KYBERNETICKÁ BEZPEČNOST

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt OPVK Vzdělávací modul Kybernetická bezpečnost

KYBERNETICKÁ BEZPEČNOST

Základní kurz kybernetické bezpečnosti

NETWORK SECURITY MONITORING CLUSTER 2015

Tento modul je financován jako projekt v rámci 5. výzvy z prostředků ESF a státního rozpočtu ČR pod registračním číslem CZ.1.07/3.2.04/05.0014.

Seznam spolupracovníků:

Pavel Minařík

minarik@invea.cz

Lukáš Vondráček

vondracek@elat.cz

Petr Mikšovič

petr.miksovic@sovanet.cz

Petr Lacina

placina@uniscomp.cz

Petr Linke

petr.linke@novicom.cz

Projekt OPVK “Vzdělávací modul Kybernetická bezpečnost”

Reg.č. CZ.1.07/3.2.04/05.0014

1. ÚVOD DO PROBLEMATIKY KYBERNETICKÉ BEZPEČNOSTI

KYBERNETICKÁ BEZPEČNOST A OCHRANA DAT[1]

Pojem informační bezpečnosti staví na definici bezpečné informace, tedy takové, jejíž důvěrnost, integrita a dostupnost jsou zachovány. Důvěrností se rozumí zajištění, že informace jsou přístupné pouze těm, kdo jsou k přístupu oprávněni, integrita znamená zajištění správnosti a úplnosti informací a metod jejich zpracování a konečně dostupnost informace je totéž, co její použitelnost pro oprávněné uživatele v okamžiku potřeby.

Protože se jedná o velice důležitou součást našeho každodenního života, není divu, že pro řízení informační bezpečnosti zanedlouho vznikla ustálená měřítka a pravidla, společně definované v obecně uznávaných standardech jak pro nástroje, tak i pro postupy, jakými lze vhodně míry informační bezpečnosti dosáhnout.

Evropské i americké pojetí bezpečnosti informací si jsou blízké a posuzování shody s požadavky se stalo součástí nadnárodních akreditačních a certifikačních schémat. Stabilizaci jistě napomáhá také vývoj v oblasti systémů zajištění jakosti. Po přibližně třiceti letech opět vystupuje do popředí myšlenka integrovaného, dříve komplexního, řízení firem. Spojení analogických požadavků a návodů pro oblasti životního prostředí, zajištění kvality, technické bezpečnosti, obecné bezpečnosti, ochrany zdraví a také informační bezpečnosti je na pořadu dne při aktualizaci norem řady ISO 9000. V jaderném průmyslu se ledy pohnuly dokonce dříve a Mezinárodní atomová agentura ve Vídni právě vydává požadavky na manažerské systémy pro bezpečnost, ochranu zdraví, ochranu životního prostředí, průmyslovou bezpečnost, systém zajištění kvality a ekonomiku.

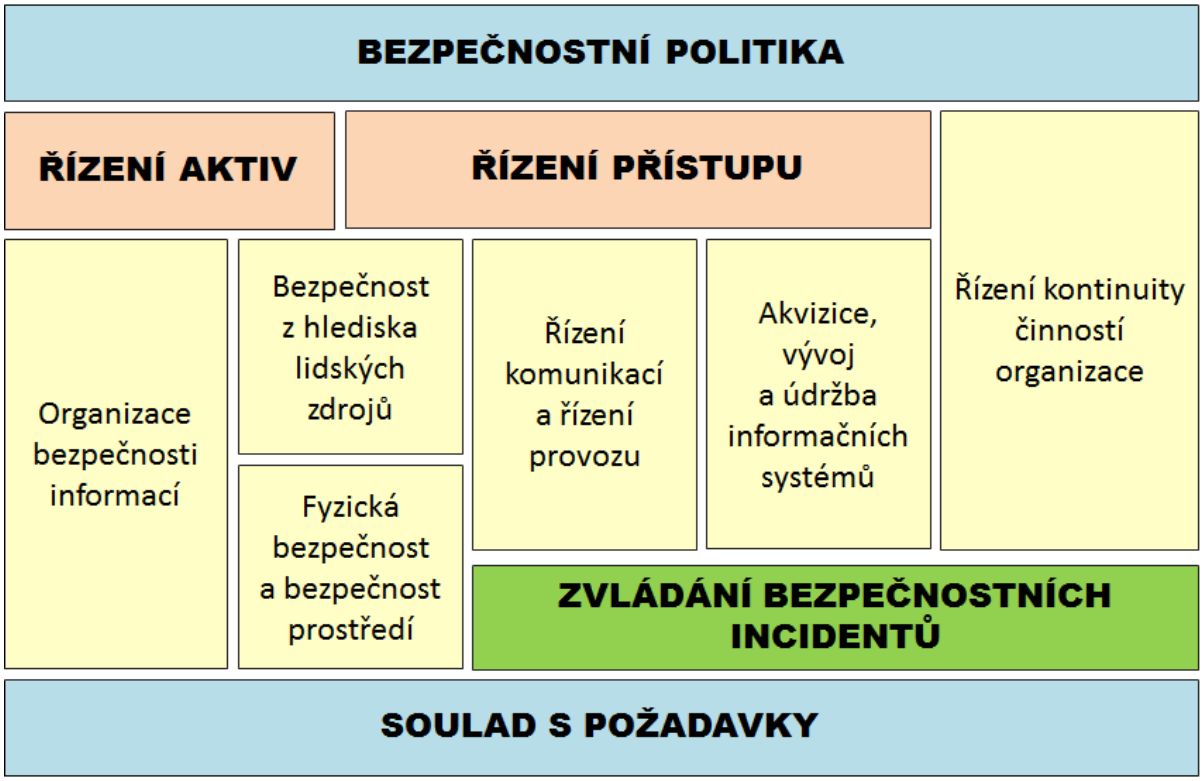
1.1.1. SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

[1] Bezpečnost informací, F. Kostiha, Ikaros – Elektronický časopis o informační společnosti 2006. Převzato z: http://ikaros.cz/bezpecnost-informaci.

Kritéria pro zavedení systému definuje ČSN ISO/IEC 27001:2014. ISMS – Information Security Management System/Systém řízení bezpečnosti informací. Informační technologie - Bezpečnostní techniky - Požadavky.

Dokumentem, který definuje nejlepší zkušenosti se zavedením ISMS je ČSN ISO/IEC 27002:2014. Informační technologie - Bezpečnostní techniky - Soubor postupů pro řízení bezpečnosti informací.

V tomto dokumentu jsou opatření rozdělena do 11 oblastí – viz obrázek.



Obrázek 2 - Oblasti bezpečnosti

Zdroj: Systém řízení bezpečnosti informací - ISMS dle ISO/IEC 27001, S. Krausova, 2010, dostupné z: http://www.krausova.eu/userfiles/image/ISMS_Oblasti.png

Oblasti bezpečnosti

Seznam oblastí:

a) Bezpečnostní politika;
b) Organizace bezpečnosti informací;
c) Řízení aktiv;
d) Bezpečnost z hlediska lidských zdrojů;
e) Fyzická bezpečnost a bezpečnost prostředí;
f) Řízení komunikací a řízení provozu;
g) Řízení přístupu;
h) Nákup/akvizice, vývoj a údržba informačního systému;
i) Zvládání bezpečnostních incidentů;
j) Řízení kontinuity činností organizace;
k) Soulad s požadavky.

Podle normy ISO 27001 ISMS specifikuje požadavky na ustavení, zavedení, provoz, monitorování, přezkoumání, udržování a zlepšování dokumentovaného systému řízení bezpečnosti informací v kontextu celkových činností dané organizace. Návrh a zavedení systému v organizaci jsou podmíněny potřebami a cíli činností (business), požadavky na bezpečnost, používanými procesy, velikostí a strukturou organizace. Systém stanovuje konkrétní požadavky na zavedení bezpečnostních opatření s možností úpravy podle potřeb konkrétní organizace nebo jejich částí. Systém řízení bezpečnosti informací je navržen tak, aby zajistil odpovídající a přiměřená bezpečnostní opatření chránící informační aktiva a poskytl odpovídající jistotu zainteresovaným stranám. Požadavky jsou obecně použitelné a jsou aplikovatelné ve všech organizacích bez ohledu na jejich typ, velikost a povahu činností.

Systém řízení bezpečnosti informací je aplikovatelný na jakýkoliv druh informací vedených na libovolném nosiči dat. Systém, v souladu s požadavky organizace a příslušných právních předpisů, umožňuje:

- definovat politiku, cíle a hranice systému,
- identifikovat informační aktiva a přístup k nim,

- identifikovat hrozby pro tato aktiva,
- specifikovat a zavést řízení rizik bezpečnosti informací,
- předcházet ztrátě, poškození nebo krádeži aktiv,
- zajistit fyzickou bezpečnost a bezpečnost prostředí,
- zavést postupy pro rychlou detekci a reakci na bezpečnostní incidenty,
- zavést bezpečnostní opatření,
- zavést programy školení a informovanosti zaměstnanců,
- monitorovat a přezkoumávat účinnost zavedeného systému.

(Viz obr. 7)
Mezi největší výhody zavedení a případné certifikace systému řízení bezpečnosti informací patří:

- soulad s legislativními požadavky (Zákon č. 101/2000 Sb., o ochraně osobních údajů)
- vybudování systémového přístupu k ochraně informací,
- snížení rizik s únikem či zneužitím důvěrných informací,
- zlepšení důvěry zákazníků a zvýšení image firmy.

V evropském civilizačním kontextu je postup pro zajištění ochrany informací dle ISO/IEC 27xxx obecně přijatým a zavedeným postupem.

Zajištění kybernetické bezpečnosti proto, společně s některými dalšími opatřeními, v podstatě naplňuje požadavky Zákona o kybernetické bezpečnosti (zákon 181/2014 Sb., účinný od 1.1.2015).

1.1.2. BEZPEČNOSTNÍ POLITIKA

Bezpečnostní politika (BP) je jedním ze stěžejních dokumentů organizace při zavádění ISMS. Jedná se o proklamativní dokument, kterým organizace vyjadřuje svůj postoj k řízení bezpečnosti informací. **Bezpečnostní politika by nám měla tedy především odpovědět na otázku, proč ISMS zavádíme.** Cílem tohoto

dokumentu je definovat směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky organice, příslušnými zákony a regulatorními požadavky.

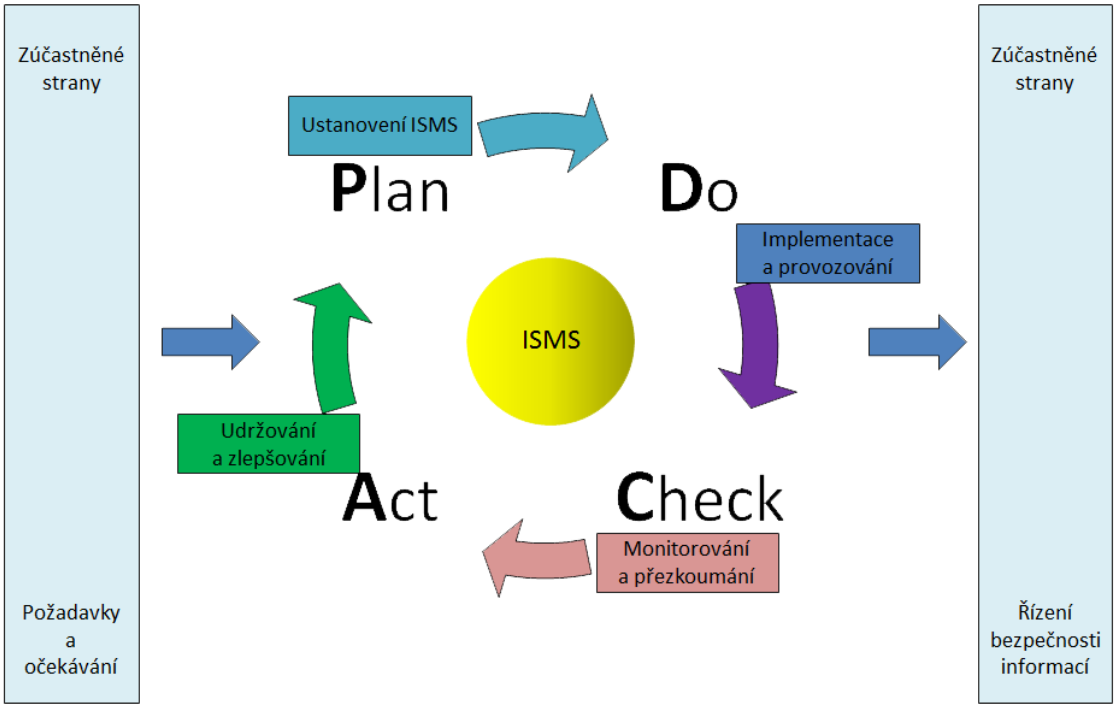
Z pohledu zaváděné ISMS normy jsou předepsána dvě opatření:

- První ukládá vytvoření dokumentu: „Dokument bezpečnostní politiky informací by měl být schválen vedením organizace, vydán a dán na vědomí všem zaměstnancům a relevantním třetím stranám."
- Druhé ukládá pravidelné přezkoumávání a aktualizaci bezpečnostní politiky informací vedením: „Pro zajištění její neustálé použitelnosti, přiměřenosti a účinnosti by bezpečnostní politika informací měla být přezkoumávána v plánovaných intervalech a vždy když nastane významná změna."

ISMS je podobně jako ostatní systémy řízení založen na metodice PDCA (Plan/Plánuj – Do/Dělej – Check/Kontroluj – Act/Jednej). Využití tohoto modelu pro ISMS je zachyceno na obrázku č. 3.

Jsou na něm definovány čtyři následující etapy celého životního cyklu ISMS:

- **Ustanovení ISMS** – vymezení rozsahu a hranic ISMS, stanovení jasného manažerského zadání, vyhodnocení rizik a výběr nezbytných bezpečnostních opatření.
- **Implementace a provoz ISMS** – vhodně a systematicky prosadit vybraná bezpečnostní opatření (dle normy) pro organizaci.
- **Monitorování a přezkoumání ISMS** – zajištění zpětné vazby a pravidelné sledování a hodnocení úspěchů i nedostatků řízení bezpečnosti informací.
- **Údržba a zlepšování ISMS** – realizace možností zlepšování systému řízení bezpečnosti informací ať už soustavným zlepšováním systému nebo odstraňováním zjištěných slabin a nedostatků.



Obrázek 3 - Procesní přístup k ISMS

Zdroj: vlastní zpracování dle normy ISO 27001

1.1.3. ROZSAH A HRANICE ISMS

Při ustanovení ISMS organizace definuje rozsah a hranice ISMS na základě posouzení specifických rysů svých činností, svého uspořádání, struktury, umístění (lokality), aktiv a technologií, včetně důvodů pro vyjmutí z rozsahu ISMS. Z toho vyplývá, že ISMS se nutně nemusí vztahovat na celou organizaci. Zpravidla se tedy ISMS implementuje pro danou lokalitu/lokality a nebo pro daný informační systém.

1.1.4. PROHLÁŠENÍ O APLIKOVATELNOSTI

Dokumentované prohlášení popisuje cíle opatření a jednotlivá bezpečnostní opatření, která jsou relevantní a aplikovatelná v rámci ISMS organizace. Opatření jsou uvedena v příloze A normy. Výběr cílů opatření a jednotlivých bezpečnostních opatření musí být proveden a zdůvodněn na základě výsledků procesů hodnocení a zvládání rizik. Při výběru musí být zohledněna kritéria pro akceptaci rizik, stejně tak

jako požadavky legislativy, regulatorní a v neposlední řadě i požadavky smluvní. Prohlášení o aplikovatelnosti musí obsahovat následující cíle a opatření:

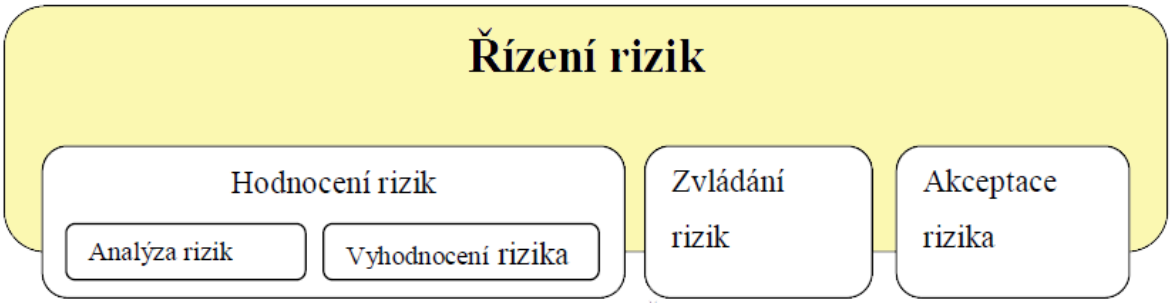
1. cíle opatření a jednotlivá bezpečnostní opatření vybraná a důvody pro jejich výběr;
2. cíle opatření a jednotlivá bezpečnostní opatření, která jsou již v organizaci implementována;
3. vyřazené cíle opatření a jednotlivá vyřazená bezpečnostní opatření uvedená v příloze A, včetně zdůvodnění pro jejich vyřazení.

POZNÁMKA

Prohlášení o aplikovatelnosti definuje, jakým způsobem bude naloženo s riziky, která jsme identifikovali. Zdůvodnění pro vyřazení cílů a jednotlivých opatření k těmto cílům nám tak poskytuje zpětnou vazbu, zda nebyly vyřazeny omylem.

1.1.5. HODNOCENÍ A ZVLÁDÁNÍ RIZIK

Řízení rizik je klíčovým nástrojem pro systémové řízení bezpečnosti. Přesná znalost rizik tak rozhoduje o výběru a prosazení bezpečnostních opatření pro snížení dopadů těchto rizik. Je tedy více než zřejmé, že řízení rizik je základem pro každý systém ISMS. Analýza a řízení rizik slouží jako nástroj pro ochranu investic vynaložených do informačních systémů.



Obrázek 4 - Řízení rizik

Zdroj: vlastní zpracování NSMC

Při hodnocení rizik identifikujeme a kvantifikujeme rizika a určujeme důležitost jednotlivých rizik. Přitom bereme ohled na kritéria pro jejich akceptaci a na cíle organizace. Výstupem z hodnocení rizik pak jsou doporučení a priority řízení jednotlivých rizik a priority implementace zvolených opatření na ochranu proti těmto

rizikům. V případě potřeby se proces hodnocení rizik a proces výběru vhodných opatření opakovaně použije pro různé části organizace nebo pro jednotlivé informační systémy. Při hodnocení rizik rovněž odhadujeme velikost rizika. Odhadnutá rizika porovnáváme se stanovenými kritérii pro určení jejich důležitosti. Hodnocení rizik provádíme metodicky (aby výsledky jednotlivých hodnocení byly srovnatelné a reprodukovatelné) v pravidelných intervalech. Tak zjistíme změny v bezpečnostních požadavcích a změny z pohledu rizik. Jedná se např. o změny aktiv, hrozeb, zranitelností, dopadů, vyhodnocení rizik, včetně významných organizačních změn. Rozsah hodnocení rizik může, dle potřeby, zahrnovat celou organizaci, část/části organizace, vybraný informační systém, specifické prvky systému a nebo tam kde je to proveditelné, reálné a užitečné, včetně služeb.

Obrázek 5 - Analýza rizik

Zdroj: Analýza rizik: Jemný úvod do analýzy rizik, M. Čermák, 2010, dostupné z: http://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/.

Než stanovíme způsob zvládání rizika, měli bychom stanovit kritéria, na základě kterých určíme, jestli je riziko pro naši organizaci akceptovatelné. Riziko můžeme akceptovat například proto, že je nízké anebo že jeho zvládnutí bude pro organizaci

nákladově neefektivní. Taková rozhodnutí je nutné dokumentovat – vedeme o nich záznamy. Po provedeném hodnocení rizik je nutné učinit rozhodnutí, jak s identifikovanými riziky naložíme.

Příklady jak je možné naložit s identifikovanými riziky:

a) aplikace vhodných opatření, kterými snížíme velikost rizika;

b) vědomá a objektivní akceptace rizika, pokud je tak učiněno v souladu s bezpečnostní politikou organizace a kritérii pro akceptaci rizika;

c) vyhnutí se riziku zamezením činností, které jsou příčinou jeho vzniku;

d) přenesení rizika na jiný subjekt (např. pojišťovny, dodavatele).

Pokud jsme učinili rozhodnutí o zvládání rizik formou aplikace vhodných opatření, výběr těchto opatření by měl být proveden v souladu s požadavky identifikovanými v rámci hodnocení rizik. Opatření by nám měla zaručit snížení rizik na přijatelnou úroveň.

Měli bychom ovšem zohlednit:

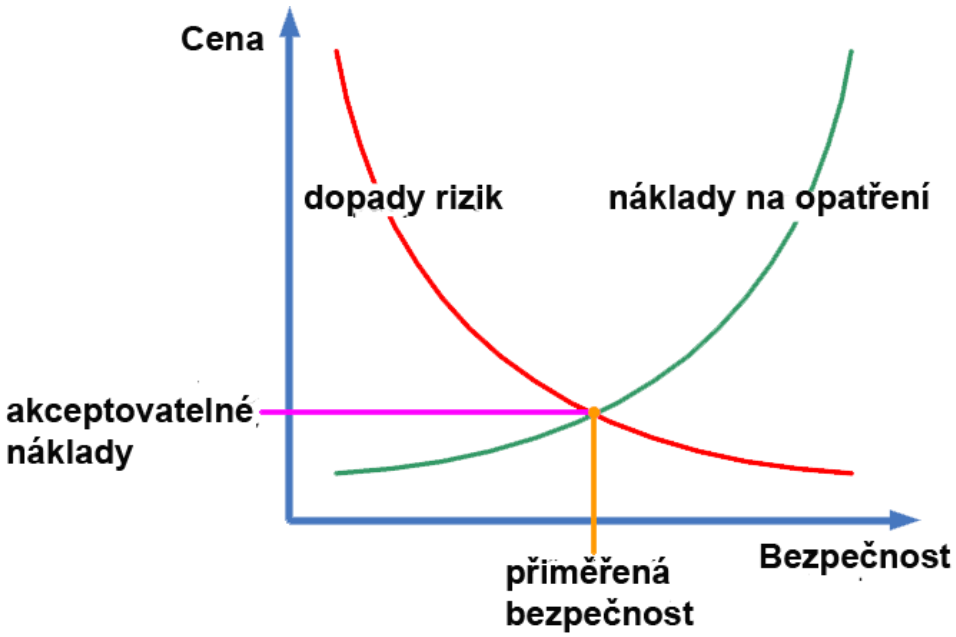
a) požadavky a omezení národní a mezinárodní legislativy a předpisů;

b) cíle organizace;

c) provozní požadavky a omezení;

d) cenu za implementaci a provozní náklady spojené s přijetím opatření na snížení rizik, dle požadavků a omezení organizace;

e) potřebu udržovat rovnováhu mezi investicemi spojenými s implementací a provozem opatření a případnými škodami způsobenými selháním bezpečnosti.



Obrázek 6 - Přiměřená bezpečnost z pohledu akceptovatelných nákladů

Zdroj: převzato z Problematika ISMS v manažerské informatice, V. Ondrák, P. Sedlák, V. Mazálek, 2013. ISBN 978-80-7204872-4.

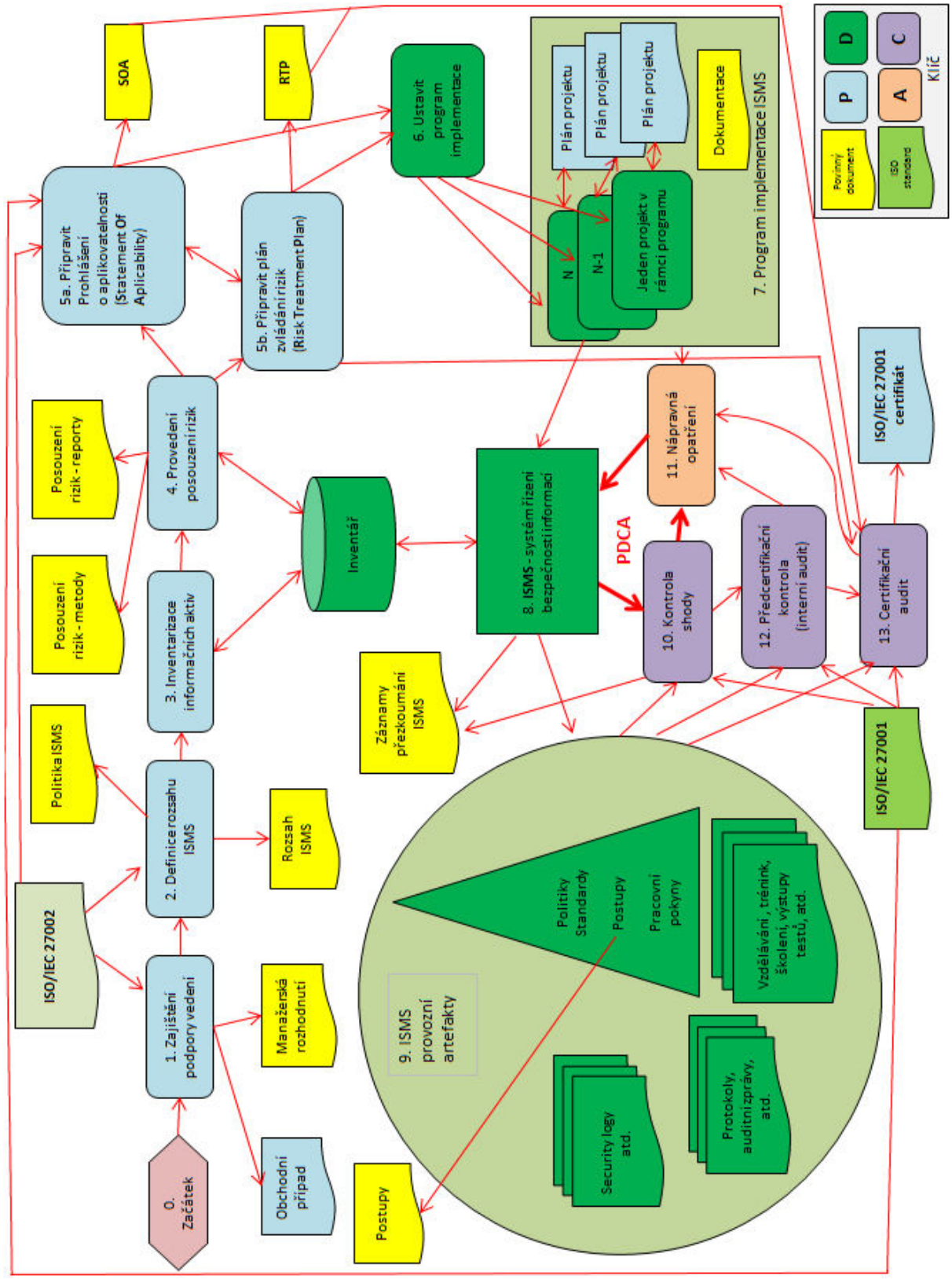
Opatření bychom měli vybírat již ve fázi návrhu nového systému a při specifikaci požadavků na projekt jeho implementace. Nedodržení tohoto pravidla může znamenat dodatečné zvýšení nákladů na implementaci, zavedení méně účinných opatření a řešení, případně neschopnost dosažení požadované úrovně bezpečnosti informací. Zajištění komplexní bezpečnosti není pouze o implementaci nějakého souboru opatření. Současně je nezbytné zavést řídící činnosti pro monitorování a vyhodnocování systému, zlepšování jeho výkonnosti a zlepšování účinnosti zavedených bezpečnostních opatření.

1.1.6. SHRNUTÍ

Kybernetická bezpečnost je rostoucí měrou stále významnější složkou bezpečnosti jako celku. Míra její komplexnosti odpovídá tomu, jak expanduje využívání informačních a komunikačních technologií v běžném životě pro stále širší škálu úloh. Bezpečnost ale není jen pocit. Je to vymezený pojem a i v oblasti kybernetické bezpečnosti existuje společný výklad pro pojmy dané problematiky. I přes to, že v rámci kyberprostoru se vyskytuje řada entit, které nemají vlastnosti zcela ekvivalentní tomu, jak je chápeme v reálném světě (například je obtížné určit hranice nebo identifikovat „útočníka“), existuje zřejmá vůle chránit oprávněné národní nebo společenské zájmy i v tomto prostoru. Využívá se při tom postupů, jež genericky vyrostly a osvědčily se již dříve, byť méně formálně, v komunitní spolupráci (spolupráce týmů) a rovněž postupů, jež jsou osvědčeny pro řízení bezpečnosti obecně.

Klíčové pojmy

bezpečnost, pojmosloví, terminologie, výklad, definice, kyberprostor, hranice, identifikace subjektu, kyberprostor, CSRIT, CERT, ISMS, systém řízení bezpečnosti informací



Obrázek 7 - Zavedení ISMS

Zdroj: upraveno a převzato z ISO/IEC 27003.

Kontrolní otázky

Kontrolní otázky slouží k ověření nastudovaných znalostí. Jsou součástí testu po prostudování každé kapitoly, kde jsou uvedeny i správné odpovědi.

Co znamená vymezení hranic ISMS?

a) Určení místa, kde je naše počítačová síť připojena k internetu.
b) Určíme fyzické a organizační meze pro implementaci ISMS.
c) Rozlišení prostor, kde se nachází ICT.

Co si představíte pod zkratkou PDCA?

a) Jedná se o metodiku, která se používá při zavedení ISMS.
b) Jedná se o metodiku pro evidenci aktiv.
c) Jedná se o metodiku pro určení hrozeb.

Uveďte nejméně 5 aktiv identifikovaných ve Vaší organizaci.

Kdo je garantem naplnění ZoKB?

a) Národní centrum kybernetické bezpečnosti.
b) Centrální bezpečnostní úřad.
c) Národní certifikační centrum bezpečnějšího internetu.

Co znamená zkratka NBÚ?

a) Národní vzdělávací úřad pro kybernetickou bezpečnost.
b) Národní certifikační úřad pro kyberneticko ubezpečnost.
c) Národní bezpečnostní úřad.

Jaká je vazba mezi NBÚ a NCKB?

a) Jsou to dvě rozdílné organizace.
b) Jedná se o jednu organizaci.
c) Jedná se o dvě podobné organizace. NBÚ má sídlo v ČR, NCKB na Slovensku.

Ze které normy čerpá ZoKB?

a) ZoKB čerpá z ČSN ISO/IEC 27001:2014.

b) ZoKB čerpá z ČSN ISO/IEC 21001:2014.

c) ZoKB čerpá z ČSN ISO/IEC 22001:2014.