ISMS – information security management system

Politiky, procedury, postupy, odpovídající zdroje a aktivity, mající za cíl chránit aktiva společnosti.

Kroky nutné k implementaci, monitorování, udržování a zdokonalování ISMS:

- identifikace informačních aktiv a jim odpovídajících bezpečnostních požadavků
- analýza bezpečnostních rizik a jejich ošetření
- výběr a implementace opatření (controls) k ošetření neakceptovatelných rizik
- monitorování, udržování a zlepšování afektivnosti opatření určených k ochraně aktiv

uvedené kroky musí být pravidelně opakovány, aby byly identifikovány změny v rizicích, strategiích organizace, nebo jejích obchodních cílech.

Bezpečnostní požadavky mohou být identifikovány na základě:

- identifikovaných informačních aktiv a jejich hodnoty
- požadavků organizace na zpracování informací, jejich ukládání a přenášení (komunikace)
- právních, regulačních a smluvních požadavků

Metodický přístup k rizikům zahrnuje analýzu hrozeb informačním aktivům, zranitelností a pravděpodobností, že se hrozba stane reálnou. Dále zahrnuje analýzu potenciálu dopadu případného incidentu na aktiva. Náklady na relevantní opatření by měly být proporcionální dopadu incidentu.

Metodologie řízení rizik je nastíněna v ISO/IEC 27005 a v lekci “Analýza rizik”.

Před tím, než dojde k procesu ošetřování rizik, musí být stanovena kritéria pro rozhodování, zda může být riziko akceptováno, či nikoli. Rizoko může být například akceptováno pokud je nízké, nebo pokud je cena za jeho ošetření pro organizaci neekonomická. Tato rozhodnutí musí být zaznamenána.

Každé identifikované riziko musí být ošetřeno. Např.:

- aplikováním odpovídajících opatření snižujících riziko
- akceptováním rizika v souladu s kritérii organizece pro akceptování rizik
- vyhnutí se riziku, eliminací (zákazem) akcí, které mohou riziko vyvolat
- sdílením rizika s dalšími stranami (pojišťovny, dodavatelé)

Příklady široce akceptovaných opatření lze nalézt v ISO/IEC 27002:2005

Opatření musí být součástí požadavků na systémy a projekty již ve fázi návrhu.

Faktory úspěšné implementace ISMS:

- politika informační bezpečnosti, cíle a aktivity nutné k dosažení cílů
- postup a framework návrhu, implementace, monitorování, udržování a zlepšování informační bezpečnosti v souladu s firemní kulturou
- viditelná podpora všech úrovní řízení, obzvláště vrcholového managementu
- porozumění požadavkům na ochranu informačních aktiv, dosažené aplikací řízení

bezpečnostních rizik
- povědomí o informační bezpečnosti napříč společností, program vzdělávání, informování všech zaměstnanců o jejich relevantních povinostech ve vztahu k bezpečnosti (na základě politik a standardů) a jejich motivace
- efektivní proces řízení incidentů
- efektivní proces business continuity
- systém metrik umožňující měřit výkonnost a efektivnost systému řízení bezpečnosti a poskytující informace využitelné ke zlepšení

Přehled některých standardů ISO/IEC:

27000 Celkový přehled a definice termínů
27001 Požadavky na ISMS
27002 Implementace opatření
27003 Návod k implementaci ISMS
27004 Metriky ISMS
27005 Řízení rizik

Bezpečnostní politiky

Můžeme tvořit sami, pokud víme čeho chceme dosáhnout.

Můžeme vycházet z norem.

Můžeme vycházet ze šablon.
http://www.sans.org/security-resources/policies/

Můžeme vycházet z již vytovořených politik a upravovat je.
http://www.princeton.edu/oit/it-policies/it-security-policy/

Při tvorby politik bychom však měli mít stále na mysli:

Musíme identifikovat a klasifikovat informace, které chceme chránit.
Musíme identifikovat potenciální nebezpečí, která jim hrozí.
Musíme definovat úroveň ochrany, kterou chceme zajistit.

Definování bezpečnostní politiky a její implementace je proces, který není nikdy zcela dokončen.

Politiku by neměl vytvářet jediný člověk (typicky pracovník bezpečnosti). Na její tvorbě by se kromě oddělení bezpečnosti měli podílet také zástupci provozu IT, vývoje, ale stejně tak zástupci z obchodního a finančního oddělení. Politika by měla podporovat procesy těcho oddělení a ne jim působit komplikace.

Bezpečnostní politika musí mít bezpodmínečně podporu u vedení společnosti. Vedení musí jasně deklarovat, že definované politiky podporuje, že vyžaduje jejich naplnění a že jsou důležité pro chod společnosti.

S politikou musí být seznámen každý, koho se týká.

Politika nesmí být tak přísná, aby narušovala/omezovala chod společnosti a musí být vynutitelná.

Jinak ji budou zaměstnanci ignorovat.

Existuje základní, nikdy nekončící cyklus životnosti politiky:

1) VYHODNOCENÍ
2) TVORBA POLITIKY
3) IMPLEMENTACE POLITIKY

VYHODNOCENÍ

Kategorizace dat, vyhodnocení hrozeb, potřeb uživatelů, bezpečnostních nástrojů a analýza zhodnocení investic.

Kategorizace dat:
- kde se data nacházejí
- kdo s nimi pracuje (kdo k nim má mít přístup)
- kdo je za ně odpovědný
- jak jsou důležitá (jakou mají hodnotu, co by se stalo, kdyby byla ztracena/ukradena)

Analýza bezpečnostních hrozeb:
- hrozby z vnějšku
- hrozby z vnitřku organizace

Neoprávněné získání přístupových údajů
Odposlech (síť, keylogger, bezdrátové technologie, tempest, fyzický)
Neoprávněný přístup klient/server (zcizená hesla, zneužití chyb, MIM, zákeřný kód, sociální inženýrství)
Výpadek služby
Fyzický přístup

Dopad hrozeb na fungování firmy

- finanční ztráty
- propad prodejů
- ztráta konkurenceschopnosti
- ztráta dobrého jména
- narušení normálního fungování
- úniky dat
- nedodržení legálních požadavků

Dopady je vhodné klasifikovat ve třech stupních:

- očekávaný dopad
- nejhorší možný dopad (maximální ztráty)
- nejlepší možný dopad

a měly by být promítnuty do finančních nákladů.

Pozor. Nasazení některých technologií s cílem osdtranění hrozby může vést k získání nových obchodních příležitostí.

Výběr zabezpečovacích mechanizmů a odpovídajících nástrojů

- autentikace (jednoznačná identifikace uživatele)
- autorizace (řízení přístupu k datům)
- ochrana integrity dat
- zabezpečení dat proti odposlechu
- implementace mechanizmů neodmítnutelné zodpovědnosti
- fyzická bezpečnost
- pravidelná školení uživatelů
- monitorování systémů
- bezpečnostní testy

Analýza návratu investic.

Můžeme například zjistit, že cena implementace zabezpečení konkrétních systémů/dat převyšuje maximální možné ztráty při jejich narušení/ztrátě.

TVORBA BEZPEČNOSTNÍ POLITIKY

Politika by měla obsahovat:

Průvodní informace od vedení.
Účel politiky
Odpovědnosti a pravomoci
Základní pojmy
Informace o vlastnictví a právu přístupu k datům
Pravidla používání výpočetních systémů
(slouží primárně k pracovním účelům, kdy a jak pokud vůbec mohou být používány k osobním účelům, zodpovědnost uživatelů za autentizační údaje, atd.)
Řízení přístupu
- identifikace a autentizece
- bezpečné uchovávání autentizačních údajů
- administrace účtů
- privilegovaný přístup
- přístup osob, které nejsou v zaměstnaneckém poměru
- vzdálený přístup k interní síti
- počítače bez dozoru
- nefiremní počítače (v osobním vlastnictví apod.)
- přimá komunikace (modemy, acces pointy)
- řízení přístupu k samostatným počítačům

Email
- privátnost informací
- šifrování zpráv
- monitorování
- předávání zpráv
- archivace zpráv

Přenosná zařízení
- prevence krádeže
- identifikace zařízení ve vlastnictví společnosti

- odpis zařízení
- postup v případě ztráty
- řízení přístupu
- odposlech
- šifrování (přenosu a lokálních dat)
- škodlivý kód (bezpečné chování a detekce)

Vracení a opravy a likvidace zařízení a přenosných médií
Software
- přístupy
- aktualizace
- licence
- osobní použití
- neautorizovaný software
- antivirová ochrana
- change management

Veřejné sítě (Internet)
- upload/download
- řízení přístupu
- šifrování
- privátnost
- využívání k osobní potřebě
- prezentace na veřejnosti

Síť
- směrovače a firewally (filtrování, směrování podle obsahu)
- rozdělení na zóny
- zcela oddělené sítě
- modemy, access pointy
- řízení přístupu

Fyzická bezpečnost
- pracovní stanice
- servery
- přenosné počítače
- síťová infrastruktura

Auditing a monitorování
- auditní záznamy a logy
- IDS
- honeypot

Vzdělávání uživatelů

Havarijní plán
- zálohy a obnova
- redundance
- zotavení po katastrofě
- řešení bezpečnostních incidentů

Disciplinární řízení

IMPLEMENTACE POLITIKY

- všeobecná informovanost
- zavedení politiky (kontrolní mechanizmy)
- přehodnocování politiky