IBM IDC Brno

IS/IT outsourcing services

Ing. Milan Jedlička

ON DEMAND BUSINESS™

OBSAH

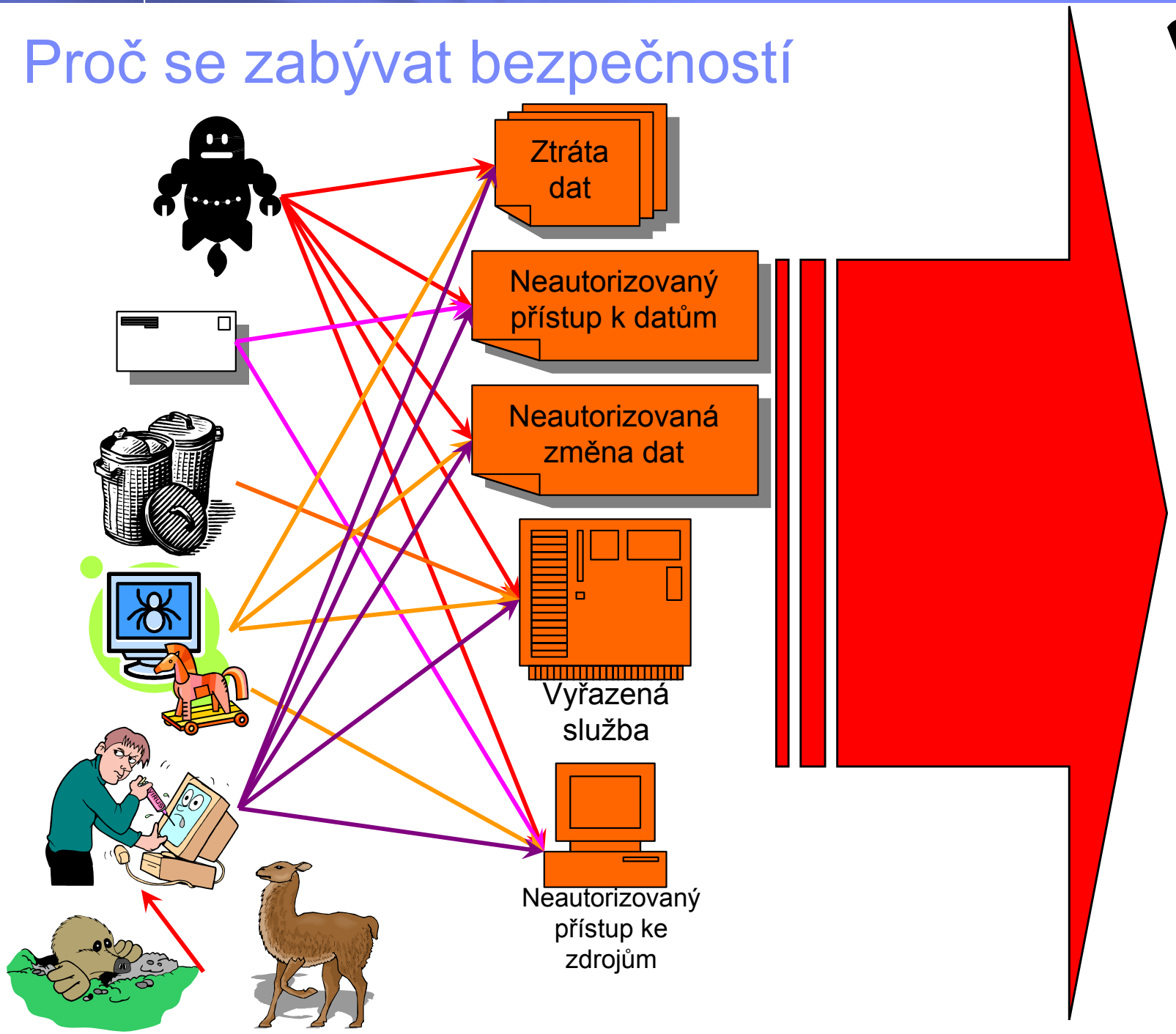
- **Úvod do problematiky**
- **Interní a zákaznické bezpečností standardy**
- **Interní procesy v rámci servisní organizace**

Motivace

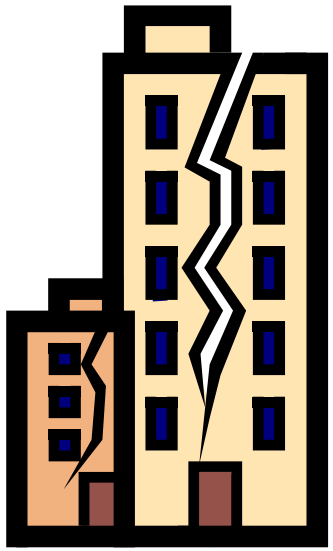
- § 257a - Poškození a zneužití záznamu na nosiči informací
- Kdo v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch získá přístup k nosiči informací a
  - takových informací neoprávněně užije,
  - informace zničí, poškodí nebo učiní neupotřebitelnými, nebo
  - učiní zásah do technického nebo programového vybavení počítače, bude potrestán **odnětím svobody až na jeden rok** nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci.

- **Odnětím svobody na šest měsíců až tři léta** bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo způsobí-li takovým činem značnou škodu nebo získá-li sobě nebo jinému značný prospěch.
- **Odnětím svobody na jeden rok až pět let** bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu nebo získá-li sobě nebo jinému prospěch velkého rozsahu.

Proč se zabývat bezpečností

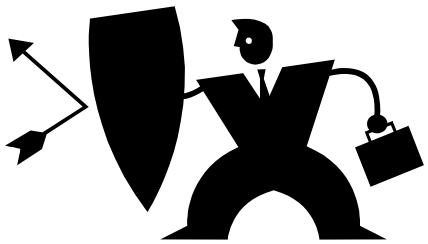


Proč se zabývat bezpečností



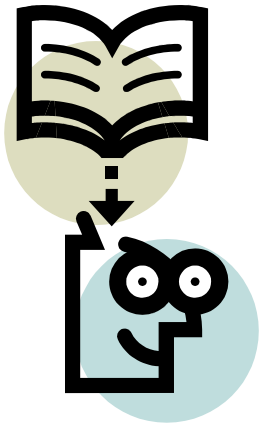
Jak se bránit

- **Vzděláním zodpovědných a zúčastněných**
- **Nastavením rolí a přístupových práv**
- **Vhodným programovým vybavením**
- **Pravidelnou aktualizací softwaru**
- **Dodržováním základních pravidel**
- **Pravidelnou kontrolou**
- **Aktivní kontrolou**
- **Fyzickým zabezpečením**
- **D/R procedura**

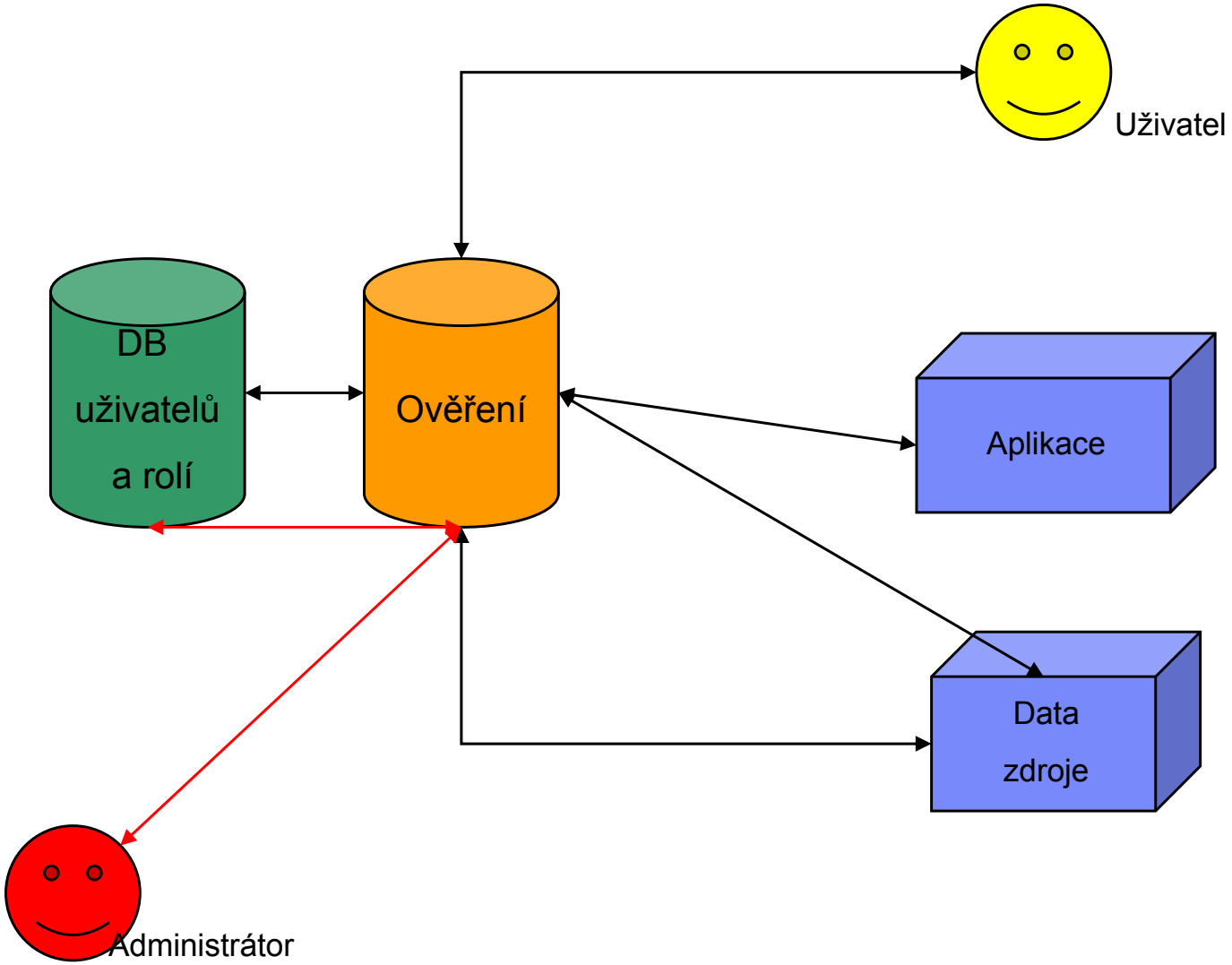


Vzděláním zodpovědných a zúčastněných

- **Vzdělání zodpovědných osob**
- **Vzdělání uživatelů**
- **Informování zákazníka**
- **Udržení vysoké úrovně znalostí**
- **Aktuální informace o stavu**
- **Varovaní před aktuálními hrozbami**

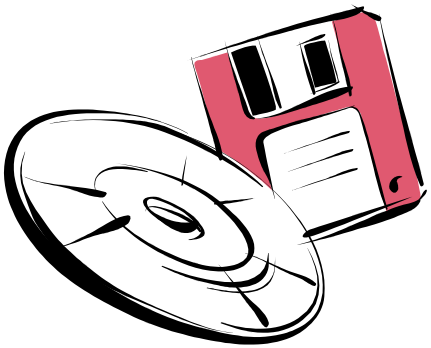


Nastavením rolí a přístupových práv



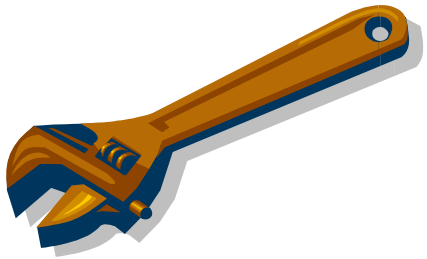
Vhodným programovým vybavením

- **Vhodně zvolený OS**
- **SW pro správu uživatelů a skupin**
- **Firewall**
- **Antivir**
- **Další sw dle potřeby (anti-spam, anti-spyware etc.)**
- **Produkční SW respektující zásady bezpečnosti**



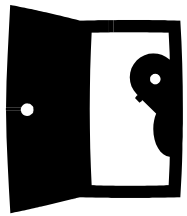
Pravidelnou aktualizací softwaru

- **Pravidelná aktualizace OS**
- **Pravidelná aktualizace SW**
- **Pravidelná aktualizace Antivirových DB**
- **Pravidelná údržba DB uživatelů a rolí**



Dodržováním základních pravidel

- **Jakékoliv zabezpečení je k ničemu, pokud se lidé uvnitř společnosti chovají nezodpovědně**
- **Volba hesel**
- **Osobní zodpovědnost**
- **Sociální inženýrství**



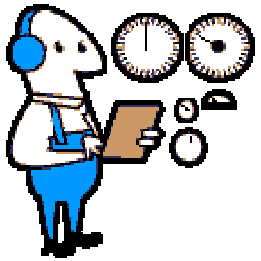
Pravidelnou kontrolou

- **Je nezbytné pravidelně kontrolovat stav**
  - Systému
  - DB uživatelů a rolí
  - Nastavení klíčových aplikací

- **Nalezené nedostatky je třeba urychleně odstraňovat**
- **Veškerá kontrola musí být řádně dokumentována**

Aktivní kontrolou

- **Monitoring provozu sítě**
- **Monitoring provozu systému**
- **Ethical hacking**



Fyzickým zabezpečením

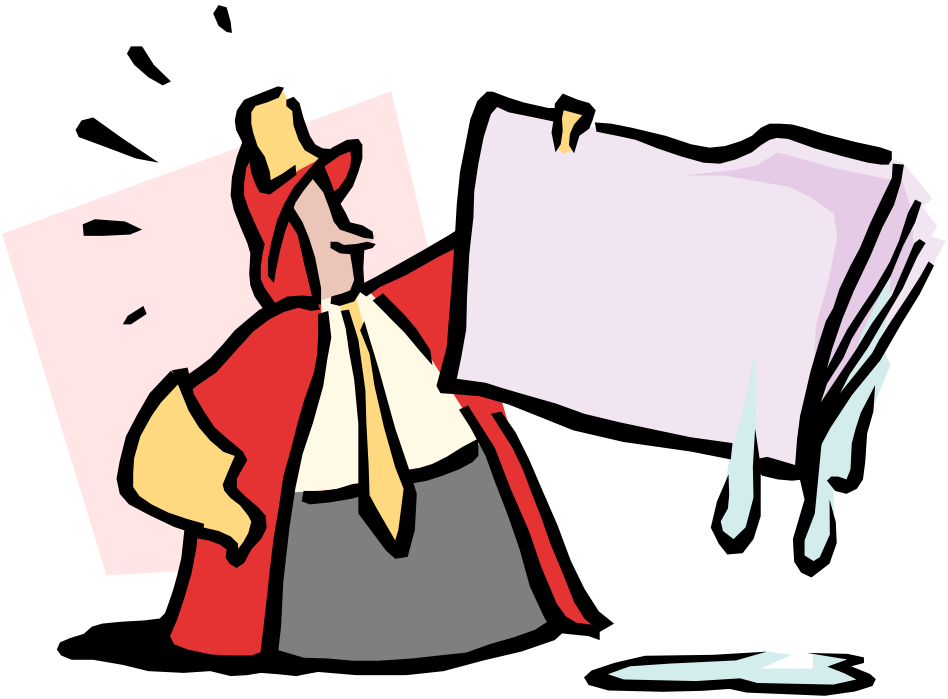
- **Možné hrozby**
  - Neautorizovaný přístup
  - Poškození
  - Krádež
  - Neúmyslné poškození
  - Poškození požárem či živelnou pohromou

Fyzickým zabezpečením

- **Umístění HW do místností s vyhrazeným přístupem**
- **Protipožární zabezpečení**
- **Záložní napájení**
- **Umístění záloh v jiné lokaci**
- **Minimalizovat pohyb cizích osob v budovách**
- **Použití elektronické zabezpečení, kamer, bezpečnostních agentur**

D/R procedura

- **Pravidelná záloha dat**
- **Bezpečné uložení dat**
- **Plán pro případ výpadku či poškození systému**



Interní a zákaznické bezpečností standardy

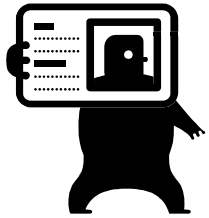
- **Příklady funkčních standardů:**
  - ITCS300 – Základní IT pravidla pro zaměstnance
  - ITCS104 – IT Bezpečnostní pravidla
  - CIO104 – IT Bezpečnost
  - LEG116 – Klasifikace a řízení IBM materiálů
  - ISO/IEC DTR 13335-1 Information technology

Interní a zákaznické bezpečností standardy

- **Identifikace**
- **Autentifikace**
- **Autorizace**
- **Ochrana a utajení informací**
- **Spolehlivost a dostupnost služeb**
- **Nastavení Auditu**
- **Kontrola**
- **Reportování a řízení bezpečnostní incidentů**
- **Správa fyzického přístupu**

Interní a zákaznické bezpečností standardy

- **Identifikace**
  - Jedinečný identifikátor pro každého uživatele
  - Digitální Certifikáty vytvořené a schválené CA



- **Skupina 1: Všechny více uživatelské vnitro firemní systémy, zařízení síťové infrastruktury podporující produkci a nebo služby mezi společností a jinými poskytovately služeb.**
- **Skupina 2: Všechny vnitro firemní aplikace a datová úložiště, která obsahují přístup k utajovaným informacím, přímo spouští klíčové procesy a nebo jsou objektem certifikace.**

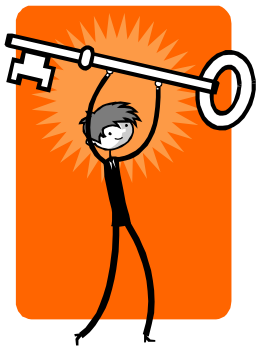
  Skupina 3: Ostatní více uživatelské vnitro firemní systémy, například takové, které poskytují podporu místním pobočkám či podporují vývoj.
- **Skupina 4: Presentace, výuka a testy systémů a připojených síťových prvků vyžadují-li to zvláštní okolnosti. Tyto systémy nemusí respektovat běžné standardy, pokud jsou jsou izolována a skryty za restriktivně nastavený firewall.**

Interní a zákaznické bezpečností standardy

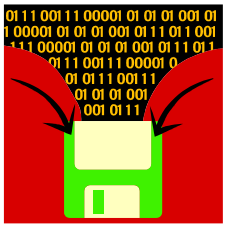
- **Autentifikace**
- **Uživatel-systém autentifikace**
  - Ověření identity uživatele
  - Hesla musí splňovat předepsaná pravidla
  - Vícekrát použitelná hesla musí být chráněna
  - Autentifikační Tokeny musí být chráněny
- **Systém-systém autentifikace**
  - Lze užít neexpirující hesla

Interní a zákaznické bezpečností standardy

- **Autorizace**
  - Přístup musí být autorizován vlastníkem aplikace s ohledem na skutečné potřeby přístupu, ale přístup k aplikaci mající přístup k vyhrazeným informacím musí být zvlášť schválen.
  - Přistupuje-li třetí osoba k vnitrofiremním službám musí být autorizována firemním managementem, souběžně se zajištěním pouze nezbytně nutných přístupových práv.
- **Vzdálený přístup pro zaměstnance**
  - Vzdálený přístup do firemní sítě musí být prováděn výhradně schváleným způsobem.
- **Varování**
  - Při přihlášení do vnitrofiremní sítě musí být zobrazeno varování a poučení.
- **Uživatelské zdroje**
  - Poskytovatel služby musí nastavit počáteční zabezpečení prostředků poskytnutých uživatelům.
  - Aplikace a datová úložiště umožňující uživatelům správu přístupových práv k vlastním zdrojům, musí obsahovat nástroj umožňující tuto správu vykonávat.

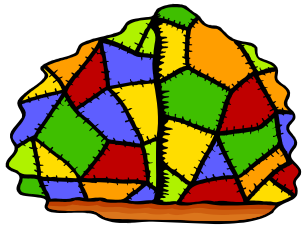


Interní a zákaznické bezpečností standardy



- **Ochrana a utajení informací**
- **Ochrana informací**
  - Je souborem technických a procedurálních opatření majících za účel zabránit neautorizovanému přístupu k chráněným firemním datům, k osobním informacím zaměstnanců, obchodních partnerů, zákazníků či návštěvníků webů.
  - Média obsahující sensitivní data musí bát řádně označena.
- **Zbytkové informace**
  - Je třeba zajistit nečitelnost zbytkových utajovaných či osobních dat způsobem vhodným pro dané médium.
- **Šifrování**
  - Firemní informace platné pro nepublikované technologie, obchodní plány, neveřejné finanční informace a osobní informace jako čísla kreditních karet, finanční či zdravotní záznamy, musí být zakryptovány, jsou-li posílány skrze internet.

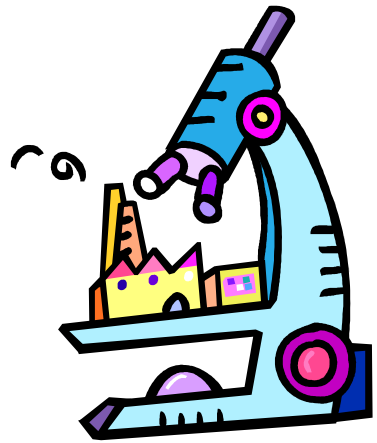
Interní a zákaznické bezpečností standardy



- **Spolehlivost a dostupnost služeb**
- **Správa systémových zdrojů**
  - Systémové zdroje musí být chráněny před běžnými uživateli..
  - Oprávnění běžného uživatele musí být založeny na jeho pracovních potřebách, kteroužto určí poskytovatel služby nebo vlastník aplikace.
- **Škodlivý kód**
  - Je nezbytné mít aktivní technické prostředky zabraňující šíření a spouštění škodlivého kódu.
  - Vývojáři aplikací musí poskytnout písemné ujištění, že provedli antivirový test jako součást závěrečných testů.
- **Monitorování slabin**
  - Dle typu sítě je třeba zvolit nástroje, pravidelnost a rozsah monitorování slabin TCP/IP.
- **Varovný systém bezpečnostních záplat**
  - Je třeba nastavit proces ke včasné instalaci záplat poskytnutých varovným systémem.
  - Je třeba upgradovat OS na podporovaný OS s ohledem na konec podpory pro danou versi OS. Tento upgrade lze odložit při prodloužené podpoře bezpečnostních záplat.
- **Modifikace softwaru**
  - Veškeré modifikace aplikačního softwaru musí být schváleno firemním managementem a instalace takového software musí projít schvalovacím procesem.
- **Dostupnost služeb**
  - Je nezbytné mít aktivní technické prostředky zabraňující útoku vyřazujícím službu (DoS atack)
  - Je nezbytné mít aktivní technické prostředky detakující a zabraňující neomezený počet neúspěšných pokusů o přihlášení se ke službě.
  - Je nezbytné mít proces pro detekci a zpracování systematického útoku.

Interní a zákaznické bezpečností standardy

- **Nastavení Auditu**
- **U systémů, aplikací, datových úložišť, síťových zařízení, kde je technický možné provést přihlášení je nutné pořídit záznam pro:**
  - Úspěšný a neúspěšný pokus o přihlášení
  - Modifikaci systémových prostředků (nelze aplikovat na aplikace a datová úložiště)
  - Pokus o čtení systémových zdrojů, které budou označeny jako výjimka. (nelze aplikovat na aplikace a datová úložiště)
  - Pokus spustit systémové zdroje, které budou označeny jako výjimka. (nelze aplikovat na aplikace a datová úložiště)
  - Veškeré aktivity provedené s authoritou security administratora.
  - Úspěšné priřazení a uvolnění IP adresy. (nelze aplikovat na aplikace a datová úložiště)
- **Pro vnitrofiremní služby je nutné pořídit záznam pro:**
  - Veškeré pokusy o vzdálený přístup do vnitrofiremní sítě.
  - Vnitrofiremní logy nesmí být uloženy na systémech určených pro poskytování služeb zákazníkům.
- **Záznamy auditu musí obsahovat datum, čas, typ a identifikaci uživatele**
- **Záznamy auditu musí být uschovány po 60 dní.**



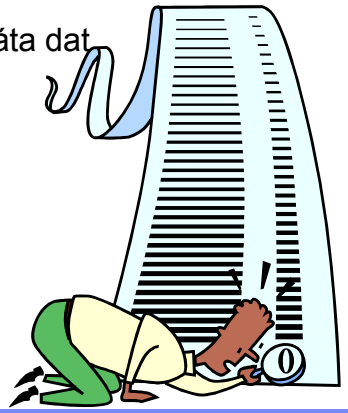
Interní a zákaznické bezpečností standardy

- **Test zdraví - Health checking**
  - Je nezbytné provádět test zdraví – health checking – v pravidelných intervalech.
- **Test technické části**
  - Test technické části je třeba provádět v pravidelných intervalech (například pro případ katastrof)
- **Ověření bezpečnostních postupů**
  - Bezpečnostní postupy musí být pravidelně ověřovány na reprezentativních vzorcích (z hlediska systémů a lokací)
- **Vnitropodniková atestace a certifikace**
  - Způsob a provedení testů a kontrol musí být změněno, kdykoliv je změněna služba.
  - Je nutné provádět roční recertifikaci pro veškeré vnitrofiremní služby.

Interní a zákaznické bezpečností standardy

- **Reportování a řízení bezpečnostní incidentů**
- **Je třeba kontaktovat zodpovědné osoby a informovat je o:**
  - Kontaktní osoby za vedení a za technickou oblast.
  - Popis problému, rozsah systémů či dat jež byly zasaženy incidentem, již provedené aktivity.
- **Je třeba okamžitě vytvořit záznam obsahující veškeré informace týkající se incidentu. Ke každé informaci je nutné uvést datum a čas. (Pro takový záznam je plně dostačující papírová forma)**
- **Technický support musí začít aktivity ke zmírnění následků, bez zbytečného zpoždění.**
- **Zodpovědné osoby poskytnou informace a instrukce jak postupovat.**

- **Je špatné:**
  - Provádět vyšetřování na vlastní pěst. Rizikem může být předčasné prozrazení vyšetřování nebo ovlivnění záznamů.
  - Kontaktovat osoby či společnosti podezřelé ze zavinění incidentu, bez přímého pokynu zodpovědné osoby.
  - Pokusit se vrátit útok útočníkovi (jeho systému). Takové jednání se snadno ocitne za hranicí zákona.
  - Pokusit se vyčistit (odstranit data), bez přímého pokynu zodpovědné osoby. Rizikem by mohla být ztráta dat nutných pro odhalení příčiny.



Interní a zákaznické bezpečností standardy

- **Správa fyzického přístupu**
- **Fyzická ochrana a systémů a sítí**
  - Systémová a síťová zařízení musí být chráněna před poškozením a krádeží.
  - Každý vstup do chráněné oblasti musí být zabezpečen.
- **Fyzická ochrana a inventarizace médií**
  - Média obsahující klíčová data, zálohy, data určená pro uchování a D/R musí být fyzicky chráněny před neautorizovaným přístupem, krádeží a poškozením.
  - Chráněná knihovna médií musí být překontrolována nejméně jednou ročně.

Interní a zákaznické bezpečností standardy

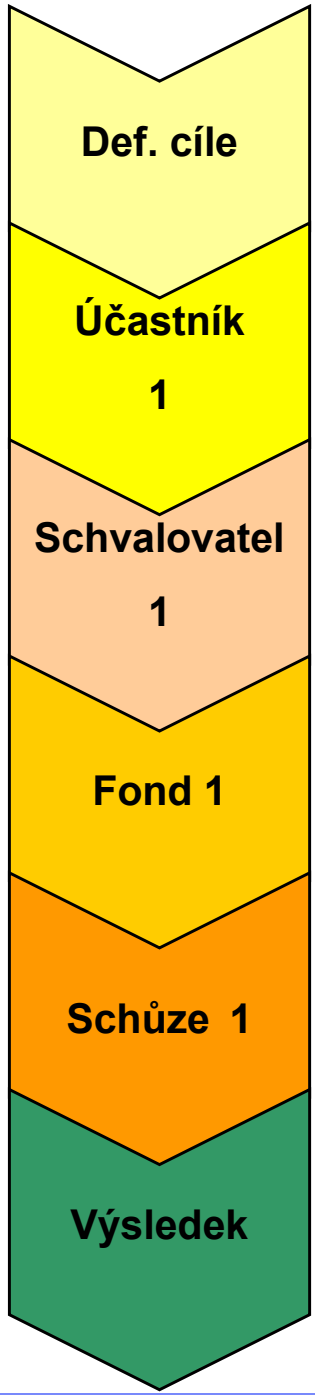
- **Operační systémy**
  - AIX Platformy
  - Linux Servery
  - Microsoft Windows 2000 Servery
  - Microsoft Windows NT Servery
  - Novell Netware
  - Na OS/2 založené OS
  - OS/400 Platformy
  - zOS, OS390 a MVS Platformy
  - z/VM and VM Platformy
  - VMWare ESX/GSX Server
  - Microsoft Windows Server 2003
- **Aplikační software/middleware**
  - Apache Web Servery
  - DB2 Universal Database
  - Lotus Domino Servery
  - Netview
  - OS/2 LAN Servery
  - Websphere Application Server
  - SSH Servery
  - Samba
- **Síťová infrastruktura**
  - Local Area Network (LAN) zařízení
  - Wireless zařízení
  - Firewally
- **Hlasová infrastruktura**
  - Avaya Media Server
  - Cisco Call Manager
  - Call Management System
- **Ostatní síťově připojitelná zařízení**
  - Tisková zařízení
  - Průmyslová zařízení
  - Vzdálené terminály

Interní procesy v rámci servisní organizace

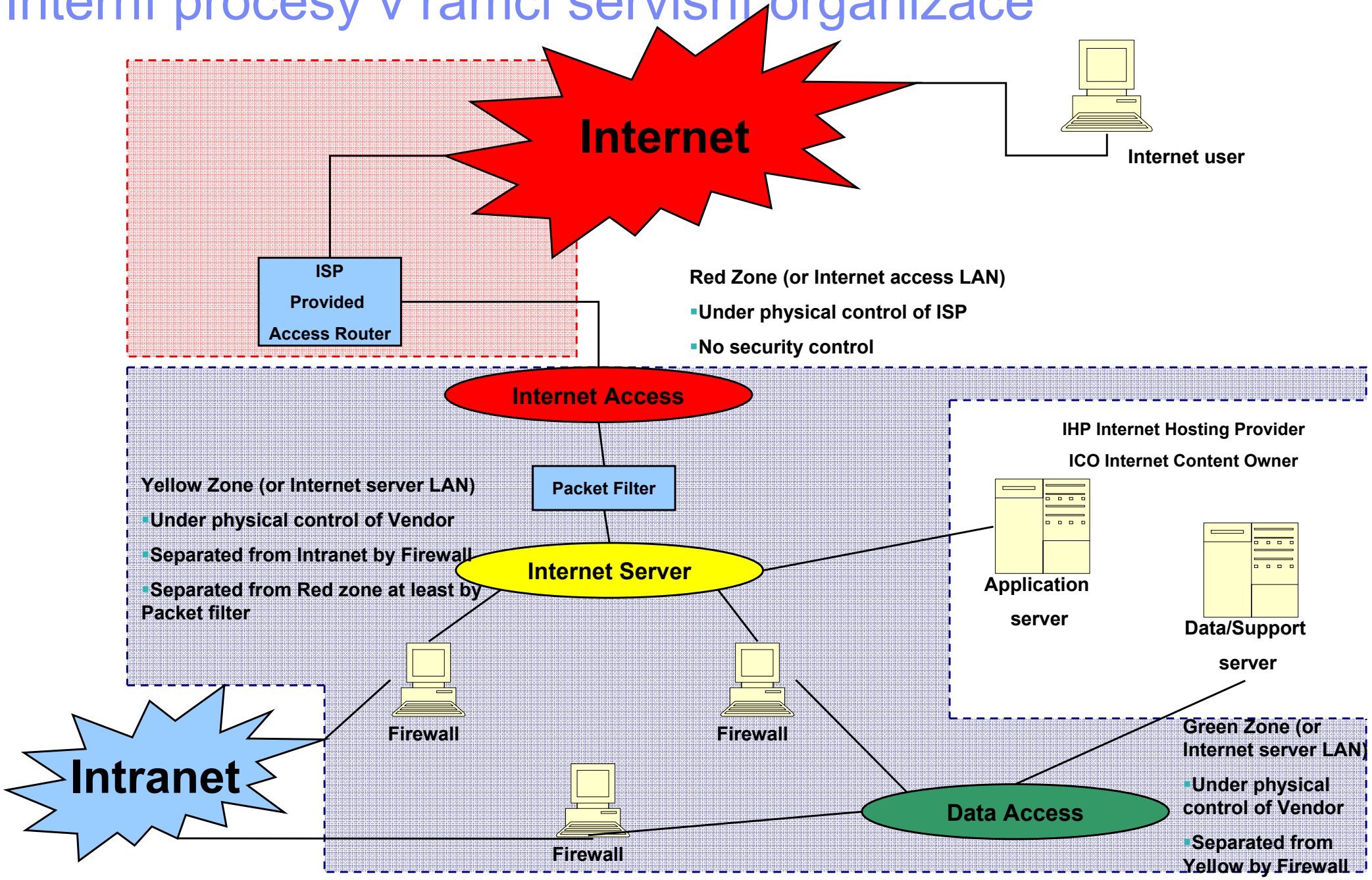
- **Příklady funkčních standardů:**
  - ITCS204 – Bezpečnostní pravidla pro poskytovatele sítí a služeb
  - ITCS329 – Bezpečnostní příručka pro Outsorcované internetové služby
  - GSD331 – Bezpečnostní řízení pro zákazníky strategického outsorcingu
  - GSD332 - IGS IT bezpečnostní standardy pro On-Demand Data Center Services (ODCS)
  - ISO/IEC 17799:2005 Ucelený soubor IT bezpečnostních pravidel založení na osvědčených zkušenostech.

Interní procesy v rámci servisní organizace

- **Proces je**
  - dlouhodobý
  - událostmi řízený
  - strukturovaná posloupnost aktivit vyžadujíc určité
    - Osoby
    - Informace
    - Technologie
- **za účelem dosáhnout cíle.**

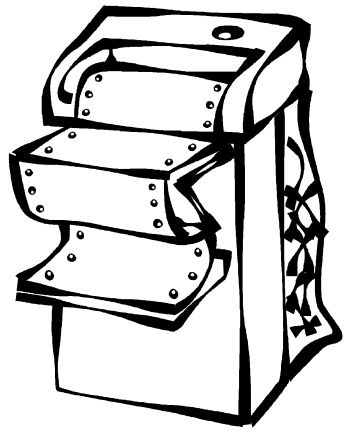


Interní procesy v rámci servisní organizace



Interní procesy v rámci servisní organizace

- **Fyzická bezpečnostní kontrola**
  - Prostory
  - Zařízení
  - Tisky
  - Zodpovědnost pouze za vlastní prostory, nikoliv za prostory zákazníka



Interní procesy v rámci servisní organizace

- **Kryptování**
  - Symetrické šifrování, používá stejný klíč pro zakryptování i pro dekryptování. Příkladem může být 56-bitový DES či 168-bitový Trojnásobný DES a nebo 128-bit IDEA.
  - Asymetrické šifrování, pomocí veřejného a soukromého klíče. Například 768-bit RSA či Diffie-Hellman
  - Pro oba způsoby je třeba zajistit řízení životního cyklu klíče, jako vytvoření, distribuce, ověření, update, uložení, používání a také expirace.

Diskuze