Řízení informační bezpečnosti

PV017

Kamil Malinka
(využity materiály Doc. Staudka a konzultace Prof. Matyáše)
Verze: podzim 2023

Osnova

- Legislativa informační bezpečnosti
- Standardy (normy) informační bezpečnosti
  - Terminologie
  - Rodina standardů ISO/IEC 27000
  - Standard NIST, rodina SP 800
  - Certifikace
- Řízení rizik
- Politika informační bezpečnosti

Legislativa informační bezpečnosti

Pavel Loutocký

Standardy (normy) informační bezpečnosti

Osnova

- Legislativa informační bezpečnosti
- Standardy (normy) informační bezpečnosti
  - Terminologie
  - Rodina standardů ISO/IEC 27000
  - Standard NIST, rodina SP 800
  - Certifikace
- Řízení rizik
- Politika informační bezpečnosti

Standardy (normy) a legislativa

- Cíl přednášky o standardech a standardizaci - umět odpovědět na otázky:
  - Co to jsou standardy, normy, doporučení?
  - Jak vznikají standardy a doporučení?
  - Kdo je kdo ve světě standardů a doporučení ?
  - Které standardy informační bezpečnosti jsou reprezentativní ?
- Standardizační organizace a principy jejich činnosti a působení
- Upozornění na hlavní de iure standardy InfoSec

Standard, norma, doporučení = dokumentovaná úmluva 1/4

- Úmluva
  - O technické specifikaci nebo
  - O jiném podobném přesně stanoveném kritériu
- Cíl úmluvy
  - Pravidlo/směrnice definující charakteristické vlastnosti materiálů, výrobků, procesů, služeb, …
  - Standardy lze použít jako měřítko pro porovnávání nebo dokonce hodnocení
  - Umožňuje, aby materiály, výrobky, procesy, služby, … byly takové, jaké se zamýšlí, že mají být
    - Formát platební karty,
    - Protokol komunikace,
    - Politika poskytování služby,
    - …

Standard, norma, doporučení = dokumentovaná úmluva 2/4

- Standard nebo norma?
- V Česku (mimo oblast IT) se tradičně používá pojem „**norma**“, což je historický vliv němčiny
- V oblasti IT celosvětově pojem „norma“ vesměs prohrává s pojmem „**standard**“ - dáno vlivem progresivní globalizací angličtiny
- **Doporučení** (*recommendation*) - termín používaný některými organizacemi vydávající standardy místo termínu „standard“ (ITU - telekomunikace, …)
- Standard vyvinutý na bázi konsensu jisté komunity, **de facto standard**
  - Standard vypracovaný v rámci jisté komunity, která si před jeho vydáním odsouhlasí, že standard odpovídá jí stanoveným cílům
  - Např. dokumenty RFC vydávané IETF pro oblast Internetu
  - De facto standard reprezentuje spíše liberální pohled na svět

Standard, norma, doporučení = dokumentovaná úmluva 3/4

- Standard „podle práva“ , **de iure standard**
  - Úmluva schválená uznávanou institucí pověřenou tímto posláním, legislativou, rozhodnutím státních autorit, …
  - Standardy implicitně nejsou právně závazné, jistá právní norma ale může předepsat povinnost vyhovění (obvykle de iure) standardu
  - Typicky standardy vydávané organizacemi ISO, IEC, ITU, …
  - De iure standard reprezentuje silně konzervativní pohled na svět
- Konzervativci od liberálů přebírají co přebírat chtějí a co přebírat stačí
  - De facto standardy se vydávají rychleji
  - Vyzrálé de facto standardy, které se ukázaly jako efektivní, se často přepracovávají/přebírají na de iure standardy

Standard, norma, doporučení = dokumentovaná úmluva 4/4

- Závaznost standardů
  - Žádný standard sám o sobě nemá charakter právního předpisu
  - Právní předpis může stanovit povinné vyhovění standardu
    - V tom případě se obvykle dává přednost de iure standardům
- Mezinárodní charakter standardů
  - Výrobci standardizovaných produktů/procesů v globálním prostředí musí zvolit standard, kterému proces/produkt vyhovuje
  - Tudíž je nutné zabránit přílišné diverzifikaci prosazování „správných“ technik, …
  - **Mnoho standardů pokroku v technologiích smrt**

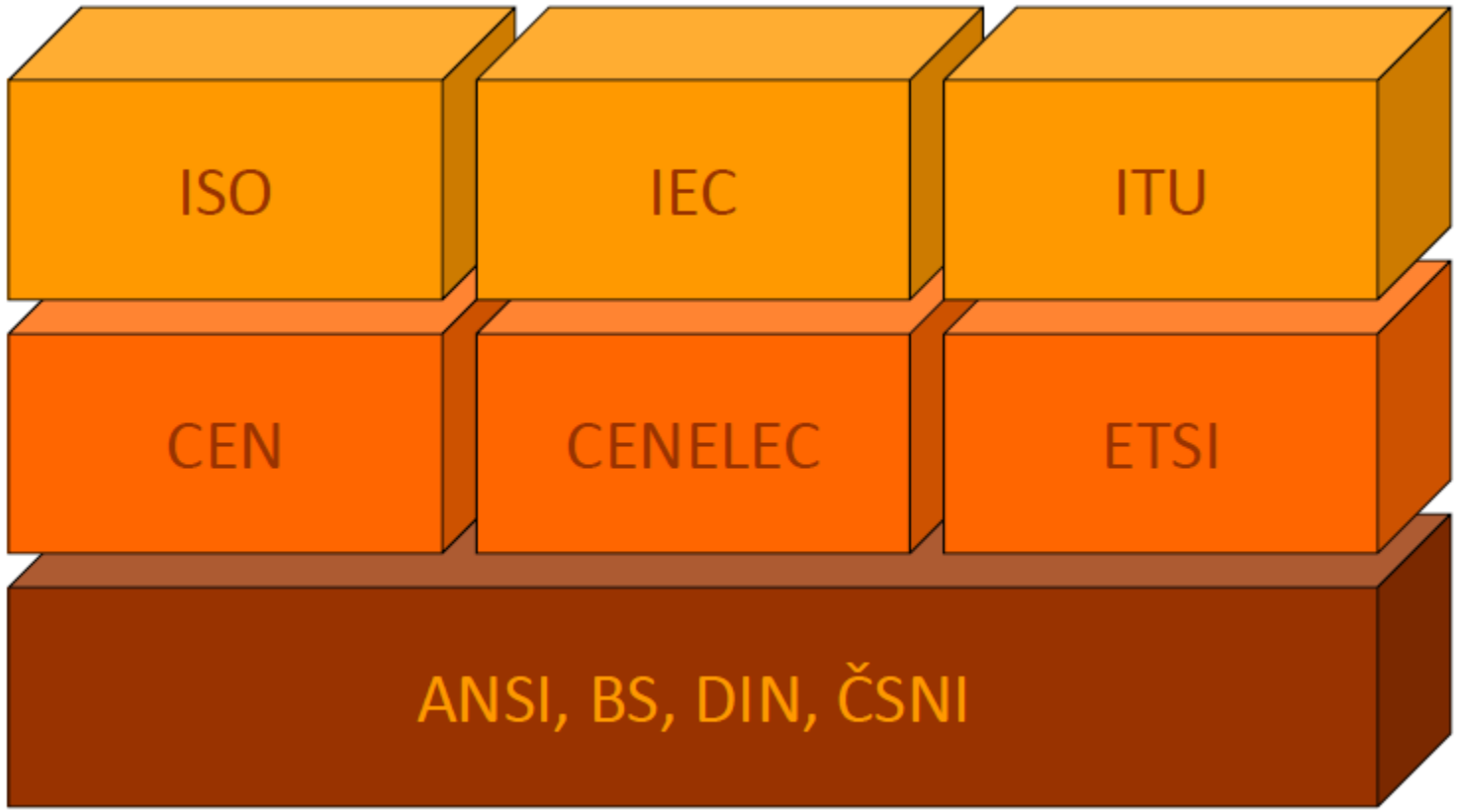
Vyhovění standardu vs. certifikace

- **Compliance** (vyhovění) vs. **Certification** (certifikace)
- Produkt, služba, proces, … může být prohlášena za **vyhovující standardu**
  - Prohlášení, že produkt, služba, proces, splňuje podmínky definované standardem
  - Požadavek vyhovění může být předepsaný zákonem, smlouvou, …
- Produkt, služba, proces, … může být **certifikovaný**, tj. existuje certifikát potvrzující, že je vyhovující standardu
  - Certifikace - neutrální důvěryhodná třetí strana prověří validitu prohlášení o vyhovění standard a vydá o tom relevantní certifikát
  - Standardy definující např. algoritmus, jsou snadno certifikovatelné
  - Standardy návodů jak budovat systém/službu jsou spíše radou a certifikace se obvykle nepožaduje

Problém standardizace

- Standard musí být odsouhlasený všemi členy komunity
  - Mnoho různých pohledů na to, co je správné
  - Pokud se do standardu dostane velká škála voleb a povinných předpokladů, obtížně a nákladně se implementuje
  - To byl jeden z důvodů proč model TCP/IP zvítězil nad modelem OSI
- Standard je **jen** dokument - interpretace se mohou lišit, zvláště při překladu do různých jazyků
- Pokud produkt splňuje jen podstatné části standardu, pak v podstatě vyhovuje standardu, ale není **vyhovující standardu**

Standardizační organizace



- Mezinárodní
- Evropské
- Národní

Příklady oblasti de facto standardů

- **RFC** (Request for Comment)
  - Název internetových standardů, dáno historickou souvislostí
  - V pozadí působí - Internet Society, ISOC, http://www.isoc.org/
    - 150 institucionálních, 6000 individuálních členů z cca 100 zemí
  - Internet reprezentuje - Internet Activities Board, **IAB**
    - Rada pro internetovské činnosti, manažersky spravuje a řídí provoz Internetu
  - Hlavní odpovědnost za vývoj a posuzování RFC IAB delegovala na technickou poradní komisi - IETF, Internet Engineering Task Force
  - Konečné rozhodnutí o vydání (přijetí) RFC dělá IAB
- **ISACA** , Information Systems Audit and Control Association
  - Mezinárodní organizace auditorů výpočetních systémů
  - V r. 1996 vydává **COBIT**, The Control Objectives for Information and related Technology - a set of best practices (framework) for information technology management

Příklady oblasti de facto standardů

- **OWASP** , *The Open Web Application Security Project*
  - A worldwide free and open community focused on improving the security of application software
  - http://www.owasp.org/
  - Standard vývoje bezpečné webovské aplikace
  - Standard testování bezpečné webovské aplikace
  - Standard hodnocení a kriteria záruk za bezpečnost bezpečné webovské aplikace
- **ISF**, Information Security Forum
  - Mezinárodní nezávislá, nezisková věnující se měření a rozvoji praktik v informační bezpečnosti
  - V r. 1996 vydává volně dostupný standard (**SoGP**), The Standard of Good Practice - a detailed documentation of best practice for information security

Firemní, proprietární standardy

- Kategorie de facto standardů
- Obvykle standardy patentovaných technik
- Významný nástroj pro „udržení trhu“ silnou společností
  - Pokud silný výrobce nahradí nezávislé standardy svými proprietárními standardy, váže zákazníky na svoji proprietární funkcionalitu
- Mnohdy hrají velmi silnou roli
  - Např. **PKCS** (Public-Key Cryptography Standards) publikovaný RSA Labs

Hlavní standardy vydané ISO/IEC

- ISO (International Organization for Standardization)
- V současnosti především **rodina standardů ISO/IEC 27000**
  - Více viz http://www.iso27001security.com/html/iso27000.html
  - Doporučení jak řídit informační bezpečnost, řešit zvládání rizik a jak implementovat opatření v kontextu celého systému systému řízení informační bezpečnosti
  - **V současnosti celosvětové uznávaný základní standard zajišťování informační bezpečnosti**

Životní cyklus ISO standardu

- Odpovědnost za tvorbu norem v dílčích oblastech mají **technické výbory**, *Technical Committees*, TC
  - cca 200
- Návrh nové pracovní položky -> úrovně návrh standardu (Committee Draft – 3 měsíce, Draft International Standard – 6 měsíců, Final DIS – 2 měsíce)
- Obvykle pětiletá perioda hodnocení mezinárodního standardu
  - Když se odhalí vada standardu (např. byla podceněna rychlost rozvoje technologie), jsou přijímána opatření, aby standardy byly revidovány i dříve než v pětiletém hodnotícím cyklu
    - Systém zpráv o vadách ve standardech (Defect Report System)

Osnova

- Legislativa informační bezpečnosti
- Standardy (normy) informační bezpečnosti
  - Terminologie
  - Rodina standardů ISO/IEC 27000
  - Standard NIST, rodina SP 800
  - Certifikace
- Řízení rizik
- Politika informační bezpečnosti

Rodina standardů ISO/IEC 27000, ISO/IEC 27001:2013

- **Information Security Management System - Requirements**
- Definuje požadavky na funkcionalitu a vlastnosti systému správy (řízení) informační bezpečnosti
- **Požadavky na možná bezpečnostní opatření vymezuje standard ISO/IEC 27002**
- ISO/IEC 27001 je původně britský standard BS 7779-2
- Standard je detailním popisem požadavků, které **musí** ISMS splnit (v originále se používá *must* a *shall*), pokud ISMS chce standardu vyhovět
- Je nezávislý na technologii, určený pro organizace všech typů, velikostí a podstat, působících v jakémkoli sektoru (komerce, státní správa, neziskovky), kdekoli ve světě

Rodina standardů ISO/IEC 27000, ISO/IEC 27001:2013

- V dodatku standard 27001 uvádí seznam cílů opatření definovaných v ISO/IEC 27002
- ISO/IEC 27002 obsahuje návody, jak je implementovat
- Povinným požadavkem 27001 je porovnat opatření zvolená při zvládání rizik proti dodatku 27001, aby byla jistota, že se na nic nezapomnělo
- 27001 nařizuje použít 27002 jak zdroj návodů pro volbu a implementaci opatření, nezakazuje použití i dalších zdrojů
- Seznam cílů a opatření v dodatku 27001 není chápán jako úplný, vyčerpávající, podle potřeby lze doplňovat další cíle a opatření
- ISMS organizace lze certifikovat na vyhovění ISO/IEC 27001

Rodina standardů ISO/IEC 27000, ISO/IEC 27002:2013

- **Code of practice for information security management**
- Doporučení jak navrhovat, implementovat, udržovat a vylepšovat opatření prosazující informační bezpečnost, používá slova *may*, *should* (může, měl by)
- Původně britský standard BS 7779, poté standard ISO/IEC 17779, nyní standard ISO/IEC 27002:2013
- Jde o mezinárodně uznávané nejlepší praktiky řízení informační bezpečnosti
- Je návodem, jak implementovat certifikovatelný ISMS, externí auditor se může na 27002 odkazovat
- Standard ISO/IEC 27002 je kodexem, radami pro budování bezpečného systému, obvyklé je deklarovat vyhovění standardu, certifikace vyhovění ISO/IEC 27002 se nedělá

Rodina standardů ISO/IEC 27000 v 05.2019

By Gary Hinson, standardy, ktere úzce souvisí s obsahem předmětu PV017, jsou v tabulce v červeném rámci

#	Standard	Published	Title	Notes
1	ISO/IEC 27000	2018	Information security management systems — Overview and vocabulary	Overview/introduction to the ISO27k standards as a whole plus a glossary of terms; FREE!
2	ISO/IEC 27001	2013	Information security management systems — Requirements	Formally specifies an ISMS against which thousands of organizations have been certified compliant
3	ISO/IEC 27002	2013	Code of practice for information security controls	A reasonably comprehensive suite of information security control objectives and generally-accepted good practice security controls
4	ISO/IEC 27003	2017	Information security management system implementation guidance	Sound advice on implementing ISO27k, expanding section-by-section on the main body of ISO/IEC 27001
5	ISO/IEC 27004	2016	Information security management — Measurement	Much improved second version, with useful advice on security metrics
6	ISO/IEC 27005	2018	Information security risk management	Discusses information risk management principles in general terms without specifying or mandating particular methods. Major revision in progress

#	Standard	Published	Title	Notes
7	ISO/IEC 27006	2015	Requirements for bodies providing audit and certification of information security management systems	Formal guidance for the certification bodies, with several grammatical errors – needs revision
8	ISO/IEC 27007	2017	Guidelines for information security management systems auditing	Auditing the management system elements of the ISMS
9	ISO/IEC TR 27008	2011	Guidelines for auditors on information security controls	Auditing the information security elements of the ISMS
10	ISO/IEC 27009	2016	Sector-specific application of ISO/IEC 27001 – requirements	Guidance for those developing new ISO27k standards (i.e. ISO/IEC JTC1/SC27 – an internal committee standing document really)
11	ISO/IEC 27010	2015	Information security management for inter-sector and inter-organisational communications	Sharing information on information security between industry sectors and/or nations, particularly those affecting "critical infrastructure"
12	ISO/IEC 27011	2016	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	Information security controls for the telecoms industry; also called "ITU-T Recommendation x.1051"
13	ISO/IEC 27013	2015	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	Combining ISO27k/ISMS with IT Service Management/ITIL
14	ISO/IEC 27014	2013	Governance of information security	Governance in the context of information security; will also be called "ITU-T Recommendation X.1054"
16	ISO/IEC TR 27016	2014	Information security management – Organizational economics	Economic theory applied to information security

#	Standard	Published	Title	Notes
17	ISO/IEC 27017	2015	Code of practice for information security controls for cloud computing services based on ISO/IEC 27002	Information security controls for cloud computing
18	ISO/IEC 27018	2014	Code of practice for controls to protect personally identifiable information processed in public cloud computing services	Privacy controls for cloud computing
19	ISO/IEC TR 27019	2017	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry	Information security for ICS/SCADA/embedded systems (not just used in the energy industry!), excluding the nuclear industry
20	ISO/IEC 27021	2017	Competence requirements for information security management professionals	Guidance on the skills and knowledge necessary to work in this field
21	ISO/IEC 27023	2015	Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002	Belated advice for those updating their ISMSs from the 2005 to 2013 versions
22	ISO/IEC 27030	DRAFT	Guidelines for security and privacy in Internet of Things (IoT)	A standard about the information risk, security and privacy aspects of IoT
23	ISO/IEC 27031	2011	Guidelines for information and communications technology readiness for business continuity	Continuity (i.e. resilience, incident management and disaster recovery) for ICT, supporting general business continuity
24	ISO/IEC 27032	2012	Guidelines for cybersecurity	Ignore the vague title: this standard actually concerns Internet security
25	ISO/IEC 27033	-1 2015	Network security overview and concepts	Various aspects of network security, updating and replacing ISO/IEC 18028

#	Standard	Published	Title	Notes
26	ISO/IEC 27033	-2 2012	Guidelines for the design and implementation of network security	Various aspects of network security, updating and replacing ISO/IEC 18028
27		-3 2010	Reference networking scenarios - threats, design techniques and control issues	
28		-4 2014	Securing communications between networks using security gateways	
29		-5 2013	Securing communications across networks using Virtual Private Networks (VPNs)	
30		-6 2016	Securing wireless IP network access	
31	ISO/IEC 27034	-1 2011	Application security — Overview and concepts	Multi-part application security standard Promotes the concept of a reusable library of information security control functions, formally specified, designed and tested
32		-2 2015	Organization normative framework	
33		-3 2018	Application security management process	
34		-4 DRAFT	Application security validation	
35		-5 2017	Protocols and application security control data structure	
36		-5-1 2018	Protocols and application security control data structure, XML schemas	
37		-6 2016	Case studies	
38		-7 2018	Application security assurance prediction framework	

#	Standard	Published	Title	Notes
39	ISO/IEC 27035	-1 2016	Information security incident management — Principles of incident management	Replaced ISO TR 18044 Actually concerns incidents affecting IT systems and networks, specifically
40		-2 2016	— Guidelines to plan and prepare for incident response	
41		-3 DRAFT	— Guidelines for incident response operations??	Part 3 drafting restarted – due out in 2019 or 2020
42	ISO/IEC 27036	-1 2014	Information security for supplier relationships – Overview and concepts (FREE!)	Information security aspects of ICT outsourcing and services
43		-2 2014	— Common requirements	
44		-3 2013	— Guidelines for ICT supply chain security	
45		-4 2016	— Guidelines for security of cloud services	
46	ISO/IEC 27037	2012	Guidelines for identification, collection, acquisition, and preservation of digital evidence	One of several IT forensics standards
47	ISO/IEC 27038	2014	Specification for digital redaction	Redaction of digital documents
48	ISO/IEC 27039	2015	Selection, deployment and operations of intrusion detection and prevention systems (IDPS)	IDS/IPS
49	ISO/IEC 27040	2015	Storage security	IT security for stored data
50	ISO/IEC 27041	2015	Guidelines on assuring suitability and adequacy of incident investigative methods	Assurance of the integrity of forensic evidence is absolutely vital

#	Standard	Published	Title	Notes
51	ISO/IEC 27042	2015	Guidelines for the analysis and interpretation of digital evidence	IT forensics analytical methods
52	ISO/IEC 27043	2015	Incident investigation principles and processes	The basic principles of eForensics
53	ISO/IEC 27050	-1 2016	Electronic discovery – overview and concepts	More eForensics advice
54		-2 2018	Guidance for governance and management of electronic discovery	Advice on treating the risks relating to eForensics
55		-3 2017	Code of practice for electronic discovery	A how-to-do-it guide to eDiscovery
56		-4 DRAFT	ICT readiness for electronic discovery	Guidance on eDiscovery technology (tools, systems and processes)
57	ISO/IEC 27070	DRAFT	Security requirements for establishing virtualized roots of trust	Concerns trusted cloud computing
58	ISO/IEC 27099	DRAFT	Public key infrastructure - practices and policy framework	Infosec management requirements for Certification Authorities
59	ISO/IEC 27100	DRAFT	Cybersecurity – overview and concepts	Perhaps this standard will clarify, once and for all, what 'cybersecurity' actually is. Perhaps not.
60	ISO/IEC 27101	DRAFT	Cybersecurity framework development guidelines	Given the above, we can barely guess what this might turn out to be
61	ISO/IEC 27102	DRAFT	Information security management guidelines for cyber insurance	Advice on obtaining insurance to reduce the costs of cyber incidents
62	ISO/IEC TR 27103	2018	Cybersecurity and ISO and IEC standards	Explains how ISO27k and other ISO and IEC standards relate to 'cybersecurity' (without actually defining the term!)

#	Standard	Published	Title	Notes
63	ISO/IEC 27550	DRAFT	Privacy engineering	How to address privacy throughout the lifecycle of IT systems
64	ISO/IEC 27551	DRAFT	Requirements for attribute-based unlinkable entity authentication	Seems more like an authentication standard than ISO27k … scope creep?
65	ISO/IEC 27552	DRAFT	Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy management — Requirements and guidelines	Explains extensions to an ISO27k ISMS for privacy management
66	ISO/IEC 27553	DRAFT	Security requirements for authentication using biometrics on mobile devices	High-level requirements attempting to standardize the use of biometrics on mobile devices
67	ISO/IEC 27554	DRAFT	Application of ISO 31000 for assessment of identity management-related risk	About applying the ISO 31000 risk management process to identity management
68	ISO/IEC 27555	DRAFT	Establishing a PII deletion concept in organizations	A conceptual framework, of all things, for deleting personal information
69	ISO 27799	2016	Health informatics — Information security management in health using ISO/IEC 27002	Infosec management advice for the health industry

Osnova

- Legislativa informační bezpečnosti
- Standardy (normy) informační bezpečnosti
  - Terminologie
  - Rodina standardů ISO/IEC 27000
  - Standard NIST, rodina SP 800
  - Certifikace
- Řízení rizik
- Politika informační bezpečnosti

NIST Special Publications (SP)

- *http://csrc.nist.gov/publications/PubsSPs.html*
- SP 800, Computer Security (December 1990-present):
  - NIST's primary mode of publishing computer/cyber/information security guidelines, recommendations and reference materials
- SP 1800, NIST Cybersecurity Practice Guides (2015-present):
  - Complement the SP 800s; targets specific cybersecurity challenges in the public and private sectors; practical, user-friendly guides to facilitate adoption of standards-based approaches to cybersecurity
- SP 500, Computer Systems Technology (January 1977-present):
  - A general IT subseries used more broadly by NIST's Information Technology Laboratory (ITL)

Standard NIST, rodina SP 800, příklady (SP Special Publication)

- SP 800-12: An Introduction to Information Security
- SP 800-30: Guide for Conducting Risk Assessments
- SP 800-45: Guidelines on Electronic Mail Security
- SP 800-50: Building a Cybersecurity and Privacy Learning Program
- SP 800-63: Digital Identity Guidelines
- SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)
- SP 800-95: Guide to Secure Web Services
- SP 800-100: Information Security Handbook: A Guide for Managers
- SP 800-184: Guide for Cybersecurity Event Recovery

Osnova

- Legislativa informační bezpečnosti
- Standardy (normy) informační bezpečnosti
  - Terminologie
  - Rodina standardů ISO/IEC 27000
  - Standard NIST, rodina SP 800
  - Certifikace
- Řízení rizik
- Politika informační bezpečnosti

Certifikace ISO/IEC 27001

- ISO/IEC 27001 - standard normálu ISMS, o jehož dosažení **lze získat certifikát**
  - ISMS - prostředí pro návrh, implementaci, řízení, údržby a systematické a konzistentní prosazování procesů a nástrojů zajišťujících informační bezpečnost v celé organizaci
- Standard ISO/IEC 27001 respektuje nástroje definované standardem ISO/IEC 27002
  - ISO/IEC 27001 obsahuje seznam nástrojů dle ISO/IEC 27002 jako menu
  - Organizace přijímající ISO/IEC 27001 si z menu potřebné nástroje vybírá
  - Výběr musí vycházet z výsledků analýzy rizik
  - Škála opatření může být adekvátně rozšířena vůči ISO/IEC 27002

Certifikace ISO/IEC 27001

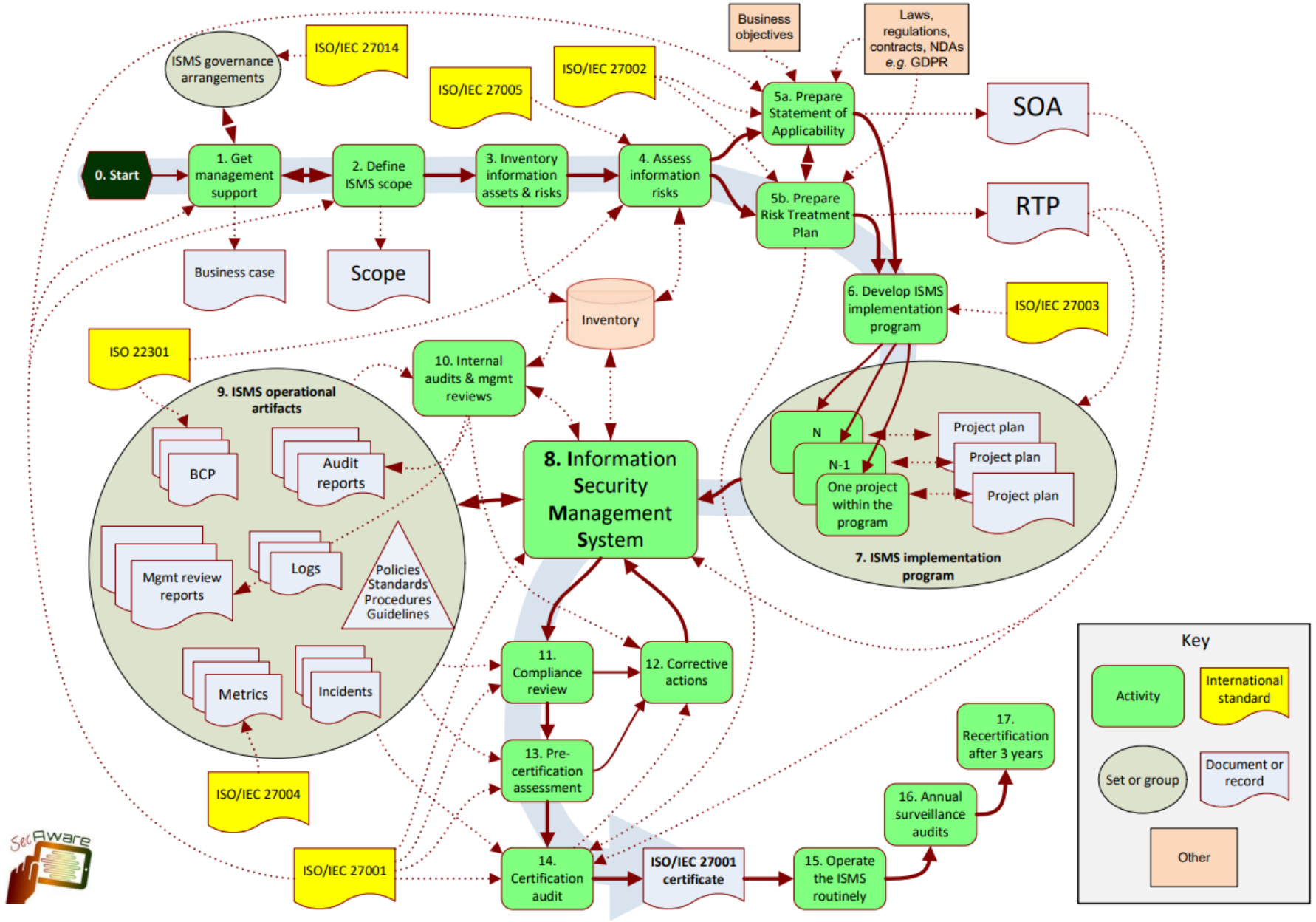
- Certifikát ISO 9001 říká -
  - My jsme organizace kvalitně fungující z hlediska procesů činnosti (byznysu)
- Certifikát ISO 27001 říká -
  - My jsme organizace kvalitně pečující o bezpečnost informací pomocí procesů cílených na zajištění informační bezpečnosti
- Certifikace je volitelná, pokud si certifikaci nevyžádá legislativa

Certifikace ISO/IEC 27001

- Existuje respektovaný model vzájemného uznávání certifikátů 27001
- Musí existovat **národní akreditační úřad** (**NAU**)
- U NAU se akredituje **certifikační autorita** (**CA**)
- CA provede audit ISMS typicky v krocích
  - Zájemce o certifikát v dotazníku CA popíše své požadavky
  - Uzavře se smlouva detailně popisující požadavky
  - Auditoři absolvují seznamovací interview
  - Auditoři provedou analýzu dokumentace
  - Auditoři provedou analýzu shody dokumentace s prostředím a provozovaným ISMS
  - Provádí se následné audity
- Existuje generická struktura ISMS
  - Šablona ISMS vyhovující standardu ISO/IEC 27001 obsahující názvy typických kapitol/podkapitol, nikoli jejich obsah, tj. nikoli předpisy/deklarace politik/opatření

Rámcová roadmapa certifikace

- Příprava - zvolte si svého šampiona, podpora managementu a gap analýza (může zahrnout i prioritizovaný plán doporučených akcí)
- Ustanovení kontextu, rozsahu a cílů (vč. nákladů a časového rámce, potřeba externího dodavatele atp.)
- Vvtvoření rámce řízení (odpovědnosti, harmonogram, audity, …)
- Analýza rizik – vznik povinných dokumentů (Prohlášení o použitelnosti (SoA) a plán ošetření rizik (RTP))
- Implementace bezpečnostních opatření – akceptace/transfer/mitigace/odstranění rizika
- Školení – zvyšování bezpečnostního povědomí zaměstnanců
- Revize a update relevantní dokumentace – bezpečnostní politika a další (standard vyžaduje určitou minimální množinu dokumentů (cca 17))
- Měření, monitorování, kontrola
- Pravidelný interní audit
- Registrační/certifikační audit



Implementation and Certification process 2022, ISO27k Implementation Forum. *https://www.iso27001security.com/*

ISO 27001: 7 kapitol definovaných požadavků

- Kontext organizace – určení záměru a potřeb organizace, rozsahu ISMS a implementace a průběžné zlepšování
- Vůdčí role – závazek vedení organizace, stanovení politiky, určení rolí a odpovědností
- Plánování – opatření zaměřená na rizika (posouzení rizik a jejich ošetření) vč. seznamu nezbytných opatření, stanovení cílů bezpečnosti a plán jejich dosažení
- Podpora – jsou zaručeny dostatečné zdroje, kompetence a povědomí, informace jsou dokumentované a aktualizované
- Provozování – plánování a řízení provozu, průběžné posuzování a ošetření rizik
- Hodnocení výkonnosti – monitoring, audit, přezkoumání vedením
- Zlepšování – neshody a nápravná opatření, neustálé zlepšování

Osnova

- Legislativa informační bezpečnosti
- Standardy (normy) informační bezpečnosti
  - Terminologie
  - Rodina standardů ISO/IEC 27000
  - Standard NIST, rodina SP 800
  - Certifikace
- Řízení rizik
- Politika informační bezpečnosti

Řízení rizik

Rizika

- Reprezentace negativního dopadu využití zranitelnosti, tj. útoku, přičemž zohledňuje jak pravděpodobnost tak i škodní dopad útoku
- Rizika mohou plynout
  - Z cílů a řešení podnikatelských procesů
  - Nedokonalého vyhovění zákonným/smluvním závazkům
  - Úrovně kvality návrhových, implementačních a provozních procedur aplikačních systémů
- Rizika mohou existovat nezávisle na naší vůli -
  - Výpadek energie, záplava, zemětřesení, požár, …
- Standard ISO/IEC 27001:2013, odst. 6.1.2 požaduje:
  - Organizace musí přistupovat k výběru a k provozování bezpečnostních opatření na základě znalosti rizik
  - K rizikům se přistupuje na bázi scénářů, nikoli pouze na bázi aktiv
  - Rizika se je nutné zvažovat napříč celé chráněné oblasti, nikoli jednotlivě vůči hrozbám jednotlivým aktivům

Riziko se vyjadřuje

- V pravděpodobnostních pojmech (s jakou pravděpodobností se hrozba uplatní)
- V pojmech charakterizujících dopad hrozby (velikost škody způsobené útokem)
- Generické kombinované vyjádření úrovně rizika:

  úroveň rizika = F(pravděpodobnost útoku) × F´(dopad útoku)

- Do úvahy se bere jak dopad relevantního útoku, tak i pravděpodobnost realizace/uplatnění hrozby (útoku)
- Velmi významné riziko se staví na roveň velkému dopadu a velké pravděpodobnosti výskytu relevantního útoku
- Nevýznamné riziko se staví na roveň malému dopadu a malé pravděpodobnosti výskytu relevantního útoku

Zvládání rizik

- Rizika se zvládají volbou a uplatňováním vhodných opatření
- Abychom riziko zvládli, tj. eliminovali ho nebo snížili jeho úroveň, musíme ho nejprve ohodnotit, tj. identifikovat a poté analyzovat a vyhodnotit (určit jeho úroveň)
  - Vynakládání velkých nákladů na zavedení opatření chránících aktiva prevencí útoků při nevýznamných rizicích není ospravedlnitelné
- Proces ohodnocení rizik usnadní např. použití **tabulky rizik aktiv** implementující relaci mezi aktivy (řádky tabulky) a faktory určujícími rizika (sloupce)
- Faktory určující riziko:
  - Hrozba, zranitelnosti, id rizika, osoba odpovědná za zvládání rizika, výše možné škody, pravděpodobnost útoku, typ útočníka …

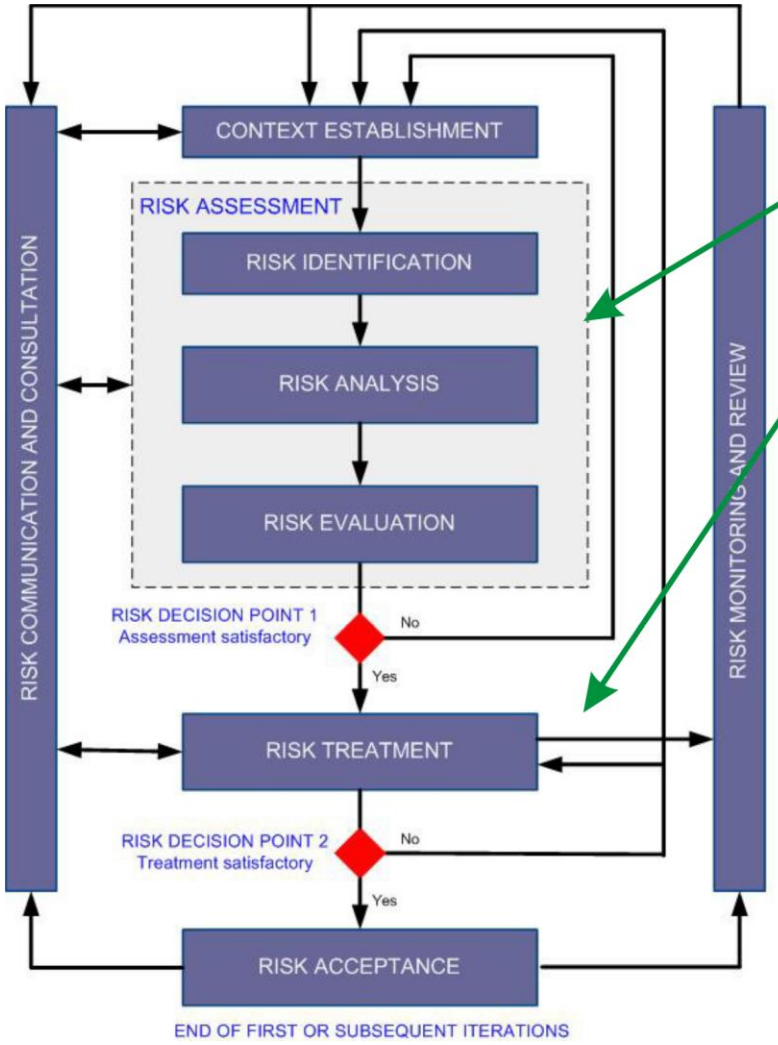
Řízení rizik pro informační bezpečnost

- **ISO/IEC 27005: 2011, Information technology – Security techniques – Information security risk management**
- Identifikace potřeb organizace
  - Z pohledu zajištění vlastní informační bezpečnosti
  - Z pohledu vytvoření účinného (efektivního) ISMS

Procesy řízení rizik (Risk Management) - výčet

- **Ustanovení kontextu** (*Context establishment*), stanovení oblasti, kritérií,…
- **Ohodnocení rizik** (*Risk Assessment*) tvoří podprocesy:
  - Identifikace rizik (*Risk Identification*)
  - Analýza rizik (*Risk Analysis*) - určení velikosti rizik
  - Vyhodnocení rizik (*Risk Evaluation*) - určení úrovní rizik porovnáním vůči stanoveným kritériím
- **Zvládnutí rizik** (*Risk Treatment, Risk Mitigation*) - proces modifikující rizika, výběr a implementace opatření snižujících rizika
- **Akceptace rizik** (*Risk Acceptance*) - rozhodování o přijatelnosti rizika dle stanovených kritérií
- **Informování o rizicích** (*Risk Communication*) - sdělení informace o rizicích všem, kdo může rizika ovlivnit či být riziky ovlivněn
- **Monitorování a přezkoumávání rizik** (*Risk Monitoring and Review*) a procesu řízení rizik

Procesy řízení rizik - architektura



Ohodnocení rizik a zvládání rizik jsou iterativní procesy

Získala se dostatečná informace pro volbu opatření ?
Pokud ne, musí se upravit kontext
(oblast, kritéria, ...)

Mají zbytková rizika akceptovatelnou úroveň ?

Cíle dílčích procesů řízení rizik 1/5

- **Ustanovení kontextu**
  - Vymezení účelu provedení řízení rizik
  - Vymezení spravované oblasti a jejích hranic
  - Zajištění zdrojů (ekonomických, profesních) pro řízení rizik
  - Stanovení kritérií pro vyhodnocení dopadů útoků, úrovní rizik, akceptovatelnosti rizik
  - Stanovení organizačního zajištění a odpovědnostních rolí za řízení rizik

Cíle dílčích procesů řízení rizik 2/5

- **Ohodnocení rizik**
  - Aktiva jsou vystavená hrozbám, hrozby jsou dané existencí útočníků a zranitelnosti, některé útoky jsou pravděpodobnější než jiné, každý útok může mít větší či menší dopad
  - Ohodnocení rizik identifikuje všechny tyto aspekty pro každou hrozbu
  - Jde o získání informací pro účinné určení/volbu opatření potřebných ke změně rizik na přijatelnou úroveň pomocí procesů
    - **Identifikace rizik**
    - **Analýza rizik** - určení velikosti rizik
    - **Vyhodnocení, evaluace rizik** porovnáním vůči stanoveným kritériím
  - Výstupem ohodnocení rizik je
    - Prioritně řazený **seznam ohodnocených rizik**, řazený podle kritérií hodnocení rizik
    - **Prohlášení o aplikovatelnosti** (*Statement of Aplicability)*, vhodných opatření řešících snižování/eliminaci ohodnocených rizik

Cíle dílčích procesů řízení rizik 3/5

- **Zvládnutí rizik**
  - Rizika pro InfoSec organizace lze zvládnout až když jsou identifikovaná, analyzovaná a posouzená rizika pro důvěrnost, integritu a dostupnost informačních aktiv organizace
  - Definuje se **plán zvládání rizik**, který má čtyři související cíle:
    - Určí rizika, která se eliminují
      - Než stavět protipovodňovou hráz, raději serverovnu přemístit na kopec
    - Určí rizika, která nelze eliminovat a sníží se na akceptovatelnou úroveň (zvládnou se) implementací určených opatření
    - Určí tolerovaná rizika, pro která se po zvážení odmítla opatření, která by je udržovala na akceptovatelné úrovni, akceptovatelná rizika
      - Zabudování nákladů na škodní řízení do byznys modelu
    - Určí rizika, která se přenesou smluvně nebo pojištěním na jinou organizaci
      - Řešení sdílením nákladů na škodní řízení

Cíle dílčích procesů řízení rizik 4/5

- **Akceptace rizik**
  - Odsouhlasení plánu zvládání rizika soupisu akceptovatelných rizik managementem organizace

Cíle dílčích procesů řízení rizik 5/5

- **Informování o rizicích**
  - Sdělování výsledků řízení rizik managementu a zaměstnancům
  - Následuje implementace zvolených opatření a zabudování jejich prosazování do procesů organizace
- **Monitorování a přezkoumávání rizik a procesu řízení rizik**
  - Rizika nejsou statická
    - Odhalování změn v kontextu, v rizicích, ve faktorech ovlivňujících úrovně rizik, …
    - Při běžné činnosti organizace

Vzorové ukázky podpůrných materiálů…

- …naleznete na stránkách NUKIB https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

HODNOCENÍ RIZIK													
ID	Aktivum	Hodnota dopadu - dostupnost	Hodnota dopadu - důvěrnost	Hodnota dopadu - integrita	Zranitelnost	Hodnota zranitelnosti	Hrozba	Hodnota hrozby	Hodnota rizika - dostupn	Hodnota rizika - důvěrnc	Hodnota rizika - integrit	Způsob zvládání rizika	Komentář
R43	PO26: Serverovna	3	Nerelevantní	Nerelevantní	Z8: Nedostatečná ochrana aktiv	4	služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	2	24	Nerelevantní	Nerelevantní	Redukce	oblasti, jedna serverovna (ministerstvo nemá žádnou záložní), blesk/požár
R44	PO26: Serverovna	3	Nerelevantní	3	Z7: Nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností lidských zdrojů	4	H2: Poškození nebo selhání technického nebo programového vybavení	2	24	Nerelevantní	24	Redukce	skladování hořlavého materiálu v serverovně
R45	PO27: Areál	3	Nerelevantní	Nerelevantní	Z8: Nedostatečná ochrana aktiv	2	H13: Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	2	12	Nerelevantní	Nerelevantní	Akceptace	přírodní katastrofy - požár, záplavy, zemětřesení atd.
R46	PO27: Areál	3	3	3	Z3: Nedostatečná ochrana perimetru	2	H6: Narušení fyzické bezpečnosti	3	18	18	18	Sledování	
R47	PO28: Kabeláž	3	3	3	Z8: Nedostatečná ochrana aktiv	3	H12: Zneužití vnitřních prostředků, sabotáž	2	18	18	18	Sledování	volně přístupné kabely/rozvodny
R48	PO28: Kabeláž	3	3	3	Z8: Nedostatečná ochrana aktiv	3	H11: Pochybení ze strany zaměstnanců a administrátorů	3	27	27	27	Sledování	
R49	PO28: Kabeláž	3	Nerelevantní	3	Z2: Zastaralost aktiv	1	H2: Poškození nebo selhání technického nebo programového vybavení	1	3	Nerelevantní	3	Akceptace	odejdou staré kabely/vadný kus, infrastruktura stará 20 let
R50	PO31: Dodavatel B	3	Nerelevantní	Nerelevantní	Z7: Nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností lidských zdrojů	4	H13: Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	3	36	Nerelevantní	Nerelevantní	Redukce	stará smlouva - nedostatečné SLA, v případě mimořádné události vypadne důležitá služba, starší smlouva než u dodavatele A
R51	PO31: Dodavatel B	3	2	3	Z7: Nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností lidských zdrojů	4	H5: Působení škodlivého kódu (například viry, spyware, trojské koně)	2	24	16	24	Redukce	dodavatel by měl aktualizovat HW/SW, ale neděla to tak často, jak by měl - nemáme to ve smlouvě

Osnova

- Legislativa informační bezpečnosti
- Standardy (normy) informační bezpečnosti
  - Terminologie
  - Rodina standardů ISO/IEC 27000
  - Standard NIST, rodina SP 800
  - Certifikace
- Řízení rizik
- Politika informační bezpečnosti

Politika informační bezpečnosti

Politika

- **Politika** - pravidla řídící dosažení cílů určenými způsoby
  - *A policy is a deliberate system of principles to guide decisions and achieve rational outcomes*
  - *A policy is a statement of intent, and is implemented as a procedure or protocol.*
- Politika organizace
  - Prohlášení o celkovém záměru a směru podnikání formálně vyjádřené vedením organizace a je implementována jako procedura/protokol kroků pro dosažení cílů
  - Organizace může mít řadu politik, jednu pro každou z oblastí činnosti, které jsou pro organizaci důležité.
    - Personální politika
    - Politika finančních toků, *Cash flow policy*
    - Politika působení v tržním prostředí
    - Sociální politika
    - …
    - **Politika zajištění informační bezpečnosti**
  - Některé politiky jsou navzájem nezávislé, jiné politiky mají hierarchický vztah nebo se doplňují

Hierarchie bezpečnostních politik

- Pro oblasti bezpečnosti organizace mají být politiky organizovány hierarchicky
- Na nejvyšší úrovni je **bezpečnostní politika organizace**
  - Souhrn bezpečnostních zásad a předpisů, množina pravidel definujících správu a ochranu aktiv organizace
  - Definuje způsob zabezpečení organizace jako celku
  - Od fyzické ostrahy, přes ochranu soukromí, přes bezpečné plnění cílů činnosti organizace až po ochranu lidských práv
- **Bezpečnostní politika organizace** je podporována řadou dalších specifických politik, mj.
  - Politikou informační bezpečnosti, zásady, pravidla zajištění InfoSec
  - Politikou ISMS, zásady, pravidla chování ISMS
  - Politikou uchování kontinuity činnosti, *Business Continuity Plan*

Politika informační bezpečnosti a politika ISMS

- **Politka InfoSec** - co proti čemu chránit
- **Politika ISMS** - jak navrhovat, vyvíjet, provozovat a hodnotit procesy plnící politiku InfoSec
- Politika InfoSec bývá podporována řadou detailních politik na konkrétních aspekty informační bezpečnosti (řízení přístupu, e-mailu, čistého stolu, používání síťových služeb, …)
- ISO/IEC 27001 (standard ISMS) žádá, aby organizace měla jak politiku ISMS tak i politiku informační bezpečnosti
  - Konkrétní vztah mezi těmito politikami nestanovuje, politiku ISMS žádá ISO/IEC 27001, politiku InfoSec ISO/IEC 27002
  - Obě mohou být vytvořeny jako doplňující se politiky, politika ISMS může být podřízena politice InfSec nebo politika InfSec může být podřízena politice ISMS

Politika informační bezpečnosti (IT Security Policy, InfoSec)

- Má vyhovovat celkové bezpečnostní politice organizace
- Definuje bezpečné používání IT v rámci organizace
- Stanovuje koncepci informační bezpečnosti organizace v horizontu 5-10 let
- Stanovuje co jsou citlivá informační aktiva, jejich klasifikaci a odpovědnosti za jejich stav
- Stanovuje bezpečnostní infrastrukturu organizace
  - Nutná je nezávislost výkonných a kontrolních rolí
- Definuje třídu (sílu) útočníků, vůči kterým se informace organizace zabezpečují
- Je nezávislá na konkrétně použitých IT

Systémová bezpečnostní politika

- **NUKIB: Návrh bezpečnosti informačního systémů**
- Také bezpečnostní politika IS, systémová bezpečnostní politika, …
- Podle ISO/IEC 27000 - **Plán zvládání rizik**
  - Detailní normy, pravidla, praktiky, předpisy konkrétně definující způsob správy, ochrany, distribuce citlivé informace a jiných IT zdrojů v oblasti vymezené systémem pro zpracování informací organizace
  - Specifikace bezpečnostních opatření, způsobu jejich implementace a určení způsobů jejich použití zaručujících přiměřenou bezpečnost
  - Musí splňovat politiku informační bezpečnosti organizace
  - Musí respektovat konkrétně použité IT
  - Určuje způsob zabezpečení informací v daném systému v horizontu 2–5 let , tj. definuje
    - Konkrétní cíle co se proti čemu chrání
    - Konkrétní opatření
    - Použité mechanismy pro implementaci opatření
    - Obsahuje havarijní plán a plány činnosti po útocích

Bezpečnostní procedury (postupy), role

- Připomínka z popisu dokumentace systému Provozní procedury
  - Popisy (krok po kroku) jak se systém provozuje v konkrétní organizaci
  - Kdo je odpovědný za provedení jednotlivých úkolů, …
- Složitost a rozsah procedur je daná stupněm potřebné interakce lidského činitele se systémem a požadavky na záruku spolehlivosti, důvěryhodnosti, …
- Typické role osob vystupujících v bezpečnostních procedurách
  - Chief Security Officer (CSO) - manažer, který je odpovědný za fyzickou, informační i personální bezpečnost v organizaci
  - Chief Information Security Officer (CISO) - manažer, který je odpovědný za informační bezpečnost v organizaci
  - Security architect, bezpečnostní architekt
  - Security manager, bezpečnostní správce,
    resp. Security officer, bezpečnostní administrátor/úředník
  - Operátor, správce, administrátor systému
  - Auditor, nezávislá osoba na exekutivě bezpečnosti

Modelový příklad bezpečnostní politiky

- Deklarovaná bezpečnostní politika při výuce nepovoluje podvod opsáním domácí úlohy (plagiát)
- Politikou stanovený bezpečný stav (bezpečnostní cíl) - nikdo nevlastní kopii domácí úlohy jiného studenta
- Studenti si uchovávají své domácí práce na školním počítači
- Alice soubor se svou domácí úlohou neoznačí jako chráněný proti čtení jinou osobou
- Bob úlohu opíše
- Kdo se choval v rozporu s bezpečnostní politikou ?
  - Alice ?? Bob ?? oba ?

Modelový příklad bezpečnostní politiky

- Odpověď - bezpečnostní politiku nedodržel pouze Bob
  - Politika zakazuje opisování domácích úloh
  - Bob opisoval
  - Systém se dostal do jiného než bezpečného stavu, Bob vlastní kopii Aliciny úlohy
- Alice si svoji domácí úlohu nechránila proti čtení
- To ale bezpečnostní politika to nepožadovala
- Alice nijak nenarušila definovanou bezpečnostní politiku
- Pokud by politika studentům předepisovala povinnost chránit své domácí úlohy před opsáním, pak by Alice bezpečnostní politiku porušila

Tvorba politiky informační bezpečnosti

- Definice politik InfoSec a ISMS je 1. krok při budování ISMS
  - Tvorba politiky je obvykle iterativní proces
  - Finální verze politiky musí odrážet výsledek **ohodnocení rizik** daný obsahem **prohlášení o aplikovatelnosti** (specifikace vhodných opatření) - dokument vzniklý jako výsledek ohodnocení rizik
- Politika je konceptuální dokument, který má
  - Respektovat charakteristiky činností, lokalit a aktiv organizace a technologií použitých organizací pro zpracování informací
  - Definovat systém stanovení cílů a strategií řízení organizace a rizik
  - Ustanovit kontext, ve kterém bude působit
  - Ustanovit kritéria pro evaluaci rizik a strukturu procesu hodnocení rizik
- Politika musí být
  - Schválená vedením organizace
  - Pravidelně přezkoumávaná (např. ročně) a aktualizovaná

Tvorba politiky informační bezpečnosti, iniciální dokument

- **Deklarace politiky informační bezpečnosti**
  - Maximální rozsah 2 až 3 strany A4
  - Odpovědi na klíčové otázky Pro koho? Kde? Co? Proč?
  - Deklaruje vrcholový management, podepisuje „šéf“ organizace
- **Pro koho** bude politika informační bezpečnosti závazná?
  - Odpovědnost za politiku (za každou revizi) má vrcholový management, musí existovat důkaz, že tomu tak je - zápisy z vedení, …
  - Vrcholový management/řídicí výbor musí zvážit a vymezit dopad politiky na konkrétní okruhy zaměstnanců, zákazníků, dodavatelů, … vč. přínosů/negativ pro byznys, …
  - Vytvářená politika má být maximálně srozumitelná, úplná (samostatně použitelný dokument) a evidentní (nezpochybnitelná), aby se v průběhu implementace nemusely opakovaně odsouhlasovat všechny dílčí alternativy politiky

Tvorba politiky informační bezpečnosti, iniciální dokument

- **Kde** bude oblast působnosti politiky informační bezpečnosti?
  - Nutno přesně vymezit podle organizačního řádu / geograficky / funkčně / …
  - Špatně se prosazuje politika v oblasti, která nepodléhá jednotnému řízení
  - Mnohdy nestačí jednostranné vymezení např. na bázi organizační struktury či geografické lokality, do oblasti musí být zahrnuty všechny související kritické funkce
- **Co** politika informační bezpečnosti chrání ?
  - Specifikace informačních aktiv pokrytých politikou
  - Specifikace relevantních rysů bezpečnosti chráněných aktiv (důvěrnost, integrita, dostupnost)
  - Stanovení kritérií pro akceptování rizik a identifikace úrovně akceptovatelného rizika

Tvorba politiky informační bezpečnosti, iniciální dokument

- **Proč** se politika informační bezpečnosti zavádí ?
  - Srozumitelné vyjádření podstaty hrozeb pro organizaci
  - Srozumitelné vyjádření výše škod způsobených narušením bezpečnosti informací (ve finančních i nefinančních pojmech)
  - Ilustrační příklady důsledků incidentů podporující zavedení ISMS

- Tak, jak jsou následně získávané dílčí výsledky z hodnocení rizik, deklarace politiky informační bezpečnosti se může rozšiřovat a upřesňovat

Deklarace politiky informační bezpečnosti, šablona - příklad

- Vedení organizace ….. provozující činnost v oblasti ….. , umístěné v ….. , se rozhodlo chránit důvěrnost, integritu a dostupnost všech svých relevantních fyzických a elektronických informatických aktiv
- Cílem ochran je udržení dobrého stavu konkurenčních výhod, hotovostních toků, ziskovosti, vyhovění zákonným a smluvním omezením a zachování dobré pověsti organizace.
- Cíle ochran, požadavky na informace a na bezpečnost informací budou vyhovovat cílům organizace v oblasti stanovených politikou informační bezpečnosti a jako zmocňovací mechanismus pro sdílení informací v elektronických operacích, pro e-komerci a pro redukci rizik vázaných na zpracování informací na akceptovatelnou úroveň se použije systém řízení informační bezpečnosti (ISMS).
- Zaměstnanci organizace činí v oblasti ….. jsou povinni plnit požadavky bezpečnostní politiky a ISMS, který tuto politiku implementuje. Totéž platí pro třetí strany definované v ISMS.
- Tato politika bude přezkoumávaná alespoň jednou ročně.
- Odpovědností za bezpečnostní politiku a ISMS je pověřen odbor …..

Tvorba politiky informační bezpečnosti 1/3

- Politika informační bezpečnosti má pokrývat/obsahovat:
  - Prohlášení, že vedení organizace bude podporovat ISMS a periodicky přezkoumávat politiku informační bezpečnosti
  - Nástin přístupu k řízení rizik (určení metodiky)
  - Kritéria evaluace (vyhodnocení) rizik
  - Strukturu procesu ohodnocení rizik
  - Kdo bude za ohodnocení rizik odpovědný
  - Stručnou identifikaci požadavků na soubory opatření zajišťujících vyhovění politice, např.
    - plán(y) reakcí na incidenty,
    - plán zachování činností,
    - plán zálohování dat,
    - plán ochran před viry,
    - politika řízení přístupu,
    - zpravodajství o bezpečnostních incidentech, …

pokrač .

Tvorba politiky informační bezpečnosti 2/3

pokrač.

- Srozumitelnou deklaraci toho, že požadavky na informace a bezpečnost informací budou vyhovovat cílům organizace a že relevantní ISMS bude předmětem trvalého vylepšování
- Jasné vyjádření, že všichni zaměstnanci budou podrobováni školení a trénování v bezpečnostním uvědomění a specialisté budou absolvovat specializovaná školení
- Ideálně by politika měla deklarovat vyhovění standardu ISO/IEC 27002 (tj. prohlášení, že se uplatňují standardní opatření), případně by politika měla deklarovat cíl získat certifikátu ISO/IEC 27001 (tj. certifikátu, že se uplatňují validní procesy ISMS)

Tvorba politiky informační bezpečnosti 3/3

- Náklady na budování politiky InfoSec
  - Vedení organizace má požadovat doložení návrhu politiky
    - Odhadem ceny vybudování ISMS a zdrojů pro vybudování ISMS
    - Hodnocením a kvantifikací potenciálních zisků
    - Návrhem plánu implementace a odpovědnosti za implementaci
- Monitorování postupu budování politiky InfoSec
  - Klíčové okamžiky pro přezkoumání postupu tvorby politiky jsou
    - Vypracování návrhu **Prohlášení o aplikovatelnosti** (specifikace vhodných opatření) v rámci ohodnocování rizik
    - Implementace iniciální sestavy procedur aplikujících opatření identifikovaná v Prohlášení o aplikovatelnosti
    - Provedení prvního auditu ISMS
    - Následně pak ročně, v termínech pravidelného přezkoumávání ISMS, určených v politice informační bezpečnosti

12 tipů pro tvorbu politiky informační bezpečnosti 1/2

- Bezpečnostní politika je nejefektivnější, když si ji organizace napíše sama.
- Politika informační bezpečnosti by měla být klíčovým faktorem při všech rozhodnutích o činnosti organizace, není pravda, že ovlivňuje činnost pouze IT oddělení.
- Zaměstnanci musí být školení pro dodržování bezpečnostní politiky.
- Bezpečnostní politika nebude organizaci chránit před všemi možnými hrozbami.
- Účinná bezpečnostní politika je bezpečnostní politika, která se trvale aktualizuje a reviduje.

12 tipů pro tvorbu politiky informační bezpečnosti 2/2

- Bezpečnostní politika má zahrnovat sledování výkonu.
- Co nemůžete obhájit/dokázat u soudu, není ani spolehlivé ani užitečné pro bezpečnost.
- Všichni musí dodržovat bezpečnostní politiky nebo čelit důsledkům.
- Účinnost a přijatelnost bezpečnosti jsou dva neoddělitelné faktory.
- Bezpečnostní politika musí být jasná, čtivá, srozumitelná.
- Předpisy a dosažení souladu s nimi jsou nutná zla.
- Když jste na pochybách, konzultujte standardy.

Politiky a systém řízení informační bezpečnosti 1/3

- Většina organizací vytváří **politiku informační bezpečnosti** podle standardu ISO/IEC 27002
  - Politika správy informační bezpečnosti založená na řízení rizik
  - Použití standardu ISO/IEC 27002 byl věnovaný vesměs dosavadní obsah

Politiky a systém řízení informační bezpečnosti 2/3

- Důvěryhodná bezpečnostní politika zpracování informací je **základní kámen systému řízení informační bezpečnosti** (*Information Security Management System*, ISMS).
- Cílem ISMS je zajistit trvalou aktuálnost politiky informační bezpečnosti a trvalou úroveň zabezpečení informací
  - Politika ISMS je buďto nadřazena politice informační bezpečnosti nebo je její přímou součástí
  - Standard definující ustavení, zavádění, provozování, monitorování, udržování a zlepšování ISMS v organizaci ISO/IEC 27001
  - Použití standardu ISO/IEC 27001 bude věnovaná následující část přednášky

Politiky a systém řízení informační bezpečnosti 3/3

- Základní ideje ISMS:
- Bázová idea: Model *Plan-Do-Check-Act* , PDCA - cyklický proces:
  → Plan (zavedení ISMS, projekt a detailní návrh ISMS) →
  → Do (implementace ISMS) →
  → Check (sledování, monitorování, měření efektivnosti ISMS) →
  → Act(definice vylepšení ISMS) →
  → Plan …
- Podpora pochopení požadavků na informační bezpečnost organizace a potřeb pro stanovení politiky a cílů informační bezpečnosti
- Zavedení a provozování opatření pro řízení informační bezpečnosti v kontextu s řízením celkových rizik činností organizace
- Monitorování a přezkoumání výkonnosti a účinnosti ISMS
- Neustálé zlepšování založené na objektivním měření

Management/správa bezpečnosti

- Požadavek na správné (bezpečné) provozování systému požaduje kontinuální provádění **správy (řízení) bezpečnosti**
- Mezi řídící úkony z hlediska bezpečnosti mj. patří
  - Zajišťování inovací systému doplňováním nových funkcí
  - Bezchybné detekování dosud neidentifikovaných zranitelností systému
- Důležitou komponentou nepřetržité správy je **auditní činnost** zabezpečovaná rolemi nezávislými na exekutivě bezpečnosti a na navrhovatelích bezpečnostního řešení
  - Typická náplň činnosti kontrolního útvaru
  - Kontrolní útvar si může ponechat odpovědnost a výkon auditu zajišťovat outsourcingem

Účel bezpečnostního auditu

- Hlavní cíle auditu
  - Kontrola, zda byly bezpečnostní procedury definované správně
  - Detekce neošetřených „bezpečnostních děr“, zranitelností nepokrytých adekvátními bezpečnostními opatřeními
- Další smysl auditu
  - Audit procedur po narušení bezpečnosti s cílem zjištění, jak k porušení došlo a kdo je za porušení odpovědný
- Role a nezávislost auditora
  - Audit provádí role plně nezávislá na bezpečnostní exekutivě
  - Žádný auditor nesmí současně pracovat jako bezpečnostní správce či bezpečnostní manažer, architekt apod. (separace odpovědností)
- Procedury/postupy auditu se definují jakou součást procedur správy a provozu systému
  - Auditor musí být schopný audit vykonat bez spoléhání se na radu „jak audit dělat“ od monitorovaných entit

Co dělat pro úspěšnost/prospěšnost auditu ISMS

- Dokumentace je úplná, pokrývá celý ISMS a je dostupná auditorům
- Jsou dostupné všechny zprávy z interních auditů a z provedených testů
- Všichni zaměstnanci musí být instruování, že vůči auditorům musí být maximálně otevření a vstřícní vč. ochotu k demonstracím činnosti
- Auditorům je nutné zpřístupnit i oblast vyššího managementu – vedení firmy
- Auditovaná strana musí být připravena diskuse s auditory
  - Zastrašování/dehonestace auditorů je cestou do pekel
  - Pomocnou ruku auditoři vesměs hodnotí pozitivně