Řízení bezpečnosti a rizik, plán kontinuity

Triáda bezpečnosti (CIA triad)

- Utajení – omezení přístupu pouze na autorizované osoby a systémy
  - princip minimálních oprávnění
  - soukromí – tj. utajení ve vztahu k personálním informacím (data narození, identifikátory, zdravotní záznamy, adresní údaje, …)
- Integrita – tj. zabránění neoprávněným manipulacím s daty
  - přesnost (věcná správnost)
  - validita
  - kompletnost
- Dostupnost
  - přístupnost dat
  - použitelnost
  - včasnost

Vzhledem k datu vzniku tohoto konceptu poněkud chybí

- Autenticita – tzn. jistota původu dat
- Nepopiratelnost – možnost doložit specifický původ dat
- Odpovědnost – akce lze trasovat ke konkrétní entitě
- Jistota – že mechanismy fungují, jak předpokládáno

Aplikace principů řízení (governance)

Řízení bezpečnosti

- odpovědnosti
- politiky
- proceduty

směřující k:

- Sesouladění bezpečnostních funkcí s obchodní strategií organizace
- Definici a řízení procesů relevantních z poledu bezpečnosti
- Vývoji rolí a odpovšědností v oblasti bezpečnosti
- Provádění due diligence a due care aktivit

Sesouladění

Prohlášení o poslání – jednoduchá deklarace účelu a způsobu fungování organizace
Obchodní strategie – jak organizace dosahuje naplnění svého poslání
Cíl – cokoliv, čeho chce organizace dosáhnout

- specifický
- meřitelný
- dosažitelný
- relevantní
- časově omezený

bezpečnost musí podporovat jak celkovou strategii, tak jednotlivé cíle organizace

správa bezpečnosti je soustava procesů zahrnujícu
- definice politik
- definice postupů
- dohled

+ specifické postupu pro spojení, akvizice a odprodeje

Musíte vybudovat bezpečnostní oranizace
- vedoucí informační bezpečnosti (CISO) – celkové řízení
- vedoucí bezprčnosti (CSO) – fyzická bezpečnost
- bezpečnostní analytik – technická expertiza
- manažer, manažer programu – implementace a provoz
- ředitel – řízení odpovědností

… a v neposlední řadě
- uživatel
    - porozumění a pochopení
    - zaškolení a kompetence
    - hlášení podezřelých okolností
    - odpovědnost

Obecné rámce řízení bezpečnosti

Proč normy a standardy?
- napoví, co máte chtít a jak to má vypadat
- certifikáty o shodě s normou zajistí, že nemusíte být experty, abyste si mohli vybrat správně
- zavádějí jednotnou kulturu a stanovují srovnatelná kriteria
- normu lze použít jako vodítko, abyste na nic nezapomněli
- usnadňují audit, kontroly, jednání s partnery

NIST framework

- Identifikace
  - Správa aktiv
  - Obchodní prostředí
  - Řízení
  - Hodnocení rizik
  - Strategie řízení rizik
- Ochrana
  - Správa identit a řízení přístupu
  - Povědomí a školení
  - Bezpečnost dat
  - Procesy a procedury ochrany informací
  - Údržba
  - Ochranná technologie
- Detekce
  - Anomálie a události
  - Kontinuální monitoring bezpečnosti
  - Detekční procesy
- Reakce
  - Plány reakce
  - Komunikace (stavu, výhledu)
  - Analýza
  - Omezení
  - Náprava (vylepšení)
- Obnova
  - Plány obnovy
  - Náprava (vylepšení)
  - Komunikace

rámec rozděluje problém na implementační skupiny, lze zpracovávat paralelně, musí mít jednotící politiku a řízení

… samozřejmě se nejedná o jediný rámec, berte to jako příklad

Obecné poznámky k právnímu rámci bezpečnosti

v současné době je již právní usazení problematiky bezpečnosti základním formujícím vlivem

z právního pohledu důležité pojmy:
due care (náležitá péče) – budete se chovat tak, jak lze očekávat od rozumného člověka v dané situaci
due dilligence (náležitá pečlivost) - soustavný dohled, že jsou dodržovány zásady náležité péče, tj. lze rozumně očekávat, že dlouhodobě je postupováno náležitám způsobem
compliance (shoda) – se stanovenými povinnostmi (zákony, normy, smluvy, …)
jurisdikce – oficiální autorita (resp. její geografická působnost) vytvářející právní rozhodnutí a rozsudky

zde zákony

- prováděcí vyhlášky
- nařízení vlády
- EU legislativa (nařízení EK, usnesení EP, …) včetně implementačních předpisů

kyberkriminalita – jakákoliv kriminální aktivita zahrnující použití počítačů a internetu

- kriminální chování vůči lidem
  - stalking (sledování)
  - online obtěžování
  - zcizení identity
  - zneužití kreditních informací
  - krádež
- kriminální chování vůči majetku
  - hackerství
  - rozšiřování počítačových virů
  - počítačový vandalismus
  - kriminalita v oblasti intelektuálního vlastnictví
  - porušování autorských práv
- kriminální chování vůči státu (vnímáno jako útok na suverenitu státu)
  - hackerství
  - krádeže utajovaných informací
  - kyberterorismus

únik dat – specifický druh kyberkriminality – jakýkoliv přístup k informacím bez odpovídajícího oprávnění

třídění je důležité – vychází z něho hodnoceni závažnosti přečinů … a rozsahu následných sankcí

Licenční ochrana – ochrana intelektuálního vlastnictví

- patenty – zákaz použití (výroba, prodej, import, neautorizované použití) vynálezu po určitou dobu
- obchodní známky (trademark) – slovo/fráze/symbol identifikující konkrétní výrobek, výrobce, pstup apod.
- autorské právo (copyright) – 70 letá ochrana výkonu specifických práv nad autorkými díly (knihy, filmy, písně, … počítačový SW, …)
- obchodní tajemství – konkrétní unikátní postup, formule, způsob výroby, informace … ke které má organizace vylučné právo.

Importní / exportní omezení – co a za jakých podmínek se smí dovážet a vyvážet
Přeshraniční přenosy dat – určité typy dat provázejí geografická omezení pro přenos, zpracování, uložení apod.
Soukromí (privacy) – bývá odlišně upraveno, např. GDPR, zpracování zdravotních záznamů, informací o dětech, …

Typy vyšetřování

- administrativní – zpravidla uvnitř organizace, lze s využitím služeb třetích subjektů, vlastní úroveň důkazů, arbitrární způsob rozhodování
- kriminální – definovanáý jurisdikce, důkaz na úrovni vyloučení pochybností, formální proces shromažďování dákazních prostředků, právní podpora procesu
- soukromoprávní – důkaz na úrovni převahy důkazů
- regulatorní – zkoumá se míra shody s regulativy, podobné kriminálnímu vyšetřování

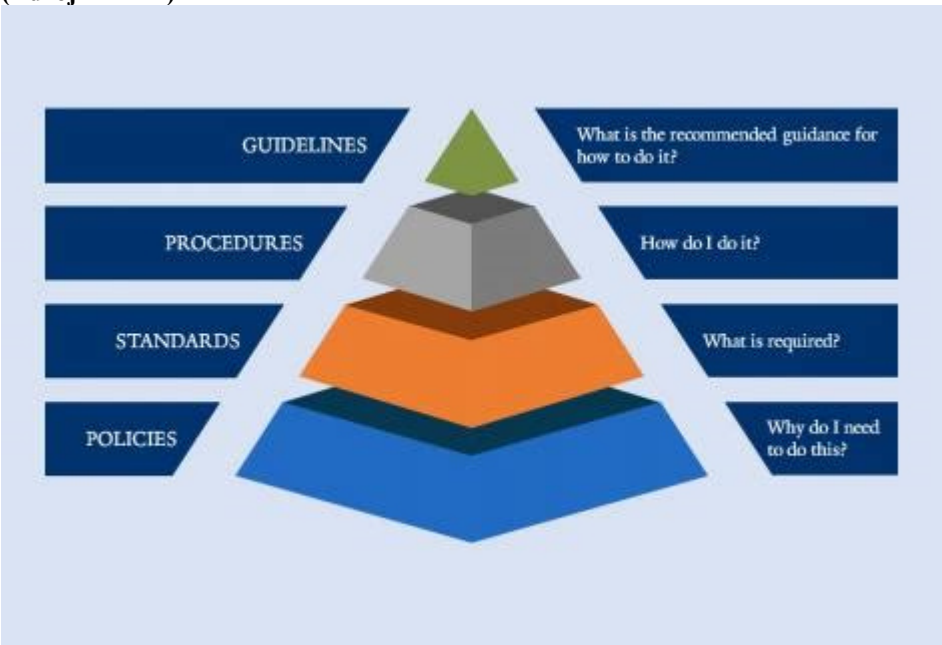
Vybrané zdroje požadavků na bezpečnost:

- Eu nařízení (
  - Budapešťská konvence – Evropská konvence o kyberkriminalitě 2001 – definice, klasifikace, kodifikace mezinárodní spolupráce
  - nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu
  - NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR)
- zákony např.
  - 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti,

    - 250/2017 Sb. o elektronické identifikaci
    - 181/2014 Sb, o kybernetické bezpečnosti
    - 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce
    - 110/2019 Sb., o zpracování osobních údajů (Adaptační zákon)
- oborové normy
- technické standardy
- vnitrofiremní směrnice
- požadavky obchodních partnerů
- ...

Vývoj, dokumentace a implementace politik, standardů, procedur a doporučení

(Zdroj -YALE)



- politika -sada principů uplatňovaných při rozhodování a provozu bezpečnostních opatření
- standard – sada specifických a konkrétních požadavků
    - základní požadavky (baseline)
- procedury – do kroků rozepsané postupy jak zajistit určitou činnost / cíl
- doporučení – návrhy jak implementovat požadavky standardů

Standardy

Podle míry utajení a spolehlivosti, které by měl systém poskytovat je podrobován různě rigorózním testům, v kterých musí obstát. Tento proces se nazývá *validace*.
lze použít několik způsobů validace:

- formální verifikace - celý systém je popsán soustavou logických formulí, tato soustava je redukována na tvrzení o bezpečnosti systému, v rámci verifikace je třeba ověřit správnost převodu
- validace - je obecnější metoda, zahrnuje verifikaci a další metody
  - ♦ testování požadavků - testuje se, zda je splněn každý z požadavků na funkčnost systému
  - ♦ kontroly návrhu a kódu - kontroly prováděné v průběhu tvorby systému
  - ♦ testování modulů a celého systému - ověřování funkčnosti na zkušebních datech
- Tiger Team Penetration Testing - dnes opět používaná metoda, nezávislý tým odborníků pověřen úkolem provést průlom bezpečnostními mechanismy

Pokud systém obstojí při validaci, může mu být vystaven v rámci následné *certifikace* certifikát, který je formálním vyjádřením shody s požadavky příslušné normy.

Orange Book

dnes již zastaralá norma, ale zavedené principy platí dál
Trusted **C**omputer **S**ystem **E**valuation **C**riteria
tvůrcem Ministerstvo obrany Spojených států, první ucelená technická norma
systémy rozděleny do čtyř základních tříd, dále dělení na podtřídy

D, C1, C2, B1, B2, B3, A1

třída D - žádná ochrana

třída C1 - volná ochrana

Oddělení uživatelů od dat, musí existovat metody umožňující uživatelům chránit vlastní data před ostatními, uživatel zvolí, zda tyto mechanismy bude používat

třída C2 - Kontrolovaný přístup

Systém stále provádí volnou ochranu zdrojů, granularita však musí být až na úroveň jednotlivých uživatelů, musí být veden access log. Navíc ochrana proti *residuím* - obsahy paměti, registrů, … poté, co proces přestane tyto používat. Residua nesmí být zpřístupněna někomu jinému.

celá třída C je označována jako *optional protection* (volitelná ochrana) – musí být k dispozici příslušný mechanismus, který uživatel může použít

třída B1 - značkovaná ochrana

Každý kontrolovaný subjekt a objekt musí mít přiřazen stupeň utajení a musí být tímto stupněm označen, každý přístup musí být ověřován dle Bell-LaPadula modelu, musí existovat popis implementovaného formálního modelu, systém je podrobován testování

třída B2 - Strukturovaná ochrana

musí být k dispozici verifikovatelný globální návrh systému, systém musí být rozdělen do dobře definovaných nezávislých modulů, návrh musí zohledňovat princip nejmenších možných oprávnění, bezpečnostní mechanismy musí být uplatňovány vůči všem subjektům a objektům včetně všech zařízení, musí existovat analýza možných skrytých kanálů
vlastní systém musí běžet v rámci své bezpečnostní domény a provádět kontroly své integrity

třída B3 - Bezpečnostní domény

Systém musí být podrobitelný extenzivnímu testování, musí existovat úplný popis celkové struktury návrhu systému, musí být konceptuálně jednoduchý
musí existovat ochranné mechanismy na úrovni jednotlivých objektů, každý přístup musí být testován, kontrola na úrovni provádění jednotlivých typů přístupu daného subjektu
Systém musí být vysoce odolný vůči průnikům. Zařízení provádějící audit log musí umět odhadnout hrozící nebezpečí.

celá třída B je zonačována jako *mandatory protection* (povinná ochrana)– musí být k dispozici odpovídající mechanismus, který uživatel nemůže obejít ani deaktivovat

tříba A1 - Verifikovaný návrh

Návrh systému musí být formálně verifikován, existuje formální model bezpečnostního mechanismu s důkazem konzistentnosti, formální specifikace systému s ověřením, že odpovídá formálnímu modelu, ověření, že implementace není odchylná od formální specifikace, formální analýza skrytých kanálů

ITSEC

The **I**nformation **T**echnology **S**ecurity **E**valuation **C**riteria
mezinárodní sada kriterií, nadmnožina TCSEC
kriteria rozdělena na třídy funkčnosti (F) a korektnosti (E)
třídy funkčnosti F-D, F-C1, F-C2, F-B1, F-B2 a F-B3 zhruba co do funkčnosti odpovídají třídám C1 až B3 hodnocení TCSEC
kriteria hodnocení funkčnosti rozdělena na hodnocení integrity systému (F-IN), zajištění dostupnosti systémových zdrojů (F-AV), integrity dat při komunikaci (F-DI), utajení komunikace (F-DC) a bezpečnosti v rámci celé sítě (F-DX)
každé z těchto kriterií může být vyhodnocováno nezávisle, vyhodnocování prováděno pro požadovanou třídu funkčnosti

kriteria pro hodnocení korektnosti přidána pro zvýšení důvěryhodnosti systému
požadavky vyšší třídy korektnosti vždy nadmnožinou předchozích
E1 - testování
E2 - kontrola konfigurace a distribuce
E3 - ověření detailního návrhu a zdrojového kódu
E4 - zevrubná analýza slabin systému
E5 - důkaz, že implementace odpovídá detailnímu návrhu
E6 - formální modely, formální popisy a jejich vzájemná korespondence
tyto třídy odpovídají požadavkům na důvěryhodnost kladeným třídami C2 až A1 hodnocení TCSEC

kromě zmíněných kriterií hodnocení zabezpečených systémů existuje celá řada norem a doporučení upravující prakticky všechny podstatné rysy chování a architektury těchto systémů

Common criteria

metanorma stanovující principy a postupy, jak odvozovat konkrétní technické normy pro vývoj, testování, výsledné vlastnosti a provoz technických bezpečnostních protiopatření v různých prostředích
úzce souvisí s materiálem Common Evaluatin Methodology – pravidla pro vyhodnocování konkrétních systémů (target of evaluation) vůči daným požadavkům
formalizuje proces vyhodnocování:
evaluační kriteria → evaluační metodologie → evaluační schéma → evaluace → výsledky evaluace → certifikace → registr certifikátů

vyžaduje síť zkušebních laboratoří
odděluje funkcionalitu (sec. functional requirements) od „jistoty“ (sec. assurance req.)
sada konkrétních funkčních a „jistotních“ požadavků tvoří *profil zabezpečení (protectin profile)*
Funkční (functional) třídy:

- FAU – bezpečnostní audit
- FCO – komunikace
- FCS – kryptografická podpora
- FDP – ochrana uživ. dat
- FIA – identifikace a autentizace
- FMT – bezpečnostní management
- FPR – soukromí
- FSP – ochrana bezp. mechanismu
- FRU – využívání prostředků
- FTA – přístup
- FTP – důvěryhodná cesta/kanál

Jistotní (assurance) třídy:

- ACM – správa konfigurací
- ADO – dodávka a provoz
- ADV – vývoj
- AGD – dokumentace, návody
- ALC – podpora životního cyklu
- ATE – testování
- AVA – vyhodnocení slabin

Vyhodnocení kvality bezpečnostního mechanismu v rámci evaluačních kriterií potom podléhá následující klasifikaci:

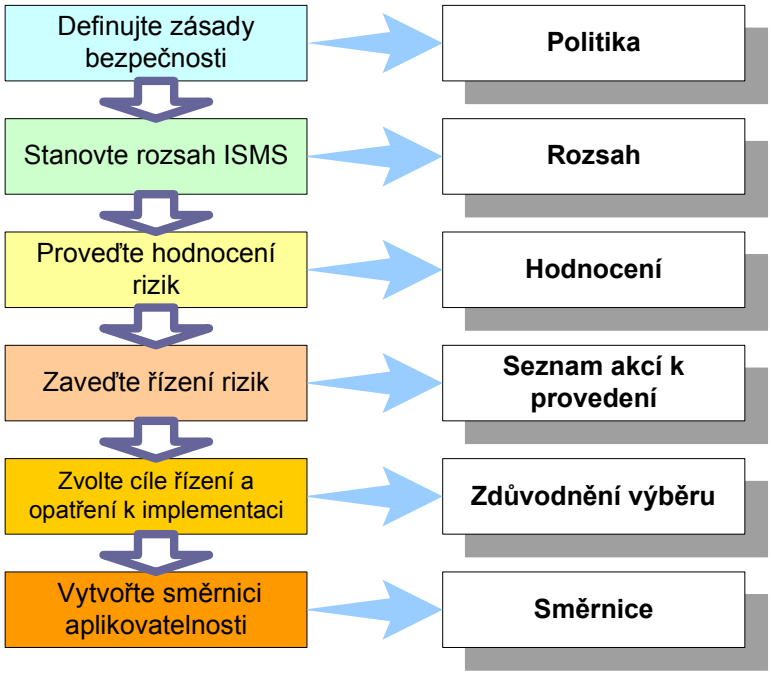
- APE – vyhodnocení profilu bezpečnosti
- ASE – vyhodnocení cíle hodnocení

Úrovně vyhodnocení (eval. assurance level) dle kriterií:

- EAL1 – funkční testování
- EAL2 – strukturální testování
- EAL3 – metodické testování a kontroly
- EAL4 – metodický návrh, testování a ověření
- EAL5 – semiformální návrh a testování
- EAL6 – semiformálně verifikovaný návrh a testování
- EAL7 – formální návrh a testování

BS7799

(ISO IEC TR 17799, ISO 2700x) organizační norma, která popisuje obecně, jaké činnosti musí organizace vykonávat pro zajištění bezpečnosti IS, nestanoví kvalitativní kriteria
založena na myšlence budování bezpečnosti shora dolů tj. od bezpečnostní politiky po implementaci protiopatření
předpokládaný proces tvorby bezpečnosti a z něho odvozené bezpečnostní dokumentace ukazuje obrázek



pokrývá tyto oblasti:

- bezpečnostní politika
- klasifikace a řízení aktiv
- personální bezpečnost
- fyzická bezpečnost a bezpečnost prostředí
- řízení provozu a komunikací
- řízení přístupu
- vývoj a údržba systémů
- řízení kontinuity operací
- soulad s požadavky (právní, technické, audit)

Pro podporu budování bezpečnosti a návrhu implementace bezpečnostních mechanismů podle BS7799 existuje standardní metodika a automatizovaný nástroj CRAMM.

Federal Information Processing Standard

FIPS 140-1: Security Requirements for Cryptographic Modules, January 4, 1994.
FIPS 140-2: Security Requirements for Cryptographic Modules, May 25, 2001. Change Notices 2, 3 and 4: 12/03/2002

ISO 27000

soustava norem pro zajištění bezpečnosti IS
hlavní oblasti bezpečnosti dle ISO27000:

- Bezpečnostní politika
- Organizace informační bezpečnosti
- Správa aktiv
- Personální bezpečnost
- Fyzická bezpečnost a kontrola prostředí
- Správa provozu a komunikací
- Řízení přístupu
- Pořizování, rozvoj a údržba bezpečnostních opatření
- Řízení bezpečnostních incidentů
- Řízení kontinuity operací
- Shoda s požadavky

- ISO 27000 - definuje pojmy a terminologický slovník pro všechny ostatní normy z této série.
- ISO 27001 (BS7799-2) - hlavní norma pro Systém řízení bezpečnosti informací (ISMS), podle které jsou systémy certifikovány
- ISO 27002 (ISO/IEC 17799 & BS7799-1) - přehled
- ISO 27003 - návod pro návrh a zavedení ISMS v souladu s ISO 27001.
- ISO 27004 - "Informační technologie – Bezpečnostní techniky – Řízení informační bezpečnosti - metriky".
- ISO 27005 - "Informační technologie – Bezpečnostní techniky – Řízení rizik informační bezpečnosti
- ISO 27006 - "Informační technologie – Bezpečnostní techniky – Požadavky na entity poskytující audit a certifikaci systémů řízení bezpečnosti
- ISO 27007 - "Informační technologie – Bezpečnostní techniky – Pravidla pro audit systémů správy informační bezpečnosti
- ISO 27008 - "Informační technologie – Bezpečnostní techniky – Guidelines for auditors on information security management systems controls
- ISO 27010 - "Informační technologie – Bezpečnostní techniky – Information security management for inter-sector and inter-organisational communications. Poskytuje doporučení pro řízení bezpečnosti informací při interní a mimo firemní komunikaci.
- ISO 27011 - "Informační technologie – Bezpečnostní techniky – Information security management guidelines for telecommunications organizations, doporučení a požadavky na řízení bezpečnosti informací v prostředí telekomunikačních operátorů.
- ISO 27013 - "Informační technologie – Bezpečnostní techniky – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1", doporučení pro implementaci ISO/IEC 20000 a ISO/IEC 27001
- ISO 27014 - "Informační technologie – Bezpečnostní techniky – Řízení informační bezpečnosti, doporučení při návrhu architektury řízení informační bezpečnosti.
- ISO 27015 - Information security management guidelines for financial services, doporučení a požadavky na řízení bezpečnosti informací v prostředí finančních institucí (banky, pojišťovny apod.).
- ISO 27016 - Information security management – Organizational economics, doporučení pro nastavení bezpečnostního programu s ohledem na předpokládané finanční výsledky.

- ISO 27017 - norma byla publikována na koci roku 2015 pod názvem *ISO*/IEC 27017:2015 / ITU-T X.1631 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services a poskytuje doporučení pro zabezpečení cloud computingu

- ISO 27018 - norma byla publikována v srpnu 2014 pod názvem ISO/IEC 27018:2014 —Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors. Poskytovatelům cloudových služeb dává vhodná bezpečnostní opatření pro zabezpečení soukromí zákazníků.

- ISO 27019 - norma byla publikována jako Technická zpráva (Technical Report) pod názvem "ISO/IEC TR 27019:2013 — Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry". Norma pomáhá organizacím v energetickém průmyslu interpretovat a aplikovat normu ISO/IEC 27002, aby byla zajištěna bezpečnost jejich systémů pro elektronické řízení procesů.

- ISO 27023 - norma byla publikována v červenci 2015 pod názvem ISO/IEC TR 27023:2015 Information technology — Security techniques — Mapping the Revised Editions of ISO/IEC 27001 and ISO/IEC 27002 a srovnává poslední vydání norem ISO/IEC 27001 a ISO/IEC 27002 s vydáními předchozími.

- ISO 27031 - norma byla publikována v březnu 2011 pod názvem "ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity".Obsahuje doporučení pro zajištění kontinuity činností organizace (business continuity).

- ISO 27032 - norma pod označením "Guidelines for cybersecurity" vyšla v červnu 2012, obsahuje bezpečnostní doporučení týkající se kyberprostoru.

- ISO 27033 - soustava norem poskytující doporučení pro implementaci protiopatření vztahujících se k bezpečnosti sítí. Prozatím bylo vydáno pět částí normy.

- ISO 27034 - soustava norem poskytující doporučení pro tvorbu, implementaci a užívání aplikačního softwaru. Byla vydána první část normy.

- ISO 27035 - norma byla publikována v roce 2011 pod názvem "Information security incident management". Norma se věnuje řízení incidentů bezpečnosti informací.

- ISO 27036 **-** soubor norem "Information security for supplier relationships" bude obsahovat doporučení organizacím pro hodnocení a snižování rizik týkajících se outsourcovaných služeb. Prozatím byla vydány první tři části.

- ISO 27037 **-** norma byla publikována v říjnu 2012 pod názvem "ISO/IEC 27037:2012 — Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence". Norma obsahuje doporučení pro zjišťování, sběr, získávání a uchovávání digitálních důkazů.

- ISO 27038 **-** norma byla publikována v roce 2014 pod názvem "ISO/IEC 27038:2014 — Information technology — Security techniques — Specification for digital redaction". Norma obsahuje doporučení pro publikování digitálních dokumentů.

- ISO 27039 **-** norma byla publikována v roce 2015 pod názvem "ISO/IEC 27039:2015 — Information technology — Security techniques — Selection, deployment and operation of intrusion detection [and prevention] systems (IDPS)" a obsahuje doporučení pro výběr, nasazení a provoz systémů pro detekci a prevenci bezpečnostních průniků (Intrusion Detection and Prevention Systems - IDPS).

- ISO 27040 **-** norma byla publikována v roce 2015 pod názvem "ISO/IEC 27040:2015 - Information technology - Security techniques - Storage security" a obsahuje doporučení pro bezpečné ukládání dat.

- ISO 27041 **-** norma byla publikována v roce 2015 pod názvem "ISO/IEC 27041:2015 — Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative methods" a obsahuje doporučení pro výběr forenzních metod pro zajištění a zkoumání digitálních důkazů.

- ISO 27042 **-** norma byla publikována v roce 2015 pod názvem "ISO/IEC 27042:2015 — Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence" a obsahuje doporučení pro analýzu a vyhodnocování digitálních důkazů.

- ISO 27043 - norma byla publikována v roce 2015 pod názvem "ISO/IEC 27043:2015 — Information technology — Security techniques — Incident investigation principles and processes" a shrnuje zásady a postupy při vyšetřování incidentů s využitím digitálních důkazů.
- ISO 27799 - doporučení a požadavky na řízení bezpečnosti informací ve zdravotnických zařízeních.

Zdroje standardů

Základní České standardy

Zákon o kybernetické bezpečnosti (zák. 181/2014 Sb.):

- dostupnost
- důvěrnost
- integrita

včetně vyhlášky 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti

Zákon o ochraně utajovaných informací (zák. 412/2005 Sb.)

- soubor opatření
  - bezpečnost informačních a kom. systémů (shodně)
  - další oblasti bezpečnosti – personální, fyzická, administrativní, průmyslová

Nařízení Evropského parlamentu č. 2016/679 ze dne 27.dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46ES (obecné nařízení o ochraně osobních údajů)

Mezinárodní standardizační instituty

ISO - International Organization for Standardization http://www.iso.ch/
IEC - International Electrotechnical Commission http://www.iec.ch/
ITU - International Telecommunication Union http://www.itu.ch/
WSSN - World Standards Services Network http://www.wssn.net/

Regionální standardizační instituty

CEN - European Committee for Standardization http://www.cenorm.be/

CENELEC - European Committee for Electrotechnical Standardization
http://www.cenelec.org/
COPANT - Pan American Standards Commission http://www.copant.org/
ETSI - European Telecommunications Standards Institute http://www.etsi.org/

Řízení kontinuity operací

Identifikace, analýza a prioritizace požadavků na obchodní kontinuitu

plánování obchodní kontinuity / kontinuity operací – metodologie a sada procedur pro zachování základních obchodních procesů v průběhu bezpečnostního incidentu a obnovy
plán pro zotavení po katastrofě – obnova informačních systémů a jejich služeb

Dopadová analýza

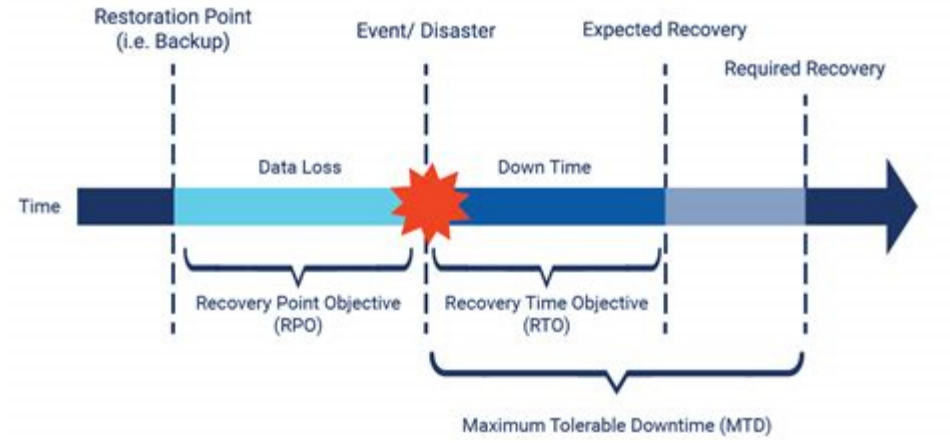
mapuje / kvantifikuje dopad přerušení služeb na organizaci v průběhu času
zpravidla začíná identifikací esenciálních / kritických *obchodních* procesů a kritických aktiv:

- lidé
- procesy
- informační systémy
- další aktiva

pro každý kritický obchodní proces je třeba provést analýzu rizik a identifikaci slabin

- pravděpodobnost výskytu
- dopad na obchodní proces

Výsledkem je tohle:



MTD – někdy též MAO (…outage) – maximální doba výpadku než nastanou významné dlouhodobé škody ohrožující existenci organizace
RTO – plánovaná, očekávaná doba na zotavení
RPO – plánovaná ztráta dat

plán kontinuity operací musí

- chránit kritické obchodní funkce
- splňovat regulatorní požadavky
- pokrývat všechny činnosti organizace ve všech regionech
- chránit příslušná aktiva
    - lidi
    - procesy
    - technologie

Řízení rizik

i na řízení rizik máme normy

- ISO31000,
- COBIT
- RiskIT
- Risk Management Framework od NIST,

Vždy se jedná o neustále probíhající proces:

- definice rozsahu a omezení
- identifikace
- analýza
- vyhodnocení
- kontrola:
    - eliminace

    - redukce
    - předání
    - zachování
- akceprace zbytkového
- komunikace a monitoring

Hodnocení rizik

je základní součástí řízení rizik

- Charakterizace systému
- Identifikace hrozeb
- Identifikace slabin
- Analýza opatření (stávajících, plánovaných)
- Určení pravděpodobnosti
- Dopadová analýza (ztráty)
- Zjištění rizika
- Dopopručená opatření
- Dokumentace

podobně jako samotné řízení, i hodnocení rizik musí být perpetuální

nutno si uvědomit, že rizika mají i netechnickou povahu:

- rozpočtová rizika
    - omezení zdrojů
    - nejisté priority
    - podhodnocení potenciálu
- rizika plánování
    - nejistota výkonu
    - dostupnost prostředků
    - dostupnost lidí
    - zajištění prostředí
    - nepřípustné podmínky
- technická rizika
    - vyzrálost technologie
    - licenční omezení
    - návrh dostupnosti
    - nebezpečí předělávek
    - vyspělost analytických metod

    - infrastruktura
- nákladová rizika
    - cena práce
    - eskalace
    - ceny materiálu a vybavení
    - kompletnost odhadů

Oblasti

- Zařízení a provozní prostředí
- Zdraví a bezpečnost
- Informační bezpečnost
- Slabiny řídícího rámce
- Právní a regulatorní požadavky
- Slabiny globálního řízení
- Reputace
- Strategie
- Provoz a chování
- Technologie
- Chyby řízení projektů
- Kriminální činy
- Personalistika
- Dodavatelé
- Informování managementu
- Etická rizika
- Geopolitická rizika
- Kulturní rizika
- Podnebí a počasí

Metody hodnocení rizik

- kvalitativní – v podrobnostech hodnotíme pravděpodopbnost a dopad
- semikvantitativní – riziko i odpad pouze zařadíme na orientační škále
- ohrožené hodnoty (VAR -value at risk) – na základě historických dat, předpokladu normálního rozdělení nebo Monte Carlo simulací se počítají potenciální ztráty v posuzovaném subjektu a pravděpodobnost, že k definované ztrátě dojde (např. za měsíc 3% prst ztráty 20% hodnoty).

ať či tak, vždy dojdete k nějaké přehledové matici rizik:

Kontrola rizik

- eliminovat – např. ukončením rizikové aktivity
- přesunout – outsourcing, pojištění
- omezit – pomocí opatření
  - preventivních – šifrování, autentizace, řízení přístupu, …
  - detektivních – logy, audit, IDS, …
  - korektivních – zálohování, reduntance, …
  - kompenzačních – posílení mechanismů (vícefaktorová autentizace)
  - odstrašujících – vystražné tabulky, odměny za dopadení pachatele, …
- přijmout

Koncepty modelování ohrožení

… identifikace potenciálních hrozeb
plocha útoků (attack surface) – rozumí se rozsah oblastí, které útočník může využít pro útok

Soustředěné na útočníka

identifikujeme různé útočníky, kteří mohou ohrozit provoz systému
profilace a rozdělení dle charekteristik – minimalizace počtu zkoumaných variant

Soustředěné na aktiva

primárně zkoumáme aktiva vysoké hodnoty

kategorizace aktiv dle ceny pro vlastníka a atraktivity pro útočníka
hledáme, jak může útok poškodit aktivum
vhodné při posuzování shody, ochraně vysoce cenných aktiv, intelektuálního vlastnictví apod.

Soustředěné na software

reprezentujeme systém jako soustavu propojených procesů
analyzujeme dopady kompromitace jednotlivých komponent na procesy
SCM

Kriteria pro výběr opatření

Opatření rozlišujeme na

- personálně orientované – nábor, restrukturalizace, vzdělávání, povědomí
- procesně orientované – politiky, postupy, toky řízení (workflow)
- technologicky orientované – šifrování, změny HW a SW, nastavení, …

Bezpečnostní efektivita - zda je opatření schopno přímo ovlivnit riziko
Nákladová efektivita – očekávaná ztráta a cena za impelementaci a provoz opatření musí být nižší, než očekávaná ztráta bez zavedení opatření

Provozní dopad opatření - náročnost zavedení, intuitivnost (složitost použití), porozumění
Nevhodně zvolené opatření může vést ke zvýšení rizika

Typy bezpečnostních opatření

- Preventivní – předchází vzniku incidentů (validace vstupů, firewally, zálohování, bezpečnostní povědomí)
- Detektivní – identifikacce události, když nastane, zjištění, co se stalo po události (bezpečnostní audit, auditní stopa, IDS, detekce průniku, …)
- Korektivní – úprava bezpečnostních mechanismů, minimalizace dopadu a opakování incidentu (patche, změny nastavení, změny politik, …)
- Obnova – postupy, nástroje obnovy funkčnosti (zálohy, záložní lokality, …)
- Odrazení – snaha přesvědčit útočníka, že nemá smysl útočit (ploty, stráže, kamerové systémy, …)

Hodnocení opatření

Je třeba pravidelně hodnotit vhodnost, přiměřenost a efektivitu opatření

- ověřování – kontroly, promýšlení postupů, pozorování, výpočty odhadů, analýza výsledků
- vyptávání – interview s relevatnními lidmi, objasňování nejasností,
- testování – provonání očekávaných a testem dosažených výsledků

nezbytný základ pro kontinuální zlepšování

Dopadová analýza

Při hodnocení rizik je zásadním určit rozsah dopadu
zpravidla závisí na okamžiku vzniku incidentu, době trvání, pochopitelně rozsahu

Hlavní složky

- náklady na náhradu – obnova komponent, znovupořízení dat, školení, spoluúčst na pojištění, …
- náklady spojené se ztrátou integrity – neautorizovaně pozměněné informace způsobí nesprávné akce, špatná rozhodnutí, poškození výroby, zranění, …
- náklady spojené se ztrátou dostupnosti – neschopnost vyrábět, obchodovat, dostát závazkům, splnit lhůty, sankce, pokuty
- náklady spojené se ztrátou důvěrnosti - ztráta konkurenčních výhod, dobré pověsti,

Personální bezpečnost

bezpečnost pracovníků je největší odpovědností bezpečnosntí politiky
zároveň procévníci představují významné riziko
činnosti v oblasti personální bezpečnosti

- prověřování a příjem uchazečů – zahrnuje kontrolu vzdělnání, pracovní historie, občanství, bezúhonnosti, kreditní a finanční historie, referencí a další činnosti dle senzitivity role, kterou bude pracovník zastávat
- pracovní smlouvy a politiky – vznik příslušných závazků
  - NDA – dohoda o zachování důvěrnosti informací
  - konkurenční doložka
  - politika akceptovatelného užívání prostředků
  - závazný způsob jednání
  - střet zájmů
- procesy nástupu, přesunu an jinou pozici, ukončení poměru
- dodhody s dodavately, konzultanty, kontraktory apod.
- požadavky na shodu

- jasně dokumentované
- zřetelně deklarované
- prokazatelně přijaté (podpis, atestace)
- iniciální školení

pravidelná recertifikace

Business Continuity Plan

… standardizován ISO 22301
zachování funkčnosti organizace
zpravidla odkazuje DRP jako svoji část

Řízení dokumentu

dokument s formálním řízením, verzování, stanovenou aktualizací
formálně schvalován

Obecné informace

stanovení účelu plánu a rozsahu řízení

- obecné informace – kontakty na kritické pracovníky, záchranný systém, informace o lokalitách, jejich povaze a obsahu, informace o záložních centrechThe types of threats, disruptions, disasters, and emergencies covered by the continuity plan.
- Seznam kritických funkcí a jejich závislostí
- Požadované časy obnovy
- Přeled strategií včetně způsobu ochrany pracovníků a kritických aktiv

Proces aktivace plánu

odpovědnost za aktivaci plánu
postup akcí pro spuštění plánu:

- Kontakty a odpovědnosti členů týmu kontinuity
- Jména a kontakty na další klíčové lidi, vlivné osoby, management a všechny, koho je třeba informovat
- Proces spuštění plánu, nutná rozhodnutí, metriky, odpovědnost za rozhodnutí.
- Pravidla a postupy, jak jsou informace o incidentu komunikovány, metody hlášení, intervaly, …

proces pro aktivaci musí být srozumitelný a všem zainteresovaným známý

Procedury obnovy a zotavení

každá jednotka organizace musí zpracovat svůj plán obnovy a zotavení na základě generálního plánu organizace

- Obecné postupy obnovy, úkoly, odpovědnosti
- Operace na zajištění životně důležitých aktiv (zejména data, klíče, …)
- Aktivity pro obnovu činností
- Procedury pro relokaci, vzdálenou práci

potřebné vzdělávací aktivity a nácvik situací pro veškeré pracovníky

Seznamy kontaktů

konktakty na všechny, kteří musí být informování
je třeba vymyslet takové uložení, které bude fungovat i v případě katastrofy
nutno zvážit, že ne všechny komunikační kanály budou funkční

- Členové týmu kontinuity obchodních operací
- Ředitelé a manažeři
- Tiskový mluvčí
- Ředitelé poboček a přidružených organizací
- Záchranný systém
- Státní agentury
- Záazníci
- Dodavatelé
- Obchodní partneři

Testování

plán musí být pravidelně testován – nutno dělat důkladně a odpovědně
Je třeba precizně zaznamenat výsledky a zejména nalezené nedostatky
nezbytné střídat různé scénáře
všechny uvažované scénáře ohrožení musí být popsány v sekci obecných informací

Vzdělávání a výcvik

Všichni pracovníci musí znát plán kontinuity a svoji roli v něm
Nutno stanovit:

- Očekávané výsledky
- Metody používané pro vzdělávání a nacvik situací, včetně simulací a vyhodnocování
- Kdo je subjektem vzdělávání a výcviku
- Jak se vyhodnocují výsledky

Dodatečné informace

- odkazy na plán obnovy po katastrofě (DRP), nebo plány klíčových dodavatelů a partnerů
- relevantní formuláře a metody pro sledování nákladů, komunikační schémata

- reference a přístupu k dokumentaci nutné pro provedení plánů

Havarijní plán

určuje, co dělat po odhalení útoku (bezpečnostního incidentu) a jak postupovat, aby se udržela kontinuita činnosti organizace.
určuje
- místa skladování a počty náhradních dílů,
- místa skladování a způsob organizace záloh dat,
- obsah pohotovostního skladu technických a softwarových náhrad,
- metodiku udržování aktuálnosti skladů dat, softwaru, hardwaru a
- metodiku aktualizace a testování hardwaru.

Součástí havarijního plánu jsou
- návody, jak postupovat v poskytování služeb po zjištění útoku – *plán činnosti po útoku*,
- dohody o poskytování náhradních řešení informaticky orientovaných úkolů organizace,
- dohody o uvedení dat IS do původního stavu po havárii (incidentu).
- návod, jak postupovat při obnově činnosti IS po havárii – *plán obnovy*.

Plán činnosti po útoku

soubore scénářů pro situace vzájemně se lišící délkou přerušení činnosti, ztrátou různých typů vybavení, omezením přístupu do areálu organizace, potřebou návratu do původního stavu před útokem apod.

obvykle předepisuje provedení analýzy incidentu, , co se stalo a kdy, zda se řešila reakce podle plánu.

Po vyřešení incidentu je potřeba přijmout závěr, zda byl plán činnosti po útoku řešitelům dostupný,
zda byl efektivní, co příště dělat jinak a zda je potřeba plán modifikovat.

Průběh reakce na incident

1. okamžitě reagují odpovídající *týmy 1. reakce*.
Cílem

- ambulantní zásah,
- zajištění činnosti ve stavu nouze.

k dispozici
- návody pro činnosti po detekci útoku,
- seznamy adres, telefonů, e-mail adres

musí informovat pracovníka odpovědného za vyřešení incidentu

2. Týmy pro řešení incidentu mají
- směrnice definující postupy řešení,
- definice lokalit archivů,
- definice zdrojů náhradních dílů

provádějí posouzení důsledků útoku.

3. *týmy pro obnovu*,
uvádějí IS do standardního stavu

Plán obnovy (disaster recovery plan)

musí obsahovat kritéria definující,
- co se chápe havárií,
- odpovědnosti za aktivaci obnovy,
- odpovědnosti za aktivaci dílčích činností podle plánu obnovy a
- návody k provádění činností podle plánu obnovy.

V plánu obnovy je potřeba prosadit obvykle následující zásady:

- segmentace informačních zdrojů podle priority obnovy (např.: nejkritičtější zdroje do 30 minut, ostatní kritické zdroje do 2 hodin a zbývající během 24 hodin).
- Zbývající zdroje kategorizovat
  - prioritní zdroje obnovované do 6 hodin,
  - žádoucí obnovované do 12 hodin
  - vhodné pro obnovu do 24 hodin.

- Shodná pořadí obnovy ve všech odděleních organizace.

- Odpovědného pracovníka za vymezení kritičnosti a priorit stanovuje celková bezpečnostní politika. Stejná pořadí obnovy v plánu obnovy stanovují systémové bezpečnostní politiky.

- Vyhodnocování kritičnosti a priorit aplikací alespoň jednou ročně
- Seznamy kritických aplikací tříděné podle priorit obnovy.

Plán činnosti organizace ve stavu nouze

- existence plánu udržení činnosti kritických aplikací při přerušení nebo při degradaci služeb.
- Tým 1. reakce je potřeba udržovat v pohotovosti
  - přehled o stavu týmu,
  - schopnost týmu bezprostředně zahájit svoji činnost
  - schopnost reagovat na odhalení incidentu
  - výchova týmu k minimalizaci publicity útoku.
- Definice činností po podezření na průnik do systému
  - nepominutelné (minimální) úkoly pro správce systému, které jsou často protichůdné vůči požadavkům a tlaku správy uživatelů,
  - postupy při odstavení kompromitovaného počítače od ostatní sítě
  - postupy pro uschování záznamů o kritických činnostech uživatelů z hlediska bezpečnosti,
  - návody jak dělat identifikace provedených změn
  - návody pro obnovu softwaru z důvěryhodného zdroje
  - návody pro re-inicializaci systému řízení přístupu (změna hesel …) atd.
- Je zaveden systém varování o podezření na průnik útočníka či jiné porušení bezpečnosti
  - musí být nejen zaveden, ale i udržován a testován. součástí seznamy potřebných čísel telefonů či faxů, e-mailových adres, faxů a osobních kontaktů nutných pro mobilizaci členů týmů 1. reakce, včetně jejich pobytů mimo pracoviště.
  - Cílem takového systému je minimalizace šance úspěchu širokého průniku.
- Je zaveden systém sběru informací o podezření na porušení bezpečnosti
  - Takový systém podporuje stav bdělosti u zaměstnanců, partnerů a konzultantů. Týká se takových skutečností, jakými jsou oznámení o poruše disku, oznámení o ztrátě souboru nebo oznámení o krádeži.
- Jsou stanoveny povinnosti zaměstnanců při účasti na procesu obnovy po porušení bezpečnosti

- Povinnosti se mohou stanovovat u zaměstnanců, nikoli u partnerů nebo konzultantů.
- Povinnosti se nemohou křížit se společenskými zájmy vyšší důležitosti, jakými je např. činnost v rámci Červeného kříže při záplavách apod.

Vyhodnocování pokrytí funkcí předepsaných v celkové bezpečnostní politice

se provádí typicky s roční periodou

- Vyhodnocování provádí vrcholový management a jeho součástí je udržování zástupnosti expertů v týmu obnovy pro kritické aplikace.
- Maximalizace automatizace znamená minimalizace ceny
- Co lze udělat manuálně, je vhodné manuálně dělat.
- Je zavedena periodicita archivace dat
  - Plán obnovy řeší rotaci použití archivního média (dědeček–otec–syn). Periodicita je pochopitelně aplikačně závislá, může být denní, týdenní nebo třeba i měsíční.
  - V současné době nabývá na významu archivace kritických dat na mobilních počítačích
  - Přirozenou nutnosti je provádět potřebné archivace před cestou.
  - Musí být zaveden systém řízení přístupu k archivním kopiím
  - Koncový uživatel nemůže archivační systém využít k obejití autorizace přístupů. To vede k šifrovaným uložením archivních souborů a vyžaduje to periodické prohlížení záznamů o činnostech uživatelů bezpečnostním správcem.
  - Je třeba zachovat důvěrnost off–line uschovávaných archivních kopií
  - Typickým opatřením je šifrované uložení takových dat i mimo prostory organizace a je tudíž potřebné mít zabezpečenou dostupnost klíčů při jejich obnově. Samozřejmé je ošetření povinnosti zachovávat důvěrnost dat archivačním týmem.
  - Násobnost archivních kopií (alespoň duplicita)
  - Dříve než se použije archivní kopie pro obnovu, je potřeba mít alespoň jednu její kopii uloženou v archivu. Kritická data se obvykle trvale uchovávají mimo organizaci alespoň ve dvou kopiích.
  - Nepominutelná je existence inventurní evidence archivních kopií
  - Musí se zavést systematizace značení kopií a zajistit on–line udržování přehledů.

  - V síťových prostředích je vhodná automatizace archivace na serveru LAN
  - Musí se řešit trvalá dostupnost, tj. zapojení připojených koncových počítačů pro automaticky prováděnou archivaci např. „v nočním provozu“, aby bylo možné provádět archivaci automaticky bez zásahu koncového uživatele. Musí se ovšem vyřešit problém přístupových práv ze serveru ke stanicím chráněným heslem.
  - Likvidace dále nepotřebných informací je zárukou zachování důvěrnosti
  - Existují mnohé legislativní závazky pro stanovení periody uchovávání kopií dat. Za jejich znalost běžně odpovídá právní oddělení organizace.
  - Pro úspěšnou obnovu je důležitá volba archivního média
  - Určení archivního média obvykle předpisuje systémová bezpečnostní politika, stejně tak předepisuje i periodicitu testování použitelnosti archivního média.
- Plán obnovy musí splňovat požadavky dané kvantitativním cílem dostupnosti zdrojů (např. sdílené počítače dostupné po dobu rovnou alespoň 95% pracovní doby ve výrobní organizaci, po dobu rovnou alespoň 99,98 % pracovní doby v telefonní společnosti apod). Limity stanovuje vrcholový management.

Zálohování kritických zdrojů

  - *Horká záloha* představuje dostupnost plně provozuschopného centra obnovy po katastrofě,které je plně vybaveno technickými i logickými prostředky (hardware,software, komunikace) i technickým personálem. Předpokládá se restart provozu řádově do několika hodin a schopnost poskytovat služby i po dobu několika měsíců.
  - *Mobilní horká záloha* může být řešena např. instalací IT v dobře vybaveném „karavanu“.
  - *Teplá záloha* znamená, že lokální koncová pracoviště (displeje, tiskárny) jsou rekonfigurovatelná tak, aby umožnila přístup do vzdáleného centra obnovy po katastrofě.
  - *Studená záloha* požaduje, aby si organizace po katastrofě mohla připravit jiné pracoviště vlastním vybavením, doba reakce je obvykle několik dní.
- Organizace může provozovat duální (záložní) datové centrum umístěné v geograficky vzdálené budově.
- Pro stanovení ekonomické optimálnosti plánu obnovy je potřeba vzít do úvahy, čím je dána cena kopie

- Na cenu kopie má vliv výše možných ztrát (roční ztráty nebo roční náklady) a náklady na pořízení, náklady na skladování kopií. Velký problém je řešení zálohování on-line systémů provozovaných 24 hod., kdy se musí využívat techniky typu kontrolní body, žurnál transakcí, tandemové nebo zrcadlové zpracování.
- Systémová bezpečností politika předepisuje správu záloh dat
- Kde se udržují, což je ovlivněno energetickou závislostí, fyzickou bezpečností, složitostí řízení provozu. V jaké násobnosti se udržují a jak se distribuují.
- Zálohy dokumentace, manuálů
- Opět systémová bezpečnostní politika určuje, kde jsou uloženy a počet jejich kopií.
- Doporučuje se udržovat „zlatou kopii“, která slouží pouze k reprodukci provozních kopií a normálně se nepoužívá.
- Zajištění dostupnosti hardwaru
- Existenci smluvního systému oprav a údržby hardwaru, provozování náhradních zdrojů apod.