEC 27001 zgodnie ze schematem PDCA można podzielić na:

- Planuj - ustanowienie polityki ISMS, celów, procesów i procedur istotnych dla zarządzania ryzykiem oraz doskonalenia bezpieczeństwa informacji tak, aby uzyskać wyniki zgodne z ogólnymi politykami i celami organizacji.
- Wykonuj - wdrożenie i eksploatacja polityki ISMS, zabezpieczeń, procesów i procedur.
- Sprawdzaj - szacowanie i pomiar wydajności procesów w odniesieniu do polityki ISMS, celów i doświadczenia praktycznego oraz dostarczanie raportów kierownictwu do przeglądu.
- Działaj - podejmowanie działań korygujących i zapobiegawczych w oparciu wyniki wewnętrznego audytu ISMS i przeglądu realizowanego przez kierownictwo lub innych istotnych informacji, w celu zapewnienia ciągłego doskonalenia ISMS.

III. Audyt bezpieczeństwa

Ze względu na częste wykrywanie nowych luk w systemie zabezpieczeń używanego sprzętu i oprogramowania, jak i doskonalenie technik w środowiskach przestępczych, bezpieczeństwo przestało być stanem, a jest ciągłym procesem. W związku z tym bardzo ważnym czynnikiem jest stały nadzór i kontrola za pomocą audytu bezpieczeństwa. Celem audytu jest systematyczna, profesjonalna i obiektywna działalność, w wyniku, której otrzymamy ocenę funkcjonowania swoich zasobów IT w zakresie realizacji wytyczonych celów oraz przyjętego systemu kontroli, mającego zapewnić optymalne, efektywne i zgodne z prawem wykorzystanie posiadanych środków. Głównymi częściami audytu są:

- praktyczne sprawdzenie poziomu bezpieczeństwa informacji (testy penetracyjne);
- identyfikacja słabych punktów w systemach i sieci;
- analiza potrzeb w zakresie bezpieczeństwa;
- określenie obszarów systemu i danych wymagających ochrony;
- weryfikacja skuteczności funkcjonujących procesów bezpieczeństwa.

Utrzymanie wysokiego poziomu bezpieczeństwa informacji organizacji wymaga coraz większego nakładu finansowego. W wielu firmach powoływane są osoby, bądź nawet działy, do zarządzania bezpieczeństwem. Wskazane jest zawsze, wykonanie oceny oraz oszacowanie ryzyka przez osobę niezależną od procesu i badanego obszaru - przez niezależnego

audytora. Ocena taka będzie bardziej obiektywna, oparta na faktycznych obserwacjach poczynionych w trakcie audytu, co podkreśli jej wiarygodność. Niezależny audytor zobowiązany jest do ujawnienia wszystkich istotnych faktów związanych z badanym obszarem, co zapewni kompletność oceny. Audyt najczęściej podzielony jest na 4 etapy:

- Etap I - Przygotowanie audytu, w którym zostanie określony rodzaj, cel, zakres oraz harmonogram.
- Etap II - Działania audytowe, na które składać się będzie zebranie, weryfikacja, analiza oraz porównanie dowodów z wzorcami odniesienia.
- Etap III - Wnioski audytowe, czyli opracowanie wyników audytu, sprawdzenie wniosków oraz uzgodnienie i zatwierdzenie raportu.
- Etap IV - Zalecenia audytowe, mające na celu określenie działań korygujących, usunięcie niezgodności oraz walidację działań naprawczych.

Korzyści jakie otrzymujemy z przeprowadzenia audytu, to między innymi większe bezpieczeństwo dzięki wykryciu i usunięciu istniejących problemów, lepsza wydajność pracy wynikająca z zoptymalizowania posiadanej infrastruktury oraz podniesienie poziomu wiedzy i świadomości w obszarze bezpieczeństwa w przedsiębiorstwie. Wszystkie wymienione korzyści przyczynią się do szybszego rozwoju organizacji.

Głównym elementem audytu są testy penetracyjne polegające na przeprowadzeniu symulowanego ataku na wybrany system teleinformatyczny taki jak np.: aplikację, bazę danych, portal internetowy, bądź infrastrukturę sieciową. Głównymi celami testów są: wyszukiwanie podatności, próba zdobycia konkretnej informacji lub też przełamanie konkretnych zabezpieczeń. Ciekawostką jest fakt, iż same testy mogą przekształcać się podczas trwania tego procesu - początkowy atak na aplikację może przerodzić się w testowanie wybranych procesów aplikacyjnych lub innych elementów. Efektem takiej symulacji powinno być zidentyfikowanie jak największej ilości słabych punktów, oraz wskazanie możliwości naruszenia bezpieczeństwa badanego systemu teleinformatycznego.

Testy penetracyjne możemy podzielić na dwie grupy: testy penetracyjne zewnętrzne oraz wewnętrzne. Testy zewnętrzne to wszelkie działania oparte o weryfikację ewentualnych podatności badanego systemu z sieci Internet lub sieci partnerów biznesowych. Swoim działaniem obejmują analizy wycieków haseł, poufnych danych, dostępnych usług sieciowych, konfiguracji usług (np. DNS) oraz analizę skuteczności systemów firewall i routingu. Testy wewnętrzne, natomiast, badają podatności systemu od strony usług oraz infrastruktury IT wewnątrz sieci komputerowej. Swoim zakresem obejmują takie obszary jak: analizę polityki antywirusowej, ujawnienie krytycznych elementów infrastruktury, jawną ocenę konfiguracji routingu i systemu firewall.

Najczęstsze sposoby przeprowadzania testów:

- Crystal Box - atakujący dysponuje pełną wiedzą o systemie, w tym czasami kodem źródłowym, pełną dokumentacją itp.
- Grey Box - atakujący dysponuje pewną wiedzą o systemie, ale bez dostępu do np. pełnej dokumentacji technicznej.
- Black Box - atakujący nie dysponuje prawie żadną wiedzą o atakowanym systemie poza niezbędnym minimum.

Każda z metod ma swoje zastosowanie, np. Crystal Box najczęściej wykonuje się robiąc wewnętrzne testy bezpieczeństwa we własnej firmie. Posługując się tą metodą najprawdopodobniej znajdziemy największą liczbę podatności i zrozumiemy skąd się wzięły. Sposób ten ułatwia także znalezienie metody na ich wyeliminowanie. Podejście Black Box to przeciwieństwo Crystal Box, w którym tester nie posiada żadnych informacji o atakowanym systemie poza niezbędnymi, takimi jak np. adresy IP lub adres strony. Pośrednią metodą testów jest Grey Box, gdzie otrzymujemy pewne informacje, ale nie otrzymujemy pełnej wiedzy o funkcjonowaniu systemu. Jest to sposób najczęściej wybierany przez firmy zewnętrzne.

IV. Złożoność bezpieczeństwa IT

W nowoczesnym świecie systemy IT nie służą już wyłącznie do zaspokajania potrzeb garstki entuzjastów. Zamiast tego, stały się one kręgosłupem teraźniejszego społeczeństwa i co za tym idzie również większości organizacji i przedsiębiorstw. Podatne systemy mogą stanowić zagrożenie dla osób, firm oraz wszelkiego rodzaju nowoczesnej infrastruktury. Nie tworząc kompleksowych rozwiązań pozwalających na podniesienie bezpieczeństwa organizacje ryzykują utratą wartości intelektualnych, wygenerowaniem strat finansowych czy nawet utratą pozytywnego wizerunku marki i pozycji na rynku. W badaniu Instytutu Ponemon przeprowadzonym w celu przybliżenia kosztów cyber przestępczości w 2010 roku, ustalone zostało, że likwidacja skutków ataków oraz poniesionych strat przez firmę lub instytucję może sięgać od 237 tysięcy do 52 milionów dolarów amerykańskich. Co ciekawe organizacje uczestniczące w tym badaniu wskazały, że na przestrzeni roku odbyło się około 205 ataków mocno zagrażających firmie, ale skutki ich działania dostrzegalne były średnio dopiero po czterech tygodniach.

Zgodnie z wynikami przeprowadzonych badań, najtrudniejszym wyzwaniem w zapewnieniu bezpieczeństwa informacjom, było zapanowanie nad złożonością metod i technologii obrony przed ich wyciekiem. Bardzo skomplikowanym zagadnieniem okazało się zachowanie standardów biznesowych, zapobieganie przekazywaniu danych osobom nieuprawnionym przez zatrudnionych pracowników oraz firmy współpracujące. Wniosek z tego badania jest taki, że organizacje coraz częściej rozpoznają potrzebę zmniejszenia złożoności swojego środowiska IT. Niestety najtrudniejszym elementem w realizacji tego celu jest konsolidacja wszystkich produktów

i technologii, które zostały już wdrożone i są używane na co dzień. Innym istotnym faktem wynikającym ze złożoności systemów IT jest to, że pracownicy mogą nie być świadomi lub mieć małą wiedzę na temat procedur bezpieczeństwa informacji biznesowych i polityk z nimi związanych. Istnieje coraz więcej dowodów na to, że brak świadomości wśród pracowników przekłada się na ilość incydentów związanych z wyciekiem informacji poufnych poprzez zaniedbania.

V. Zarządzanie ryzykiem bezpieczeństwa IT

Zarządzanie ryzykiem bezpieczeństwa składa się z trzech następujących procesów: oceny bezpieczeństwa, ograniczania ryzyka oraz ewaluacji i oceny ryzyka. Jest to proces, który pozwala firmom i instytucjom na balansowanie pomiędzy realnymi kosztami operacyjnymi, a kosztami ekonomicznymi różnorodnych mechanizmów ochronnych w celu osiągania możliwie najwyższego zysku ze swojej działalności. Proces ten nigdy nie podlega bezpośrednio pod kadrę IT, a raczej powinien obejmować większość kadry zarządzającej. Co ważne, osoby odpowiedzialne za poszczególne jednostki organizacyjne muszą posiadać narzędzia do realizacji misji. Ponadto kadra zarządzająca musi zawsze określać funkcje i zadania bezpieczeństwa w taki sposób, by ich obecne systemy IT zapewniały odpowiedni poziom obrony przed zagrożeniami w realnym środowisku. Bardzo często zdarza się tak, że poszczególne działy IT mają bardzo napięty budżet, dlatego wydatki związane z zapewnieniem bezpieczeństwa muszą być poddawane przeglądom, analogicznie do wszystkich innych decyzji związanych z zarządzaniem firmą. Należy mieć też świadomość, że dobrze skonstruowana analiza ryzyka, oparta o profesjonalne metodologie oraz stosowana z zachowaniem odpowiedniej dbałości, może pomóc w identyfikacji realnych potrzeb firm i tym samym podnieść jakość zarządzania.

VI. Niebezpieczeństwo biznesu - ocena problemu

Załóżmy, że organizacja poważnie myśli o zapewnieniu bezpieczeństwa swoich informacji i stosuje najlepsze praktyki. Prawdopodobnie ma również specjalistę lub zespół odpowiedzialny za zapewnienie bezpieczeństwa. Zarząd zatwierdził stosowanie polityk bezpieczeństwa i standardów biznesowych, systemy wymagają silnych haseł, może nawet kart inteligentnych czy systemów PKI, a użytkownicy dostali wytyczne i zostali przeszkoleni z zasad ich stosowania. Dział bezpieczeństwa wdrożył dobre rozwiązania, takie jak zapory ogniowe i kompleksowe oprogramowanie antywirusowe. Organizacja ma nawet wdrożone procedury poparte certyfikacją ISO 27001:2005.

Pytanie brzmi: jak bezpieczna jest ta organizacja? Warto zadać sobie w tym momencie kilka kluczowych pytań, doprecyzowujących zagadnienie:

- Jak bardzo doświadczony i kompetentny jest zespół odpowiedzialny za zapewnienie bezpieczeństwa teleinformatycznego i bezpieczeństwa informacji. Czy zespół jest technicznie wykwalifikowany i czy posiada doświadczenie w zarządzaniu bezpieczeństwem? W jakim stopniu zespół dostał wsparcie kierownictwa w kwestiach organizacji polityki bezpieczeństwa informacji? Jakie ma cele i jakie ma procedury kontroli?
- Czy wszyscy pracownicy rozumieją i wykonują zalecenia zapisane w politykach bezpieczeństwa i przestrzegają jej sumiennie?
- Czy zespół, który wdrożył techniczne rozwiązania, sprawdza je pod względem nowych zagrożeń? Czy rutynowo instaluje poprawki bezpieczeństwa i testuje system?

Wszystkie powyższe pytania dotyczą ludzi, a nie technologii. Oczywiście bardzo ważne jest wdrożenie silnych zapór ogniowych. Jednak biorąc pod uwagę fakt, że większość komercyjnie oferowanych zapór jest porównywalnych pod względem bezpieczeństwa, warto zadbać o to, by być pewnym, że są one właściwie skonfigurowane, monitorowane i zarządzane przez odpowiednich specjalistów. Takie same argumenty dotyczą większości rozwiązań łącznie z rozwiązaniami antywirusowymi, infrastrukturą PKI czy systemami IDS i IPS.

Przyglądając się problemowi bezpieczeństwa, należy mieć na uwadze to, że należy inwestować w równym stopniu w technologie i w ludzi.

Wydawca:

RCI LTT
REGIONALNE CENTRUM INNOWACJI i TRANSFERU TECHNOLOGII
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Regionalne Centrum Innowacji
i Transferu Technologii

tel./fax +48 91 449 43 54
innowacje@zut.edu.pl
www. innowacje.zut.edu.pl