Normy ISO/IEC 27001 a 27002

Katalog opatření ISMS – oblasti bezpečnosti informací

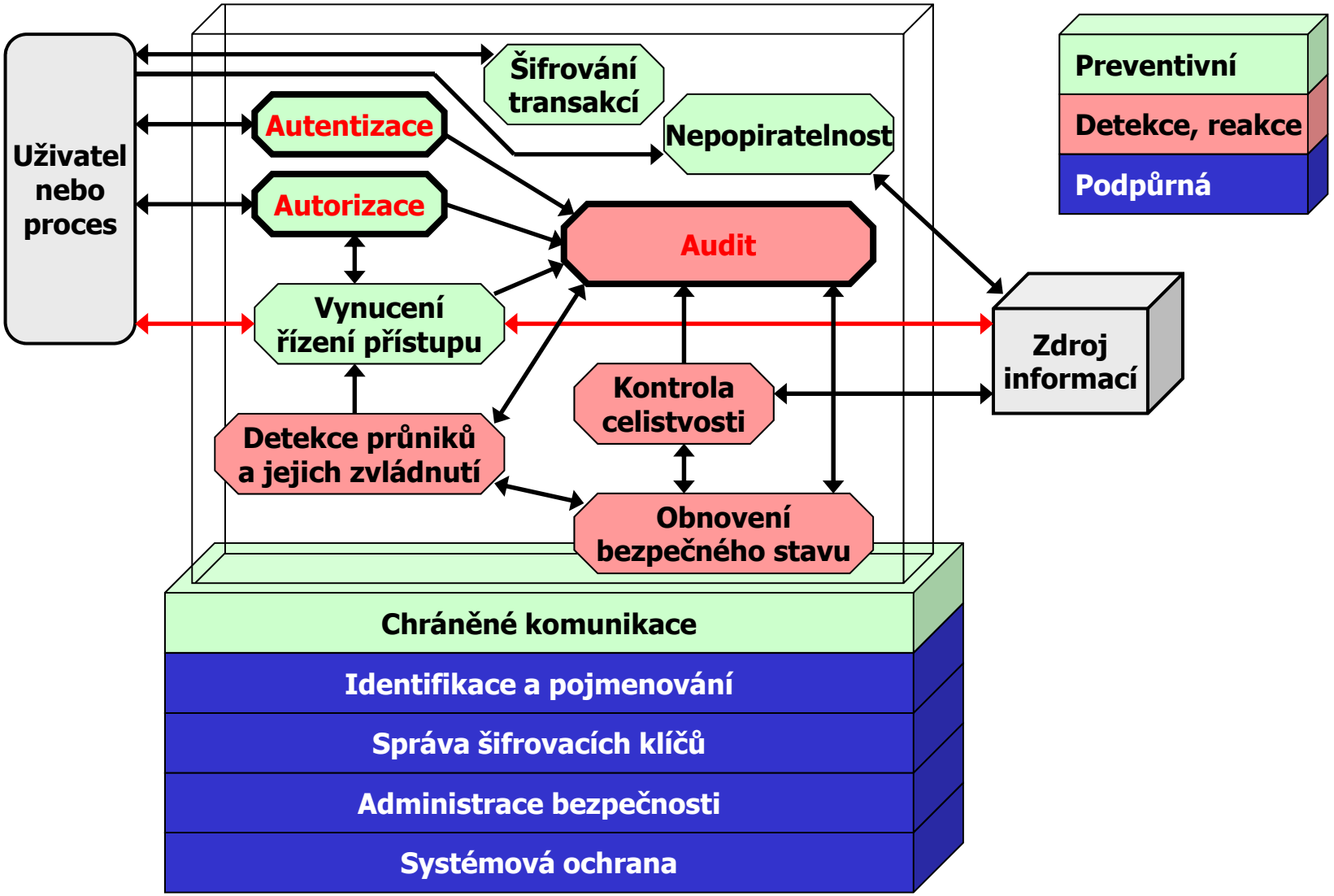
V Brně dne 13. října 2014

Opatření

- **Bezpečnostní opatření** – je proces, procedura, technický prostředek apod., speciálně navržené ke zmírnění působení hrozby (její eliminaci), snížení zranitelnosti, nebo dopadu hrozby.
- Základní rozlišení bezpečnostních opatření na typy:
  - preventivní
  - detekce a reakce
  - podpůrná
- Bezpečnostní opatření IS se dělí na oblasti:
  - řízení a správa bezpečnosti
  - technologická bezpečnost
  - bezpečnost provozního prostředí
- Výběr opatření dle metodik
  - CRAMM (databáze opatření) – expert, express
  - dle ČSN ISO/IEC 27002 (A.5 až A.15)

    alternativně dle ISO/IEC 27002:2013 (A.4 až A.18)

Technologická bezpečnostní opatření



Dělení opatření

- Mezi nejdůležitější jsou řazena takzvaná „všeobecně aplikovatelná ochranná opatření". Jedná se o základní kategorie:

  - řízení a politiky bezpečnosti IT

  - kontrola bezpečnostní shody

  - řešení incidentů

  - personální opatření

  - provozní problémy

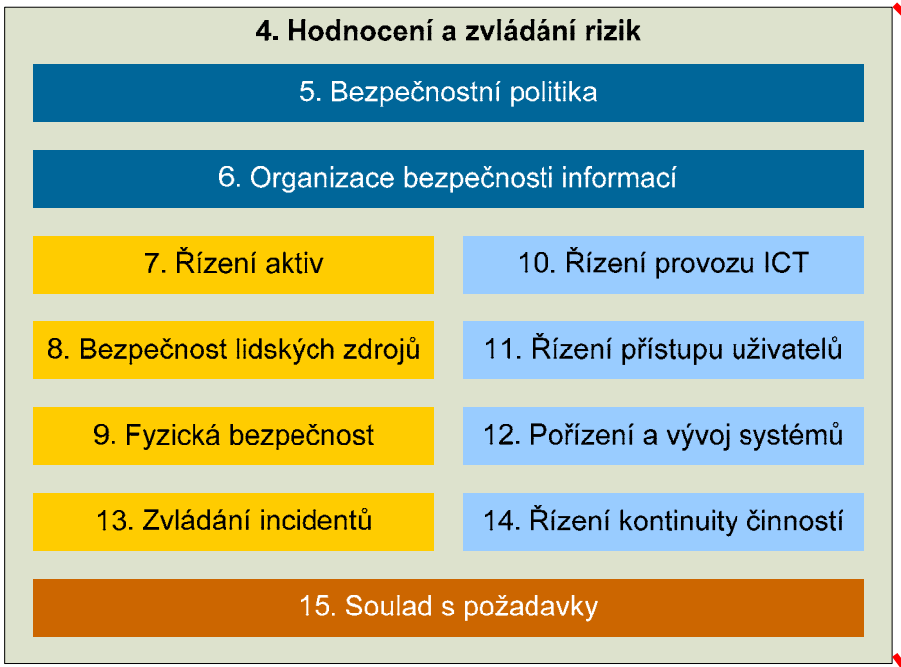
  - plánování kontinuity činnosti organizace

  - fyzická bezpečnost

ČSN ISO/IEC 27002

- Soubor popisů pro řízení bezpečnosti informací je dalším východiskem pro realizaci bezpečnostních opatření v rámci ISMS.
- Doporučení normy obsahuje 133 bezpečnostních opatření rozdělených do 11 oblastí.

Oblasti opatření ISMS dle ISO/IEC 27001, přílohy A



2013

A.5	**Politiky informační bezpečnosti informací**
A.6	**Organizace bezpečnosti informací**
A.7	**Bezpečnost lidských zdrojů**
A.8	**Management aktiv**
A.9	**Opatření k přístupu a řízení přístupových práv**
A.10	**Technologie kryptování**
A.11	**Fyzická bezpečnost pracovišť a zařízení**
A.12	**Bezpečnost provozu**
A.13	**Bezpečná komunikace a přenos dat**
A.14	**Bezpečná akvizice, vývoj a podpora informačních systémů**
A.15	**Bezpečnost pro dodavatele a třetí strany**
A.16	**Management incidentů**
A.17	**Kontinuita podnikání s ohledem na informační bezpečnost**
A.18	**Shoda s interními i externími požadavky**

Struktura přílohy A normy ISO/IEC 27001: 2013

ČSN ISO/IEC 27002:2013

- Doporučení normy nyní obsahuje 113 bezpečnostních opatření rozdělených do 14 oblastí.

5. Bezpečnostní politika

- **Bezpečnostní politika** (Security Policy) jsou pravidla, směrnice a zvyklosti určující způsoby, jimiž jsou v dané organizaci a jejích systémech řízena, chráněna a distribuována aktiva včetně citlivých informací.
- Bezpečnostní politika zajišťuje potřebnou úroveň důvěrnosti, autenticity a integrity dat v IS a dále zajišťuje požadovanou bezpečnost transakcí v distribuovaném prostředí (Internet).
- Je postaven na faktu, že vrcholové vedení organizace je srozuměno se záměrem zavedení a provozování ISMS. Obnáší to navíc jejich plnou podporu.
- Politiku bezpečnosti informací je třeba prakticky přezkoumávat a revidovat pravidelně (jedenkrát ročně) vedením společnosti. Revize vždy zohlední efektivitu politiky na základě vyhodnocení počtu incidentů, příčin, dopadů a nákladů přijatých opatření.
- Bezpečnostní politika IS organizace odpovídá bezpečnosti informací.
- Politika bezpečnosti informací pro vztahy s dodavateli – prověření dodavatelů, identifikace rizik třetích stran a bezpečnostních opatření s promítnutím do smluv.
- Politika mobilních zařízení – evidence, kontrola platforem OS, BYOD, MDM (Mobile Device Management).

2013

- *Existují dva základní dokumenty:*

  - Strategická (globální) bezpečnostní politika organizace
  - Bezpečnostní politika IS organizace

6. Organizace bezpečnosti informací

- Rozdělení na dvě základní skupiny:

  - interní organizace (A.6.1)

  - externí subjekty (A.6.2) 2013 **A.15 Bezpečnost pro dodavatele a třetí strany**

- Infrastruktura informační bezpečnosti
  - role, které odpovídají za řízení bezpečnosti v celé organizaci a útvaru IT
  - dohody o mlčenlivosti
  - nezávislé audity bezpečnosti
- Bezpečnost přístupu třetí strany
  - vyhodnocování rizik pro ustanovení ve smlouvách při přístupu třetí strany k zařízením a službám IT
- Outsourcing
  - vyhodnocování rizik pro ustanovení ve smlouvách při předání části IT do provozu a správy jiné organizaci

- Obsahuje dvě skupiny opatření:

1. Odpovědnost za aktiva

- určení vlastníků aktiv a vedení evidence aktiv

2. Klasifikace informací

- stupně ochrany aktiv podle jejich citlivosti či kritičnosti
- pravidla manipulace s informacemi podle jejich klasifikačního stupně
- Podle klasifikačního schématu (Classification Scheme)

Komerční sféra			***Státní sektor***	
důvěrné	(Confidentional)		**přísně tajné**	(Top Secret)
soukromé	(Private)		**tajné**	(Secret)
citlivé	(Sensitive)		**důvěrné**	(Confidentional)
veřejné	(Public)		**citlivé neklasifikované**	(Sensitive but Unclasified)
			neklasifikované	(Unclasified)

8. Bezpečnost lidských zdrojů 2013 8. Řízení aktiv

- A.8.1 – před vznikem pracovního vztahu
- *Bezpečnost v popisu práce a při zajišťování lidských zdrojů*
  - kritéria výběru pracovníků
  - závazek mlčenlivosti v pracovních smlouvách
- A.8.2 – během pracovního vztahu
- *Bezpečnostní povědomí zaměstnanců*
  - pravidelná bezpečnostní školení zaměstnanců
  - disciplinární řízení
- A.8.3 – po změně či ukončení pracovního vztahu
- *Výstup zaměstnanců*
  - vrácení prostředků IT
  - odebrání přístupových práv

9. Fyzická bezpečnost a bezpečnost prostředí (1. část)

- A.9.1 - Zabezpečné oblasti
  - vytváření zabezpečených zón s různou úrovní kontrol vstupu osob
    - fyzický bezpečnostní perimetr
    - kontrola fyzického vstupu
    - zabezpečení místností a prostředků
    - vnější hrozby a vliv prostředí
    - práce v zabezpečených oblastech
    - veřejný přístup (recepce, nakládka a vykládka, vizuální kontrola)

- A.9.2 - Bezpečnost zařízení
  - umístění zařízení v odpovídajícím prostředí
  - zabezpečení dodávky energie
  - údržba zařízení
  - mazání a likvidace paměťových médií

9. Fyzická bezpečnost a bezpečnost prostředí (2. část)

Spolehlivé smazání dat dle A.9.2.6 podle tří metod:

- mazání dat pomocí speciálních SW nástrojů (elektronická skartovačka dat)
- mazání elektromagnetickým impulzem
- fyzická likvidace (mechanicky, požárem, atd.)

- SW – **elektronická skartovačka dat** (HDD, SSD, Flash, externí disky)
- Nedostatečné je mazání souborů i formátování disku!
- *Metody mazání:*
  - **rychlá** skartace s jedním průběhem, přepis náhodným vzorcem
  - **U.S.DoD** - metoda amerického Ministerstva obrany, podle standardu DoD 5220.22-M od NSA (sedm přepisů skartovaných dat)
  - **Peter Gutmann** – doporučovaná metoda s 35 průběhy skartace (lze ji použít i pro komprimované disky)

Demagnetizace

- **Degaussing (demagetizace)** – bezpečné mazání dat
- Demagnetizátor vytváří silné elektromagnetické pole, které je klíčové pro eliminaci dat (datové pásky, pevné disky, floppy, audio a video kazety a pásky, magnetické karty).
- Příklad:

  Profesionální degausser ProDevice ASM120 je prvním automatickým demagnetizátorem, který je schopen vytvořit magnetické pole o intenzitě 11 000 Gaussů. Doba demagnetizace je cca 30 sekund.

- Požadavky a normy na bezpečné odstranění dat podle následujících předpisů:

  - PCI DSS (Payment Card Industry) Data Security Standard
  - NIST (National Institute of Standards and Technology)
  - HIPAA (Health Insurance Portability and Accountability Act)
  - PIPEDA (Personal Information Protection and Electronic Documents Act)

Likvidace médií - drtící stroj MAXXeGUARD

- **Tichá gilotina nakrájí disk, USB paměť i telefon**
- Gilotina je poháněna hydraulickým systémem a vyvíjí tlak až 220 barů.
- Na připojenou USB paměť nahraje protokol o likvidaci, včetně fotografie, času likvidace, jemnosti střihu
- Celý tento proces splňuje bezpečnostní kritéria kterékoli vlády, bezpečnostní služby, policejní složky či finanční instituce.

9. Fyzická bezpečnost a bezpečnost prostředí - rekapitulace

Zabezpečené oblasti chrání prostředí organizace jako celku.

Bezpečnost zařízení osahuje opatření chránící prvky infrastruktury ICT.

- *Obecná opatření:*
  - **pravidlo prázdného stolu a obrazovky** při opuštění pracoviště
  - pravidla pro přemísťování zařízení

2013 9. Opatření k přístupu a řízení přístupových práv

- Viz 11. Řízení přístupu uživatelů IS

10. Řízení komunikací a provozu IT (1. část)

Rozděleno 2013 → 12. Bezpečnost provozu
13. Bezpečná komunikace a přenos dat

- A.10.1 - Provozní postupy a odpovědnosti
  - dokumentace postupů
  - řízení provozních změn
  - rozdělení povinností (administrátorských privilegií)
  - oddělení vývoje od provozu

- A.10.2 – Řízení dodávek třetích stran
  - dodávky služeb (SLA)
  - monitorování a přezkoumávání služeb (třetích stran)
  - řízení změn služeb (třetích stran)

- A.10.3 - Plánování a akceptace systému
  - řízení kapacit (sledování míry využívání stávajících prostředků IT)
  - Přejímání systémů (do rutinního provozu)

10. Řízení komunikací a provozu IT (2. část)

- A.10.4 – Ochrana proti škodlivým virům a mobilním kódům
  - používání antivirových prostředků
  - pravidelné aktualizace ochranných prostředků
  - Pravidelné vzdělávání manažerů a koncových uživatelů

- A.10.5 – Zálohování informací
  - existence metodiky (plánu) zálohování
  - dodržování plánu zálohování
  - testování čitelnosti dat
  - Správné uložení záložních médií

- A.10.6 - Správa sítě
  - odpovědnost za provoz sítě
  - správa vzdálených zařízení
  - ochrana důvěrnosti dat přenášených po síti

10. Řízení komunikací a provozu IT (3. část)

- A.10.7 - Bezpečnost při zacházení s médii
  - správa počítačových médií
  - likvidace médií
  - manipulace a označování médií
  - bezpečnost systémové dokumentace
- A.10.8 - Výměna informací a programů
  - výměna dat s jinými organizacemi
  - bezpečnost médií při přepravě
  - bezpečnost elektronických služeb výměny dat
  - bezpečnost elektronické pošty
  - veřejně přístupné elektronické systémy





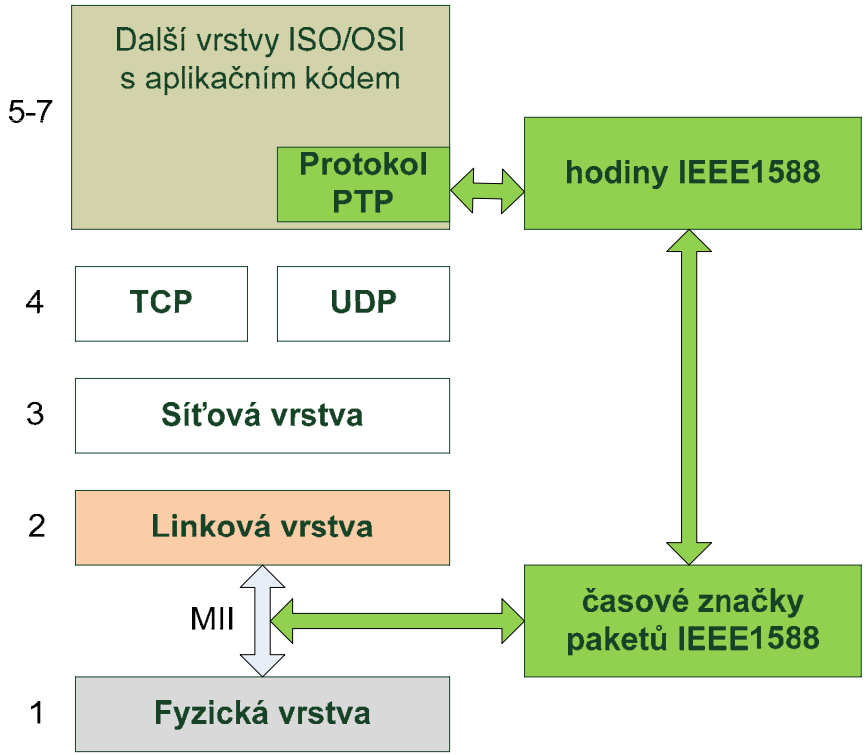
10. Řízení komunikací a provozu IT (4. část)

- A.10.9 – Služby elektronického obchodu
  - elektronický obchod
  - On-line transakce
  - Veřejně přístupné informace

- A.10.10 – Monitorování provozu
  - pořizování auditních záznamů (archivace chybových hlášení)
  - monitorování používání IS
  - ochrana vytvořených záznamů
  - administrátorský a provozní deník
  - záznam selhání
  - synchronizace hodin (P2P server)

P2P

- Základem synchronizace času je Precision Time Protocol (PTP) podle IEEE 1588.
- Princip synchronizace hodin reálného času podle IEEE 1588 spočívá v zasílání speciálních zpráv s časovými značkami mezi entitami komunikujícími v rámci jedné domény.



2013 10. Technologie kryptování

- Viz 12. Akvizice, vývoj a údržba informačních systémů

2013 11. Fyzická bezpečnost pracovišť a zařízení

- A.11.1 - Politika řízení přístupu
  - stanovení závazných pravidel pro přidělování přístupových oprávnění
- A.11.2 - Řízení přístupu uživatelů
  - registrace uživatele
  - evidence přidělených oprávnění
  - řízení privilegovaných oprávnění administrátorům
  - správa hesel
  - kontroly přístupových oprávnění
- A.11.3 - Odpovědnosti uživatelů
  - používání hesel
  - neobsluhovaná zařízení
  - zásada prázdného stolu a prázdné obrazovky

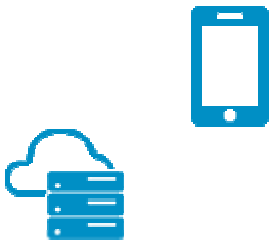
11. Řízení přístupu uživatelů IS (2. část)

- A.11.4 - Řízení přístupu k síti
  - mechanismy autentizace a řízení přístupu k síti
  - ochrana rozhraní sítě
  - oddělení v sítích
  - bezpečnost síťových služeb
- A.11.5 - Řízení přístupu k operačnímu systému
  - přihlašování uživatelů (identifikace a autentizace)
  - použití bezpečnostních mechanismů operačních systémů
  - časově omezené relace a spojení
- A.11.6 - Řízení přístupu k aplikacím
  - omezení přístupu k funkcím a datům aplikace
  - oddělení citlivých systémů (izolované aplikace)

11. Řízení přístupu uživatelů IS (3. část)

- *Monitorování přístupu k systému a jeho použití*
  - zaznamenávání událostí
  - monitorování využívání systému
  - kontrola zaznamenaných událostí
  - synchronizace času

- A.11.7 - Mobilní výpočetní prostředky a práce na dálku
  - opatření pří použití notebooků (BYOD)
  - vzdálený přístup k síti, systémům a aplikacím (VPN)



AAA

- Základní principy řízení přístupu k IS:

Identifikace – rozpoznání entity systémem.

Autentizace – ověření identity entity nebo zprávy.

Autorizace - ověření údajů při vstupu do systému či aplikace.

Předpokladem autorizace je úspěšná autentizace.

AAA protokol (Authentication, Authorization, Account).

Account je účtování po autentizaci a autorizaci neboli zápis výsledku předchozích procesů.

Servery pracující s AAA protokolem:

- ***RADIUS (DIAMETER)*** - Remote Authentication Dial In User Service
- ***TACACS (TACACS+)*** - Terminal Access Controller Access-Control System
- ***KERBEROS*** - síťový autentizační protokol ověřující uživatele a procesy v síti

Dvoufaktorová autentizace 2FA

- Běžná praxe

  Procedura zadání uživatelského jména a hesla se nazývá autentizace.

  Jako ověřovací faktor zde slouží jediný faktor – heslo.

- **Dvoufaktorová autentizace 2FA**

  Přidává ke standardnímu heslu jeden faktor navíc, který podstatně sníží riziko bezpečnostního incidentu.

- *3 typy nezávislých faktorů:*

  - **něco vím** (přístupová hesla, správná kombinace znaků, pro bankomaty nebo mobilní telefony PIN kódy a také správné odpovědi na „bezpečnostní otázky“)
  - **něco jsem** (využívání biometrických senzorů pro snímání otisků prstů, sítnice a duhovky nebo algoritmy pro měření charakteristiky chování, jako rytmus psaní nebo identifikace hlasu)
  - **něco mám** (fyzické klíče, průkazy totožnosti a také komunikační zařízení, například HW token, standardní mobilní telefon nebo smartphone)

- **Nejčastějším a neznámějším příkladem využití dvoufaktorové autentizace v internetových službách je kombinace faktoru „něco vím“ ve formě hesla se zasíláním SMS zpráv na mobilní telefon (něco mám) nebo využitím aplikace pro tvorbu jednorázových hesel ve smartphonech.**

IEEE 802.1X - autentizace v počítačových sítích

- Princip protokolu IEEE 802.1X je postaven na tom, že stanici při připojení k síti je povolena pouze výměna autentizačních informací.
  Jakákoli jiná jeho komunikace je blokována.
- Suplikant (speciální program pracující na uživatelské stanici) zajišťuje výměnu uživatelského jména a hesla (o které si může požádat, nebo je má uloženo v konfiguraci).
- Po úspěšné autentizaci dojde k odblokování stanice, ta pak může normálně komunikovat.
- Při autentizaci protokolem IEEE 802.1X se ověřuje totožnost uživatele, nikoli hardware, který používá.
- Řízení přístupu obsahuje tři části:

  - ***supplicant*** – *klientská aplikace snažící se připojit do sítě*

  - ***autentizátor*** – *aplikace na síťové straně ověřující klienta*

  - ***autentizační server*** – *poskytující autentizací údaje autentizátoru*

2013 12. Bezpečnost provozu

- A.12.1 - Bezpečnostní požadavky na systémy
  - analýza bezpečnostních požadavků při návrhu aplikačního SW
- A.12.2 - Bezpečnost v aplikačních systémech
  - validace vstupních dat
  - kontroly vnitřního zpracování
  - integrita zpráv
  - validace výstupních dat
- A.12.3 - Kryptografická opatření
  - šifrování
  - digitální podpisy
  - správa klíčů

Kryptologie

- **Kryptologie** je věda zabývající se šifrováním.
- **Kryptografie** je část kryptologie zabývající se převedením srozumitelné zprávy do nesrozumitelné podoby a zpět (šifrování a dešifrování textu - kryptoanalýza).
- Kryptologické systémy:

  DES (Data Encryption Standard) - *založen na blokovém symetrickém šifrování privátním klíčem, blok má délku 64 bitů.*

  IDEA (International Data Encryption Algorithm) - *založen na algoritmu s délkou klíče 128 bitů se symetrickým šifrováním, blok má délku 64 bitů.*

  RSA (Rivest, Shamir a Adleman algoritmus) - *založeno na „neschopnosti“ člověka vymyslet rychlý algoritmus pro rozklad velkých čísel na jeho prvočinitele*

  AES (Advanced Encryption Standard) - *s délkou vstupně-výstupního bloku AES 128 bitů a délkou klíče 128, 192, resp. 256 bitů*

- **Steganografie** je věda a umění schovat informaci jejím vložením do zdánlivě neškodné zprávy.

Elektronický (digitální) podpis

- Základní myšlenkou elektronického podpisu je obdoba klasického podpisu, jež má zaručit jednoznačnou identifikaci osoby v prostředí digitálního světa.

- **Od elektronického podpisu se vyžadují tyto vlastnosti:**

  - Jednoznačná identifikace původce podpisu - příjemce ví, kdo dokument poslal.

  - Zajištění integrity zprávy - příjemce má jistotu, že dokument došel kompletní a nebyl během přenosu pozměněn.

  - Zaručení nepopiratelnosti - odesílatel nemůže popřít, že daný dokument opravdu odeslal.

  - Podpis nelze napodobit ani zneužít pro jiný dokument.

Haš (Hash) je proces zajištění nečitelnosti dat digitálního podpisu konverzí na zhuštěnou zprávu s pevnou délkou prostřednictvím odolné kryptografie.

Klíč

- **Klíč (Key)** - V kryptografii je klíč hodnotou určující výstup šifrovacího algoritmu při transformaci hladkého textu na text šifrovaný.
- Podniková certifikační autorita pro interní použití v organizaci založená na OS Windows 2003 Enterprise Server.
- **Vytvoří základ PKI (Public Key Infrastructure) a umožní využívat funkce PKI pro následující typické PKI aplikace:**
  - autentizace do domény Active Directory (příp. k jiné adresářové službě založené např. na protokolu LDAP) - smartcard logon
  - autentizace k LAN síti dle 802.1x (AAA) s využitím certifikátů
  - autentizace k podnikovým webovým službám
  - zabezpečený VPN přístup k podnikové síti přes Internet
  - šifrování vnitropodnikové e-mail komunikace (např. pomocí Outlook)
  - šifrování uložených podnikových dat (např. EFS)
  - šifrování přenášených dat v LAN/WAN (IPSec)
  - zaručené elektronické podpisy interních elektronických dokumentů

12. Akvizice, vývoj a údržba informačních systémů (2. část)

- A.12.4 - Bezpečnost systémových souborů
  - integrita souborů aplikace
  - testovací data
  - ochrana zdrojových kódů

- A.12.5 - Bezpečnost procesu vývoje a podpory
  - postupy řízení změn
  - technické přezkoumání aplikací po změnách OS
  - řízení změn programových balíků
  - únik informací
  - externí programové vybavení (dohled a monitorování)

- A.12.6 - Řízení technických zranitelností
  - řeší instalace bezpečnostních záplat s ověřením jejich funkčnosti

2013 13. Bezpečná komunikace a přenos dat

- **Bezpečnostní incident** (Security Incident) je událost nebo události narušující bezpečnost IS.
- **Bezpečnostní událost** (Security Event) je identifikovaný stav narušující pravidla bezpečnostní politiky.
- A.13.1 - Hlášení bezpečnostních incidentů (uživatelé)
  - způsob oznamování (Helpdesk)

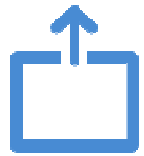
- A.13.2 – Zvládání bezpečnostních incidentů a náprava (ISMS odborníci)

- Reakce na bezpečnostní incidenty
  - odpovědnosti a postupy
  - kroky k nápravě

- Vyhodnocení bezpečnostních incidentů
  - kvantifikace a monitoring typů, rozsahu, škod a nákladů

14. Řízení kontinuity činností organizace

2013 14. Bezpečná akvizice, vývoj a podpora IS

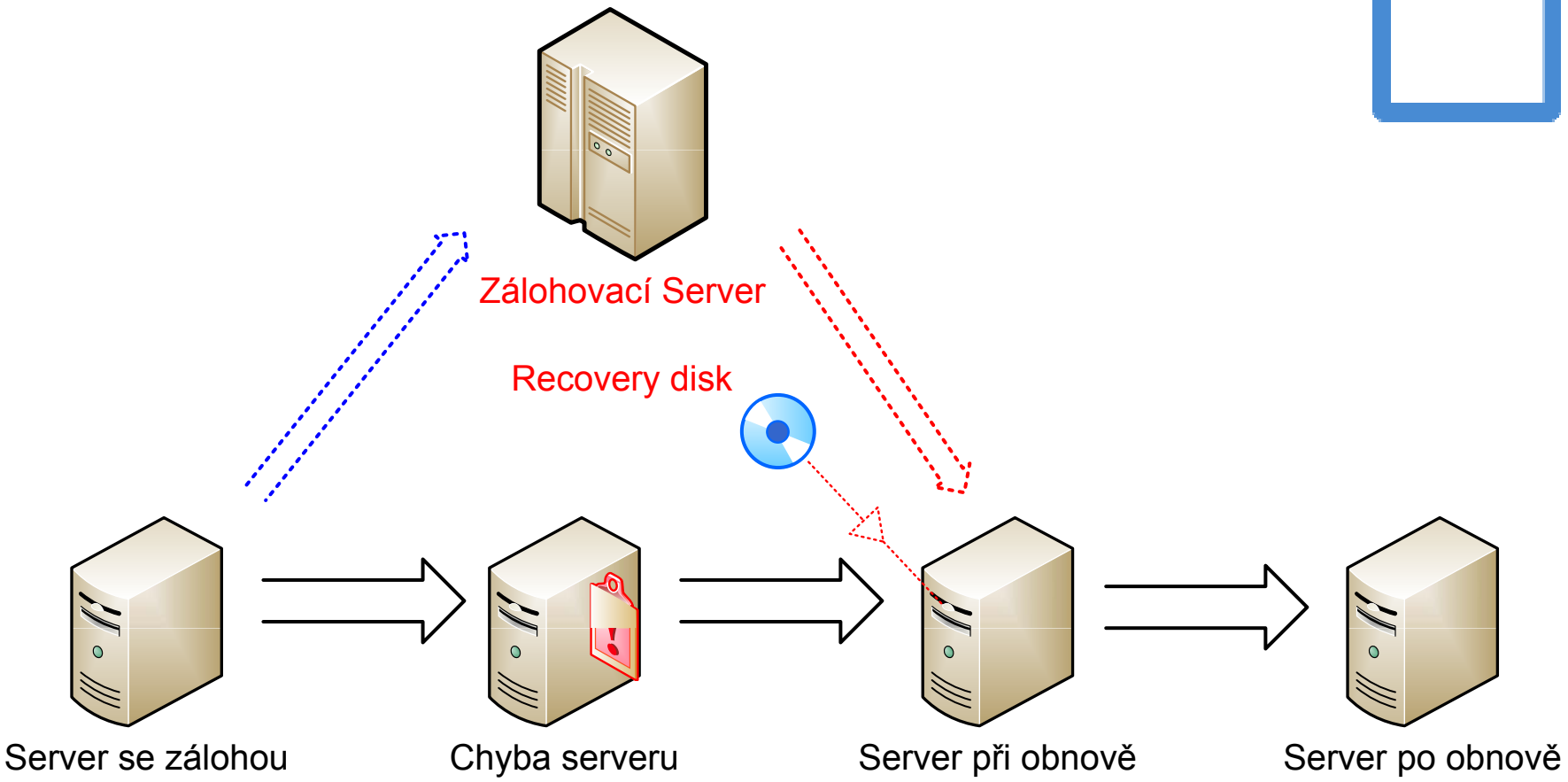


- **BCM** (Business Continuity Management) - *Řízení kontinuity činností organizace*
- **DR** (Disaster Recovery) – *Obnova po havárii*
- **DR plán** - shromažďuje postupy pro zajištění obnovy IT služeb po živelných pohromách a jiných zásadních událostech. Je to v podstatě návod jak v co nejkratším čase s minimem výdajů a rizik obnovit chod kritických aplikací.

- Strategie řízení kontinuity
  - analýzy obchodních dopadů při přerušení procesů
- Plány kontinuity
  - vytváření a testování plánů kontinuity
- ISO/IEC 24762:2008 - Information technology - Security techniques - Guidelines for information and communications technology disaster recovery services
  Norma nabízí směrnice pro obnovu po havárii (ICT DR) jako části BCM.

Příklad DR plánu

- Důležitost zálohování a bezproblémové obnovy



15. Soulad s požadavky

- A.15.1 - Shoda s právními požadavky
  - sledování a zavádění požadavků právních a technických norem
  - ochrana duševního vlastnictví (autorský zákon)
  - ochrana záznamů organizace (archivnictví a spisová služba)
  - ochrana osobních údajů
  - prevence zneužití prostředků pro zpracování informací
  - regulace kryptografických opatření

- A.15.2 - Posouzení bezpečnostní politiky a technické shody
  - kontroly dodržování interních předpisů
  - technické kontroly bezpečnosti technologických systémů

- A.15.3 - Aspekty auditu IS
  - opatření k auditu IS
  - ochrana nástrojů k provádění technických auditů IT

Audit IS

- **Audit IS** je periodické prověřování připravenosti IS a personálu na situace, kterým je lépe předcházet.
- Mezi základní oblasti auditu patří:

  - Funkcionalita IS
  - Provozní bezpečnostní politika
  - Vyhodnocování provozních statistik
  - Vzdělávání správců a uživatelů
  - Zálohování a profylaxe

2013 15. Bezpečnost pro dodavatele a třetí strany

- Viz 6. Organizace bezpečnosti informací, 6.2

2013 16. Management incidentů

- nové

2013 17. Kontinuita podnikání s ohledem na informační bezpečnost

- Viz 14. Řízení kontinuity činností organizace

2013 18. Shoda s interními i externími požadavky

- Viz 15. Soulad s požadavky