Információs Rendszerek Üzemeltetése
2007/08 tavasz

Zsoldos Viktor - zv602@hszk.bme.hu

Forrás: EA slide-ok

2. Az informatikai infrastruktúra

2.1. Személyes gépek (végberendezések)

2.2. Szerverek

2.3. Hálózat, a hálózat üzemeltetése

2.4. Adattárolás, adattárolók

2.5. Szabványok IT eszközök üzemeltetéséhez

3. IT Szolgáltatások

3.1 Általános kívánalmak & alapelvek

Alapkérdések

- Megbízhatóság
- Felhasználói kívánalmak
- Szerver minőségű gépek, szerverterem, szerverek alaptulajdonságai
- Szolgáltatások függősége
- Hozzáférés a szervergépekhez: csak SysAdmin

A jól karbantartható szolgáltatás legyen:

- egyszerű
- kevés függőséget tartalmazó
- „szabványos" hadveren
- „szabványos" szoftverekkel
- szabványosított konfigurációkkal
- dokumentált
- független a gazdagép hardverétől

Vastag (fat) kliens: az applikáció főleg a felhasználói gépen fut
Vékony (thin) kliens: az applikáció jelentős része szerver(ek)en fut

Megbízhatóság
Redundancia:

- Redundáns hardver; hatékony kihasználás, Pl: egy gép két tápegységgel – külön áramforrásra
- Backup szolgáltatáskülön telephelyen

Nem-redundáns szolgáltatás-elemek legyenek nagyon összefogottak:

- Kisebb függőség, kevesebb SPF (Single Point of Failure, egyszeres hibapont, egy hiba ami önmagában megbénítja a szogáltatást)

3.2 E-mail szolgáltatás

Az e-mail küldés lépései

- Üzenettovábbítás: ahogyan az e-mail szerverről szerverre jut
- Kézbesítés: amikor az email a fogadó mailbox-ába kerül
- Üzenet-listák feloldása: amikor a listacímre küldött levél megsokszorozódik és így kerül továbbításra

E-Mail üzenetformátum

- Fejléc (header), kódolás 7-bit U.S. ASCII text: „type: value" alakú sorok
- Törzs (body), szintén 7-bit U.S. ASCII text: struktúrálatlan

Problémák:

- Nem US nyelvű szöveg küldése
- Nem szöveg küldése (jpg, exe, stb)

Megoldás: Nem-ASCII karaktereket átkódolni ASCII-vé (3 bitből 4 bites ASCII – Base64 kódolás)

Probléma:
- Többféle adat egy üzenetben: hogy szeparáljuk ezeket?
- Több üzenet egy üzenetben (Digest)

Megoldás: MIME - Multipurpose Internet Mail Extensions:
- Hozzáadott fejlécek a törzs leírására
  - MIME-Version: melyik MIME verziót használja
  - Content-Type: milyen adattípus van a törzsben
  - Content-Transfer-Encoding: hogyan kódolt az adat (pl Base64)
- Tartalom-típusok és altípusok definíciói
  - image – altípus: gif, jpeg
  - text – altípus: plain, html, és richtext
  - application – altípus: postscript és msword
  - multipart – több adattípust tartalmazó üzenet

E-mail cím komponensei:
- Helyi mailbox (pl. pvarga vagy john.smith)
- Domain név (pl. tmit.bme.hu)

Mail szerverek
- mindig bekapcsolva és mindig hozzáférhetően
- e-mailek „szállítása” más szerverektől / szerverekhez

Store-and-Forward Protocol
Az üzeneteket szerverek sorozata szállítja: A szerverek a bejövő üzeneteket sorokban tárolják és amikor alkalom adódik, továbbítja a következőnek (next hop). Ha a következő nem elérhető, a szerver tárolja az üzenetet; később újra próbálkozik. Minden „hop” beírja az azonosítóját az üzenetbe, a “Received” fejléc így sokat segít a hibák keresésekor

Simple Mail Transfer Protocol

Kliens-szerver típusú protokoll:
- Kliens a küldő mail szerver
- Szerver a fogadó mail szerver

Megbízható adattovábbítás: TCP fölött (port 25)
„Push” protokoll: A küldő szerver benyomja a file-t a fogadó szerverbe, ahelyett, hogy kivárná, amíg a fogadó elkéri.

Post Office Protocol (POP)
POP célok:
- Időszakosan kapcsolódó felhasználók igényeihez alkalmazkodik
- Tegye lehetővé az e-mail-jeik leszedését amikor kapcsolódnak
- … és megnézhesse/manipulálhassa őket, amikor nincs csatlakozva

Az User Agent még SMTP-t használ az üzenetküldéshez.

A POP korlátai:

- Nem könnyen kezel többszörös mailbox-okat: a felhasználó bejövő e-mailjeinek egy helyre rakására tervezve.
- Nem az üzenetek szerveren tárolására tervezték, hanem az üzenetek kliensre való letöltésére
- Nagy hálózati sávszélességet igényel: minden üzenetet átvisz, gyakran sokkal elolvasásuk előtt (...és lehet,hogy sosem lesznek elolvasva...).

Interactive Mail Access Protocol (IMAP)

„Connected" és „Disconnected" módok támogatása:

- A felhasználók igény szerint tölthetik le az üzenetet

Egyszerre több kliens is csatlakozhat a mailboxra:

- Detektálja a más kliensek által a mailbox-on történt változtatásokat.
- A Szerver figyeli és tárolja az üzenet állapotát (pl. olvasatlan, olvasott, megválaszolt)

Hozzáférés az üzenetek MIME részeihez & részleges letöltés

- A kliensek darabonként is leszedhetik a MIME részeket
- Pl. Az üzenet szöveges részét – a csatolmány letöltése nélkül

Webes E-Mail

User agent: hagyományos Web browser

- A felhasználó HTTP-n kommunikál a szerverrel, pl.: Gmail, Yahoo mail, Hotmail, freemail

E-mail olvasás:

- A Weboldalak a folderek tartalmát jelenítik meg
- és lehetővé teszik az üzenetek megnézését, letöltést
- "GET" kérés a különféle Weboldalak megjelenítéséhez

E-mail küldés:

- A szöveget egy „form"-ba írjuk, majd „submit" a szervernek
- "POST" kérés és adatfeltöltés a szerverhez
- A Szerver SMTP-vel küldi az üzenetet más szerverhez

Egyszerűség

Ne használjunk desktop PC-ket (csak az UA).

Kis telephely:

- üzenettovábbítás ┐
- kézbesítés ├ egy gépen
- listakezelés ┘

Nagy telephely:

- fentiek külön gépeken / gép-csoportokon
- a desktop gépek és nem-email szerverek SMTP portja legyen letilva

Kerüljük a protokoll- vagy formátum-gateway-ek használatát.

Monitorozás

- Minden, az e-mail küldésben részt vevő gépet figyeljünk
- Hálózat: ping (ICMP echo üzenetet küld) - TCP 25-ös port elérhető?
- Tárterület
- Visszapattanó üzenetek – diagnosztikai info, naplóállományok

3.3 Távoli hozzáférés

Példák
„Remote Desktop (Windows)”:
- IP cím : port
- Felhasználónév/jelszó

VNC – Virtual Network Computing:
„Bármilyen OS alatti gép” felületének megjelenítése bármilyen másik gépen
Két komponensű:
- VNC szerver: a megjelenítendő gépen fut (pl. távoli szerver)
- VNC kliens: a megjelenítő gép (pl. IT-s kollega laptopja)
  - vncviewer alkalmazás
  - Web-Browseren futó Java alkalmazás

Kockázat
A külső alkalmazások eléréséhez (pl. Remote Desktop) a
- vállalti tűzfal(ak)on
- a helyi gép tűzfalán

az alkalmazás protokolljához rendelt portot átjárhatóvá kell tenni. Ez jobb helyeken hosszas engedélyezési folyamat

Szolgáltatási szint
Tisztázni kell a felhasználókkal
- a lehetőségeket
- a szabályokat (policy), beleértve a biztonságot
- a felelősségeket
- a fizetési konstrukciót (ki miért fizet)

Amennyire lehet, adjuk ki a RAS (Remote Access Service) szolgáltatásának feladatát (outsource)
A Biztonsági feladatokat NEM adjuk ki:
- authentication (username/password)
- authorization (jogosultságkezelés)
- hálózat-védelem

Outsourcing (RAS)
VPN (Virtual Private Network)
- A felhasználó otthon belép az ISP-jéhez, innen VPN-en jön be a vállalati hálózatba

„Virtual Circuits” – virtuális áramkörök
- Modem pool a „RAS-outsource” cégnél
- A „RAS-outsource” és a Vállalat között dedikált kapcsolat

3.4 Nyomtatás

A nyomtatás mint alapszolgáltatás
A felhasználóknak szüksége van rá
- v.ö. Papírmentes iroda

- aláírás: tintával, kézzel
- átolvasás/javítás
- nyomtatás a 2. legkritikusabb szolgáltatás (az e-mail után!)

Hálózati nyomtatás - protokollok
Klienstől a szerverhez:
- SMB – Server Message Block (port 137-139)
- LPR (LPD) - Line Printer Remote (-Daemon) Protocol (port 721-731, >1023)
- IPP – Internetwork Printing Protocol /(HTTP, 80)

Szervertől a nyomtatóig:
- LPR
- IPP
- TCP app. socket (port 9100), RAW

Hálózati nyomtatás - formátumok
- RAW – „nyers”, a nyomtató által emészthető formátum:
  - PCL – Printer Command Language (HP)
  - PostScript
- EMF – Enhanced Metafile: Windows: GDI konvertálja át RAW-ba
- ANSI Text
- Egyéb formátumok: GDI vagy Printer Driver konvertálja az adott nyomtató által emészthetővé

Centralizáció
Különféle feladatokra más-más követelmények:
- gyors
- jóminőségű (felbontás)
- színes
- ezek kombinációi…

Sok nyomtató sokba kerül. Megoldás:
- Központi nyomtatók + egyes embereknek saját nyomtató

Nyomtatási standardok
Ha a rendszergazda standard nyomtatással tervez, később kevesebb dolga lesz
- Postscript vagy PCL
- Mikor kell duplex-egység?
- Támogatott protokollok
- Nyomtató kapcsolódásai (USB, Eth, p.port)
- Lista: Jelenleg támogatott nyomtatók / driverek

Hozzáférés elvei
- Ki mihez férhet hozzá
- Ki adja ehhez a jogokat
- Ki melyik sorból mit lőhet ki?

Névadás
- típus (pl. duplex, color...)
- fizikai hely azonosítás (1. em, 221-es szoba...)
- logikai hely azonosítás (hr-esek, helpdesk...)

P2P hozzáférés (a felhasználók direktben bármelyik nyomtatóra spool-ozhatnak)
Központi elosztás:

- nagy központi spool
- intelligens döntésekre van lehetőség
- „Single point of failure!”

Csoportonkénti spool
Többszörösen redundáns spool-ok

Dokumentáció
Hogyan kell nyomtatni? (manual)
Fel kell sorolni a nyomtatókat: képességeikkel, helyükkel, szabályaikkal
Feliratozzuk a nyomtatót:

- legyen rajta a neve
- ha tálcákra külön lehet nyomtatni, akkor azokon is legyen rajta a tálca/sor neve!

Monitorozás
Spool: a nyomtató jelzi, ha baja van (pl. SNMP)

- tele a sora
- tele a diszkje
- túl van terhelve (CPU), stb.

Printing: Maga a nyomtatási környezet rendben van-e, hogyan állunk tartalékokkal

- toner
- papír
- papír a polcokon
- beragadás van-e

Dedikált nyomtató-karbantartó személy (akár külsős)

Printer Abuse (túlzott használat)

- “You can’t solve social problems using technology”
- fizetés oldalanként (akár jelképes is…)
- Top 10 nyomtató személyek publikálása

4. Szolgáltatási szintű üzemeltetés

4.1 SLM, SLA

SLM (Service Level Management) célja: fenntartsa és javítsa az IT szolgáltatás minőségét.
Módja: biztosítani a szolgáltatási szint

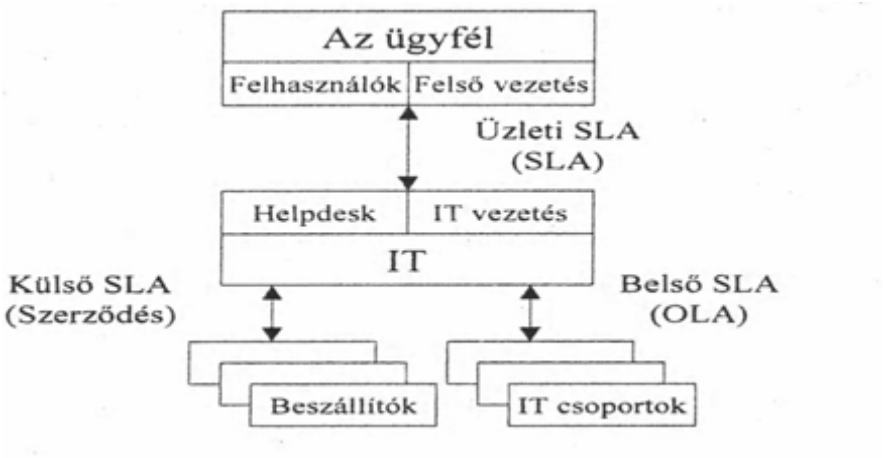
- jóváhagyásának
- ellenőrzésének
- naplózásának, jelentésének folyamatát.

Haszna:

- ne kelljen mindent elölről kezdeni (mások tapasztalatának használata)
- a piac szereplői közös nyelven beszéljenek
- nagy rendszer csak általánosan elfogadott alapelvek szerint működhet (jól)

SLA (Service Level Agreement): megállapodás az üzleti folyamatokért felelős döntéshozó és az IT szolgáltató között.
Tartalma:

- az informatikai szolgáltatások definíciója
- mérhető, számszerűsített paraméterei
- a paraméterek megengedhető szintjei
- mindkét fél felelősségi területei



1. ábra SLA Modell (példák)

A jó SLA tartalmazza a következőket:

- azonosítja és leírja a szolgáltatást
- megadja a megfelelőség mérésének módját
- megadja az elfogadhatóság szintjeit
- megadja a jelentési, jegyzőkönyvezési eljárásokat
- intézkedéseket határoz meg elégtelen szolgáltatás esetére
- megadja az SLA lejárati időt

Az SLA „üzleti nyelven” készül, nem tartalmaz műszaki részleteket. A műszaki specifikációkat SLS (Service Level Specification) vagy SLO (Service Level Objective) adja meg.
SLS: egy SLA műszaki interpretációja (műszaki előírások egy-egy szolgáltatás

megvalósítására).
SLO: az SLS része (szolgáltatási paraméterek, elérendő szolgáltatási állapot, stb.)
OLA (Operational Level Agreement): megállapodás két szervezeten belüli terület között.

4.2 COBIT

ISACF (Information Systems Audit and Control Foundation - IT Governance Institute, USA)
Control OBjects for Information & related Technology - elsősorban az USA-ban terjedt el.
Fő irányelvek:

- Vezérlő célok megfogalmazása és audit

Kik használják?

- IT: menedzsment, auditorok, biztonsági szakemberek

COBIT – SLA: SLA-k létrehozása a teljesítmény kritériumok formalizálására: a szolgáltatás minőségi és mennyiségi jellemzőinek mérésére

MOF (Microsoft Operation Framework)
Fő irányelv: technikai útmutatót ad Microsoft termékekre, technológiákra épülő kritikus rendszerek megbízhatóságának, rendelkezésre-állásának növeléséhez, támogathatóságának biztosításához. Elsősorban változás, probléma, konfiguráció kezelés.

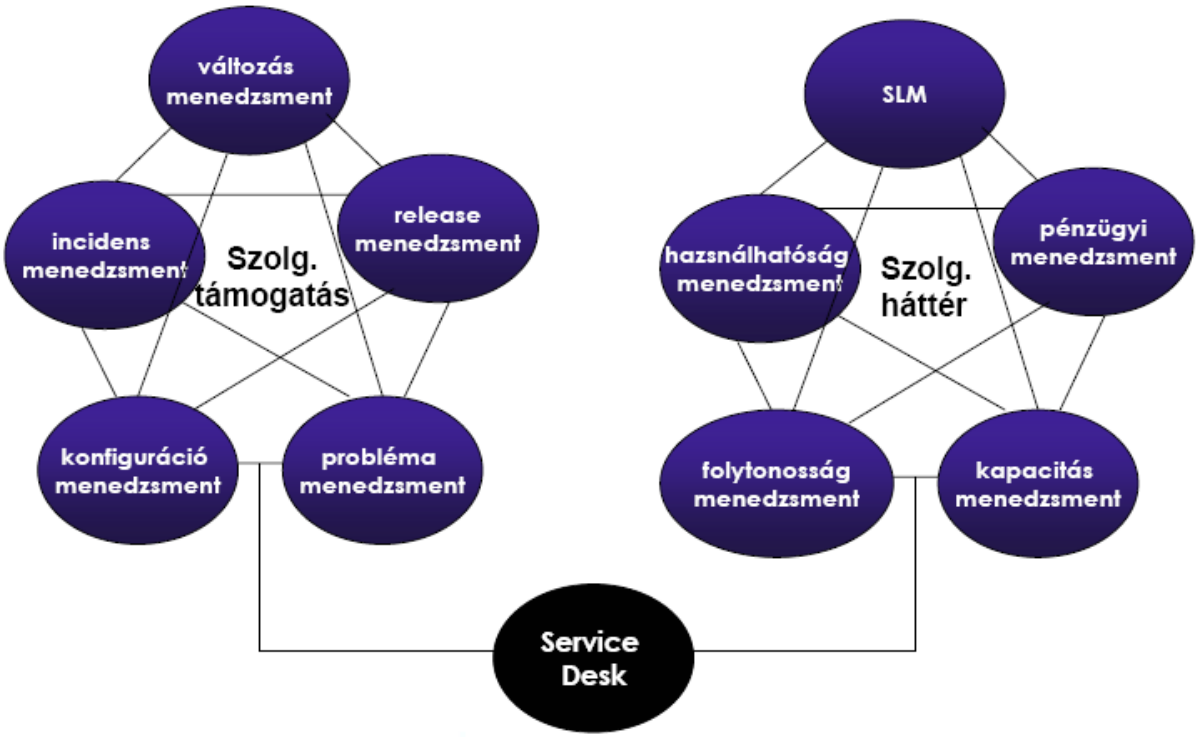
4.3 ITIL folyamat menedzsment

Information Technology Infrastructure Library, legjobb gyakorlatok (best practices) az IT szolgáltatási folyamatok menedzsmentjében (nyílt forrású)
ITIL – SLM: Írásos megállapodás az IT szolgáltató és a felhasználó között; dokumentálja a megállapodott szolgáltatási szinteket.

ITIL témakörök (ITSM - ITIL Service Management)

- Service Support - Szolgáltatás támogatás: IT szolgáltatások napi támogatására (konfiguráció, incidens, probléma, kiadás menedzsment, változáskezelés)
- Service Delivery - Szolgáltatás biztosítás: IT szolgáltatások hosszú távú tervezéséhez és fejlesztéséhez (pénzügy, kapacitás, rendelkezésre állás menedzsment)

E két komponens a szolgáltató központon (Service Desk) keresztül kapcsolódik össze (kapcsolati pont, aminek feladata a normál működés gyors helyreállítása).



Service Support - Szolgáltatás támogatás:
Változás menedzsment:
Cél: biztosítani, hogy szabványos módszereket és eljárásokat alkalmazzunk minden változás hatékony és gyors kezelésére; ezzel minimalizálva a hatásokat a kapcsolódó szolgáltatásokra.
Definíció: A változás egy akció, ami egy vagy több IT infrastruktúra konfigurációs elem (configuration item - CI) új állapotát eredményezi

Konfiguráció menedzsment:
Cél: az IT infrastruktúra logikai modellje (hw, sw és dokumentáció), tartalmazza, kezeli és ellenőrzi a konfiguráció minden elemének azonosító adatait (verziót is)
Definíció: Egy konfigurációs elem (CI) az infrastruktúra egy eleme. A konfigurációkezelési adatbázis (CMDB) egy adatbázis, ami az IT infrastruktúra minden eleméről tartalmaz bejegyzést.

Incidens menedzsment:
Cél: a normál működés helyreállítása amilyen gyorsan csak lehet, továbbá a felhasználókra gyakorolt hatás minimalizálása.
Incidens: egy esemény, ami a szolgáltatásminőség (quality of service - QoS) megszakadását vagy csökkenését okozza (vagy okozhatja).

Probléma menedzsment:
Cél: az incidensek ártalmas hatásainak minimalizálása és megismétlődésük megelőzése. A probléma gyökerét keressük és a hiba elhárítására kezdeti beavatkozást indítunk.
A probléma egy ismeretlen, egy vagy több incidens alapjául szolgáló ok.
Ismert hiba: amikor egy probléma oka (gyökere), és a probléma kikerülése vagy elhárítási módja ismert.

Release menedzsment:

Cél: adott hw/sw/dokumentáció kiadásában (release) érintett szolgáltatók és szállítók koordinálása, elosztott környezetben.
Definíció: egy release IT szolgáltatásokban engedélyezett változások gyűjteménye

Service Delivery - Szolgáltatás biztosítás:
SLM
Cél: az IT szolgáltatás-minőség fenntartása és javítása, a felhasználói elvárások figyelemmel kísérése útján.
SLA (Service Level Agreement): írásos megállapodás a megrendelővel, ügyféllel.
OLA (Operational Level Agreement): megállapodás két szervezeten belüli terület között.

Használhatóság menedzsment
Cél: az IT infrastruktúra képességeinek optimalizálása; szolgáltatás és támogatásának szervezése annak érdekében, hogy a célokat költséghatékony és fenntartható szinten érjük el.
Használhatóság: egy IT szolgáltatás vagy komponens képessége arra, hogy a szükséges feladatát adott időben vagy időtartamig ellássa.

Kapacitás menedzsment
Cél: az üzleti elvárások jelenlegi illetve jövőbeli IT kapacitás és teljesítmény vonatkozásait költséghatékonyan biztosítani.

Pénzügyi menedzsment
Cél: adott IT szolgáltatásokhoz a vagyonelemekkel, erőforrásokkal költéghatékonyan sáfárkodni ☺.

Folytonosság menedzsment
Cél: biztosítani, hogy a kívánt IT műszaki és szolgáltatási adottságok adott időn belül helyreállíthatók legyenek.
Krízis: nem tervezett helyzet, amikor egy vagy több IT szolgáltatás elérhetetlen, amikor az üzemszünet meghaladja a felhasználó elvárásait.

ITIL szolgáltató központ (Service Desk)
Cél: „egyablakos” szolgáltató központ: tanácsadás, segítség a normális szolgáltatás gyors helyreállításához
Szolgáltatás kérés: olyan kérés a szolgáltatásra, amelyik előzménye nem hiba, leállás.

5. Üzemeltetési politika

5.1 Rendszerüzemeltetési etika

5.2 Névter-politika

Névtér (namespace): bizonyos típusú elemek (pl. személynevek, földrajzi nevek, műszaki kifejezések, stb.) felsorolása és összefüggéseinek megadása egy rögzített szabályokon alapuló tároló elrendezésben

Absztrakt névtér: valamilyen szempontból összetartozó nevek
- felhasználói szerepkörök nevei („account" típusok)
- szolgáltatásnév lista

Konkrét névtér: pl. egy vállalat számítógépének használói, stb.

Egyszerű névtér: a névtér elemeinek egy és csak egy értelmezése lehet. (Két „valaminek" nem lehet ugyanaz a neve.)
Hierarchikus névtér: konténereket is tartalmaz valamilyen elrendezésben, pl könyvtár-szerkezetben: egy könyvtárban nem lehet két egyforma név, de két különböző könyvtárban igen)

Határozott, egyértelmű, rögzített, írott politika kell. (Minél több rendszeradminisztrátor van a rendszerhez, annál fontosabb.)
- kötelező ajánlások (pl. elnevezés, élettartam, megtalálhatóság, érvényesség)
- kötelező eljárások (létrehozásra, változtatásra és törlésre)
- menedzsment (központosított – nem központosított)

Ez a rögzített politika beépül:
- a rendszeradminisztrátorok közötti kommunikációba
- új rendszeradminisztrátorok betanítási anyagába
- a névtér karbantartó eljárások specifikációjába
- a használókkal kapcsolatos elvárások gyűjteményébe

Elnevezési politika
Szabályokat kell felállítani, hogy milyen nevek kerülhetnek a névtérbe. Erre vannak:
- technikai szabályok, pl. Unix login ID csak alfanumerikus + néhány speciális karakter
- vállalati szabályok, pl. login név nem lehet sértő, támadó
- szabványok, pl. RFC 1123

A névválasztás fő módszerei
Formuláris: szigorú, kötött szabályok szerint adunk neveket pl: gépnév: pc + 4 számjegy, login név: vezeték első hat jegye + keresztnév kezdőbetűje + n jegyű azonosítószám
Téma szerinti: a különböző típusú nevek különböző téma köré csoportosulnak, pl. szerverek csillagok, printerek bolygók stb.
Funkcionális: felhasználói szerepek (admin, titkár, vendég) a gép által betöltött szerep (dns, cpuserver12, web001) szervezeti egységer/projektre utaló diszk partíciók (/penzugy, /fejlesztes, /szerzodesek)

„Nincs szabály”: az a szabály, hogy nincs szabály; mindenki úgy nevez el valamit, ahogy ő gondolja, az ütközések feloldása elsőbbségi alapon történik.

Névtér séma

- egy séma-típus megadása
- kizárólag a rendszerünkben használt neveket és definícióikat tartalmazza

Alkalmazási profil: Egy séma-típus alkalmazása, az alkalmazási környezetben használt nevek leírása.

- névelem használati irányelvek
- névtér-sémában definiált nevek (újra)felhasználása
- több névtér-séma kombinációja is lehetséges egy alkalmazási profilban

Séma nyilvántartó
Névtér-elemek, -sémák és alkalmazási profilok tároló és hozzáférési megoldása.
Tartalmazhat:

- névtér-sémákat
- sémák közötti megfeleltetést (mapping)
- alkalmazási profilokat
- séma-magyarázatokat
- útmutatókat

5.3 A rendkívüli helyzetek teendői

Katasztrófa terv:

- a rendszert milyen katasztrófa fenyegetheti
- mit tegyünk ennek megelőzésére (hogyan lehet a katasztrófa lehetőségeket csökkenteni)
- hogyan tudunk katasztrófára reagálni (felkészülni a szükséges szolgáltatások minél hamarabbi visszaállítására)
- szolgáltatások fontossági listája, ezek visszaállítási időtartama

IT katasztrófa: Olyan nem kívánt esemény, amely az adattovábbító, -tároló és feldolgozó képesség elvesztését okozza, hosszabb időre.

Kockázat: Annak veszélye, hogy egy esemény, fenyegetettség bekövetkezése vagy intézkedés hátrányosan befolyásolja egy szervezet lehetőségeit céljainak és stratégiájának megvalósítása során.

Kockázatelemzés: A kockázat azonosításának, és a lehetséges kárkövetkezmény felbecsülésének módszere. A kockázatelemzési folyamat során a kockázati szinteket a védendő eszközök értékéből, valamint az eszközöket érintő fenyegetésekből és az eszközök sérülékenységéből lehet kiszámolni.

Kockázatkezelés: Azon kockázatkezelési szint meghatározása, mely szinten a felmért és kezelt kockázati tényezők az üzleti folyamatokat csak az előre meghatározott mértékben befolyásolják. (A biztonsági kockázatok azonosítása, elfogadható költségen a minimalizálása, és az ellenőrzése.)

Kockázattal arányos védelem: Olyan informatikai kockázatkezelés, amikor a védelem költségei arányosak a potenciális kárértékekkel. (Ezt életszerűen nagy időintervallumban kell mérni illetve biztosítani.)

Jogi elvárások: A műszaki és a jogi (szabályozási) aspektusok kiegészítik, és nem kiváltják egymást! (Ugyanazt a dolgot más nézőpontból ragadják meg.)
Gyorsan változó terület: új fenyegetettségek, új műszaki védelmi eszközök illetve módszerek. A szabályozásnak egyértelmű felelősségeket és következményeket kell megállapítania.

A katasztrófaterv jellemző tartalma:

- kit kell értesíteni, hogyan
- katasztrófahelyzet deklarálása (ki teheti meg ezt? hogyan?)
- vészhelyzet elhárítás teendői, kinek a felelőssége?
- újraindítás, tartalékműködés beindítása
- helyreállítási tevékenység
- a rendszer visszatelepítése, a normális működés újraindítása

A katasztrófaterv karbantartása, ellenőrzése:

- nyilvántartások karbantartása,
- prioritások, a működési jellemzők változásának követése (pl. az üzleti stratégia változása, az alkalmazás funkcióinak módosulása, a rendszerkörnyezet módosulása miatt)
- rendszeres oktatás

5.4 Változáskezelés

Az információs rendszerek változásmenedzsmentje a rendszer megváltoztatásának tervezésével és megvalósításával foglalkozik

Tipikus változáskezelési folyamat

I: Előkészítés		
A változás szükségessége	**II: Végrehajtás**	
Változáskezelési projekt terv	Előrehaladás monitorozása	**III: Beépülés**
Kommunikációs feladatok felmérése	Reagálás az ellenállásra	Eredmények „intézményesítése”
Résztvevők, partnerek meghatározása	Tanulságok felhasználása	Rögzítés politikákban, eljárásokban, képzésekben
Teljesítési kritériumok meghatározása	Áttervezés	A tanulságokból szabályok
Adatgyűjtés	Kommunikáció	A sikerek kommunikálása
Készültség felmérése	Dokumentálás	
Érdekeltek elkötelezése	Képzés, ha kell	

Nagyobb IT rendszerekben (hálózati szegmensek, szerverek tucatjai/százai; sokféle alkalmazás) az automatizálás nélküli módszerek nem elégségesek
Az IT környezetre vonatkozó döntések nagy része adott szabályok és politikák alapján történik → ezért automatizálható
IT rendszer-üzemeltetési szoftverek: Autonomic Managers & Policy Engines

Az autonóm változáskezelés
Metaadatok segítségével történik az információ és alkalmazás integráció:

- *Ma* – kézi integráció, egyedi „hard-wired" integráció
- *Holnap* – félautomatikus integráció (a komponensek szabványos csatlakozópontokkal rendelkeznek, ezeket szerkesztő eszközzel kapcsolgatjuk össze)
- *Holnapután* – automatizált integráció szabványos metaadatok és eszközök révén (névtér, szótár, taxonómia, ontológia)

5.5 IT biztonsági politika

Egy szervezet legértékesebb vagyona az információ, amely sokféle formában jelenhet meg (papíron, elektronikusan).

Információbiztonság

Az információvédelem az információ bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása, valamint a biztonsági kockázatok folyamatos menedzselése.

- **Bizalmasság:** annak biztosítása, hogy az információ csak az arra felhatalmazottak számára legyen elérhető.
- **Sértetlenség (integritás):** az információk és a feldolgozási módszerek teljességének és pontosságának megőrzése.
- **Rendelkezésre állás:** annak biztosítása, hogy a felhatalmazott felhasználók mindig hozzáférjenek az információkhoz és a kapcsolódó értékekhez, amikor szükséges.

IT üzemeltetés biztonsági szabályozása

Információbiztonsági politika

- általános irányelvek, felelősségi körök
- a legfelső vezetés biztonsági elkötelezettsége
- hosszú távra készül
- legfelső szintű vezetői jóváhagyás kell

Információbiztonsági Szabályzat

- Információ Biztonsági Politikának (IBP) megfelelő intézkedések
- középtávra készül
- legfelső szintű vezetői jóváhagyás kell

Eljárásrendek, kézikönyvek, utasítások

- technikai, technológiai irányultságú intézkedések, folyamatok
- rövidtávra készülnek
- informatikai vezetői jóváhagyás kell
- pl. mentési rend, incidenskezelési folyamat, vírusvédelmi eljárás

Információbiztonsági szerepek, feladatok

Információbiztonsági vezető: Információbiztonsági keretrendszer kidolgozása és működtetése, stratégiai tervezés, törvényeknek, szabványoknak való megfelelés biztosítása.
Információ gazda: Adat-, rendszer-, alkalmazás- és hálózatgazda, általában üzletági vezetők, akik teljes felelőséggel tartoznak a hozzájuk rendelt információ és információs rendszerek biztonságáért.
Információkezelő: Az információgazdák a napi feladatokat az információkezelőknek delegálják, pl. rendszer-, hálózatadminisztrátorok, ügyfélszolgálat (help desk).
Információ-felhasználó: Bárki aki az információt napi munkája során használja.

Üzemeltetés biztonsága

Védelem rosszindulatú kódok ellen
Virusvédelmi szoftver:

- központilag menedzselt, felhasználók ne tudják hatástalanítani
- rendszeresen frissített virusminta-adatbázis és viruskereső motor (lehetőleg automatikusan)
- email gateway

Virusvédelmi folyamatok:

- Vírusmegelőzés (rendszeres szkennelés, cserélhető adathordozók kezelése, oktatás)
- Vírusmentesítés: Dokumentált folyamat szerint: izolálás, helyreállítás, tesztelés

Adatmentés és adatmegőrzés
Az adatokat kritikussági szintjüknek megfelelően rendszeresen menteni kell

- elfogadható adatvesztési ablak definiálása, ennek megfelelően alkalmazott mentési technika kiválasztása
- telephelyen kívüli tárolás

Mentés fajtái:

- Teljes mentés: minden adat
- Differenciális mentés: a teljes mentés óta változott adatok
- Inkrementális mentés: az utolsó teljes, differenciális vagy inkrementális mentés óta megváltozott adatok

Törvényi előírások és üzleti érdekek szerint:
Pl. naplóállomány, változáskezelési jegyzőkönyvek, emailek, könyvelési adatok

- titkosítási kulcsok megőrzése
- megőrzési idő után az adatok szakszerű megsemmisítése

Naplózás
Gyűjteni kell minden olyan adatot, amely biztonsági események észlelésénél, kiderítésénél fontos lehet.
Naplózandó attributumok:

- esemény típusa
- dátum
- felhasználó azonosító
- IP cím

Biztonsági frissítések

A szoftverek biztonsági réseket tartalmaznak. Megoldás: rendszeres biztonsági frissítés.
Kritikus a frissítés gyorsasága: a sebezhetőség felfedezése és az exploit (rosszindulatú kód) megjelenése közötti idő drasztikusan lecsökkent (Zero-day attack).
Szoftver/biztonsági frissítés a változáskezelési folyamattal összhangban (lehet manuális vagy automatizált)

Adathordozók kezelése
Probléma: adatszivárgás

- Cserélhető/hordozható adathordozók kezelése (USB eszközök, CD/DVD)
- Titkosítás, bizalmas adatok tárolása
- Adathordozók biztonságos elhelyezése, kezelése, szállítása, megsemmisítése

Internet biztonság
Belső IT infrastruktúrát meg kell védeni a nyilvános hálózati szegmenstől!
Határvédelem: Tűzfalak, Intrusion Detection/Prevention System - IDS/IPS
Protokollok:

- biztonságos: HTTPS, SSL, SSH, SFTP,SNMPv3
- nem biztonságos: FTP, Telnet, SNMPv1, NFS

Web-szerver:

- Dedikált server a Demilitarized zone-ban (DMZ)
- Adatokat nem tárol → 2 vagy 3 szintű architektúra

Titkosítás: erős algoritmusok és kulcsok alkalmazása

E-mail biztonság
Egyike a legrégebben használt internetes protokolloknak: smtp, pop, kidolgozásukkor a biztonság nem volt szempont.
A kapcsolódó mail szervereket nem lehet szűrni, bárhonnan jöhet levél.
Probléma:

- Spam
- Hitelesség, bizalmasság, sértetlenség nem biztosítható (phishing, whaling)
- Adatszivárgás

Megoldások – intézkedések:

- Spam szűrés
- Email továbbítás (email relaying) tiltása
- Antivirus gateway
- Bizalmasság és sértetlenség session (TCP/IP transport) illetve alkalmazás szinten védhető: Kulcskezelés megoldása (PGP, PKI)
- Fontos a felhasználói viselkedés szabályozása, felhasználók oktatása

Logikai hozzáférés kezelés

- **Azonosítás**: Egyedi azonosítók, pl. felhasználói név, telefonszám
- **Hitelesítés** (authentikáció): Tényleg ő? Azonosítás az alábbi faktorok alapján:
  - Amit a felhasználó ismer (jelszó)
  - Amit a felhasználó birtokol (token, smartcard)
  - Amit a felhasználó visel (ujjlenyomat, hangminta)

  Erős authentikáció, ha a felhasználó a hitelesítéshez a kulcsot nem fedi fel a hitelesítő előtt sem!
- **Authorizáció**: Mit csinálhat?

- Hozzáférési jogosultságok
- Normál ←→ privilegizált

Alapelvek:

- **Need-to-know:** a felhasználó csak annyi információt tudhat, ami feltétlenül szükséges a munkája ellátásához.
- **Minimális jogosultság** (least privilege): a felhasználó a legszűkebb körű jogosultsággal rendelkezhet, amely elegendő a munkavégzéséhez
- **Feladatok elhatárolása** (separation of duties): Egy személy nem lehet felelős egy tranzakciólánc több lépéséért (pl. végrehajtás és ellenőrzés)

Távoli elérés: a telephelyen kívülről vállalati erőforrások elérése
Problémák:

- Nyilvános hálózaton keresztül történik
- Jelszóval való visszaélés (gyenge jelszavak, illetéktelen belépés)
- Távoli munkaállomások nem biztonságosak (nincsenek felügyelve)
- Egyidejűleg két kapcsolat a távoli gépen
- Mobil munkaállomások (laptopok, pda-k)

Megoldás: Virtual Private Network - VPN (IPSec, SSL)

- 2-faktoros hitelesítés: kombinálja a felhasználó által ismert információt (jelszó, PIN) egy egyszer használatos adattal.
- otthoni eszközök biztonságos konfigurálása vagy vállalati számítógép használata adminisztrátori jogosultság nélkül (antivirus, személyes tűzfalak, stb.)
- oktatás

Infrastruktúra biztonság
Hálózatbiztonság:
Tűzfalak: biztonsági zónák közötti forgalom ellenőrzése: Internet ↔ DMZ ↔ belső hálózat
Típusai:

- Csomagszűrő
- Stateful inspection (dinamikus csomagszűrés, kapcsolatok állapotát is vizsgálja)
- Proxy

IDS/IPS Behatolás-észlelő és megakadályozó rendszerek

- Minta-alapú (signature-based)
- Anomáliadetektorok
- Honeypot (mézesmadzag)

Leglényegesebb funkciók:

- Aggregálás
- Korrelálás
- Riasztás

Incidenskezelés
Incidens: minden olyan esemény, amely negatívan befolyásolja az információ és információs rendszerek biztonságát, pl. DoS, vírusfertőzés, jogosulatlan hozzáférés
Az incidensek bekövetkezése még a legjobb intézkedések (kontrollok) alkalmazása esetén sem küszöbölhető ki.
Incidenskezelés: incidensek észlelésének, analizálásának, helyreállításának a szervezett folyamata, melynek célja a károk minimalizálása és további károk elkerülése

Incidenskezelés lépései:
Előkészület:

- Folyamat és utasítások meghatározása
- Szerepek és felelősségi körök definiálása
- Eszközök, programok beszerzése, előkészítése
- Incidens követő eszköz bevezetése

Detektálás és Analízis:
Detektálás:

- Emberek által
- Rendszereken keresztül (pl. IDS/IPS)
- Probléma: Gyakran nem pontos adatok, téves riasztás (false positive)

Analízis: incidensek validálása (téves riasztások kizárása)
Hatókör definiálása: érintett alkalmazások, hálózatok, rendszerek és szolgáltatások azonosítása
Rangsorolás üzletmenetre kifejtett hatás alapján:

- Kritikusság és sürgősség
- Jelenlegi és lehetséges hatások

Érintettek értesítése (pl. Információbiztonsági vezető, rendszergazdák, HR, jogi osztály, stb)
Dokumentálás

Behatárolás:
Cél az incidens lokalizálása, hatásának korlátozása, mindezt előredefiniált utasítások végrehajtásával.
Stratégia kiválasztása az alábbi szempontok alapján:

- Incidens prioritása
- Szükség van-e bizonyíték megőrzésre
- A stratégia erőforrásigénye
- A megoldás időtartama
- Szolgáltatások rendelkezésre állása

Kiirtás:
Cél az incidens összetevőinek kiküszöbölése, támadás megfékezése, rendszer alap biztonsági konfigurációjának visszaállítása
A műveletek meghatározásánál tekintettel kell lenni

- Szükség van-e bizonyíték megőrzésre
- A korábbi mentések fertőzöttek-e
- Megbízható forrásból kell visszaállítani a sérült programokat

Helyreállítás:
Cél a rendszer normál működésének visszaállítása, biztonságossá tétele hasonló incidensek elkerülése céljából
Feladatok:

- biztonsági frissítések alkalmazása
- a rendszer fölösleges komponenseinek eltávolítása
- határvédelem erősítése
- rendszer újratelepítése

Post-incidens tevékenységek:

- tanulni az adott esetből, javítani a gyakorlaton
- incidens áttekintő megbeszélést az incidens lezárását követő pár napban kell megtartani
- kiváltó okok megkeresése (root cause analysis)

Információbiztonsági Incidens Elhárító Csapat - Computer Security Incident Response Team (CSIRT) feladata:

- Kivizsgálni hogyan történt az incidens, milyen kárt okozott
- A sérült rendszerek és szolgáltatások visszaállítása
- A nem sérült kritikus rendszerek működőképességének megóvása
- Hasonló incidens újbóli bekövetkezésének megakadályozása
- Az információbiztonsági szabályozórendszerre vonatkozó javaslatok kidolgozása
- Negatív visszhang elkerülése (megfelelő kommunikáció alkalmazása)

Eszkaláció

Ha az incidens nem oldható meg egy előre rögzített időn belül, akkor több szakértelem vagy hatáskör bevonása szükséges

- Funkcionális eszkaláció: nagyobb gyakorlattal rendelkező, képzettebb egyén bevonása pl. Ügyfélszolgálat → IT szakember → Szoftver vagy hardver szállító/gyártó
- Hierarchikus eszkaláció: a vállalati szervezetben egy magasabb szintű pozíció bevonása, pl. Ügyfélszolgálat → CSIRT Vezető → Informatikai vezető