Řízení informační bezpečnosti

PV017

Kamil Malinka
(využity materiály Doc. Staudka a konzultace Prof. Matyáše)
Verze: podzim 2024

Osnova

- Úvod a motivace
- Informační bezpečnost
- Základní pojmy
  - Aktiva
  - Zranitelnost
  - Hrozba
  - Útok
  - Riziko
  - Opatření
  - Bezpečnostní mechanismus
- Generické rysy zabezpečení

(„Safety“ X „Security“) X „Bezpečnost“

- Co tyto pojmy znamenají?
- Jaký je mezi nimi rozdíl?

(„Safety“ X „Security“) X „Bezpečnost“ 1/2

- Safety, (bezpečí)
  - Bezpečí se mnohdy chápe jako chránění proti nahodilým událostem
  - Bezpečí může mít podobu chránění osob nebo hmotných či nehmotných hodnot (aktiv) před událostmi nebo vystaveními skutečnostem způsobujícím ztráty/škody (fyzické, sociální, duchovní, finanční, politické, emocionální, pracovní, psychologické, …)
  - Tedy - bezpečí je stav bytí, ve kterém platí, že za definovaných podmínek někdo či něco nezpůsobí škodu

(„Safety“ X „Security“) X „Bezpečnost“ 2/2

- Security, (bezpečnost)
  - Ochránění proti úmyslným škodám na aktivech
  - V širším slova smyslu ochránění před poškozením osob nebo hmotných či nehmotných aktiv v důsledku úmyslných (trestných) činů, jako jsou přepadení, vloupání nebo vandalismu, krádež, …
- Information Security, (informační bezpečnost)
  - Ochrana proti úmyslným škodám, nežádoucím akcím na informačních aktivech

V čem spočívá problém informační bezpečnosti?

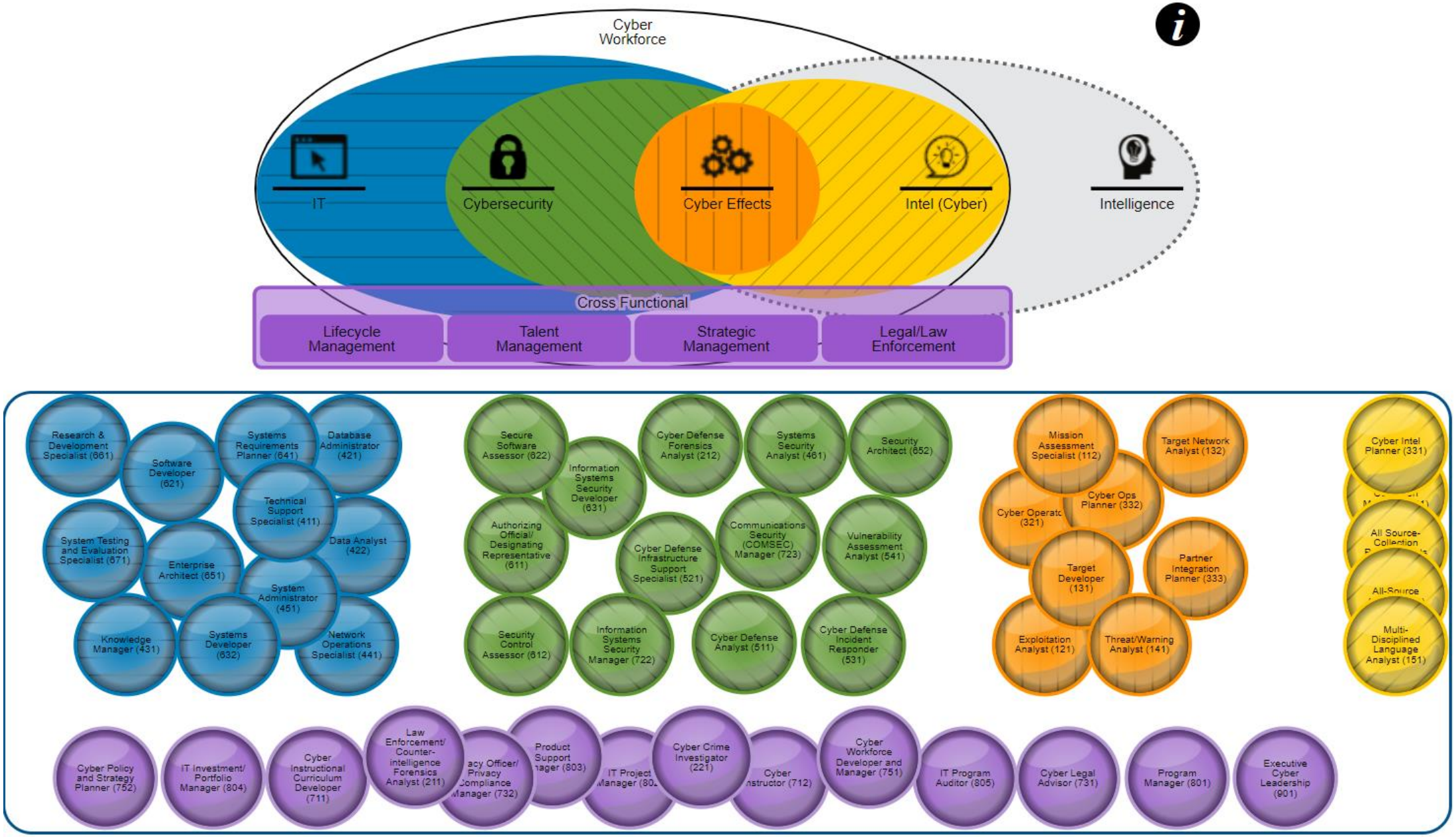
- Žijeme v informačním věku
  - Systémy zpracovávající informace jsou bází mnoha (většiny) každodenních transakcí, na nichž je založena naše společnost
  - Informace se přenáší, zpracovávají, uchovávají …
  - S informacemi souvisí procesy, systémy, lidé, sítě …
  - To vše čelí řadě rizik – cílené útoky, chyby, přírodní katastrofy…

  - Pro zajištění informační bezpečnosti je třeba systematicky zavádět vhodná opatření a zároveň zohlednit měnící se rizika i účinnost opatření, tak aby byly splněny definované bezpečnostní cíle

Motivace

- IBM: Cost of the Data Breach Report (2023)
  - Celosvětové průměrné náklady, které způsobil únik dat, dosáhnou v roce 2023 výše 4,45 milionu dolarů
  - Historicky nejvyšší hodnota a 15% nárůst za poslední tři roky
- Zákazníci bezpečnost vyžadují
- Rostoucí zákonné požadavky – ochrana soukromí (GDPR), NIS2 (Network and Information Security - širší než zákon o kyberbezpečnosti), …
- Samotné firmy si uvědomují dopady

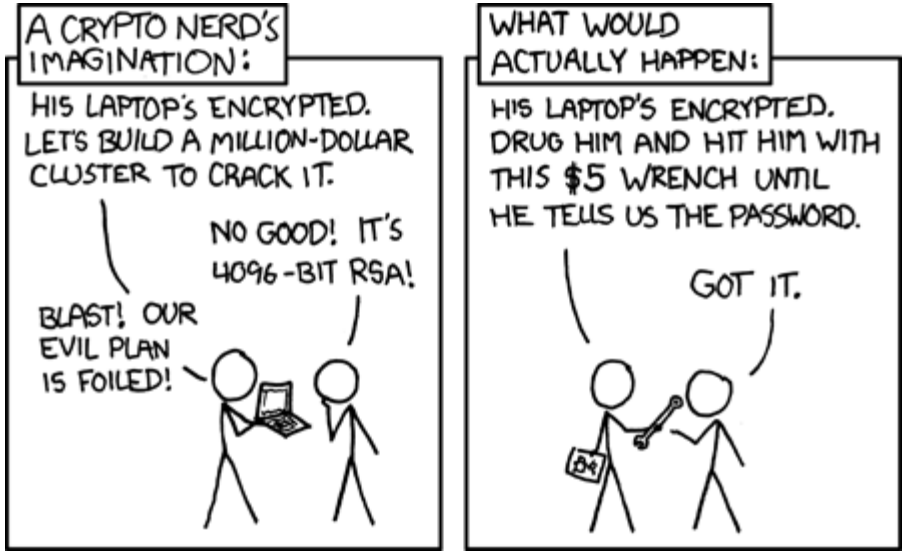
=> nedostatek pracovníků v oboru



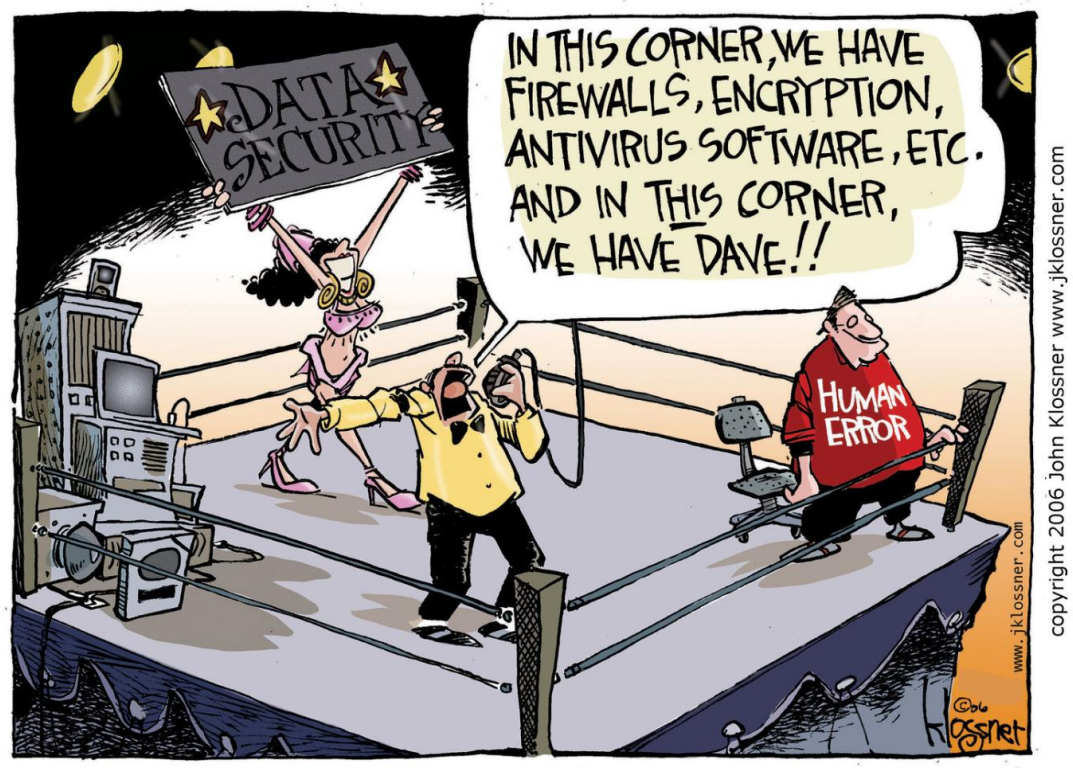
https://niccs.cisa.gov/workforce-development/career-pathways

Existuje řešení problému zajištění informační bezpečnosti ?

- **Je dosažitelná perfektní bezpečnost (absolutní eliminace všech rizik)?**



https://imgs.xkcd.com/comics/security.png



Existuje řešení problému zajištění informační bezpečnosti ?

- **Je dosažitelná perfektní bezpečnost (absolutní eliminace všech rizik)?**
- Rozlomení všech způsobů zabezpečení je otázkou pouze času (a energie)
  - Od (mili)sekund po miliardy násobků dob existence sluneční soustavy
- Na každý bezpečnostní algoritmus lze útočit „hrubou silou“
- Jaké chceme řešení?
  - Každý použitý nástroj „dostatečně“ zabezpečující jisté aktivum, musí být odpovídající uživatelskou komunitou akceptovatelný
  - Zabezpečují nástroje musí být použité vyrovnaně, systém je tak bezpečný, jak je bezpečný jeho nejslabší článek
- **Dosažení bezpečnosti informací je nekonečný proces**

Zajištění informační bezpečnosti je proces nikoli jednorázová záležitost

- Vyvíjejí se technologie
- Vznikají nové/dokonalejší formy útoků
- Mění se regulační prostředí byznysu (legislativa)
- Je nutné udržovat aktuálně validní bezpečnostní politiku
- Je nutné plánovat procesy vedoucí k periodickému vypracování a prosazování bezpečnostní politiky
  - Evidence aktiv
  - Zjištění rizik
  - Volba, vývoj, nákup, ... adekvátních opatření
  - Vypracování bezpečnostní politiky
  - Vyhodnocování účinnosti bezpečnostní politiky v provozu …
- Problém řeší manažerský systém – **Systém řízení informační bezpečnosti**

Systém řízení informační bezpečnosti

- Information Security Management System (ISMS)
- Systematický přístup pro vybudování, implementaci, provozování, monitorování, přezkoumávání, udržování a vylepšování informační bezpečnosti (InfoSec) v organizaci
- Skládá se z vhodné organizační struktury, definovaných zodpovědností, politik, obvyklých metody, procedur, plánovacích činností, zdrojů …
- Typické fáze (PDCA cyklus):
  - Ustanovení (*Estabilish*)
  - Zavádění a provoz (*Implement and Operate*)
  - Monitorování a přezkoumání (*Monitor a Review*)
  - Udržování a zlepšování (*Maintain and Improve*)

PDCA cyklus vývoje ISMS

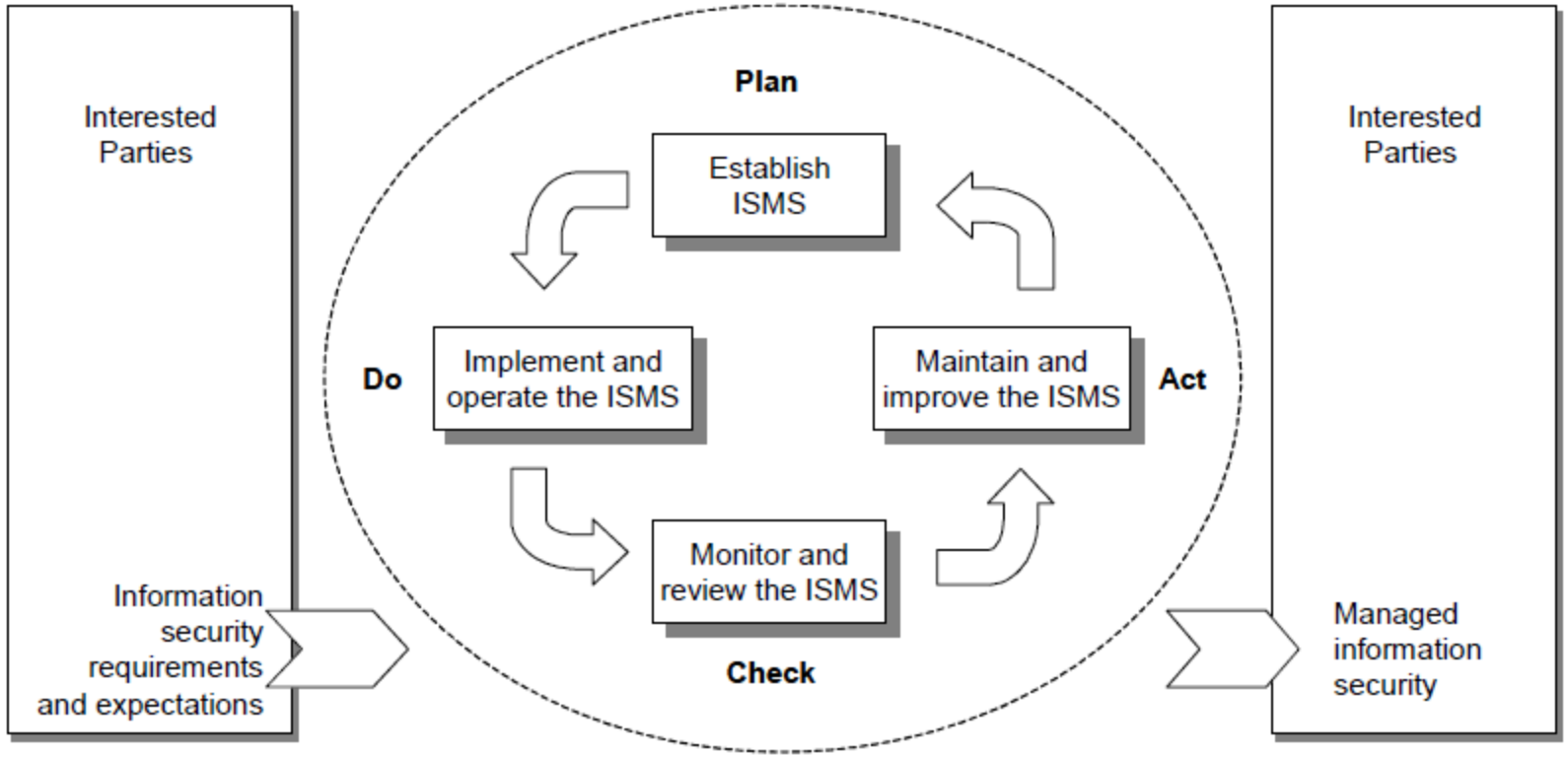
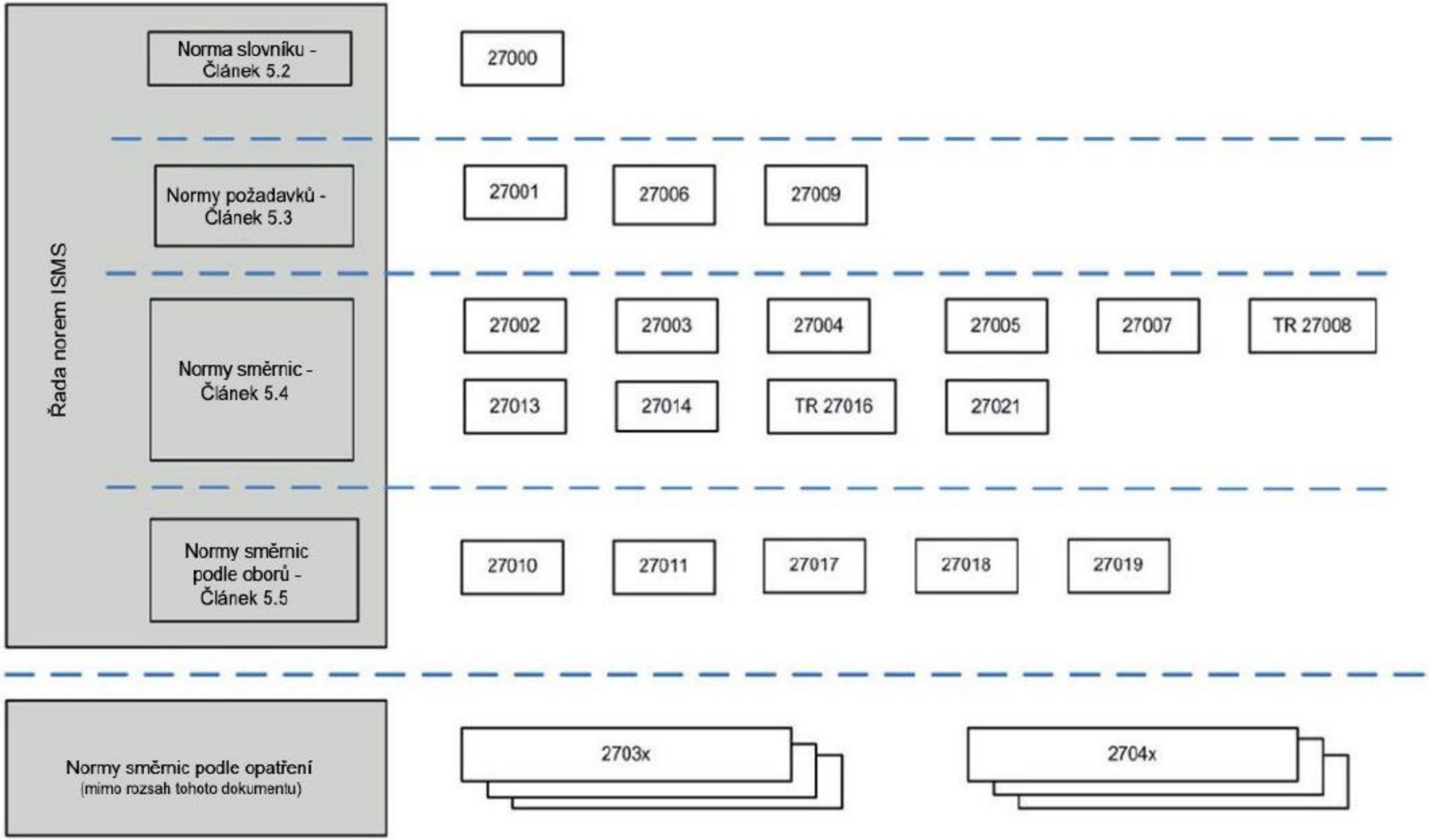


Figure 1 — PDCA model applied to ISMS processes

Převzato z ISO/IEC 27001

Roadmapa ISO standardů, na kterých je přednáška vybudována

- Rodina ISO/IEC 27k
  - Důraz na:
    - **ISO/IEC 27001: 2014 - Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky**
    - **ISO/IEC 27002: 2014 - Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací**
    - ISO/IEC 27003: 2018 - Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Pokyny
    - ISO/IEC 27004: 2018 - Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací - Monitorování, měření, analýza a hodnocení
    - ISO/IEC 27005: 2019 - Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací
    - ISO/IEC 27014: 2021 - Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí - Správa a řízení bezpečnosti informací
- ISO/IEC 15408

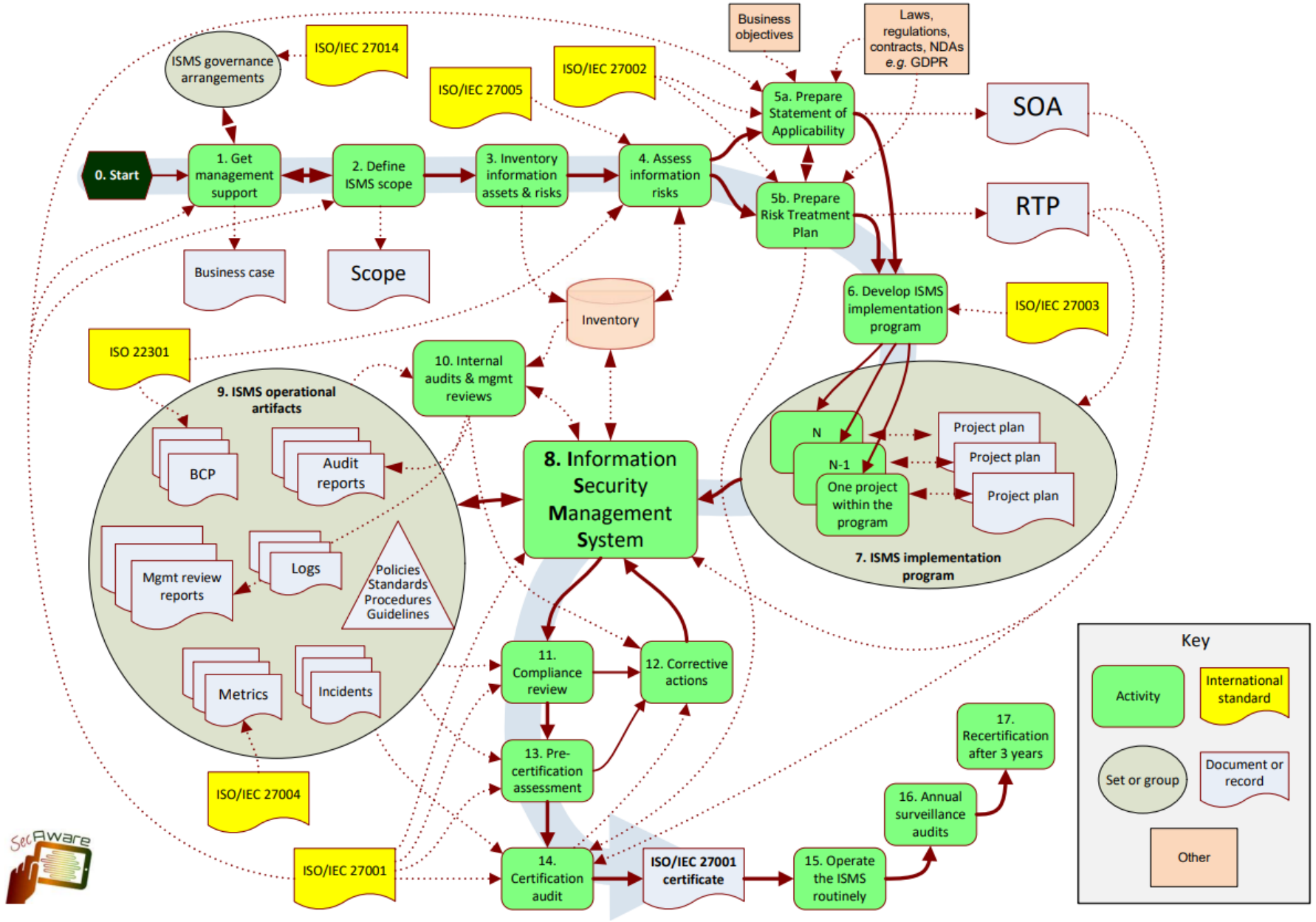


Převzato z ISO/IEC 27001

Klíčové komponenty ISMS

- Společné pro jakýkoliv typ řízení:
  - Politika
  - Osoby s definovanými odpovědnostmi
  - Procesy řízení pro:
    - Ustanovené politiky, zvyšování povědomí, plánování, implementace, provozování, posuzování, přezkoumání, zlepšování
  - Dokumentované informace

- Specifické pro ISMS:
  - Posuzování rizik bezpečnosti informací
  - Ošetření rizik vč. určení a implementace kontrolních opatření



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

Osnova

- Úvod a motivace
- Informační bezpečnost
- Základní pojmy
  - Aktiva
  - Zranitelnost
  - Hrozba
  - Útok
  - Riziko
  - Opatření
  - Bezpečnostní mechanismus
- Generické rysy zabezpečení

Co se rozumí informační bezpečností? 1/5

- ISO/IEC 27002: 2005, Information technology — Security techniques — Code of practice for information security management
  - Kodex, dokument, obsahující výčet technologií, standardů, politik a manažerských praktik vhodných pro zajištění informační bezpečnosti

- Standard říká, že informace je bezpečná, když je
  - Přístupná pouze oprávněným subjektům
  - Modifikovatelná pouze oprávněnými subjekty
  - Dostupná oprávněným subjektům (do stanovené doby)

Co se rozumí informační bezpečností? 2/5

- Informace je bezpečná, když je zajištěná její
  - Důvěrnost (*Confidentiality*, C)
  - Integrita (*Integrity*, I)
  - Dostupnost (*Availability*, A)

- Dále se k těmto třem rysům informační bezpečnosti řadí udržování dalších vlastností:
  - Autenticita (*Authenticity)*
    - Pravost, původnost
  - Zodpovědnost, prokazatelnost (*Accountability)*
  - Nepopiratelnost (*Non-repudiation)*
  - Spolehlivost (*Reliability)*
    - Bezporuchovost, činnost ve shodě se specifikací, někdy se dává specificky mimo počítačovou bezpečnost

Co se rozumí informační bezpečností? 3/5

- **Důvěrnost** (*Confidentiality)*
  - Cílem je omezení přístupu k informacím a jejich zpřístupnění pouze oprávněným uživatelům („správným lidem“) a zabránění přístupu k informacím nebo jejich prozrazení neoprávněným uživatelům („špatným lidem“)
  - Zajištěním důvěrností se rozumí ochrana informací před neautorizovaným zpřístupněním - odhalením, prozrazením
  - Důvěrnost se nevztahuje pouze na uchovávání informací, ale také na přenos informací
  - Neautorizované, neočekávané, nežádoucí zpřístupnění může vést ke ztrátě důvěry, k potížím, k právním akcím vůči organizaci, …
  - Důvěrnost úzce souvisí s omezováním přístupu k osobním údajům fyzických osob

Co se rozumí informační bezpečností? 4/5

- **Integrita**, celistvost (*Integrity)*
  - Cílem je zajištění důvěryhodnosti informačních zdrojů
  - Integrita zdroje znamená, že změny zdroje smí provádět pouze autorizované subjekty a autorizované mechanismy
  - **Integrita dat** - data nesmí být nevhodně, náhodně a/nebo záměrně nějakou škodlivou činností změněna
  - **Integrita původu** - data skutečně pochází od osoby/subjektu, který je validně poskytuje, nikoli od podvodníka
  - Dotčená osoba či subjekt přistupují ke správným informacím, tj.
    - K platným (validním) informacím (odrážejí skutečné okolnosti) a
    - K spolehlivým informacím (za stejných okolností lze generovat stejná data)
  - Informace mají být chráněné před podvodnou, nezákonnou, nepatřičnou modifikací - neautorizovanými změnami dat, software, hardware, …
  - Aktiva musí být kompletní a korektní
  - Nepatřičná modifikace může být úmyslná nebo neúmyslná
  - Ignorování škod na integritě může vést k vydání chybných rozhodnutí, k podvodu, k nesprávným akcím, …

Co se rozumí informační bezpečností? 5/5

- **Dostupnost** (informačních zdrojů) (A*vailability)*
  - Nedostupný IS v okamžiku potřeby je přinejmenším stejně špatný jako žádný IS
  - Informace vytvořené a uložené organizací musí být dostupné autorizovaným subjektům.
  - Dostupnost, stejně jako jiné aspekty bezpečnosti, může být ovlivněna
    - Ryze technickými problémy (např. nefunkční část počítače nebo komunikační infrastruktury)
    - Přírodními jevy (např. větrem nebo vodou)
    - Lidskými faktory (havárie nebo záměrné útoky)
  - Pokud dojde ke ztrátě dostupnosti systému/informace kritické pro plnění podnikatelských činností organizace pro koncového uživatele, může to podnikatelské činnosti negativně ovlivnit
  - Ztráta funkcionality či snížení efektivnosti provozu může snižovat výkonnost uživatelů podporujících podnikání organizace

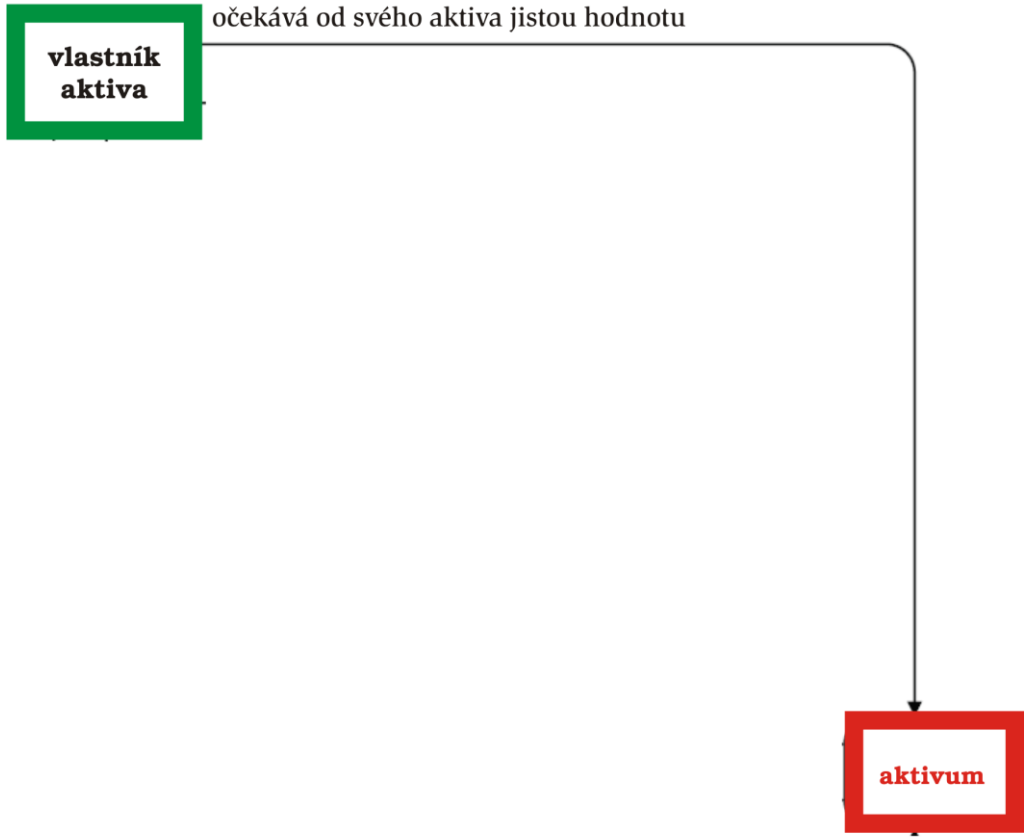
Osnova

- Úvod a motivace
- Informační bezpečnost
- Základní pojmy
  - Aktiva
  - Zranitelnost
  - Hrozba
  - Útok
  - Riziko
  - Opatření
  - Bezpečnostní mechanismus
- Generické rysy zabezpečení

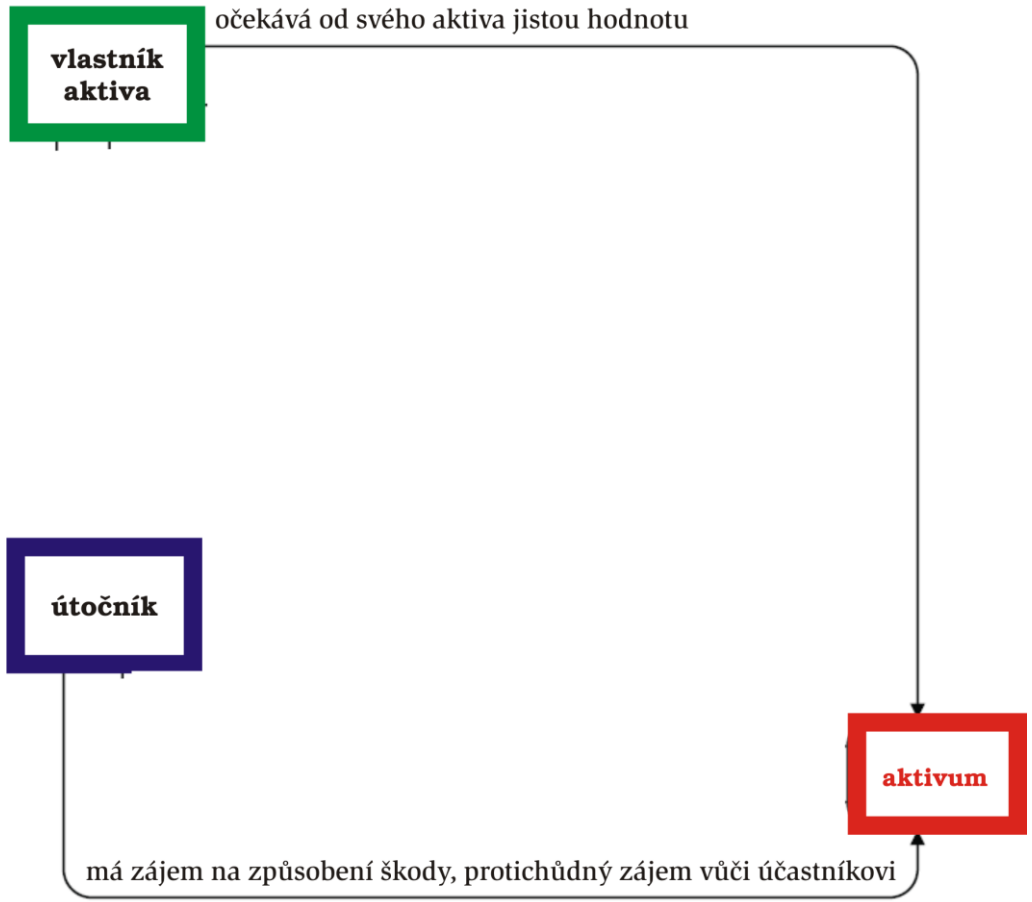
Základní pojmy informační bezpečnosti

- **Aktivum** (*Asset*) - cokoli hodnotného, užitečného, věc, výhoda, zdroj
- **Zranitelnost** (*Vulnerability*) - slabina využitelná ke způsobení škod/ztrát organizaci útokem
- **Hrozba** (*Threat*) – potenciální příčina nechtěného incidentu
- **Útok** (*Attack*) – pokus o způsobení škody na aktivech (útočník využije slabinu v ochranách aktiv (zranitelnost) s cílem způsobit škodu
- **Bezpečnostní incident** (*Security incident*) – událost, která může ohrozit bezpečnost informací
- **Riziko** (*Risk*) - pravděpodobnost, že se v daném zranitelném místě uplatní hrozba
- **Opatření** (*Control*) – prostředek, který modifikuje riziko

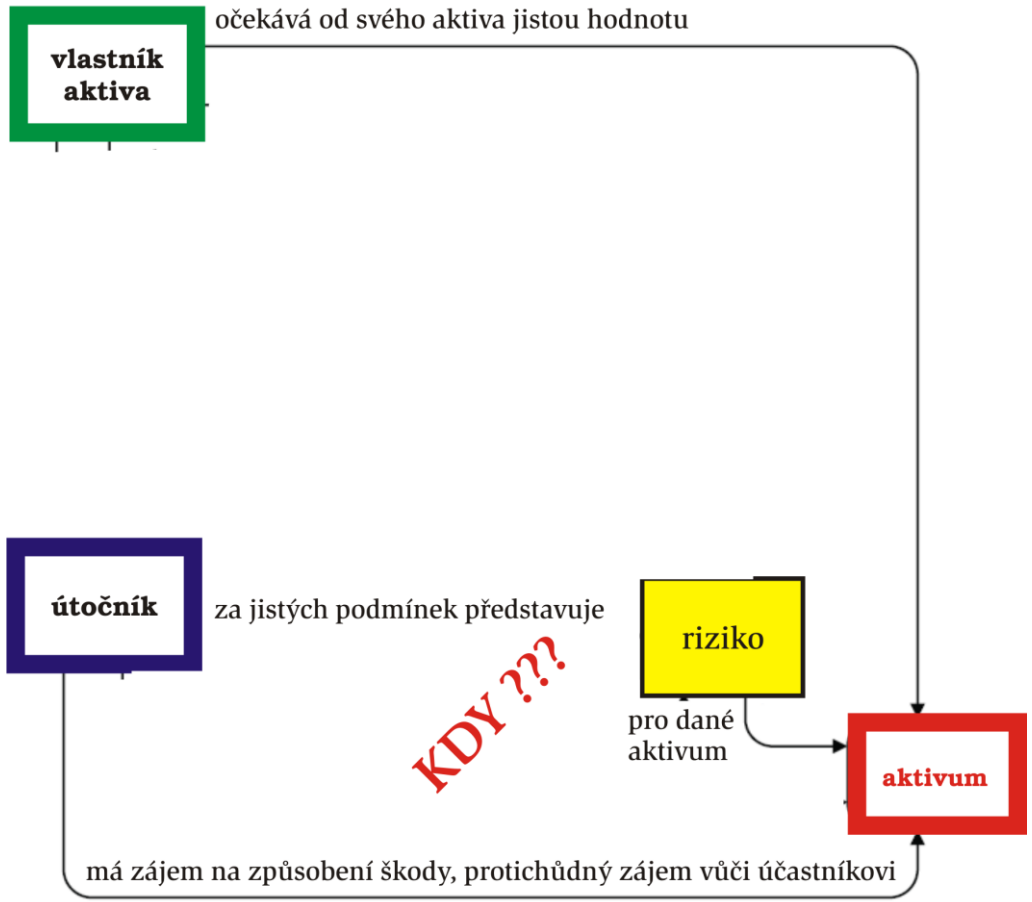
Obecný model zabezpečování



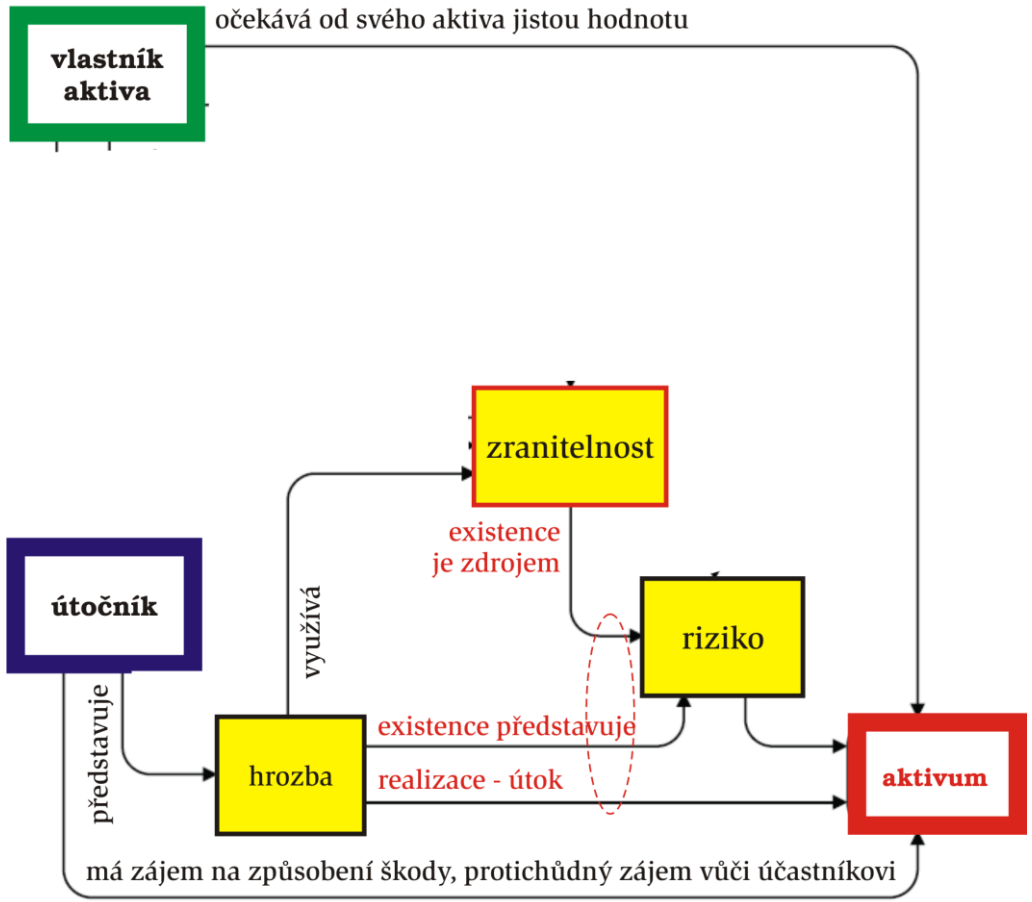
Obecný model zabezpečování



Obecný model zabezpečování



Obecný model zabezpečování

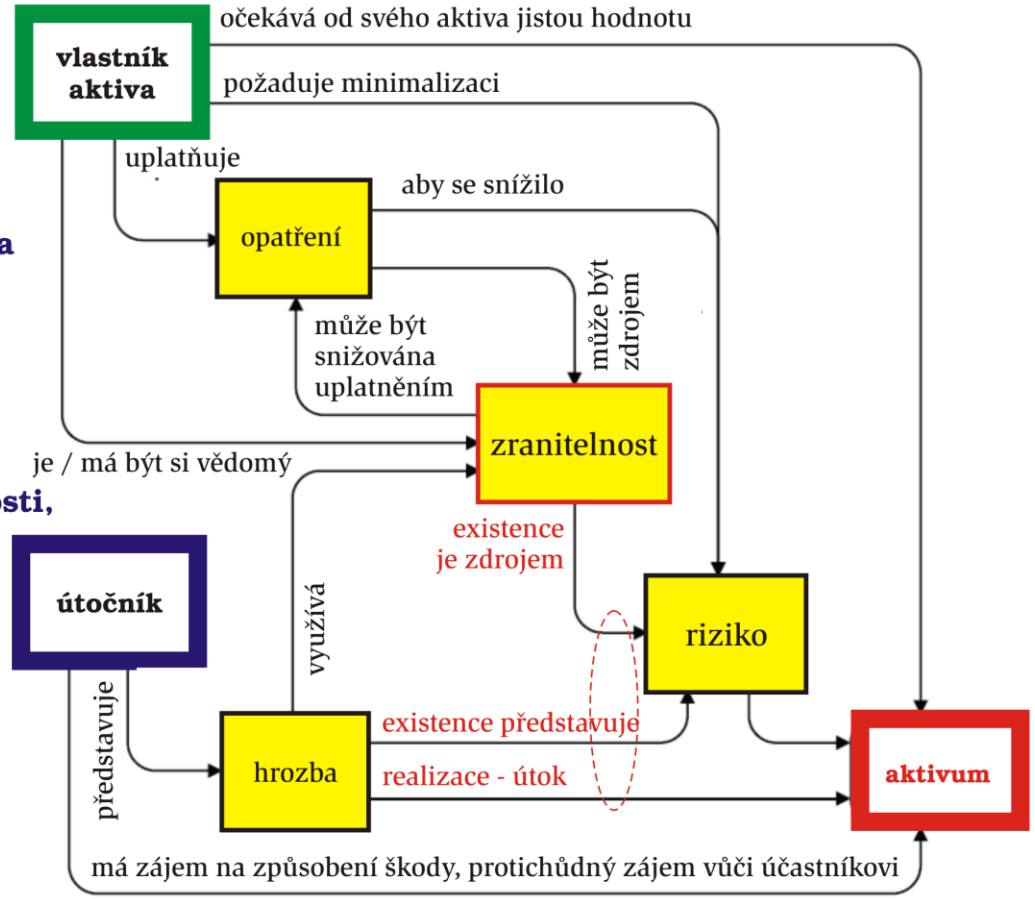


Obecný model zabezpečování

Účinná opatření determinují procesy **řízení rizik**

Validní uplatňování opatření předpisuje **bezpečnostní politika**

Aktuálnost opatření a bezpečnostní politiky zajišťují procesy **systému řízení informační bezpečnosti,** ISMS *(Information Security Management System)*



Generický problém budování bezpečných (IT) systémů

- Systém bude úspěšný (bezpečný), když bude zajišťovat ochranu proti všem možným útokům, a to vč. útoků, které se v době jeho tvorby dosud nevyskytly
- **Útočník bude úspěšný, když pro útok využije jedinou nedokonalost v bezpečnostních ochranách**
  - Může vyčkávat až mu technologický rozvoj poskytne adekvátní útočný nástroj, jehož existenci tvůrci systému vůbec nepředpokládali
  - Škála dostupných relevantních bezpečnostních nástrojů nebude nikdy úplná z hlediska množiny v budoucnu potenciálních hrozeb
  - Reálné účinky dostupných bezpečnostních nástrojů mnohdy nesplňují nebo postupně přestávají efektivně plnit jejich původně zamýšlený cíl

Zajištění informační bezpečnosti je komplexní problém 1/2

Příklad

- Pokud často necháváte notebook (s podnikovými daty) na zadním sedadle auta, pravděpodobně Vám ho dříve nebo později někdo ukradne
- Jak snížit riziko takové krádeže? Jak zabránit úniku dat?
  - Lze zavést pravidla (vydáním předpisu/politiky):
    - Notebook nelze nechávat bez dozoru
    - Parkovat auto lze pouze v prostoru s fyzickou ochranou,
    - Přístup k notebooku se musí chránit silným heslem,
    - Citlivá data uložená v notebooku musí být zašifrovaná
    - V pracovní dohodě zaměstnanec podepíše odpovědnost za ztrátu, vyzrazení, …, citlivých dat
- Tato pravidla ovšem nebudou účinná, pokud s nimi firma zaměstnance neseznámí

Zajištění informační bezpečnosti je komplexní problém 2/2

- Informační bezpečnost se nezajistí jedním opatřením, pro její dosažení se jich musí uplatňovat více, současně
  - Opatření se nebudou týkat pouze IT
  - Musí se řešit organizační problémy, řízení lidských zdrojů, fyzická bezpečnost, dodržování legislativních omezení, proškolování
  - Nestačí chránit pouze notebooky, firma může mít uložená data na serverech, v zásuvkách pracovních stolů, v mobilech zaměstnanců, na USB pamětech, v hlavách zaměstnanců, …
- Zajištění informační bezpečnosti vyžaduje vytvoření a udržování komplexního bezpečného prostředí
  - Taková prostředí jsou již definovaná standardy: ISO 27001, COBIT, NIST SP 800,…

Příklad - Přihlášení do IS MU

- Uživatel?
- Aktiva?
- Útočník?
- Škoda?
- Hrozba?
- Zranitelnost?
- Riziko?

Příklad

- Účastník – studenti, akademici, úředníci, alumni, … třetí strany?
- Aktiva – data, osobní údaje,
- Útočník – jiný student, generický hacker hledající zdroje
- Škoda – únik osobních dat, uniklá hesla, změna známky – poškození na pověsti
- Hrozba – DoS, phishing, cross-site scripting
- Zranitelnost – slabá hesla, špatná kontrola vstupů, OS, nešifrovaná data, absence TLS,
- Riziko – …

Osnova

- Úvod a motivace
- Informační bezpečnost
- Základní pojmy
  - Aktiva
  - Zranitelnost
  - Hrozba
  - Útok
  - Riziko
  - Opatření
  - Bezpečnostní mechanismus
- Generické rysy zabezpečení

Předmět ochrany – aktiva (*assets*) 1/2

- **Aktivum** - předmět, myšlenka, informace, … mající pro organizaci hodnotu
- Jedná se o ekonomický zdroj, zdroj podnikatelských procesů - cokoliv **hmotné** (*tangible*) či **nehmotné** (*intangible*) povahy, co může být vlastněno nebo ovládáno (řízeno, spravováno) nějakou entitou (organizací, …) s cílem produkovat pozitivní ekonomickou hodnotu
- **Hmotná** aktiva (konkrétní, jasná, zřejmá, hmatatelná, …) - peníze, budovy, pozemky, dopravní prostředky, sklady, zařízení, služby, lidé, …
- **Nehmotná** aktiva (neurčitá, nepostižitelná, …) - software, data, patenty, autorská práva, licence, obchodní známka, jméno, pověst, …
- V oblasti IT existují tři hlavní kategorie aktiv:
  - Data
  - Systémy obsahující data a komunikační infrastruktura
  - Lidské zdroje k provozu, pro plnění cílů organizace …

Předmět ochrany – aktiva (*assets*) 2/2

- Informační aktivum dle zákona o kybernetické bezpečnosti:
  - Informace nebo služba, kterou zpracovává nebo poskytuje informační nebo komunikační systém
  - Zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a/nebo komunikačního systému,
  - Technické vybavení,
  - Komunikační prostředky
  - Programové vybavení
  - Objekty informačního a/nebo komunikačního systému

Osnova

- Úvod a motivace
- Informační bezpečnost
- Základní pojmy
  - Aktiva
  - Zranitelnost
  - Hrozba
  - Útok
  - Riziko
  - Opatření
  - Bezpečnostní mechanismus
- Generické rysy zabezpečení

Zranitelnost (*Vulnerability*)

- Slabina využitelná ke způsobení škod/ztrát organizaci útokem - materializací hrozby provedenou útočníkem
- Zanechávání hořlavého materiálu (papíru) v serverovně je zranitelností využitelnou externí hrozbou - požárem, ohněm
- Ne každá zranitelnost je známá, např. zranitelnost nultého dne (zero day vulnerability)

Zranitelnosti

- Zranitelnosti se mohou nacházet
  - ve fyzickém uspořádání,
  - v organizačních schématech,
  - v administrativních opatřeních,
  - v personální politice,
  - v logických a technických opatřeních,
  - v hardwaru, v softwaru, v datech,
  - v návrhu architektury systému,
  - v systému řízení informační bezpečnosti informací.
- Konkrétní příklady naleznete v dodatku této přednášky
  - Příklady zranitelností dle zákona o kybernetické bezpečnosti

Common Vulnerabilities and Exposures (CVE)

- CVE poskytuje organizacím bezplatný slovník pro zlepšení jejich kybernetické bezpečnosti
- Provozováno neziskovou organizací MITRE
- Záznam CVE popisuje známou zranitelnost
- Každá položka CVE obsahuje standardní identifikační číslo s indikátorem stavu (např. "CVE1999-0067", "CVE-2014-12345", "CVE-2016-7654321"), stručný popis a odkazy na související zprávy o zranitelnostech a doporučení
- Každé ID CVE je formátováno jako CVE-YYYY- NNNNN. Část YYYY je rok přidělení ID CVE nebo rok zveřejnění zranitelnosti.
- Na rozdíl od databází zranitelností neobsahují záznamy CVE informace o riziku, opravě dopadu nebo jiné technické informace

CVE-2023-28858 PUBLISHED

View JSON

Important CVE JSON 5 Information +

Assigner: Mitre
Published: 2023-03-26 **Updated:** 2023-03-30

redis-py before 4.5.3 leaves a connection open after canceling an async Redis command at an inopportune time, and can send response data to the client of an unrelated request in an off-by-one manner. NOTE: this CVE Record was initially created in response to reports about ChatGPT, and 4.3.6, 4.4.3, and 4.5.3 were released (changing the behavior for pipeline operations); however, please see CVE-2023-28859 about addressing data leakage across AsyncIO connections in general.

Product Status

Learn About the Versions Section +

Information not provided

References

- https://github.com/redis/redis-py/pull/2641
- https://github.com/redis/redis-py/issues/2624
- https://github.com/redis/redis-py/compare/v4.5.2...v4.5.3
- https://github.com/redis/redis-py/compare/v4.4.2...v4.4.3
- https://github.com/redis/redis-py/compare/v4.3.5...v4.3.6
- https://openai.com/blog/march-20-chatgpt-outage

View additional information about CVE-2023-28858 on NVD.
(Note: The NVD is not operated by the CVE Program)

Osnova

- Úvod a motivace
- Informační bezpečnost
- Základní pojmy
  - Aktiva
  - Zranitelnost
  - Hrozba
  - Útok
  - Riziko
  - Opatření
  - Bezpečnostní mechanismus
- Generické rysy zabezpečení

Hrozba (Threat)

- Potenciální možnost využití zranitelného místa k útoku útočníkem
  - Tj. potenciální příčina bezpečnostní události/incidentu, jejímž důsledkem může být poškození aktiva z hlediska zajištění jeho důvěrnosti, integrity a/nebo dostupnosti
- Co je hodnotné pro vlastníka aktiva, je pravděpodobně hodnotné i pro někoho jiného

Typy hrozeb 1/2

- **Odhalení** (*Disclosure*) citlivých důvěrných dat, postupů, …
  - Např. analýza komunikačního provozu - pasivní zjišťování kdo s kým kdy co komunikuje
- **Podvod**, klamání (*Deception*)
  - Modifikace dat, falšování identity, popírání autorství (zprávy, dat), odmítání faktu přijetí zprávy, hoaxs (šíření falešných zpráv), maškaráda (Masquerade) - útočník vystupuje jako legitimní uživatel
  - Diseminace zlomyslného software (Planting) - trojský kůň, vir, …
  - Modifikace systému, příprava předmostí pro příští útoky
- **Narušení**, ničení (*Disruption*)
  - Modifikace (dat, programu, chování technického prostředku, …)
    - Neautorizovaná osoba získá přístup do systému a modifikuje v něm uložená data, neoprávněně používá zdroje,
  - Modifikace přenášených dat
    - Neoprávněné aktivní zásahy do komunikací autorizovaných entit
- Konkrétní příklady naleznete v dodatku této přednášky
  - Příklady hrozeb dle zákona o kybernetické bezpečnosti

Typy hrozeb 2/2

- Příklady hrozeb pro dotčenou organizaci
  - Vnitřní hrozby
    - Zdroj hrozby (útočník) se nachází uvnitř (zranitelné) organizace
    - Nespokojený zaměstnanec přihlásí k serveru své sítě a v jemu dostupných sdílených složkách vymaže všechna data důležitá pro organizaci, která dosud nebyla zálohována
    - Nedostatečně znalí zaměstnanci dělající chyby při používání a implementaci aplikací, …
  - Vnější hrozby
    - Zdroj hrozby (útočník) se nachází mimo vnitřní síť organizace
    - Útočník z Internetu nalezl hraniční směrovač sítě organizace, připojil se k němu a pomocí slovníkového útoku se snaží zjistit hesla uživatelů
    - Hackeři na Internetu, konkurence, cílení či náhodní nepřátelé, …

STRIDE - Framework pro modelování hrozeb

- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nformation Disclosure
- **D**enial of Services
- **E**levation of Privilege

- https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN

STRIDE příklady

- **S**poofing: poslání emailu pod jinou identitou, odposlechnutí WiFI jména a hesla, vykonání finanční transakce pod jinou identitou, falešná webová stránka zjišťující jména a hesla, …
- **T**ampering: přístup do DB skrze rozhraní pro správu (default admin credentials), změna svých zdravotních údajů v medicínské aplikaci VZP, změna stavu onboardingu
- **R**epudiation: nelze zjistit kdo poslal příkaz k mazání záloh
- **I**nformation Disclosure: získání admin přístupu, únik dat z chybně zpřístupněného cloudového prostoru
- **D**enial of Services: rušení rádiových frekvencí vybrané IoT sítě
- **E**levation of Privilege: neoprávněné čtení dat z paměti, kde mohou být uložené hesla

Osnova

- Úvod a motivace
- Informační bezpečnost
- Základní pojmy
  - Aktiva
  - Zranitelnost
  - Hrozba
  - Útok
  - Riziko
  - Opatření
  - Bezpečnostní mechanismus
- Generické rysy zabezpečení

Útok, bezpečnostní incident (*Attack, Security incident*)

- Útok provádí útočník využitím zranitelnosti informačního aktiva (realizovaná hrozba)
- Způsobuje škodu na aktivech
  - Snížením hodnoty, zničením, znepřístupněním, … aktiva, … zveřejněním důvěrného aktiva, …
- Generická kategorizace útoků
  - Přírodní katastrofy - hurikán, zemětřesení, požár, mohou zničit nezálohovaná data (zálohovat ve vzdálené lokalitě!)
  - Externí útoky - krádeže dat o kartách/lidech, hackery, profesionály
  - Interní útoky - např. web Wikileaks vznikl z interně zcizených dat
  - Selhání, neúmyslné lidské chyby - výpadek napětí, spojů, disků, …, vylití kávy do klávesnice, omylem zrušená data, …

Klasifikace (citlivých) aktiv dle zákona o kybernetické bezpečnosti 1/3

- **Stupnice pro hodnocení důvěrnosti aktiv**
- Nízká
  - …
- Střední
  - Aktiva nejsou veřejně přístupná a tvoří know-how odpovědných orgánů a osoby, ochrana těchto informací **není** vyžadována žádným právním předpisem nebo smluvním ujednáním
  - *Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu*
- Vysoká
  - Aktiva nejsou veřejně přístupná a jejich ochrana **je** vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními
  - *Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu*
  - *Přenosy informací jsou chráněny pomocí kryptografických prostředků*
- Kritická
  - …

Klasifikace (citlivých) aktiv dle zákona o kybernetické bezpečnosti 2/3

- **Stupnice pro hodnocení integrity aktiv**
- Nízká
  - …
- Střední
  - Aktivum **může vyžadovat** ochranu z hlediska integrity
  - Narušení integrity aktiva **může vést** k poškození oprávněných zájmů odpovědných orgánů a osob a může se projevit **méně závažnými** dopady na ostatní aktiva
  - *Pro ochranu integrity jsou využívány standardní nástroje např. omezení přístupových práv pro zápis*
- Vysoká
  - Aktivum **vyžaduje** ochranu z hlediska integrity
  - Narušení integrity aktiva **vede** k poškození oprávněných zájmů odpovědných orgánů a osob s **podstatnými** dopady na ostatní aktiva
  - *Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu*
- Kritická
  - …

Klasifikace (citlivých) aktiv dle zákona o kybernetické bezpečnosti 3/3

- **Stupnice pro hodnocení dostupnosti aktiv**
- Nízká
  - …
- Střední
  - Narušení dostupnosti aktiva by nemělo překročit **dobu pracovního dne**, **dlouhodobější** výpadek vede k možnému ohrožení zájmů odpovědných orgánů a osob
  - *Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy*
- Vysoká
  - Narušení dostupnosti aktiva by nemělo překročit **dobu několika málo hodin**
  - **Jakýkoli** výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů odpovědných orgánů a osob. Aktiva jsou považována jako velmi důležitá.
  - *Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy či výměnou technických aktiv*
- Kritická
  - …

Reálný příklad - ransomware

- Kyberútoky na české nemocnice
- Ransomware v Nemocnici Rudolfa a Stefanie Benešov
  - 11.12.2019, 3 týdny omezení provozu, škoda 59 milionů Kč
  - Nešlo o cílený útok, napadeny i další státní instituce
  - Dopady: omezení lékařských výkonů, nemocnice nedostala proplacené finanční prostředky od zdravotních pojišťoven na plánovaná vyšetření, zákroky, operace apod., dále pak ztráty transfúzní stanice z důvodu omezení výroby a prodeje krevních derivátů, nákupu krevních přípravků apod. Nemalé finanční prostředky nemocnice investovala do nového zabezpečovacího systému, reinstalace jednotlivých softwarů a do práce na obnově systémů včetně proškolení personálu.
  - https://www.policie.cz/clanek/stredocesti-kriminaliste-ukoncili-vysetrovani-ransomware-utoku-na-benesovskou-nemocnici.aspx
- Fakultní nemocnice u sv. Anny v Brně (FNUSA)
  - 2020, 4 týdny omezení provozu
- Psychiatrická nemocnice v Kosmonosech
  - 2020, 10 dní omezení provozu

Osnova

- Úvod a motivace
- Informační bezpečnost
- Základní pojmy
  - Aktiva
  - Zranitelnost
  - Hrozba
  - Útok
  - Riziko
  - Opatření
  - Bezpečnostní mechanismus
- Generické rysy zabezpečení

Riziko (*Risk*)

- Velikost rizika je daná pravděpodobností provedení útoku a výší škody vzniklé útokem)
- Pravděpodobnost uplatnění hrozby je determinovaná
  - Snadností/obtížností využití zranitelností aktiva
  - Množstvím a schopnostmi (dovednostmi) potenciálních útočníků

- V užším slova smyslu - pravděpodobnost, že se v daném zranitelném místě uplatní hrozba
- Charakteristika šířeji chápaného pojmu „riziko“
  - Pravděpodobnost výskytu incidentu x způsobená škoda
  - Význam rizika se odvozuje z kombinace pravděpodobnosti výskytu a dopadu relevantního útoku (výše způsobené škody)
  - Rizika mohou být různě závažná (katastrofická/velká, akceptovatelná, nevýznamná, …)

Model útočníka

- Atributy protivníka, které je třeba zvážit:
  1. *Cíle* - často naznačují cílové aktiva vyžadující zvláštní ochranu
  2. *Metody* - např. předpokládané techniky útoku nebo typy útoků
  3. *Schopnosti* - výpočetní zdroje (CPU, úložiště, šířka pásma), dovednosti, znalosti, personál, příležitosti (např. fyzický přístup k cílovému zařízení),
  4. *Úroveň financování* - ovlivňuje odhodlání útočníka, metody a schopnosti
  5. *Outsider vs. insider* - útok provedený bez předchozího přístupu k cílovému systému je útok zvenčí. Insider má obvykle určitou počáteční výhodu– např. znalosti, oprávnění na nižší úrovni atd.

Klasifikace útočníků

- Rozdělení možných útočníků podle jejich znalostí, schopností, finančních možností, přístupu ke speciálnímu vybavení apod.
- Klasifikace firmy IBM:
  - **Třída 0 – script kiddies**
    - Bez znalosti systému, využití již existujících nástrojů metodo pokus/omyl
  - **Třída 1 – chytří nezasvěcení útočníci**
    - Často velmi inteligentní, nedostatečné znalosti systému, přístup pouze ke středně sofistikovanému vybavení, využití zranitelností existujících v systému
  - **Třída 1,5 – dobře vybavení lidé z venku**
    - S dobrým laboratorním vybavením a základními znalostmi systému – např. univ. laby.
  - **Třída 2 – zasvěcení insideři**
    - Mají značné specializované technické vzdělání i zkušenosti, sofistikované nástroje, …
  - **Třída 3 – dobře finančně podporované organizace**
    - Schopné vytvořit týmy specialistů, zajištěné dobrými finančními zdroji, provádí detailní analýzy systému, nejkvalitnější nástroje, tvorba nových útoků…

Osnova

- Úvod a motivace
- Informační bezpečnost
- Základní pojmy
  - Aktiva
  - Zranitelnost
  - Hrozba
  - Útok
  - Riziko
  - Opatření
  - Bezpečnostní mechanismus
- Generické rysy zabezpečení

Opatření (*control, measure, security enforcing function*)

- Nástroj pro snížení/eliminaci rizika
- Problém eliminace či snižování rizik řeší uplatňování/prosazení opatření
  - Plné odstranění rizika bývá vesměs neefektivní
  - Opatření typicky rizika redukují/snižují, neodstraňují je
  - Opatření se mají implementovat pouze pro řešení specifických, identifikovaných rizik
- Pro implementaci opatření se používají mechanismy na bázi vhodných technologií (software, hardware, administrativa)
- Typické opatření je kombinací technologie a procesů (výrazná role politiky a vzdělávání uživatelů)
  - Např. antivirové opatření:
    - Software instalovaný v bráně a v počítači
    - Procedura zajišťující pravidelné aktualizace báze dat
    - Výchova uživatele k neotevírání neočekávaných příloh mailů

Jak a co si vybrat?

Autentizace, autorizace, řízení přístupu, podpisování, ochrana komunikací, Audit, detekce útoků, návraty do bezpečného stavu, detekce virů, Identifikace, správa krypto-klíčů, licenční politiky, Řízení opakovaného použití objektů, Zamykání objektů pro zajištění logické konzistence objektů zpracovávaných paralelními transakcemi,, Stínění, trezory, zámky, strážní, visačky - jmenovky, protipožární ochrana, záložní generátory energie, autentizátory na bázi identifikačních karet, autentizační kalkulátory, šifrovače, firewally, archivační paměť páskového typu, Funkce řízení přístupu, kryptografické utajování, digitální podepisování, antivirové prostředky, Normy pro návrh, kódování, testování, údržbu programů, Směrnice pro výběr a školení důvěryhodných osob, pro tvorbu hesel, pro autorizační postupy, pro přijímací a výpovědní postupy, Právní normy, zákony, vyhlášky, předpisy, etické normy,

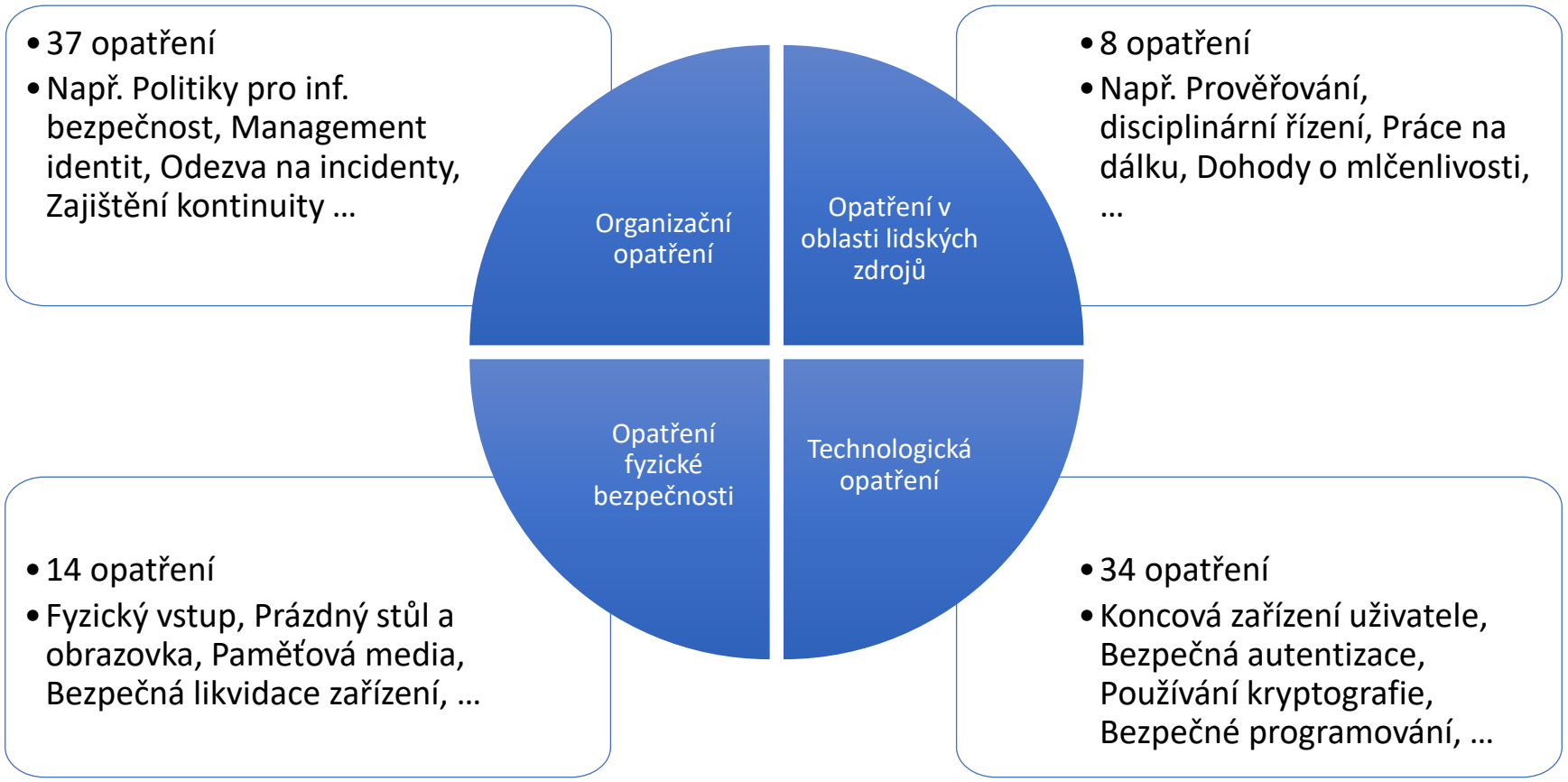
Přidělení adresné odpovědnosti za bezpečnost kritických podnikatelských procesů, Vypracování a udržování aktuálních plánů bezpečnosti systému dokumentujících používaná opatření a uvádějící plánovaná opatření, Implementace personálních opatření typu "rozdělení oprávnění", "přidělování nejmenších potřebných oprávnění", povolení přístupu pouze po registraci, Průběžné vedení školení cílených na zvyšování bezpečnostního uvědomění a technický výcvik zaměstnanců a uživatelů systému, Periodické zkoumání efektivnosti bezpečnostních opatření, Periodický audit systému, Vedení průběžného řízení rizik pro ohodnocování a zvládání rizik, Zmocnění systému k určení a akceptování zbytkového rizika, Plán zachování kontinuity činnosti po havárii, Plán činnosti po detekci incidentu (útoku na bezpečnost), Řízený fyzický přístup k datovým médiím, Virové ochrany, Bezpečné strukturované vodiče, Procedury pro uchovávání a zajištění bezpečnosti archivů dat, Protipožární ochrana, Zajištění trvalosti dodávky energie, Zajištění fyzické bezpečnosti (detektory pohybu, televizní sledování, …), Zajištění bezpečnosti prostředí (detektory kouře/ohně, …), …

Zásady výběru

- **Dle kontextu a analýzy rizik!**
- Podmínka efektivnosti opatření: cena opatření ≤ výše škody
- Vesměs platí, že s každým aktivem se druží více rizik
- Na identifikované riziko se musí vázat efektivní opatření
- Některá opatření lze aplikovat pro řešení více rizik
- Pro volbu opatření dává návod k volbě nejlepších praktik standard ISO 27002

ISO/IEC 27002:2022 Opatření informační bezpečnosti

- 4 témata
- 93 opatření
- 5 atributů



ISO/IEC 27002 Opatření informační bezpečnosti – atributy 1/3

- Typ opatření - kdy a jak opatření mění riziko s ohledem na výskyt incidentu
  - Preventivní – má incidentu zabránit
  - Detekční – působí při výskytu incidentu
  - Nápravné – působí po výskytu
- Vlastnosti informační bezpečnosti – jaké charakteristiky informace opatření pomáhá chránit
  - Důvěrnost
  - Integrita
  - Dostupnost

ISO/IEC 27002 Opatření informační bezpečnosti – atributy 2/3

- Koncept kybernetické bezpečnosti – popisuje vhodné činnosti
  - Identifikace – analýza obchodních cílů, aktiv, procesů, legislativy atp.
  - Ochrana – vhodná opatření
  - Detekce – proaktivní zjišťování událostí
  - Odezva – reakce na incident, komunikace, …
  - Obnova – minimalizace škod
- Provozní schopnosti:
  - Správa a řízení, Bezpečnost aplikací, Fyzická bezpečnost, Bezpečnost dodavatelských vztahů, Právní požadavky a soulad, … celkem 15

ISO/IEC 27002 Opatření informační bezpečnosti – atributy 3/3

- Domény bezpečnosti:
  - Správa a řízení a ekosystém – např. Management kybernetické bezpečnosti
  - Ochrana – např. architektura IT bezpečnosti, fyzická bezpečnost
  - Obrana – např. detekce, management incidentů,
  - Odolnost – např. kontinuita provozu, …

Konkrétní příklad ze standardu

5.33 Ochrana záznamů

Typ opatření	Vlastnosti informační bezpečnosti	Koncepty kybernetické bezpečnosti	Provozní schopnosti	Domény bezpečnosti
#Preventivní	#Důvěrnost #Integrita #Dostupnost	#Identifikace #Ochrana	#Právní_požadavky_a_soulad #Management_aktiv #Ochrana_informací	#Obrana

Převzato z ISO/IEC 27002

Osnova

- Úvod a motivace
- Informační bezpečnost
- Základní pojmy
  - Aktiva
  - Zranitelnost
  - Hrozba
  - Útok
  - Riziko
  - Opatření
  - Bezpečnostní mechanismus
- Generické rysy zabezpečení

Bezpečnostní mechanismy

- (Bezpečnostní) opatření musíme účinnou formou implementovat vhodnými (bezpečnostními) **mechanismy** různé síly
  - Mechanismy administrativního, technického, logického, … charakteru
  - Opatření řešící problém nepopiratelnosti
    mechanismus = digitální podpis
  - Opatření řešící řízení přístupu v souladu s přijatou politikou řízení přístupu
    mechanismus = fyzické klíče, identifikační karty, biometriky, …
  - Opatření řešící problém důvěrnosti v souladu s přijatou politikou zajištění důvěrnosti
    mechanismus = šifrování, trezory, smluvní závazek (NDA), …

Osnova

- Úvod a motivace
- Informační bezpečnost
- Základní pojmy
  - Aktiva
  - Zranitelnost
  - Hrozba
  - Útok
  - Riziko
  - Opatření
  - Bezpečnostní mechanismus
- Generické rysy zabezpečení

Generické rysy zabezpečování informací 1/4

- Minimalizovat prostor využitelný pro útok
  - Každá nadbytečná vlastnost aplikace zvyšuje rozsah rizik pro celou aplikaci
  - Např. k webové aplikaci se doplní on-line help s vyhledávací funkcí
  - Vyhledávací funkce může být zranitelná útokem *SQL injection*
  - Když help zpřístupníme pouze autentizovaným uživatelům, riziko se sníží
  - Když každý vstup vyhledávací funkce bude kontrolovat centralizovaný validační program, riziko se sníží dramaticky
  - Když se odstraní vyhledávací funkce, riziko zmizí úplně a help vlastnost lze dát na veřejný Internet jako samostatnou aplikaci
- Jako implicitní řešení používat bezpečná řešení
  - Např. časové omezení platnosti hesla a nárok na minimální netriviálnost hesla má být implicitně zapnutá
  - Uživatel si může tyto vlastnosti vědomě vypnout, na své riziko

Generické rysy zabezpečování informací 2/4

- Princip nejmenších práv
  - Každému mají být přidělena ta nejmenší možná práva, která potřebuje pro řešení svých činností
  - Jestliže middlewarový server potřebuje mít přístup k Internetu, číst databázové tabulky a zapisovat logování dějů, pak má mít k tomu přidělená příslušná práva, ale nikoli práva administrátora/superuživatele
- Důkladný a komplexní princip ochran
  - Chyba v rozhraní administrátora bude pravděpodobně zřídka využita anonymním útočníkem, pokud rozhraní bude správně hlídat, kontrolovat autenticitu administrátora, logovat žadatele, …
- Každý externí systém vůči bezpečné aplikaci musí být implicitně považovaný za nedůvěryhodný

Generické rysy zabezpečování informací 3/4

- Chybný je koncept „**Security through Obscurity**“ (zabezpečení na základě utajení)
- Spoléhá na utajení vnitřních mechanismů před útočníkem – např. ukrytí klíče pod rohožkou
- Útočníci jsou chytří, znají všechny triky a mají spoustu času

SECURITY

Hacker Will Expose Potential Security Flaw In Four Million Hotel Room Keycard Locks

Andy Greenberg Former Staff

htpp://goo.gl/b03ncJ

Generické rysy zabezpečování informací 4/4

- Separace rolí
  - Určité role mají jinou úroveň důvěry než normální uživatelé
  - Administrátor systému × normální uživatel
  - Administrátor nemá být normálním uživatelem aplikace:
    - administrátor OS může nastavit politiku hesel, vypnout systém, …
    - administrátor nemůže nakoupit akcie, i když je "superuser"
- V jednoduchosti je síla
  - Dvojnásobná negace ještě nemusí v reálné praxi být pozitivem
- Správně opravovat chyby
  - Vypracovat test příčiny chyby
  - Porozumět bázovému problému způsobujícímu chybu
  - Porozumět souvislostem - např. při odhalení chyby v návrhovém vzoru

Dodatek

Příklady zranitelností dle zákona o kybernetické bezpečnosti

1. Nedostatečná údržba informačního a komunikačního systému
2. Zastaralost informačního a komunikačního systému
3. Nedostatečná ochrana vnějšího perimetru
4. Nedostatečné bezpečnostní povědomí uživatelů a administrátorů
5. Nedostatečná údržba informačního a komunikačního systému
6. Nevhodné nastavení přístupových oprávnění
7. Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů

Příklady zranitelností dle zákona o kybernetické bezpečnosti

8. Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování
9. Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí
10. Nedostatečná ochrana aktiv
11. Nevhodná bezpečnostní architektura
12. Nedostatečná míra nezávislé kontroly
13. Neschopnost včasného odhalení pochybení ze strany zaměstnanců

Příklady hrozeb dle zákona o kybernetické bezpečnosti

1. Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů
2. Poškození nebo selhání technického anebo programového vybavení
3. Zneužití identity
4. Užívání programového vybavení v rozporu s licenčními podmínkami
5. Škodlivý kód (například viry, spyware, trojské koně)
6. Narušení fyzické bezpečnosti
7. Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie
8. Zneužití nebo neoprávněná modifikace údajů

Příklady hrozeb dle zákona o kybernetické bezpečnosti

9. Ztráta, odcizení nebo poškození aktiva
10. Nedodržení smluvního závazku ze strany dodavatele
11. Pochybení ze strany zaměstnanců
12. Zneužití vnitřních prostředků, sabotáž
13. Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb
14. Nedostatek zaměstnanců s potřebnou odbornou úrovní
15. Cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik
16. Zneužití vyměnitelných technických nosičů dat
17. Napadení elektronické komunikace (odposlech, modifikace)

Klasifikace (citlivých) aktiv dle zákona o kybernetické bezpečnosti 1/3

- **Stupnice pro hodnocení důvěrnosti aktiv**
- Nízká
  - Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění např. na základě zákona o svobodném přístupu k informacím. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy odpovědných orgánů a osob
  - *Není vyžadována žádná ochrana*
- Střední
  - Aktiva nejsou veřejně přístupná a tvoří know-how odpovědných orgánů a osoby, ochrana těchto informací není vyžadována žádným právním předpisem nebo smluvním ujednáním
  - *Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu*
- Vysoká
  - Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními
  - *Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu*
  - *Přenosy informací jsou chráněny pomocí kryptografických prostředků*
- Kritická
  - Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (např. strategické obchodní tajemství, citlivé osobní údaje apod.)
  - *Pro ochranu důvěrnosti je požadována evidence osob, které k aktivům přistoupily, a metody ochrany zabraňující kompromitaci ze strany administrátorů*

Klasifikace (citlivých) aktiv dle zákona o kybernetické bezpečnosti 2/3

- **Stupnice pro hodnocení integrity aktiv**
- Nízká
  - Aktivum nevyžaduje ochranu z hlediska integrity
  - Narušení integrity aktiv neohrožuje oprávněné zájmy odpovědných orgánů a osob
  - *Není vyžadována žádná ochrana*
- Střední
  - Aktivum může vyžadovat ochranu z hlediska integrity
  - Narušení integrity aktiva může vést k poškození oprávněných zájmů odpovědných orgánů a osob a může se projevit méně závažnými dopady na ostatní aktiva
  - *Pro ochranu integrity jsou využívány standardní nástroje např. omezení přístupových práv pro zápis*
- Vysoká
  - Aktivum vyžaduje ochranu z hlediska integrity
  - Narušení integrity aktiva vede k poškození oprávněných zájmů odpovědných orgánů a osob s podstatnými dopady na ostatní aktiva
  - *Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu*
- Kritická
  - Aktivum vyžaduje ochranu z hlediska integrity
  - Narušení integrity vede k velmi vážnému poškození oprávněných zájmů odpovědných orgánů a osob s přímými a velmi vážnými dopady na ostatní aktiva
  - *Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu např. pomocí technologie digitálního podpisu*

Klasifikace (citlivých) aktiv dle zákona o kybernetické bezpečnosti 3/3

- **Stupnice pro hodnocení dostupnosti aktiv**
- Nízká
  - Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne)
  - *Pro ochranu dostupnosti je postačující pravidelné zálohování*
- Střední
  - Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení zájmů odpovědných orgánů a osob
  - *Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy*
- Vysoká
  - Narušení dostupnosti aktiva by nemělo překročit dobu několika málo hodin
  - Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů odpovědných orgánů a osob. Aktiva jsou považována jako velmi důležitá.
  - *Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy či výměnou technických aktiv*
- Kritická
  - Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení zájmů odpovědných orgánů a osob. Aktiva jsou považována jako kritická.
  - *Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná*