Kybernetická bezpečnost - informační systémy
Bezpečnostní pohledy

Ing. Vladimír Lazecký
vladimir.lazecky@viavis.cz

VIAVIS střežíme podstatné

Aktuality z kyber světa

- Prezentace studentů ☺

Proč informační systémy v kybernetické bezpečnosti?

- Zopakujme:
  - Kybernetická x informační bezpečnost
  - Co je a co není bezpečnost?
  - Co je cílem bezpečnosti?
  - Co je bezpečnostní incident?

Proč informační systémy v kybernetické bezpečnosti?

- **Cílem útoků:**
  - Informace (reprezentována daty)
  - Informační systém (v celém kontextu)
  - Lidé informační systém využívající
  - Sociální systémy (stát, komunita…)

- Dopady útoků – mohou být extrémní:
  - Politická rozhodnutí
  - Likvidace firem
  - Likvidace osob

- Je nutno znát architekturu a části informačního systému
  - **Musím vědět - co chráním a před čím chráním**
  - **Obecná ochrana neexistuje**

Informační systémy - obsah přednášky

- Informační systém x ICT systém
- Možné pohledy na ICT systém
- Mikro IT x makro IT
- Architektura, vrstvy, provoz
- Specifické systémy

- Pohled důležitý z hlediska bezpečnosti

Informační systém

- Informační systém – systém, který:
  - Sbírá informace
  - Transformuje informace na data
  - Zajišťuje přenos, zpracování a uchování dat
  - Data prezentuje a interpretuje
  - Zajišťuje archivaci nebo ničení dat

- Je informační systém vždy ICT (počítačový) systém?
  - Kartotéka u lékaře
  - Pořadač vizitek

Informační systém – ICT systém

- ICT systém - informační a komunikační systém využívající počítače
  - Komunikační a informační systémy splývají
  - Komunikační systémy jsou samy informačními systémy
  - ICT systém je pouze podmnožinou informačního systému
  - Je chybou zužovat bezpečnostní aspekty pouze na ICT systém (*dále v přednášce*)

- *Jak vypadá profesionální hacker, cracker, kyber terorista?*
- *PR kreativec – zdroj útoků?*

- *Proč je třeba se alespoň orientovat v architektuře informačních systémů?*
- *Proč je třeba znát principy?*
- *Mohu se bez těchto znalostí chovat „bezpečně“?*

Možné pohledy na informační systém využívající ICT systém

- Existuje mnoho pohledů:
  - Manažerský pohled
  - Black box x Crystal box
  - Mikro ICT systémy x makro ICT systémy
  - Funkční pohled
  - Procesní pohled
  - Architektonický pohled
  - Pohled dle rolí

- **Bezpečnostní přístup – musí zahrnovat všechny pohledy a aspekty**

Možné pohledy na informační systém využívající ICT systém

- **Manažerský pohled – je rozhodující:**
  - **Rozhodnutí k neznalosti**:
    - *„Jsem přetížen, zahlcen, nechci tomu rozumět“*
    - *„Od toho mám ajťáky“*
  - **Iluze znalosti:**
    - Čtenář časopisů a účastník konferencí
    - Znalost detailu bez nadhledu
    - Znalost minulosti
  - **Manažerský nadhled a manažerská pokora:**
    - Přehled základních principů a jejich pochopení
    - Umění naslouchat a hodnotit
    - Schopnost dělat správné závěry a rozhodnutí
    - Schopnost nést odpovědnost

Možné pohledy na informační systém využívající ICT systém

- **Manažerský pohled:**
  - Manažerská arogance:
    - Vím nejlépe jak
    - Jak jsem rozhodl, tak to bude
  - Neznalost:
    - Rozhodnutí dle špatných východisek a kritérií
    - Nic se mi nemůže stát, nikdy se nestalo
  - Zájem, ale neznalost:
    - Věřím svým *ajťákům*
    - Snažím se chápat, ale kde informace ověřit?

Možné pohledy na informační systém využívající ICT systém

- **Manažerský problém:**
  - Jak se orientovat, kde získat relevantní informace a nadhled?
  - Manažeři jsou přehlceni informacemi/šumem
  - Problém nutnosti rychlých rozhodnutí/žádné podklady

  - Experti mluví nesrozumitelným jazykem
  - Bez elementárních znalostí nelze vypěstovat manažerský cit

  - **PROČ - manažerský pohled je zdrojem vážných incidentů**

Manažerské incidenty

Systém veřejné správy napadli hackeři, útok se týkal Prahy i ministerstva práce

AKTUALIZOVÁNO 5. 3. 2021

Systém veřejné správy napadli ve čtvrtek hackeři. O masivním kybernetickém útoku informoval na Twitteru pražský primátor Zdeněk Hřib (Piráti), data magistrátu podle něj nebyla poškozena. Jedním z cílů

https://ct24.ceskatelevize.cz/domaci/3278730-system-verejne-spravy-napadli-hackeri-utok-se-tykal-prahy-i-mpsv?fbclid=IwAR2KTRD0o4re2rGio-hpIqQmROzmk_NVMVaV47pCdDK_D-3wZQ-k7AmBcqA

ICT sytém black box x crystal box

- **Black box** – interní architektura systému se nezkoumá, pouze:
  - Vstupy
  - Transformace - funkce, vlastnosti (neřeší se jak)
  - Výstupy

- Typický pohled uživatele, managera

- Prvky systému typu black box – např. komerční software

  - *Co dělá excel?*

  - ***Praxe víry – existuje cesta limitace rizik?***

ICT sytém black box x crystal box

- **Black box -** diskuse:
  - *WIN, Mac OS, iOS, Android – jaká je jejich míra bezpečnosti?*
  - *Bezpečnostní aspekty black box, výhody, nevýhody*
  - *Kdy je možné z bezpečnostního hlediska využít black box?*
  - *Čím je dána bezpečnost systému black box*
  - *Jak lze ošetřit bezpečnostní aspekty systému black box*
    - ***Kyber bezpečnost x právní instrumenty – smlouvy, odpovědnost***

ICT sytém black box x crystal box

- **Crystal box** – je známa podrobná architektura a všechny prvky systému:
  - Vstupy
  - Transformace - funkce, vlastnosti:
    - Prvky systému, jejich vlastnosti, funkce
    - Vazby mezi nimi – funkční, bezpečnostní
    - Interní architektura
  - Výstupy

  - Pohled architekta, designéra, správce, auditora
  - Pohled manažera – opět důvěra k profesionálovi
  - Prvky systému – např. Open Source software

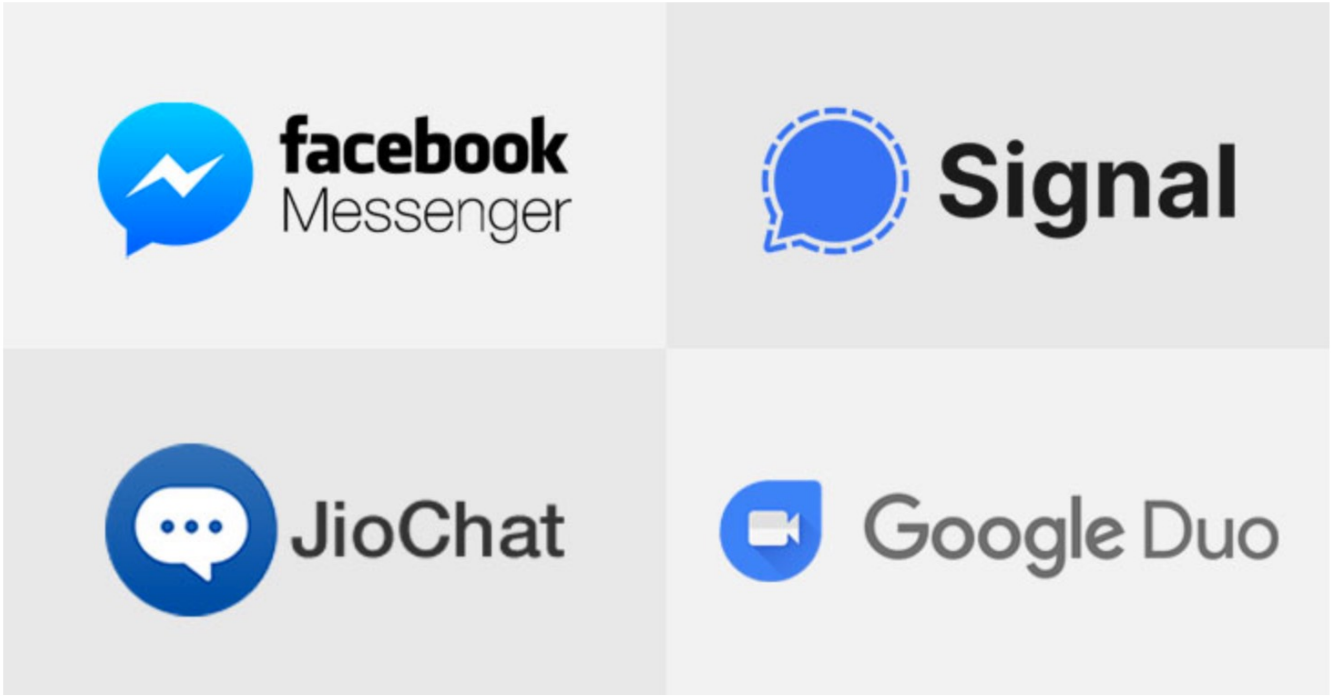
ICT sytém black box x crystal box

- *Bezpečnostní aspekty, výhody, nevýhody*
- *Čím je dána míra bezpečnosti?*
- *Kdy je výhodné použít crystal box x black box*
- *Kritické místo?*
- *Právní aspekty*
- *Vynutitelnost odpovědnosti za open source SW*

Jsme ve světě víry

Google Details Patched Bugs in Signal, FB Messenger,

January 20, 2021 Ravie Lakshmanan



https://thehackernews.com/2021/01/google-discloses-flaws-in-signal-fb.html

Odezvy výrobců

- **Signal** (fixed in September 2019) - A audio call flaw in Signal's Android app made it possible for the caller to hear the callee's surroundings due to the fact that the app didn't check if the device receiving the connect message from the callee was the caller device.

- **JioChat** (fixed in July 2020) and **Mocha** (fixed in August 2020) - Adding candidates to the offers created by Reliance JioChat and Viettel's Mocha Android apps that allowed a caller to force the target device to send audio (and video) without a user's consent. The flaws stemmed from the fact that the peer-to-peer connection had been set up even before the callee answered the call, thus increasing the "remote attack surface of WebRTC."

- **Facebook Messenger** (fixed in November 2020) - A vulnerability that could have granted an attacker who is logged into the app to simultaneously initiate a call and send a specially crafted message to a target who is signed in to both the app as well as another Messenger client such as the web browser, and begin receiving audio from the callee device.

- **Google Duo** (fixed in December 2020) - A race condition between disabling the video and setting up the connection that, in some situations, could cause the callee to leak video packets from unanswered calls.

https://thehackernews.com/2021/01/google-discloses-flaws-in-signal-fb.html

Mikro ICT systémy x makro ICT systémy

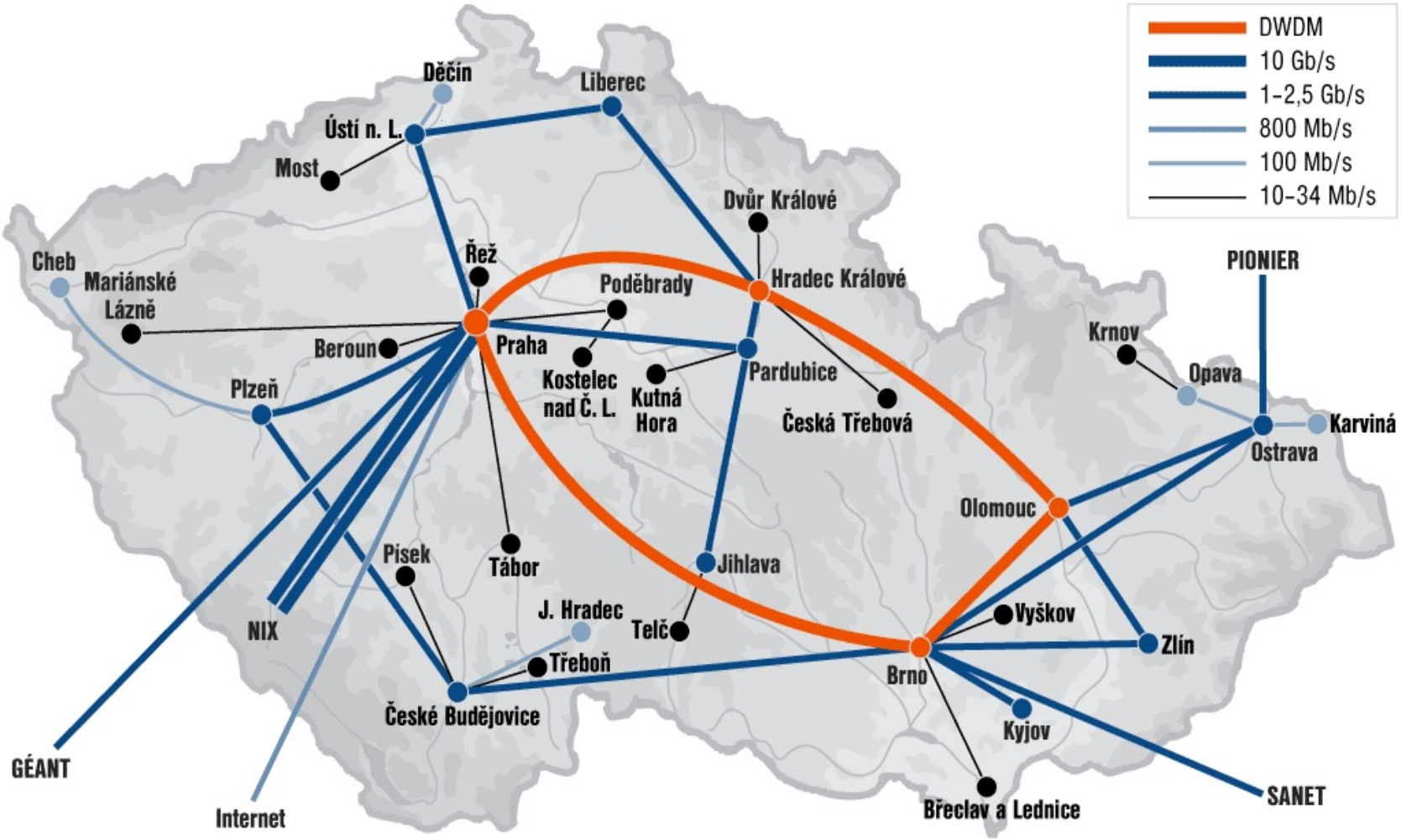
- **Mikro ICT systémy:**
  - Zjednodušeně – **lze definovat jejich perimetr**
  - Interní ICT systémy korporací, firem, organizací veřejné správy, domácností
  - Feudální charakter řízení – vlastníkem
  - Větší možnosti vynucení bezpečnostní politiky
  - Častý cíl interních útoků
  - Rychlá reakce na incident
  - Omezené zdroje (opravdu?)
  - Bezpečnost je často neřešeným problémem
  - Nevnímání některých rizik:
    - Nedostupnost správce
    - Otevřenost komunikace

Mikro ICT systémy x makro ICT systémy

- **Makro ICT systémy:**
  - ICT systémy na úrovni velkých celků – státu, silových složek, nadnárodních organizací
  - Velmi obtížně lze definovat jejich perimetr
  - Jiná architektura a charakter, než mikro ICT systémy
  - Nelze obvykle uplatnit feudální (hierarchické) řízení
  - Pomalejší reakce
  - Problematická definice odpovědnosti
  - Obtížná vynutitelnost pravidel hry
  - Jakou mají vůbec strukturu? Je hierarchická – pouze u této lze velet…

    - ***Diskuse: Jak lze „vypnout internet“?***

Hierarchická struktura?



VIAVIS střežíme podstatné

Makro ICT systémy

- **Jak lze vynutit regulaci v ne hierarchickém systému**:
  - Vypnutím služby?
  - Represí?
  - Regulace bez kontroly nedává smysl
  - Kde je míra regulace?

- **Regulace vždy zaostává za vývojem** (z principu reaktivního řízení)
- Klíčové systémy veřejné správy jsou provozovány nad internetem
  - *Diskuse:*
    - *Proč?*
    - *Výhody?*
    - *Rizika?*
    - *Nové systémy zvyšují rizika, např. EET…*

  - Prosazení zákona o kybernetické bezpečnosti – je řešením?

Internet

- Co je internet:
  - Množina vzájemně propojených sítí
  - Základem – síť ARPANET (vznik 1969)
  - Souvisí se vznikem síťového protokolu (protokolů) TCT/IP
  - *Víte, co je síťový protokol?*
  - *Znáte základní pojmy?*

Historie internetu – zdroj www.wikipedia.cz

- 1962 – vzniká projekt počítačového výzkumu agentury ARPA[1]
- 1969 – vytvořena experimentální síť ARPANET, první pokusy proběhly 2. září s přepojováním 4 uzlů
- 1972 – ARPANET rozšířena na cca 20 směrovačů a 50 počítačů, použit protokol NCP (Network Control Program)
- 1972 – Ray Tomlinson vyvíjí první e-mailový program
- 1973 – zveřejněna idea vedoucí později k TCP/IP jako náhrady za stávající protokol NCP
- 1980 – vydáno RFC 760, které popisuje IPv4, experimentální provoz TCP/IP v síti ARPANET
- 1983 – z ARPANETu oddělena síť MILNET (Military Network), TCP/IP přeneseno do komerční sféry, zavedeno DNS (Domain Name System)
- 1984 – vyvinut program BIND pro DNS, k ARPANETu připojeno pouhých 1000 počítačů
- 1985 – zahájen program NSFNET, sponzoruje rozvoj sítě ve výši 200 mil. dolarů, první komerční služby
- 1987 – vzniká pojem „Internet“
- 1987 – v síti je propojeno 27 000 počítačů
- 1989 – Tim Berners-Lee publikuje návrh vývoje WWW
- 1990 – Tim Berners-Lee a Robert Cailliau publikují koncept hypertextu

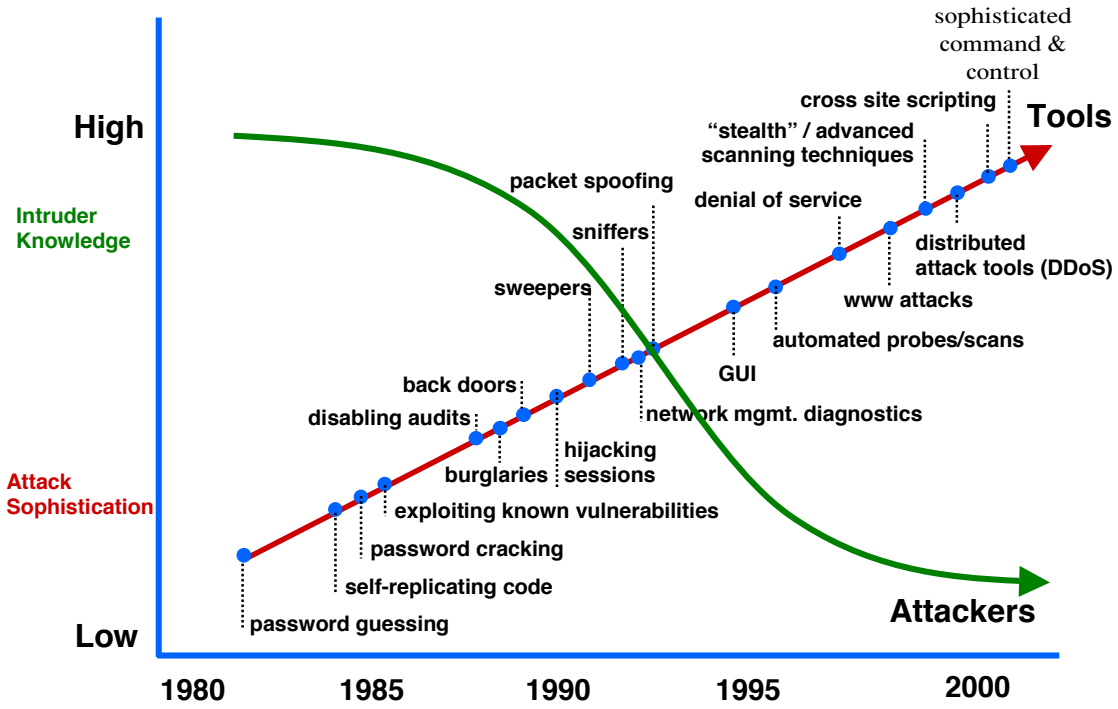
Historie internetu – zdroj www.wikipedia.cz

- 1990 – končí ARPANET
- 1991 – nasazení WWW v evropské laboratoři CERN
- 1992 – připojen Bílý dům (vstup vládních institucí na Internet), oficiálně připojeno Československo (13. února připojeno ČVUT v Pražských Dejvicích)
- 1993 – Marc Andreessen vyvíjí Mosaic, první WWW prohlížeč, a dává ho zdarma k dispozici
- 1994 – vyvinut prohlížeč Netscape Navigator
- 1994 – Internet se komercionalizuje
- 1996 – 55 milionů uživatelů
- 1998 – v České republice probíhá první ročník kampaně Březen – měsíc Internetu (konané až do roku 2008)
- 1999 – rozšiřuje se Napster
- 2000 – 250 milionů uživatelů
- 2003 – 600 milionů uživatelů
- 2005 – 900 milionů uživatelů
- 2009 – 1,8 miliardy uživatelů
- 2010 – ve Finsku jako první zemi na světě mají lidé podle zákona nárok na Internet
- 2010 - přes 2 miliardy uživatelů
- 2011 - došlo k vyčerpání adres protokolu IPv4

Některé aspekty Internetu

- Internet byl navržen s odolností vůči útokům zvenčí
- Návrh neobsahuje principy pro trasování uživatelů
- Nemá mechanismy rezistence proti nedůvěryhodným uživatelům
- Pokrývá globální prostor – různé jurisdikce
- Obrovská míra heterogenity
    - **Bezpečnost je na připojeném systém**

Trendy v oblasti útoků



https://resources.sei.cmu.edu/asset_files/SpecialReport/2002_003_001_13928.pdf

Informační systémy nad internetem

- Provoz distribuovaných systémů:
  - Systémy ve více lokalitách s požadavkem sdílení dat
    - Systémy veřejné správy – registr vozidel, registr obyvatel…
    - Systémy soukromých společností – více poboček
  - Možná řešení:
    - Vlastní telco infrastruktura
    - Pronajatá – vyhrazená – telco infrastruktura
    - Provoz nad Internetem – nejlevnější řešení

Informační systémy nad internetem

- Provoz distribuovaných systémů nad internetem
  - Hlavní výhody:
    - Nízká cena
    - Dostupnost připojení – rozšíření Internetu
  - Problémy k řešení:
    - Řízení kapacity přenosu – QoS
      - Kapacita linek je omezená – opět kapacita je dána kritickým místem
      - Kapacita internetu se sdílí
      - Komunikuje více služeb najednou
      - Různé požadavky na přenos – hlas, data, video
    - Bezpečnost při sdílené komunikaci – přenos nepřátelským prostředím
    - Kdo komunikace sleduje?

Informační systémy nad internetem

- **Problémy k řešení:**
  - Podvržení identity – autentizace a autorizace
  - Odposlech dat – šifrování přenosu
  - Změna – podvržení – dat – šifrování přenosu, kontrolní mechanismy, podepisování zpráv
  - Zneužití meta dat
  - Dostupnost služby – redundantní spoje, záložní systémy
  - Fyzická bezpečnost – různé lokality, fyzická přítomnost správce
  - Zadní vrátka v systémech – mobily
  - Převažující black box systémy

Informační systémy nad internetem

- Klientské systémy
  - K informačnímu systému přistupuje klient:
    - Vlastní uživatel – lze vynutit pravidla hry
    - Cizí oprávněný uživatel – vynucení pravidel hry je obtížnější Anonymní uživatel
  - Bezpečnostní problémy – mimo již uvedené:
    - Identita uživatele – autentizace, autorizace
    - Bezpečnost přistupujícího zařízení – různé bezpečnostní úrovně
    - Přenos dat
  - Příklady:
    - Bankovní systémy
    - Mailové služby
    - Přístupy do podnikových sítí

Informační systémy nad internetem

Novinky.cz

Hledat...

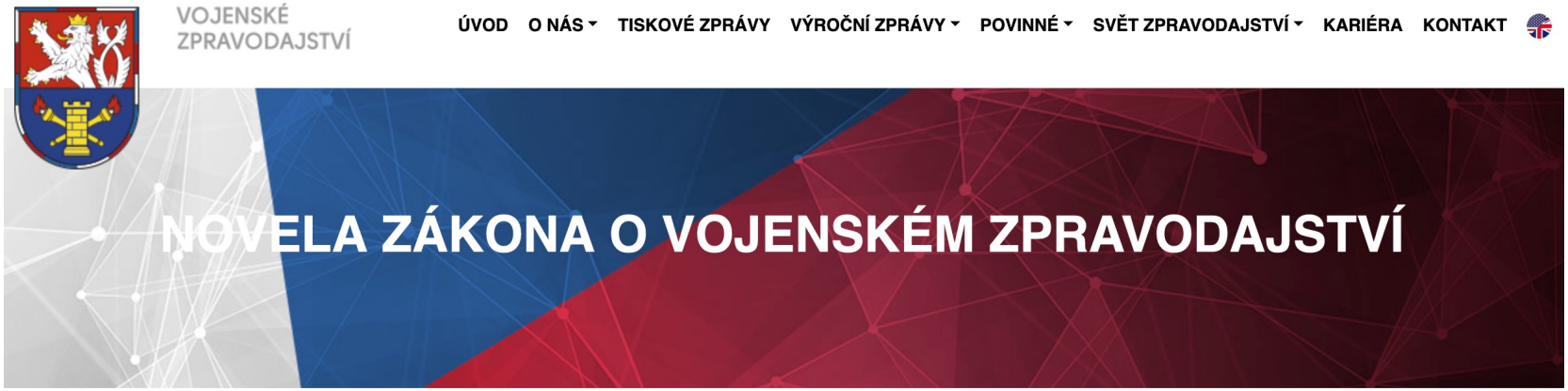
FormBook útočí stále častěji. Je to největší hrozba v Česku, varovali experti

Dnes 12:39 – Ondřej Husák, Novinky

Ještě na začátku letních prázdnin se nedostal ani do první trojky, aktuálně je však virus FormBook vůbec tou nejrozšířenější hrozbou v České republice. Před masivním nárůstem počtu útoků tohoto nezvaného návštěvníka varovali experti z kyberbezpečnostní společnosti Check Point.

https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/formbook-utoci-stale-casteji-je-to-nejvetsi-hrozba-v-cesku-varovali-experti-40373379#dop_ab_variant=0&dop_source_zone_name=novinky.sznhp.box&dop_req_id=oDVAriXuUgq-202109291220&dop_id=40373379&source=hp&seq_no=1&utm_campaign=&utm_medium=z-boxiku&utm

Informační systémy nad internetem



Dnem 1. července 2021 nabývá účinnosti novela zákona o Vojenském zpravodajství, která se zabývá kybernetickou obranou. Zákon vychází z požadavků strategie vytvořené Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) a schválené vládou. Nutnost vychází i ze členství v Severoatlantické alianci (NATO), která uznala kybernetický prostor v roce 2016 za operační doménu.

https://vzcr.cz/novela-zakona-o-vojenskem-zpravodajstvi-151

Informační systémy nad internetem

- Noční můry bezpečnostního managera:
  - Vlastní mobilní zařízení – BYOD (Bring Your Own Device)
    - Jak vynutit bezpečnost na cizím zařízení
  - Snadné zcizení mobilního zařízení
    - Kritická doba mezi ztrátou zařízení a nahlášením
    - Ochrana IS – sílou autentizace uživatele
  - Uživatelská nekázeň
    - Instalace SW (black box)
    - Půjčování zařízení
    - Nedodržování pravidel hry
  - Technologická rozmanitost
    - Vysoké nároky na znalosti
    - Vysoké nároky na technická řešení bezpečnosti

Procesní pohled na ICT

- ICT je chápáno jako množina procesů, kterými je zajištěno zpracování informací
- Příklady ICT procesů:
  - Vstupy dat – automatizované, ruční
  - Správa počítačové sítě
  - Správa uživatelských stanic
  - Správa serverů
  - Řízení ICT
  - Podpůrné procesy – nákup, ekonomika, kontrola
- Procesní pohled dnes v ICT světě převažuje
- Velice často ICT procesy neobsahují bezpečnostní aspekty – ona otřepaná hesla v obálkách

Procesní pohled na ICT – některé bezpečnostní procesy (bez úplnosti)

- Risk management – jak identifikovat a zvládat rizika
- Business continuity – jak co nejefektivněji zvládnou výpadek
  - Zálohovací schémata
  - Havarijní plány
  - Plány obnovy
- Incident management – jak efektivně identifikovat a zvládnou incident
- Řízení zastupitelnosti
  - Zastupitelnost klíčových rolí
- Identity management
  - Uživatelé a řízení jejich přístupových oprávnění
  - Procesy zavedení nového, změna, ukončení prac. Poměru
- Release management
- Change management

Procesní pohled na ICT

- ICT procesy – měly by být popsány
- Role v ICT procesech:
  - ICT manager
  - ICT administrátor
  - Správce sítě
  - Uživatelská podpora – helpdesk
  - ICT architekt
  - Bezpečnostní manager
  - Bezpečnostní administrátor
  - Auditor
  - Zákazník ICT služeb
- Organizační struktura je optimalizována pro procesní řízení
- Podceňované hrozby – socioútoky, útoky „na role“
- ***Které role lze sdílet jednou osobou? Diskuse***

Procesní pohled na ICT – personální bezpečnost

- Zaměstnanec v ICT či bezpečnostní roli
  - Vysoká míra rizika
  - Omezená možnost kontroly
  - Kreativita v obcházení pravidel
  - Zaměstnanec po výpovědi
  - Rodinní příslušníci

Procesní pohled na ICT – personální bezpečnost

- **Cíl – zdroj incidentu musí být identifikovatelný**
- Nástroje
  - Zbavení anonymity
  - Vědomí o hodnotách – přijetí zodpovědnosti
  - Školení a vzdělávání
  - Definice pravidel hry:
    - Politiky a směrnice
    - Etické kodexy
    - Smlouvy a závazky mlčenlivosti
  - Firemní kultura a prostředí
  - Sociotechniky
  - Důsledná kontrola
    - Audit
    - Penetrační testy

Procesní pohled na ICT – personální bezpečnost

- Úmyslné incidenty
- Rizikové faktory:
  - Výpověď
    - Podcenění výpovědi ne manažerských pozic
    - Podcenění procesního a technického řešení
    - Trénink manažerů, jak se rozejít
  - Pocit křivdy – nespravedlnost, nedodržení podmínek, demotivace
  - Vážná rodinná situace
  - Charakter zaměstnance - chamtivost

Pohled na ICT – po vrstvách

- Infrastruktura
  - Vše, co je potřeba k provozu aplikací
- Aplikační vrstva
  - Aplikační software, ERP systémy…
- Vrstva služeb
  - Správa a vše okolo

Infrastruktura

- Fyzická vrstva:
  - Datové spoje
  - Hardware

- Software infrastruktury:
  - SW spojený s HW – ovladače, speciální komunikační software, protokoly
  - Operační systémy
  - Databázové systémy
  - Komunikační software
  - Bezpečnostní software

Infrastruktura

- Výpočetní technika:
  - Servery
  - Síťové systémy
  - Pracovní stanice
  - Mobily, PDA, tablety
  - Automatizované čtečky
  - Multifunkční tiskové sestavy
  - …

Infrastruktura

- Bezpečnostní problémy:
  - **Důvěrnost** – autentizace, autorizace, nakládání s vadnými díly, otevřené přístupy, infrastrukturní software - zabezpečení
  - **Dostupnost** – business continuity – zálohování a obnova funkcí, odezvy, přístupy, servisní smlouvy
  - **Integrita** – nedochází ke změnám uložených dat? Jsou kompletní?

- Problém dneška – heterogenní prostředí, mobily, tablety…

- **Kde je optimum mezi uživatelským komfortem a náklady na bezpečnost**

Infrastrukturní software

- Firmware
- Síťové a komunikační protokoly
- Operační systémy
- Databázové stroje
- Specializované servery – http servery, autentizační servery…
- Bezpečnostní software – identity management, firewally, SIEM atd.

Infrastrukturní software

- Stálý spor:
  - Black Box x Crystal Box
- Black Box:
  - Software (ale i hardware) obvykle na komerční bázi, není k dispozici úplná dokumentace, zdrojové kódy
  - Microsoft, Apple, Oracle, CheckPoint, McAfee, Symantec …
  - Přemýšlejte: výhody x nevýhody, kdy je vhodné nasadit
- Crystal Box:
  - Většinou Open Source, je k dispozici zdrojový kód a dokumentace
  - Přemýšlejte: výhody x nevýhody, kdy je vhodné nasadit

  - Publikace Back Doors – co je ještě důvěryhodné?

Bezpečnostní praxe

- Jde o nejčastější cíle technických útoků – **proč??**
- Mnoho publikovaných chyb
- Podcenění správy a podpory
- Podcenění bezpečnostních aspektů
- Incident:
  - Nedostupný správce
  - Nedostupná nebo nesjednaná podpora
  - Zanedbaná údržba
  - EXIT podmínky smluv
  - Vendor lock

- Ne vždy to nejlepší a nejdražší řešení je optimální

Infrastrukturní incidenty

After joining my personal WiFi with the SSID "%p%s%s%s%s%n", my iPhone permanently disabled it's WiFi functionality. Neither rebooting nor changing SSID fixes it :~)
pic.twitter.com/2eue90JFu3

— Carl Schou (@vm_call) June 18, 2021

https://thehackernews.com/2021/06/beware-connecting-to-this-wireless.html

Cloud – jeho principy a rizika

- **Stará myšlenka nově marketingově uchopená**
  - Jak mámit z uživatelů více peněz ☺
  - Obecně nelze cloud ani zatratit ani nekriticky doporučit
  - Racionální úvaha
- Princip:
  - Sdílení zdrojů je levnější
  - Platím jen to, co opravdu potřebuji
- Obsah cloudu:
  - Uložiště dat
  - Synchronizace, sdílení dat
  - Poskytování aplikací
  - Zajištění provozu – SLA

Cloud – jeho principy a rizika

- Bezpečnostní rizika:
  - Data nejsou pod kontrolou – i „triviální operace“ (výmaz dat…)
  - Jurisdikce, kde jsou data uložena
  - Bezpečnostní řetězec - kdo má k datům přístup – poskytovatel, telco služby
  - Důvěryhodnost a stabilita poskytovatele
- Bezpečnostní výhody:
  - SLA
  - Zajištění drahých bezpečnostních služeb (zálohování, incident management)
  - Sdílení drahých technologií (uživatel by si je sám nikdy nekoupil)

Cloud – jeho principy a rizika

- Bezpečnostní shrnutí:
  - Cloud je nástroj
  - Obecně jej nelze ani doporučit, ani odmítnout, záleží na konkrétních podmínkách
  - Vlastní IT infrastruktura může představovat větší riziko než cloud a naopak
  - Vždy je třeba při úvahách zapojit zdravý rozum
  - Bezpečnost cloudu není jen problematika šifrování
  - Šifrování je ale podstatné

Cloud – jeho principy a rizika

- Pokud uvažuji cloud – co bych měl řešit:
- **Kupuji si co – ne jak**
  - Obsah služby
    - **Výkon – ne konfiguraci**
  - Rozsah služby – jak bude měřena účtována
  - SLA
    - Dostupnost
    - Business continuity
  - Bezpečnostní otázky
    - Split dat, šifrování dat
    - Identity management
    - Management dat, výmaz dat
    - EXIT služby

Jak se lze k datům na cloudu neoprávněně dostat

- Poskytovatel služby:
  - Má obvykle neomezený přístup datům
  - Má přístup ke klíčům? – Pozor na klientské aplikace

- Odposlech komunikace, telco záznamy – řeší šifrovaný přenos, přenáší se klíče?
- Přístup ke klientské stanici
  - Speciální sw – pozor, co si instalujeme
  - Fyzický přístup – export klíče
- Krádež identity uživatele
- Rizikové chování uživatele

Aplikační vrstva

- Zjednodušeně – software, který pracuje nad infrastrukturou, využívá ji a zpracovává data – interpretuje na informace
- Členění je různé:
  - Podnikové systémy – ERP, CRM, APS, MES, Document Management, Workflow Management…
  - Kancelářské systémy – Office, mail…
- Bezpečnostní problémy:
  - **Důvěrnost** – přístupy, způsob uložení dat, přístupy podpory, logy
  - **Dostupnost** – SLA, business continuity
  - **Integrita** – jsou data korektní, zpracovávají se popsaným způsobem? Je aplikační logika dokumentována a testována?

Opomíjené problémy aplikací

- Licenční čistota, podmínky rozšíření licencí
- Vendor Lock
- Podmínky podpory – SLA, obsah, podmínky, řešení incidentů
- Práce s datovými médii
- Know how – dostupnost implementačních konzultantů
- Vzdálené přístupy – neexistence NDA
- Stabilita dodavatele
- Struktura dat
- Aplikační logika
- Archivace dat
- Formát dat
- Odezva a rychlost

Užívání informačního systému

- Nastavená pravidla hry – bezpečnostní politika, provozní směrnice, popis procesů
- Absence kontroly
- Nevyvozování důsledků

- „***Nejhorší bezpečnostní problém je mezi židlí a klávesnicí*** ☺“

Forma realizace některých služeb

- **Insourcing** – realizace vlastními zaměstnanci

- **Outsourcing** – realizace najatými subjekty
  - Výběr dodavatele
  - Ustavení vztahu
  - Provoz, hodnocení
  - Změny vztahu
  - Ukončení vztahu
- Kombinace obou
- Ad hoc
- Přemýšlejte – výhody, nevýhody, bezpečnostní aspekty

Standardy a best practices

– Proč:

- Využití v zákonné úpravě
- Oborové standardy
- Dobré vodítko pro praxi

Standardy a best practices

- Řízení x management
- Procesní pohled (PDCA)
- ISMS
  - Přehled součástí systému managementu bezpečnosti informací
  - Role v oblasti ISMS
  - Risk management
  - Plán kontinuity obchodních činností

Řízení nebo management?

- Systém řízení
  - Ekonomické řízení
  - Procesní řízení
  - Projekt management

- Systém managementu – management ve smyslu „zvládání“
  - Risk management
  - Oblast personální, HR
  - Systém managementu bezpečnosti (objektová, personální, požární, …)
  - ITIL (IT service management, ISO 20000)
  - ISMS (ISO 27000), včetně analýzy rizik

ITSM / ITIL / ISO 20000

- **Procesy určují požadavky na IT služby, které pak slouží k zajištění chodu procesů**
- **Podniková strategie určuje podobu procesů**
- **ITSM** (IT Service Management) = řízení služeb informačních technologií
  - Definice a popis služby poskytovaných ICT
  - Pravidla pro užívání služeb
  - Řízení služeb na operativní, taktické a strategické úrovni
- **ITIL** (Information Technology Infrastructure Library)
  - Soubor prověřených postupů, které umožňují plánovat, využívat a zkvalitňovat využití ICT
  - Metodika založená na procesním řízení
- **ISO 20000**
  - Mezinárodní norma definující požadavky a řízení služeb IT
  - Část 1 – specifikace, část 2 – soubor postupů

ITIL - Information Technology Infrastructure Library

- **Seznam částí ITIL:**
  - Podnikatelský pohled (Business Perspectives)
  - Správa aplikací IT (Application Management)
  - Dodávka IT služeb (IT Services Delivery) => ITSM
  - Podpora IT služeb (IT Services Support) => Správa IT infrastruktury (IT Infrastructure Management)
  - Řízení IT projektů (IT Project Management)

ITIL - Information Technology Infrastructure Library

- **ITIL obsahuje 26 procesů**, z nichž klíčové jsou následující:
  - Incident management
  - Event management
  - Request fulfilment
  - Access management
  - Problem management
  - Service asset and configuration management
  - Change management
  - Release and deployment management
  - IT service continuity management
  - Capacity management
  - Availability management
  - Service level management
  - Service catalogue management
  - Financial management for IT services

ITIL - Information Technology Infrastructure Library

- **Service Desk** - účelem je poskytnout u jedno místo pro adresování požadavků
- **Configuration Management** - proces, jehož výstupem je model infrastruktury pomocí identifikace, řízení, správy a verifikace všech konfiguračních položek
- **Incident management** - proces pro co nejrychlejší obnovení služby a minimalizaci důsledků výpadků
- **Problem Management** - proces zjišťování příčin incidentů
- **Change Management** - proces efektivního a rychlého řízení změn
- **Release Management** - proces zajišťující distribuci a nasazení změny do ICT architektury

ITIL - Information Technology Infrastructure Library

- **Service Level Management** - plánování, koordinace, návrh, uzavírání a vyhodnocování smluv o poskytování servisní podpory (SLA)
- **Capacity Management** - zajištění trvale dostatečné kapacity infrastruktury
- **Availability Management** - dosažení stanovené úrovně dostupnosti IT služeb
- **IT Service Continuity Management** - řízení schopnosti poskytování definované úrovně služeb při výpadku
- **Financial Management for IT Services** – evidence a řízení nákladů na IT služby

ISO 20000

- **Mezinárodní norma definující požadavky a řízení služeb IT. (část 1 – Specifikace, část 2 – Soubor postupů). Norma definuje celkem 19 procesů, z nichž se skládá systém řízení služeb:**
  - 1. Ustanovení systému řízení služeb a jeho zlepšování
  - 2. Řízení dokumentace
  - 3. Řízení zdrojů
  - 4. Plánování nových nebo změněných služeb
  - 5. Návrh a vývoj nových nebo změněných služeb
  - 6. Přechod na novou nebo změněnou službu
  - 7. Management incidentů
  - 8. Management problémů
  - 9. Management konfigurací
  - 10. Management změn
  - 11. Proces uvolnění
  - 12. Management kontinuity a dostupnosti služeb
  - 13. Management kapacit
  - 14. Management úrovně služeb
  - 15. Rozpočtování a účtování pro IT služby
  - 16. Management bezpečnosti informací
  - 17. Management vztahů s byznysem
  - 18. Management vztahů s dodavateli
  - 19. Výkazy o službách

ISMS – Information Security Management System

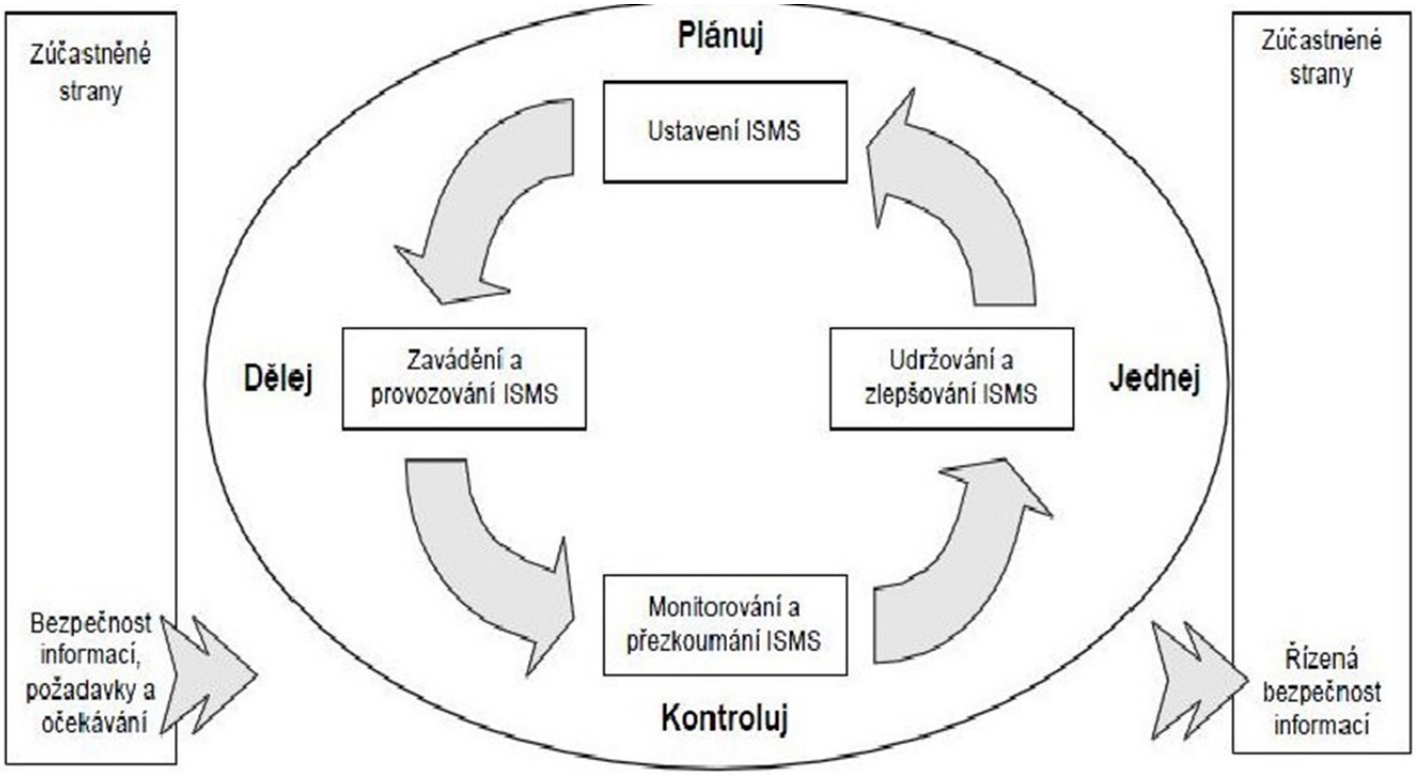
- Důvody pro ISMS
  - ISMS - Systém managementu bezpečnosti informací
  - Management bezpečnosti informací – zvládání, spíše než řízení
- ISMS:
  - Je soustava organizačních a technických opatření k eliminaci rizik
  - Rizika spojená se zachováním důvěrnosti, integrity a dostupnosti informací
  - Pokrytí hrozeb s vyšší mírou rizika vhodnými protiopatřeními

- ISMS nemusí být cílem certifikovat, je ale dobrým východiskem, jak informační bezpečnost řídit (management) systematicky a efektivně

Cyklus PDCA

- Kolbův cyklus učení (zkušenost-reflexe-pojem-experimentální ověření)
- W. Edwards Deming, Walter A. Shewhart
  - Demingův (Hemmingsův) PDCA model
- Jednoduchá metoda zlepšování s univerzálním použitím
  - **P(lan), D(o), C(heck), A(ct)**
  - Plánovat, realizovat, přezkoumat, reagovat
  - Total (*nejen*) Quality Management

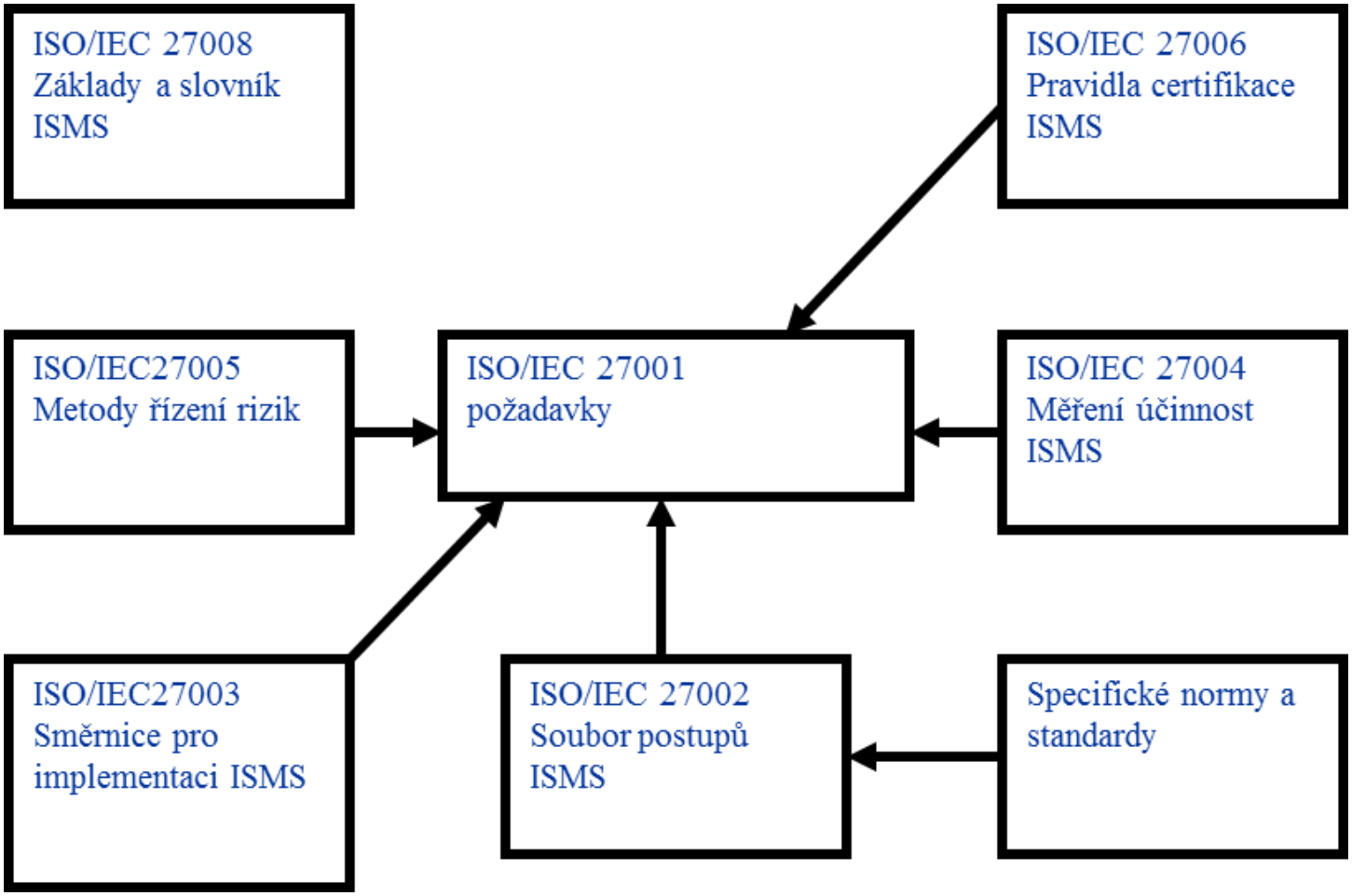
PDCA ve vztahu k ISMS



PDCA v ISMS

- Plánuj (ustavení ISMS)
  - Ustavení politiky ISMS, cílů, procesů
  - Ustavení managementu rizik
  - Ustavení navazujících částí – BCP, IcM, CHM
- Dělej (zavádění a provozování ISMS)
  - Zavedení a využívání politiky ISMS, opatření, procesů a postupů.
- Kontroluj (monitorování a přezkoumání ISMS)
  - Měření výkonu vůči politice ISMS, cílům
- Jednej (udržování a zlepšování ISMS)
  - Přijetí opatření k nápravě a preventivních opatření

Standardy pro ISMS



Standardy

- 27000 – definice pojmů a terminologický slovník (ČSN 2010, ISO/IEC 2012)
- 27001 - Systém řízení bezpečnosti informací (ISMS) (ČSN 2006, ISO/IEC 2013)
- 27002 – Soubor postupů pro řízení bezpečnosti informací (ČSN 2006, ISO/IEC 2013)
- 27003 - Směrnice pro implementaci systému řízení bezpečnosti informací (ČSN 2011, ISO/IEC 2013)
- 27004 - Řízení bezpečnosti informací – Měření (ČSN 2011, ISO/IEC 2009)
- 27005 - Řízení rizik bezpečnosti informací (ČSN 2013, ISO/IEC 2008)
- 27006 - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací (ČSN 2013, ISO/IEC 2007)
- 27007 – Směrnice pro audit systémů řízení bezpečnosti informací (ČSN 2013, ISO/IEC 2011)

Struktura ISMS – založená na PDCA

- Ustavení ISMS
- Zavádění a provozování ISMS
- Monitorování a přezkoumávání ISMS
- Udržování a zlepšování ISMS

Ustavení a řízení ISMS

- Určení rozsahu a hranice ISMS (scope)
- Definice politiky ISMS
- Stanovení přístupu k hodnocení rizik:
  - Identifikace rizik
  - Analýza a hodnocení rizik
  - Identifikace a hodnocení variant pro zvládání rizik
  - Výběr cílů a opatření pro zvládání rizik
  - Získání souhlasu vedení s navrhovanými zbytkovými riziky
- Získání povolení ze strany vedení k zavedení a provozu ISMS
- Prohlášení o aplikovatelnosti

Zavádění a provozování ISMS

- Formulace plánu zvládání rizik
- Zavedení plánu zvládání rizik v život
- Zavedení vybraných bezpečnostní opatření
- Určení způsobu měření účinnosti vybraných opatření
- Programy školení a programy zvyšování informovanosti
- Řízení provozu ISMS
- Řízení zdrojů ISMS
- Zavedení postupů pro rychlou detekci a reakci na bezpečnostní incidenty

Monitorování a přezkoumání ISMS

- Kontinuální monitorování
- Pravidelné přezkoumání účinnosti ISMS
- Měření účinnosti zavedených opatření
- V plánovaných intervalech hodnocení rizik a přezkoumání zbytkových rizika a úroveň akceptovatelného rizika

Udržování a zlepšování ISMS

- Zavádění identifikovaných zlepšení ISMS
- Nápravné a preventivní činnosti
- Návrhy na zlepšení na požadované úrovni detailu se všemi zainteresovanými stranami
- Analýza zlepšení – musí vést k předpokládaným cílům

Struktura ISMS – povinná dokumentace

- Rozsah a hranice ISMS
- Politika ISMS
- Definice a popis přístupu k hodnocení rizik
- Identifikace rizik
- Analýza a vyhodnocení rizik
- Identifikace a varianty pro zvládání rizik
- Cíle opatření a bezpečnostní opatření pro zvládání rizik (viz příloha A)
- Akceptace rizik
- Získání povolení k provozování ISMS v rámci organizace
- Prohlášení o aplikovatelnosti

Struktura ISMS dokumentace

- Bezpečnostní strategie
- Bezpečnostní politika
- Metodické dokumenty
  - Metodika RM
- Akty interního řízení
  - Směrnice:
    - Pro uživatele
    - Pro řízení provozu
    - Pro řízení přístupu
    - Pro zálohování
    - …

Bezpečnostní strategie

- Základní dokument bezpečnosti celku
- Všechny oblasti bezpečnosti
- Cíle
- Strategie
- Význam bezpečnosti pro fungování celku
- Souhlas a podpora vedení
- Často součást statutu, podnikatelského záměru, strategického plánu apod.

Politika informační bezpečnosti

- **Základní dokument informační bezpečnosti:**
  - Cíle
  - Strategie
  - Organizační aspekty
    - Role
    - Management bezpečnosti
  - Procesy
    - Řízení rizik
    - Správa systémů a aplikací
    - Helpdesk
    - Vývoj a údržba aplikací
    - Řízení změn
  - Vztahy mezi politikami
  - Vydávání a revize politik

Risk management – analýza rizik

- AR odpovídá na otázky:
  - Co vlastním a jakou to má hodnotu?
  - Jak o tuto hodnotu mohu přijít?
- Aktiva:
  - Zjištění hodnoty aktiva
- Identifikace a hodnocení hrozeb
  - Zásahy vyšší moci
  - Organizační nedostatky
  - Technická selhání
  - Lidská selhání
  - Úmyslná škodlivá činnost
- Hodnocení míry zranitelnosti
- Účinnost ochranných opatření
- Hodnocení frekvence hrozeb
- Hodnocení účinnosti protiopatření

Bezpečnostní politika

- Technická a organizační bezpečnostní opatření, ISO/IEC 27002
  - Politika bezpečnosti
  - Organizace bezpečnosti informací
  - Personální zabezpečení
  - Řízení priorit
  - Řízení přístupu
  - Kryptografie
  - Fyzikální a environmentální bezpečnost
  - Bezpečnost provozu
  - Bezpečnost komunikace
  - Systém akvizicí, vývoj a údržba
  - Dodavatelské vztahy
  - Řízení incidentů informační bezpečnosti
  - Informačně bezpečnostní aspekty kontinuity podnikání
  - Shoda

Audit

- Zjištění shody požadovaného a skutečného stavu (*co je a co není audit*)
  - Obvykle dle ČSN ISO/IEC 27001
  - Interní audit
- Audit třetí stranou
- Audit akreditovaným certifikačním orgánem

- Technický audit
- Penetrační testování
- Socioinženýrství

Role v řízení informační bezpečnosti

- Manažer informační bezpečnosti
- Správce informační bezpečnosti
- Auditor – interní/externí
- Řídící výbor informační bezpečnosti
- Požadavky:
  - Separace rolí, zamezení koncentraci pravomocí bez možnosti kontroly
  - Výkonné role v oblasti funkčnosti x výkonné role ve správě bezpečnosti
  - Správce systému x správce bezpečnosti
  - Metodická role x auditor
  - Manažer bezpečnosti x auditor

Manažer informační bezpečnosti

- Organizační a metodické řízení informační bezpečnosti
- Příprava směrnic, politik a nástrojů k jejich prosazování
- Definuje pravidla pro informační bezpečnost společně s vlastníky procesů a informací
- Odpovědný za vytváření povědomí o bezpečnosti
- Poradce vedení v otázkách informační bezpečnosti
- **Neměl by být součástí oddělení IT, měl by mít přístup k vedení**

Správce informační bezpečnosti

- Provádí výkonné úkony v oblasti informační bezpečnosti
- Stanovuje správnou konfiguraci systémů z hlediska bezpečnosti
- Zpracovává a prosazuje směrnice
- Monitoruje činnost správců systémů
- Musí disponovat pravomocí pro bezprostřední zásah v případě incidentu
  - Odpojení uživatele od sítě, zastavení činnosti subsystému, přerušení konektivity, apod.

Auditor informační bezpečnosti

- Nezávislá osoba uvnitř nebo vně, která kontroluje stav informační bezpečnosti
- Auditor musí být nezávislý na administraci bezpečnosti.
- Interní audit
  - Interní zaměstnanec vyškolený v postupech provádění auditu, formálně nezávislý na výsledcích
- Externí audit
  - Vyšší míra nezávislosti a odbornosti
  - Menší znalost reálií a detailů

Risk management

- Důvody pro RM (ochrana aktiv, OOÚ, OT, přiměřenost personálních opatření, …)
- Ochrana osob a majetku může být funkční pouze tehdy, pokud jsou známy:
  - Hodnoty - aktiva
  - Hrozby - před čím je třeba chránit - analýza rizik,
  - Protiopatření – jak chránit
- Risk management – nejen v informační bezpečnosti
  - PO, BOZP, finanční rizika, personální rizika …
  - RM v oblasti finančních rizik, strategických rizik
  - RM: možnosti zobecnění
- Nástrojem RM je analýza rizik

Základní pojmy analýzy rizik

- Aktivum
- Hodnota
- Hrozba
- Zranitelnost
- Četnost
- Dopad hrozby
- Riziko
- Ochranné opatření
- Účinnost

Aktivum

- **Aktivum - všechno, co má hodnotu**
  - Informační aktivum – samotná informace
  - Hmotná aktiva
  - Nehmotná aktiva (např. programy, data, morálka pracovníků, pověst ...)
  - Systémy aktiv - spojují jak hmotné, tak nehmotné prvky – lidé, informační systémy

Komponenta

- Množina příbuzných aktiv dle vhodně zvoleného klíče
  - Dle funkční podobnosti
  - Dle Technologické podobnosti
- Informační systém je dekomponován nejdříve na komponenty, následně jsou v rámci komponenty identifikována aktiva
- Příklad:
  - Komponenta – HR informační systém
  - Aktivum – databáze zaměstnanců, HR manager, správce systému, server

Hodnota aktiva

- Základní charakteristikou aktiva
- Bez hodnoty nemá smysl ochrana
- Hodnota aktiva:
  - Objektivní vyjádření ceny
  - Subjektivním ocenění důležitosti (kritičnosti) aktiva
  - Kombinaci obou přístupů
  - Hodnota aktiva je relativní v závislosti na úhlu pohledu hodnocení
  - Hodnota by měla být vyjádřena cenou (výhoda pro hodnocená nákladů protiopatření)
  - *Jaká je hodnota aktiva – lidského života?*

Hrozba

- Hrozba - síla, událost nebo aktivita, která může způsobit škodu na aktivech
  - Hrozby - např. požár, přírodní katastrofa, krádež zařízení, získání přístupu k informacím neoprávněnou osobou, chyba obsluhy apod.
- Dopad hrozby - škoda, kterou způsobí hrozba při jednom působení na aktivum
  - Lze jej odvodit od ztrát, do kterých jsou zahrnuty náklady na znovuobnovení činnosti aktiva nebo
  - Náklady na odstranění následků škod způsobených hrozbou
- Základní charakteristikou hrozby je její úroveň

Zranitelnost

- Zranitelnost - nedostatek, slabina nebo stav aktiva, který využívá hrozba
  - Je vlastností aktiva
  - Vyjadřuje, jak citlivé je aktivum na působení dané hrozby
- Zranitelnost vznikne všude tam, kde dochází k interakci mezi hrozbou a aktivem
- Základní charakteristikou zranitelnosti je úroveň
  - Úroveň zranitelnosti aktiva se hodnotí podle citlivosti (náchylnost aktiva být poškozeno danou hrozbou) a kritičnosti (důležitost aktiva pro organizaci)

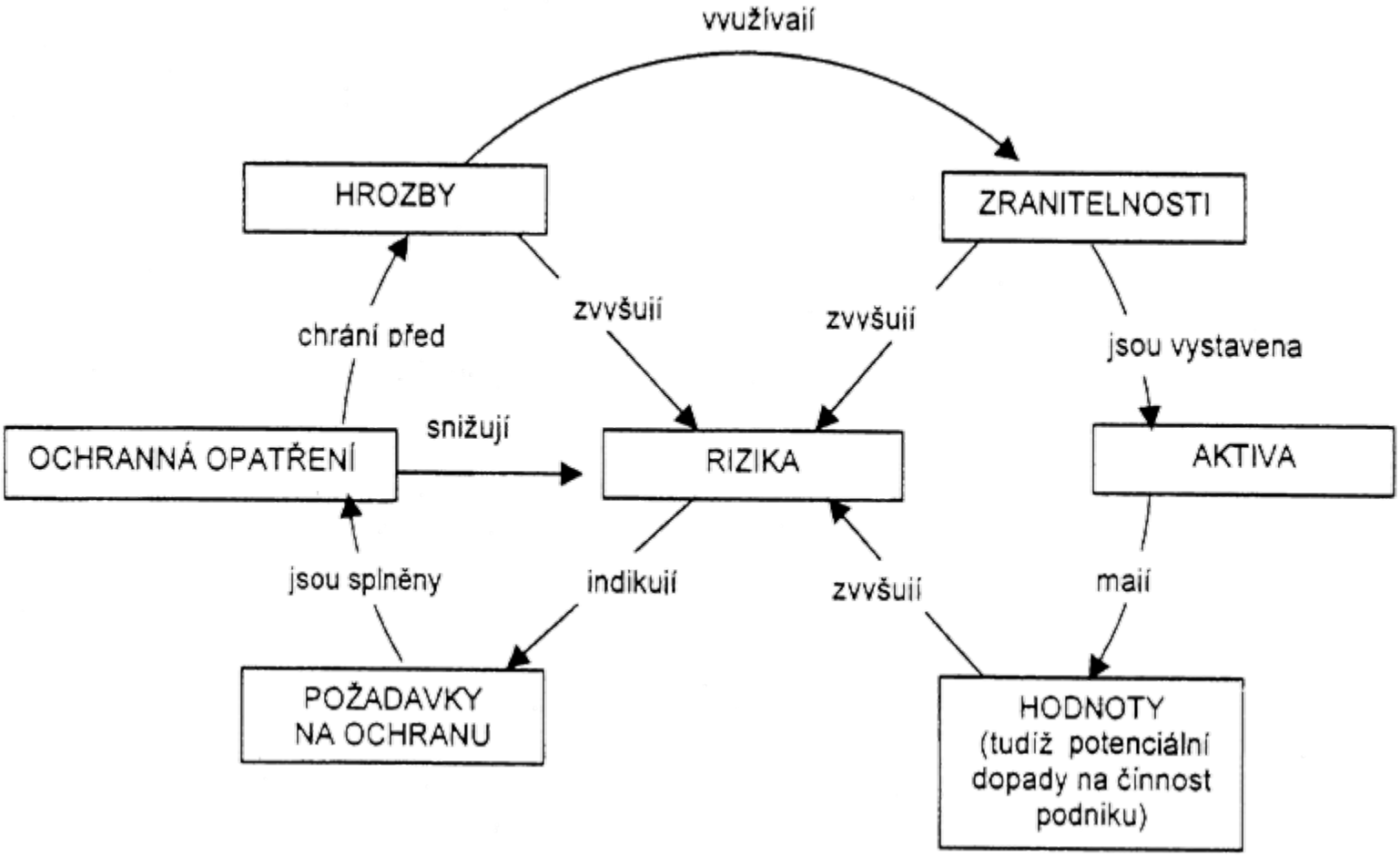
Riziko

- Riziko - míra ohrožení aktiva, míra nebezpečí, že se uplatní hrozba a dojde ke vzniku škody. Velikost rizika je vyjádřena jeho úrovní.
- Úroveň rizika je určena hodnotou aktiva, zranitelností aktiva a úrovní hrozby
  - Pouze protiopatření úroveň rizika snižuje
- Zbytkové riziko – malé riziko, že je pro systém přijatelné a není nutné podnikat další protiopatření k jeho snížení

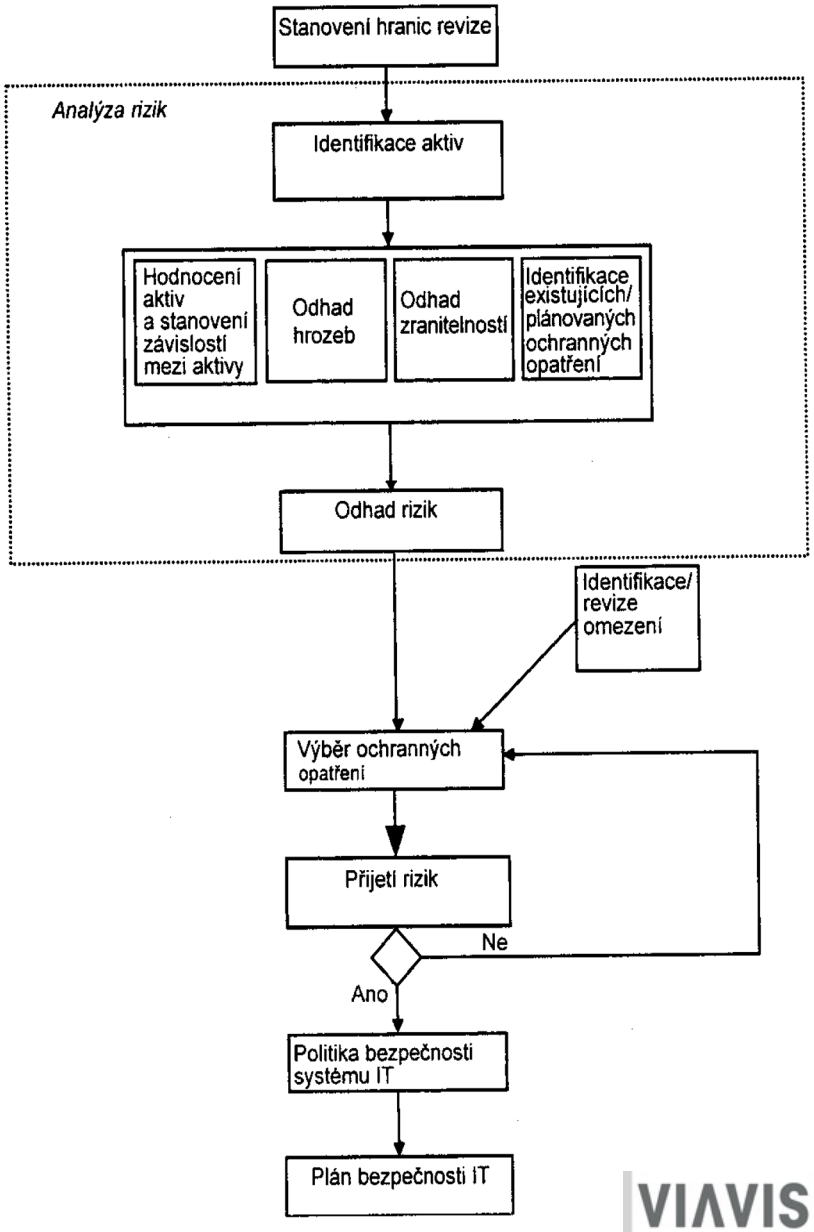
Protiopatření (ochranné opatření)

- Protiopatření - proces, procedura, technický či právní prostředek nebo cokoliv jiného vedoucí ke
  - Zmírnění působení hrozby
  - Eliminaci hrozby
  - Snížení zranitelnosti nebo dopadu hrozby
- Protiopatření se měří efektivitou a náklady
  - Efektivita - jak sníží účinek hrozby
  - Náklady – cena za protiopatření – v relaci s hodnotou aktiva
  - Výběr vhodného protiopatření spočívá v optimalizaci, kdy se hledají nejúčinnější protiopatření, jejichž realizace přinese co nejmenší náklady

Základní vztahy



Proces risk managementu



Volba strategie AR

- Analogie k přístupu k managementu informací
- Základní přístup
- Neformální přístup
- Podrobná formální analýza
- Kombinovaný přístup

Proces risk managementu

- Vstupy do procesu RM jsou především:
  - Inventura aktiv
  - Obecné definice politik a strategií
- Výstupy procesu RM jsou především:
  - Model IT/IS organizace - seznam komponent, seznam aktiv, relevantních hrozeb, jejich hodnocení, včetně identifikace protiopatření a hodnocení míry rizika.
  - Definice kritérií pro akceptaci rizik a variant pro zvládání rizik.

Proces risk managementu

- Model systému
  - Informační systém – obecně chápaný systém zpracování informací organizace od jejich vzniku až po likvidaci
    - Komponenta – ohraničená skupina elementů (aktiv) kde každý element musí:
      - Být pod tímtéž přímým řízením,
      - mít tutéž funkčnost nebo účel činnosti,
      - mít v podstatě tytéž funkční charakteristiky a bezpečnostní potřeby,
      - být umístěn v tomtéž obecném provozním prostředí.
    - Aktivum

Vlastník aktiva

− Osoba, která je odpovědná za aktivum v rámci procesu risk managementu. Vlastník musí být schopen posuzovat relevantně aktivum, nemusí být fyzickým či organizačním vlastníkem aktiva. Vlastník aktiva odpovídá zejména za:

- Ocenění aktiva
- Odhad hrozeb příslušných k danému aktivu
- Odhad frekvence hrozeb
- Odhad zranitelnosti aktiva
- Identifikaci stávajících protiopatření
- Odhad účinnosti protiopatření

Proces risk managementu

- I. krok RM (AR):
  - Hranice posuzování (scope)
    - Nelze provádět analýzu rizik v neomezeném rozsahu
    - Časový snímek – čím delší expozice, tím rozmazanější
    - Čím větší rozsah, tím nepřesnější výsledky
    - Čím menší rozsah , tím vrůstá riziko „bílých míst“ (neodhalených slabin)
  - Volba metody (strategie):
    - Neformální přístup
    - Vysoce formalizovaný přístup
    - Kombinovaný přístup
  - Metodika (CRAMM, RANIT…)

Proces risk managementu

- II. krok - Identifikace komponent
  - Model Informačního systému (**NE POUZE IT systému**)
  - Komponentám jsou přiřazeni jejich vlastníci
  - BIA – Business Impact Analysis - analýza dopadů incidentu
    - Jaká bude škoda, když dojde:
      - Prolomení důvěrnosti komponenty
      - Dostupnosti komponenty
      - Integrity komponenty
      - Vše s parametry (nedostupnost 1 hodinu, 4 hodiny, 24 hodin…)

Proces risk managementu

- III. krok RM (AR) – Identifikace a ocenění aktiv
  - Identifikace aktiv, jejich příslušnost ke komponentám a jejich vlastníků
  - Hodnota aktiv je stanovována v relativní stupnici nebo finančním rozsahu
- IV. krok RM (AR) – Odhad hrozeb
  - Hrozby jsou vybírány katalogu, který závisí na charakteru aktiva
  - Aktivum – data registru obyvatel x administrátor databáze
  - Katalog hrozeb je navržen v technických standardech ČSN ISO/IEC TR 13335.

Proces risk managementu

- V. krok RM (AR) – Odhad frekvence hrozeb
  - Jak často se hrozba může uplatnit
- VI. krok RM (AR) – Odhad zranitelnosti
  - Jak je aktivum vůči dané hrozbě citlivé?

Proces risk managementu

- VII. krok RM (AR) – Identifikace stávajících protiopatření
  - Jaká protiopatření jsou již implementována
  - Jak jsou účinná
  - Katalog protiopatření je navržen ve standardu ČSN ISO/IEC 27001.
  - Protiopatření jsou kontextově závislá na typu aktiva, jeho ceně a typu hrozby

Proces risk managementu

- VIII. krok RM (AR) – Hodnocení míry rizika
  - Míra rizika je stanovena pro jednotlivé hrozby
  - Hrubá míra rizika –bez zohlednění účinnosti protiopatření
  - Aktuální míra rizika –se zohledněním účinnosti stávajících protiopatření
  - Míra rizika modelovaná –se zohledněním účinnosti uvažovaných protiopatření
- IX. krok RM - Kritéria pro akceptaci rizik
  - Rozhodnutí o kritériích pro akceptaci rizik stanovuje svým rozhodnutím management
  - Hlediska – náklady, neexistující protiopatření, nízká míra rizika

Proces risk managementu

- X. krok RM – Varianty pro zvládání rizik
  - Aplikování vhodných opatření – technických, procesních, smluvních…
  - Vědomé a objektivní akceptování rizik
  - Vyhnutí se rizikům
  - Přenesení rizik na třetí strany, např. na pojišťovny, dodavatele

Řízení kontinuity činností

- Proč:
  - Významné incidenty (povodně, teroristické činy, black out…)
  - Běžné (nedostatek personálu, popření, poruchy, výpadky, incidenty…)
- Cíle:
  - Zabránit nežádoucímu přerušení činností
  - Chránit kritické procesy před následky závažných chyb, incidentů a katastrof
  - Rychlé, nenákladné a bezpečné zotavení systémů

Řízení kontinuity činností

- BCP zahrnuje
  - Management rizik – bez risk managementu nelze BPC ani navrhnout
  - BIA - analýzu dopadů, které přerušení činnosti může mít
  - Návrh strategie a plánu kontinuity činnosti
  - Realizace plánu
  - Pravidelného testování a aktualizace plánů a postupů (opět PDCA)

Řízení kontinuity činností

- Plánování kontinuity činností zahrnuje:
  - Určení všech rolí, odpovědností a nouzových postupů
  - Nastavení nouzových postupů tak, aby bylo možné zotavení v požadovaných lhůtách (*REPAIR TIME x RESPONSE TIME*)
  - Hodnocení a optimalizace vnějších závislostí (smlouvy…)
  - Dokumentace odsouhlasených procedur a postupů
  - Proškolení personálu
  - Testování a aktualizace plánů

Řízení kontinuity činností v praxi

- Podkladem je analýza rizik (risk management)
- Parametry pro havarijní plán
  - Efektivní doba nedostupnosti - doba nedostupnosti, která způsobí finanční ztrátu, ale její výše nedosahuje nákladů na protiopatření, které zajistí obnovení funkčnosti v efektivní době dostupnosti.
  - Kritická doba nedostupnosti - doba, nedostupnosti, ve které již vznikají zásadní ztráty přesahující náklady na efektivní protiopatření
- Definice pro smluvní parametry:
  - Repair Time
  - Response Time
  - Maximální ztráta dat
  - Dostupnost systému

Máte nějaké dotazy?

Děkuji za pozornost

Ing. Vladimír Lazecký