# Dodatek k přednášce Anatomie InSec
# Příklady opatření, zranitelností a hrozeb

PV 017 ◇ Bezpečnost IT

Jan Staudek
http://www.fi.muni.cz/usr/staudek/vyuka/


Verze : podzim 2019

## Obsah





## Kategorie opatření podle ISO/IEC 27001/27002

- ✓ 14 tříd pokrývajících většinu aspektů InfSec
- ✓ Všechny uváděné generické typy opatření (114) patří mezi nejlepší známé pro dosažení InfSec, jsou volitelné, vybírají se podle prohlášení o jejich aplikovatelnosti v vydávaném na základě hodnoceni rizik
- ✓ Pro konkrétní implementace ISMS lze opatření libovolně doplňovat

- A.5, Politiky informační bezpečnosti
  - ✓ A.5.1, Cíl: směrnice pro management o informační bezpečnosti, jak politiky psát, aktualizovat a revidovat
  - ✓ A.5.1.1, Politiky InfSec: musí být definovány, schválené příslušným managementem, publikované a sdělené zaměstnancům a příslušným vnější (třetím) stranám
  - ✓ A.5.1.2, Přezkum politik InfSec: musí být v plánovaných intervalech nebo v případě výskytů významných změn přezkoumávané, aby se zajistila jejich trvalá vhodnost, přiměřenost a účinnost.



## Kategorie opatření podle ISO/IEC 27001/27002

- ✓ politiky zajišťují potřebnou úroveň důvěrnosti, autenticity, integrity, dostupnosti vč. bezpečnosti transakcí v distribuovaném prostředí
- ✓ jsou vypracovávané pro chráněné oblasti a jsou, tam kde je to potřeba, doplňované
  politikou bezpečnosti informací pro vztahy s dodavateli,
  – prověření dodavatelů, identifikace rizik třetích stran a bezpečnostních opatření s promítnutím do smluv apod.,
  politikou používání mobilních zařízení – evidence, kontrola platforem OS, BYOD, MDM (Mobile Device Management) apod.
- ✓ management má definovat a prosazovat účinné bezpečnostní politiky, musí být srozuměn se záměrem zavedení a provozování ISMS a má plně podporovat jeho vývoj a provoz
- ✓ bezpečnostní politiky má relevantní personál znát
- ✓ musí být v souladu se strategickou (globální) bezpečnostní politikou organizace

## Kategorie opatření podle ISO/IEC 27001/27002

- A.6, Organizační zajištění informační bezpečnosti
  - ✓ A.6.1, Cíl v oblasti vnitřní organizace: vytvoření rámce pro iniciaci, řízení implementace a provozování péče o informační bezpečnost v rámci organizace
  - ✓ má být definovaná řídicí A kontrolní infrastruktura
    – odpovědný člen vedení, bezpečnostní architekt, bezp. správce, ...
    – každý člen organizace si je vědom svých odpovědností
    – existují kanály pro sdělování info o útocích relevantním autoritám
  - ✓ organizační zajištění pří existenci třetích stran viz A.15
  - ✓ A.6.1.1, Role a odpovědnosti: musí být definované a přidělené
  - ✓ A.6.1.2, Oddělení povinností: konfliktní povinnosti a oblasti odpovědnosti musí být odděleny, aby omezily příležitosti pro neoprávněné nebo neúmyslné změně nebo zneužití aktiv organizace.
  - ✓ A.6.1.3, Kontakt s orgány: musí se udržovat příslušné kontakty s příslušnými orgány



## Kategorie opatření podle ISO/IEC 27001/27002

- ✓ A.6.1.4, Kontakt se speciálními zájmovými skupinami: musí se udržovat příslušné kontakty se zájmovými skupinami nebo s jinými odbornými bezpečnostními fóry a profesními sdruženími
- ✓ A.6.1.5, Informační bezpečnost v projektovém řízení: musí být řešena v při projektovém řízení, bez ohledu na typ projektu
- ✓ A.6.2, Cíl v oblasti používání mobilních zařízení a teleworkingu: zajistit InSec při používání mobilních zařízení a teleworkingu
- ✓ A.6.2.1, Politika používání mobilních zařízení
- ✓ A.6.2.2, Politika teleworkingu



## Kategorie opatření podle ISO/IEC 27001/27002

- A.7, Perzonální bezpečnost, bezpečnost lidských zdrojů
  - ✓ A.7.1, před přijetím:
  - ✓ A.7.1.1, Definice kritérií pro výběr pracovníků
  - ✓ A.7.1.2, Deklarace pravidel a podmínek při zaměstnaní, NDA, ...
  - ✓ A.7.2, během zaměstnání:
  - ✓ A.7.2.1, Odpovědnost managementu, musí požadovat po všech zaměstnancích a dodavatelích udržování InfSec v souladu se zavedenými zásadami a postupy organizace
  - ✓ A.7.2.2, Pěstování bezpečnostního uvědomění, pravidelná bezpečnostní školení zaměstnanců
  - ✓ A.7.2.3, Disciplinární řízení po způsobení narušení InfSec
  - ✓ A.7.3, ukončení zaměstnání, změna funkce v zaměstnání:
  - ✓ A.7.3.1, Ukončení / změna povinností a odpovědností při ukončení zaměstnání a změně funkce , vrácení prostředků IT, odebrání přístupových práv, ...



## Kategorie opatření podle ISO/IEC 27001/27002

- A.8, Správa (řízení) aktiv
  - ✓ A.8.1, Odpovědnost za aktiva, informační aktiva mají být známá (ex. soupis) a chráněná pro každé aktivum má být definovaná odpovědná role (vlastník aktiva)
  - ✓ A.8.2, Klasifikace aktiv, (tajné, důvěrné, ...) a každá třída musí být relevantně chráněná
  - ✓ A.8.3, Pravidla pro zacházení médii

## Kategorie opatření podle ISO/IEC 27001/27002

- A.9, Řízení přístupu
  - ✓ A.9.1, Politika řízení přístupu – požadavky dané činnosti organizace, stanovení závazných pravidel pro přidělování přístupových oprávnění
  - ✓ A.9.2, Řízení přístupu uživatelů – (de)registrace, evidence přidělených oprávnění, správa privilegovaných oprávnění administrátorů, správa hesel, kontroly validity přístupových oprávnění
  - ✓ A.9.3, Odpovědnosti uživatelů – používání hesel, neobsluhovaná zařízení, zásada prázdného stolu a prázdné obrazovky
  - ✓ A.9.4, Řízení přístupu k aplikacím a k systémům – ochrana před neautorizovaným přístupem, registrační procedury, řízení přístupu na úrovni sítě/OS/aplikace, zohlednění vzdálených přístupů, správa hesel, . . .



## Kategorie opatření podle ISO/IEC 27001/27002

- A.10, Kryptografie
  - ✓ A.10.1, Kryptografická opatření – pro zajištění správného a efektivního využití šifrování na ochranu důvěrnosti, autenticity a / nebo integrity informačních aktiv
  - ✓ A.10.1.1, Politika používání kryptografických opatření
  - ✓ A.10.1.2, Správa klíčů
- A.11, Fyzická bezpečnost a bezpečnost prostředí
  - ✓ ochrana proti neautorizovanému fyzickému zpřístupnění
  - ✓ ochrana proti vnějším vlivům přírody, krádežím, . . .



## Kategorie opatření podle ISO/IEC 27001/27002

- A.12, Řízení provozu, provozní bezpečnost
  - ✓ ex. aktualizované, auditované, dokumentované provozní postupy
  - ✓ ex. plánování dostupnosti potřebných zpracovávatelských kapacit
  - ✓ je zavedena ochrana proti škodlivému software
  - ✓ provádí se archivace
  - ✓ provádí se monitorování incidentů a informování o incidentech (i o podezřeních na ně)
- A.13, Bezpečnost komunikací
  - ✓ A.13.1, Správa síťové bezpečnosti
  - ✓ A.13.2, Přenos informací, výměna informací mezi organizacemi, transakce, je řízená



## Kategorie opatření podle ISO/IEC 27001/27002

- A.14, Akvizice, vývoj a údržba
  - ✓ Správa a řízení vývoje systémů
  - ✓ A.14.1, InfSec informačních systémů
  - ✓ A.14.2, InfSec při vývoji a údržbě
    typy prostředí: vývojové, testovací, akceptační, provozní (živá data)
  - ✓ A.14.3, Testovací data
- A.15, Vztahy s dodavateli
  - ✓ zajištění InfSec ve vztazích s dodavateli
  - ✓ správa doručování dodavatelských služeb
- A.16, Zvládání bezpečnostních incidentů
  - ✓ hlášení bezpečnostních incidentů
  - ✓ plány/procedury reakcí na zjištěný bezpečnostní incident

## Kategorie opatření podle ISO/IEC 27001/27002

- A.17, Řízení kontinuity činnosti organizace
  - ✓ A.17.1, plán pro udržení nebo obnovu činností organizace po přerušení nebo selhání kritických procesů a pro zajištění dostupnosti informací v požadovaném čase a na požadovanou úroveň
  - ✓ A.17.2, zajištění dostupnosti redundancí prostředků pro zpracování informací
- A.18, Soulad s požadavky
  - ✓ A.18.1, Soulad s právními a smluvními normami
    - – Specifické požadavky vyplývající ze zákona by měly být konzultovány s právními poradci organizace nebo jinými kvalifikovanými právníky.
    - – Legislativní požadavky na informace vzniklé v jedné zemi a přenášené do jiné země jsou různé a mění se podle zemí.
    - – Soulad s bezpečnostními politikami, normami a technická shoda
  - ✓ A.18.2, Audit InfSec – nástroj ověření dosažení souladu



## Příklady opatření dle zákona o kybernetické bezpečnosti

- Kategorie bezpečnostních opatření jsou dvě organizační opatření a technická opatření.
- Organizačními opatřeními jsou
  - ✓ systém řízení bezpečnosti informací, ISMS
  - ✓ procesy řízení rizik,
  - ✓ bezpečnostní politika,
  - ✓ organizační bezpečnost – management bezpečnosti v organizaci,
  - ✓ stanovení bezpečnostních požadavků pro dodavatele,
  - ✓ řízení aktiv,
  - ✓ bezpečnost lidských zdrojů,
  - ✓ řízení provozu a komunikací informační infrastruktury
  - ✓ řízení přístupu osob k informační infrastruktuře
  - ✓ akvizice, vývoj a údržba informační infrastruktury,
  - ✓ zvládání bezpečnostních událostí a bezpečnostních incidentů,
  - ✓ řízení kontinuity činností a
  - ✓ kontrola a audit informační infrastruktury



## Příklady opatření dle zákona o kybernetické bezpečnosti

- Technickými opatřeními jsou
  - ✓ nástroje pro zajištění fyzické bezpečnosti,
  - ✓ nástroje pro ochranu integrity komunikačních sítí,
  - ✓ nástroje pro ověřování identity uživatelů,
  - ✓ nástroje pro řízení přístupových oprávnění,
  - ✓ nástroje pro ochranu před škodlivým kódem,
  - ✓ nástroje pro zaznamenávání činnosti informační infrastruktury, jejich uživatelů a administrátorů,
  - ✓ nástroje pro detekci bezpečnostních událostí,
  - ✓ nástroje pro sběr a vyhodnocení bezpečnostních událostí,
  - ✓ nástroje pro zajištění aplikační bezpečnosti,
  - ✓ kryptografické prostředky,
  - ✓ nástroje pro zajišťování úrovně dostupnosti informací a
  - ✓ nástroje pro zajištění bezpečnosti průmyslových a řídících systémů



## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

- Systém řízení bezpečnosti informací, ISMS,
  *Information Security Management System*
  - ✓ jsou stanovené hranice systému řízení bezpečnosti informací určující, kterých organizačních částí a technických prvků se systém řízení bezpečnosti informací týká
  - ✓ zajišťuje provádění procesů řízení rizik
  - ✓ zajišťuje vytvoření a schválení bezpečnostní politiky v oblasti ISMS, která obsahuje hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení informační bezpečnosti
  - ✓ zajišťuje trvalé monitorování účinnosti bezpečnostních opatření
  - ✓ zajišťuje pravidelné vyhodnocování vhodnosti a účinnosti bezpečnostní politiky
  - ✓ zajišťuje pravidelné provádění auditu bezpečnosti, a to nejméně jednou ročně
  - ✓ zajišťuje nejméně jednou ročně vyhodnocení účinnosti ISMS

## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

- ✓ zajišťuje aktualizaci ISMS a příslušné dokumentaci na základě zjištění auditů bezpečnosti, výsledků vyhodnocení účinnosti ISMS a v souvislosti s prováděnými či plánovanými změnami
- ✓ zajišťuje provedení nejméně jednou za tři roky aktualizace zprávy o hodnocení rizik, bezpečnostní politiky, plánu zvládání rizik a plánu rozvoje bezpečnostního povědomí



## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

- □ Procesy řízení rizik
  - ✓ mají stanovenou metodiku pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik vč. stanovení kritérií přijatelnosti rizik
  - ✓ identifikují a hodnotí důležitost aktiv, které patří do rozsahu ISMS a výstupy zapracují do zprávy o hodnocení rizik
  - ✓ identifikují rizika, při kterých zohlední hrozby a zranitelnosti, posoudí možné dopady na aktiva, hodnotí tato rizika, určí a schválí přijatelná rizika a zpracují zprávu o hodnocení rizik
  - ✓ zpracují na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti, které obsahuje přehled vybraných a zavedených bezpečnostních opatření a popis vazeb mezi identifikovanými riziky a příslušnými bezpečnostními opatřeními
  - ✓ zpracují zpracují a zavedou plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik, určí osoby odpov. za prosazování bezpečnostních opatření pro zvládání rizik, nutné finanční, technické, lidské a informační zdroje a termín jejich zavedení



## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

- □ Bezpečnostní politika se stanovuje pro oblasti
  - ✓ systém řízení bezpečnosti informací, ISMS
  - ✓ organizační bezpečnost, management informační bezpečnosti
  - ✓ řízení dodavatelů,
  - ✓ klasifikace aktiv,
    která zahrnuje pravidla pro bezpečné nakládání s aktivy,
  - ✓ bezpečnost lidských zdrojů,
  - ✓ řízení provozu a komunikací,
  - ✓ řízení přístupu,
  - ✓ bezpečné chování uživatelů,
  - ✓ zálohování a obnova,
  - ✓ bezpečné předávání a výměna informací,
  - ✓ řízení technických zranitelností,



## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

- ✓ bezpečné používání mobilních zařízení,
- ✓ licencování software a informací,
- ✓ dlouhodobé ukládání a archivace informací,
- ✓ ochrana osobních údajů,
- ✓ fyzická bezpečnost,
- ✓ bezpečnost sítě,
- ✓ ochrana před škodlivým kódem,
- ✓ nasazení a používání nástroje pro detekci bezpečnostních událostí,
- ✓ využití a údržba nástroje pro sběr a vyhodnocení bezpečnostních událostí
- ✓ používání kryptografické ochrany.

## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

- Management informační bezpečnosti v organizaci
  - ✓ Bezpečnostní role v organizaci
    - manažer informační bezpečnosti,
    - architekt informační bezpečnosti,
    - auditor informační bezpečnosti a
    - garant (vlastník) aktiva
  - ✓ Manažer informační bezpečnosti – osoba odpovědná za ISMS, která je pro tuto činnost řádně vyškolena a prokáže odbornou způsobilost praxí po dobu nejméně XXX (tří) let s řízením informační bezpečnosti.
  - ✓ Architekt informační bezpečnosti je osoba odpovědná za návrh a implementaci bezpečnostních opatření, která je pro tuto činnost řádně vyškolena a prokáže odbornou způsobilost praxí po dobu nejméně XXX (tří) let s navrhováním bezpečnostní architektury



## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

  - ✓ Auditor informační bezpečnosti je osoba odpovědná za provádění auditu informační bezpečnosti, která je pro tuto činnost řádně vyškolena a prokáže odbornou způsobilost praxí po dobu nejméně XXX (tří) let s prováděním auditů informační bezpečnosti. Auditor informační bezpečnosti vykonává svoji roli nestranně a výkon jeho role je oddělen od výkonu rolí manažer, architekt a garant.
- Stanovení bezpečnostních požadavků pro dodavatele
  - ✓ před uzavřením smlouvy se provádí hodnocení rizik podle, která jsou spojena s dodávkami od jednotlivých dodavatelů
  - ✓ s dodavateli se uzavírá smlouva o úrovni služeb, která stanoví způsoby a úrovně realizace bezpečnostních opatření a určí vztah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření
  - ✓ provádí se pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných služeb jednotlivými dodavateli a zjištěné nedostatky po dohodě s dodavatelem se odstraňují



## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

- Řízení aktiv
  - ✓ identifikace a evidence aktiv,
  - ✓ určení garantů aktiv
  - ✓ hodnocení vlastností aktiv z hlediska důvěrnosti, integrity a dostupnosti a zařazení aktiv do klasifikačních úrovní při zohlednění
    - míry podílu osobních údajů nebo obchodního tajemství,
    - rozsahu dotčených právních povinností či jiných závazků,
    - rozsah narušení vnitřních řídících a kontrolních činností,
    - poškození veřejných, obchodních či ekonomických zájmů,
    - možné finanční ztráty,
    - rozsahu narušení běžných činností
    - dopadů na ztrátu dobrého jména nebo dobré pověsti
  - ✓ stanovení a zavedení pravidel ochrany, nutných pro zabezpečení jednotlivých úrovní aktiv
  - ✓ určení způsobů pro spolehlivé smazání nebo ničení paměťových médií s ohledem na úroveň aktiv



## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

- Bezpečnost lidských zdrojů
  - ✓ plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a délku potřebných školení a určuje osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny
  - ✓ v souladu s plánem rozvoje bezpečnostního povědomí se provádí poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení
  - ✓ pravidelně se kontroluje dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role
  - ✓ je zajištěno vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role
  - ✓ udržují se přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly

## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

- ✓ jsou stanovená pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů
- ✓ pravidelně se hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí
- ✓ jsou stanovená pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů,

  administrátorů a osob zastávajících bezpečnostní role
- ✓ je stanovený postup změn přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role



## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

- □ Řízení provozu a komunikací
  - ✓ Existují provozní pravidla a postupy obsahující
    - – práva a povinnosti osob zastávajících bezpečnostní role, administrátorů a uživatelů,
    - – postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání, pro ošetření chybových stavů anebo mimořádných jevů
    - – postupy pro sledování kybernetických bezpečnostních událostí a pro ochranu přístupu k záznamům o těchto činnostech,
    - – spojení na kontaktní osoby, které jsou určeny jako podpora při řešení neočekávaných systémových nebo technických potíží,
    - – postupy řízení a schvalování provozních změn a
    - – postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.



## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

- □ Řízení provozu a komunikací, pokrač.
  - ✓ je zajištěno oddělení vývojového, testovacího a produkčního prostředí,
  - ✓ provádí se pravidelné zálohování a prověřování použitelnosti provedených záloh
  - ✓ zajišťuje se bezpečnost a integrita komunikačních sítí a bezpečnost komunikačních služeb
  - ✓ jsou stanovená pravidla a postupy pro ochranu informací, které jsou přenášeny komunikačními sítěmi
  - ✓ provádí se výměna a předávání informací na základě pravidel stanovených právními předpisy za současného zajištění bezpečnosti informací a tato pravidla se dokumentují
  - ✓ provádí se výměna a předávání informací na základě písemných smluv, jejichž součástí je ustanovení o bezpečnosti informací



## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

- □ Řízení přístupu osob k informační infrastruktuře
  - ✓ přidělí přistupujícím aplikacím samostatný identifikátor,
  - ✓ omezí přidělování administrátorských oprávnění,
  - ✓ přiděluje a odebírá přístupová oprávnění v souladu s politikou řízení přístupu,
  - ✓ provádí pravidelné přezkoumání nastavení přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách nebo rolích,
  - ✓ využívá nástroj pro ověřování identity uživatelů a nástroj pro řízení přístupových oprávnění a
  - ✓ zavede bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení, případně i bezpečnostní opatření spojená s využitím technických zařízení, kterými povinná osoba nedisponuje.

## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

- Akvizice, vývoj a údržba informační infrastruktury
  - ✓ identifikují, hodnotí a řídí rizika související s akvizicí, vývojem a údržbou informačního systému nebo komunikačního systému
  - ✓ zajišťují bezpečnost vývojového prostředí a ochranu používaných testovacích dat a
  - ✓ provádějí bezpečnostní testování změn informačního systému nebo komunikačního systému před jejich zavedením do provozu.



## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

- Zvládání bezpečnostních událostí a bezpečnostních incidentů
  - ✓ zajišťuje se u informačního systému a u komunikačního systému, aby uživatelé, administrátoři a osoby zastávající bezpečnostní role oznamovali bezpečnostní události a o oznámeních se vedou záznamy,
  - ✓ připravuje se prostředí pro vyhodnocení oznámených bezpečnostních událostí a událostí detekovaných technickými nástroji, provádí se jejich vyhodnocení a identifikují se bezpečnostní incidenty,
  - ✓ provádí se klasifikace bezpečnostních incidentů, přijímají se opatření pro odvrácení a zmírnění dopadu bezpečnostního incidentu, provádí se hlášení bezpečnostního incidentu a zajišťuje se sběr věrohodných podkladů potřebných pro analýzu bezpečnostního incidentu,
  - ✓ prošetřují se a určují se příčiny bezpečnostního incidentu, vyhodnocuje se účinnost řešení bezpečnostního incidentu a na základě vyhodnocení se stanovují nová bezpečnostní opatření k zamezení opakování řešeného bezpečnostního incidentu a
  - ✓ dokumentuje se zvládání kybernetických bezpečnostních incidentů.



## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

- Řízení kontinuity činností
  - ✓ jsou definovaná práva a povinnosti garantů aktiv, administrátorů a osob zastávajících bezpečnostní role
  - ✓ jsou definované cíle strategie jejich dosažení v oblastech:

    Minimální úroveň poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního a komunikačního systému.

    Doba obnovení chodu, během které bude po bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního a komunikačního systému.

    Doba obnovení dat jako termínu, ke kterému budou obnovena data po bezpečnostním incidentu
  - ✓ vyhodnocují se a dokumentují se možné dopady různých bezpečnostních incidentů a posuzují se možná rizika související s ohrožením kontinuity činností
  - ✓ je vypracován, aktualizován a pravidelně se testuje plán kontinuity činností informačního systému a komunikačního systému



## Příklady organizačních opatření dle zákona o kyb. bezpečnosti

- Kontrola a audit informační infrastruktury
  - ✓ posuzuje se soulad obecně závazných právních předpisů, vnitřních předpisů, jiných předpisů a smluvních závazků vztahujících se k informačnímu systému a komunikačnímu systému a určují se opatření pro jejich prosazování
  - ✓ provádí se a dokumentuje se pravidelná kontrol dodržování bezpečnostní politiky a výsledky těchto kontrol zohledňují v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik

## Příklady technických opatření dle zákona o kyb. bezpečnosti

- Nástroje pro zajištění fyzické bezpečnosti
  - ✓ zamezují neoprávněnému vstupu do vymezených prostor, kde jsou uchovávány informace a umístěna technická aktiva
  - ✓ zamezují poškozením a zásahům do vymezených prostor, kde jsou uchovány informace a umístěna technická aktiva
  - ✓ předcházejí poškození, krádeži nebo kompromitaci aktiv nebo přerušení poskytování služeb informačního systému
  - ✓ příklady
    - mechanické zábranné prostředky,
    - zařízení elektrické zabezpečovací signalizace,
    - systémy pro kontrolu vstupu,
    - kamerové systémy,
    - zajištění ochrany před selháním dodávky elektrického napájení
    - zařízení pro zajištění optimálních provozních podmínek



## Příklady technických opatření dle zákona o kyb. bezpečnosti

- Nástroje pro ochranu integrity komunikačních sítí
  - ✓ řízení bezpečného přístupu mezi vnější a vnitřní sítí,
  - ✓ segmentace použitím demilitarizovaných zón jako speciálního typu sítě používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí,
  - ✓ kryptografické prostředky pro vzdálený přístup nebo pro přístup pomocí bezdrátových technologií a
  - ✓ opatření pro odstranění nebo blokování přenášených dat, které neodpovídají požadavkům na ochranu integrity komunikační sítě.
- Nástroje pro ověřování identity uživatelů
  - ✓ zajišťují ověření identity uživatelů a administrátorů před zahájením jejich aktivit v informačním systému



## Příklady technických opatření dle zákona o kyb. bezpečnosti

- Nástroje pro řízení přístupových oprávnění
  - ✓ pro přístup k jednotlivým aplikacím a datům
  - ✓ pro čtení dat, pro zápis dat a pro změnu oprávnění
  - ✓ pro zaznamenává použití přístupových oprávnění
- Nástroje pro ochranu před škodlivým kódem
  - ✓ ověřují a kontrolují
    - komunikace mezi vnitřní sítí a vnější sítí,
    - serverů a sdílených datových úložišť a
    - pracovních stanic,
  - ✓ provádějí pravidelnou aktualizaci nástrojů pro ochranu před škodlivým kódem, jeho definic a signatur.



## Příklady technických opatření dle zákona o kyb. bezpečnosti

- Nástroje pro zaznamenávání činnosti informační infrastruktury, jejich uživatelů a administrátorů
  - ✓ zajišťují sběr informací o provozních a bezpečnostních činnostech (typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti, úspěšnost nebo neúspěšnost činnosti) a ochranu získaných informací před neoprávněným čtením nebo změnou
  - ✓ zaznamenávají
    - přihlášení a odhlášení uživatelů a administrátorů,
    - činnosti provedené administrátory,
    - činnosti vedoucí ke změně přístupových oprávnění,
    - neprovedení činností v důsledku nedostatku přístupových oprávnění
    - zahájení a ukončení činností technických aktiv,
    - automatická varovná nebo chybová hlášení technických aktiv,
    - přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností
    - použití nástrojů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.

## Příklady technických opatření dle zákona o kyb. bezpečnosti

- Nástroje pro sběr a vyhodnocení bezpečnostních událostí
  - ✓ zajišují integrovaný sběr a vyhodnocení bezpečnostních událostí z informačního systému
  - ✓ zajišují poskytování informací pro určené bezpečnostní role o detekovaných bezpečnostních událostech v informačním systému
  - ✓ nepřetržité vyhodnocují bezpečnostních událostí s cílem identifikace bezpečnostních incidentů a včasně varují určené bezpečnostní role.
  - ✓ zajišťují pravidelnou aktualizaci nastavení pravidel pro vyhodnocování bezpečnostních událostí a včasné varování
  - ✓ zajišťují využívání informací, které jsou připraveny nástrojem pro sběr a vyhodnocení bezpečnostních událostí, pro optimální nastavení bezpečnostních opatření informačního systému



## Příklady technických opatření dle zákona o kyb. bezpečnosti

- Nástroje pro zajištění aplikační bezpečnosti
  - ✓ zajišťují trvalou ochranu aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou a
  - ✓ zajišťují trvalou ochranu transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním
- Kryptografické prostředky
  - ✓ používají odolné kryptografické algoritmy a kryptografické klíče; minimální požadavky na kryptogr. alg. a klíče stanovuje vyhláška
  - ✓ zajišťují ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a prokázání odpovědnosti za provedené činnosti
  - ✓ zajišťují systém správy klíčů, který zajistí generování, distribuci, ukládání, archivaci, změny, ničení, kontrolu a audit klíčů



## Příklady technických opatření dle zákona o kyb. bezpečnosti

- Nástroje pro zajišťování úrovně dostupnosti
  - ✓ zajišťují dostupnost informačního systému a komunikačního systému pro splnění cílů řízení kontinuity činností
  - ✓ zajišťují dostupnost informačního systému a komunikačního systému vůči bezpečnostním incidentům, které by dostupnost mohly snížit
  - ✓ zajišťují zálohování důležitých technických aktiv informačního systému a komunikačního systému využitím redundance v návrhu řešení a zajištěním náhradních technických aktiv v určeném čase
- Nástroje pro zajišťování bezpečnosti prům. a řídicích systémů
  - ✓ omezují fyzický přístup k síti a zařízením průmysl. a řídicích systémů
  - ✓ omezují propojení a vzdálený přístup k síti průmysl. a řídicích systémů
  - ✓ zajišťují ochranu jednotlivých technických aktiv průmyslových a řídicích systémů před využitím známých zranitelností
  - ✓ zajišťují obnovení chodu průmyslových a řídicích systémů po kybernetickém bezpečnostním incidentu



## Příklady zranitelností dle zákona o kybernetické bezpečnosti

- ✓ nedostatečná ochrana vnějšího perimetru chráněného systému
- ✓ nedostatečné bezpečnostní povědomí uživatelů a administrátorů
- ✓ nedostatečná údržba informačního a komunikačního systému
- ✓ nevhodné nastavení přístupových oprávnění
- ✓ nedostatečné postupy pro identifikování a odhalování negativních bezpečnostních jevů – bezpečnostních událostí a incidentů
- ✓ možnost nezjistitelnosti nedodržování bezpečnostní politiky, provádění neoprávněných činností, zneužívání oprávnění administrátory kritické informační infrastruktury
- ✓ pochybení ze strany zaměstnanců a neschopnost jeho včasného odhalení
- ✓ možnost útoku z vnitřní sítě a zneužití vnitřních prostředků
- ✓ možnost dlouhodobého přerušení komunikačních služeb, dodávky elektrické energie nebo jiných důležitých služeb
- ✓ nedostatek zaměstnanců s potřebnou odbornou úrovní

## Příklady zranitelností dle zákona o kybernetické bezpečnosti

- ✓ zneužitelnost vyměnitelných paměťových médií
- ✓ nedostatečná míra provádění nezávislé kontroly
- ✓ nedostatečná ochrana prostředků informační infrastruktury
- ✓ nevhodná bezpečnostní architektura
- ✓ nedostatečné monitorování činnosti administrátorů
- ✓ nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné či závadné způsoby chování
- ✓ nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí.



## Příklady hrozeb dle zákona o kybernetické bezpečnosti

- ✓ porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,
- ✓ poškození nebo selhání hardwaru nebo softwaru,
- ✓ zneužití identity jiné fyzické osoby,
- ✓ užívání software v rozporu s licenčními podmínkami,
- ✓ kybernetický útok z vnější komunikační sítě,
- ✓ škodlivý kód (např. viry, spyware, trojské koně),
- ✓ nedostatky při poskytování služeb informačního a/nebo komunikačního systému,
- ✓ projevy přírodních jevů (např. povodně, klimatické jevy),
- ✓ přerušení dodávky komunikačních služeb nebo elektrické energie,
- ✓ zneužití nebo modifikace údajů a
- ✓ odcizení nebo poškození aktiva.
- ✓ . . .