



Karczub Béla

Szoftver és adatvédelem



A követelménymodul megnevezése:
Korszerű munkaszervezés

A követelménymodul száma: 1180-06 A tartalomlelem azonosító száma és célcsoportja: SzT-013-55



SZOFTVER

ESETFELVETÉS – MUNKAHELYZET

Munkahelyén azt a feladatot kapta, hogy vizsgálja felül a szoftverállományt és az adatvédelem állapotát.

A szoftvervizsgálat terjedjen ki a szoftverek típusára, eredetére, továbbá arra, hogy a felhasználásuk legális vagy illegális, és különösen a licencszerződésekre vonatkozóan

A vizsgálat célja kideríteni, hogy a szoftverek eredetiek vagy másoltak.

Az adatvédelem ellenőrzése, felülvizsgálata terjedjen ki az adatok védelem struktúrájára, megbízhatóságára és a módszerekre

Az adatvédelem módjára, eszközeire, biztonságára, megbízhatóságára, jogosultságokra

Jelen tananyag alapvető célja összefoglalni azokat a szoftver és adatvédelmi alapismereteket melyek alkalmazásához, a munkahelyi struktúrába, rendszerbe való alkalmazáskor, a megfogalmazott munkahelyzet megoldása során nélkülözhetetlenek.

SZAKMAI INFORMÁCIÓTARTALOM

SZOFTVER ALAPFOGALMAI:

1. Szoftver fogalma:

A szoftver a hardver egységeket működtető, vezérlő programok összessége. A szoftver (software) mesterséges szó, azokat a szellemi javakat hívják összefoglalóan így, amelyekkel kihasználhatjuk a hardverben rejlő teljesítményt és lehetőségeket. A szoftvert egyrészt a gépet működtető programok, másrészt a számítógéppel való feldolgozásra előkészített adatok alkotják

A szoftver teszi használhatóvá a számítógépet, biztosítja a hardver-egységek együttes működését, valamint a felhasználó kiszolgálását. Szoftvernek nevezzük azokat a szellemi termékeket, programokat, amelyek az adatfeldolgozó berendezések működtetéséhez szükségesek.

Szoftver fogalma: a számítógépen futó, illetve futtatható programok összefoglaló neve.

Szoftvernek nevezzük a számítógépre írt programokat (operációs rendszer, szövegszerkesztő, böngésző, stb.) és az ezekhez mellékelt írásos dokumentációkat. A szoftvereket programozók készítik, szellemi termékek, a szoftvereket hordozó eszközökön tárolják – CD, DVD. A szoftver a számítógépen futó programok összefoglaló neve, a hardver egységeket működtető-, és vezérlő programok összessége.



1. ábra. Szoftver

2. Mi a szoftver?

A számítógépes programok, a hozzájuk kapcsolódó dokumentációk és konfigurációs adatok összessége

3. A szoftver funkciói

- Több, különböző célra megírt program összessége
- Csoportosítás funkció szerint:
 - Rendszerszoftverek – Operációs rendszerek
 - Alkalmazói programok
 - Segédprogramok
 - Programozási nyelvek – programfejlesztő eszközök

4. Szoftver fogalma:

Az összes olyan adat, amely végrehajtható utasításként értelmezve a számítógép működtetéséhez szükséges és nem tartozik annak fizikai összetevőjéhez

5. A szoftver általában három fő részből áll:

forrásprogram (kód), mely valamely programnyelven készül, és általában funkciók, műveletek, kapcsolatok vázát tartalmazza a feldolgozandó adatokkal, felhasználó részére szóló utasításokkal. A forrásprogram tehát egyrészt utasítás, másrészt kommentár. A forrásprogramból fordítóprogram (compiler) segítségével automatikusan gépi programmá alakul, ami nem más, mint a **tárgyi program**, ami képes arra, hogy a computer működését irányítsa a felhasználó utasításainak megfelelően, **kísérő anyag**, ami tulajdonképpen a kiegészítő dokumentáció, amely mint önálló írásmű is jogi védelmet élvez.

6. A szoftverek telepítése, beállítása, eltávolítása

A szoftvereket általában egy futtatható állomány (pl. setup.exe) segítségével telepíthetjük a gépünkre, amiben pusztán a telepítési varázsló lépéseit kell követnünk.

Kiválaszthatjuk, hova szeretnénk telepíteni az adott szoftvert, esetleg hogy milyen verziót szeretnénk (telepítse-e az összes adott komponenst, vagy csak a szokásosat, esetleg egyénileg választjuk ki), vagy, akarunk-e reklámokat, sidebar-t a böngészőbe, ikont az asztalon, gyorsikont a tálcán stb.

Eloolvashatjuk a licencszerződést, amit el kell fogadnunk, hogy a program feltelepüljön. Néhány program már a telepítés során felajánlja, hogy konfiguráljuk, azaz beállítsuk a legfőbb jellemzőit, de általában létezik egy alapértelmezett beállítás, és ha meg akarjuk változtatni, azt már az első indítás után ezt közölnünk kell.

A szoftverek szakszerű eltávolítása a Vezérlőpultban történik (Windows operációs rendszer esetén természetesen), a Programok hozzáadása/eltávolítása címszó alatt, ami általában elindítja a programhoz mellékelte uninstallt, ami törli a szoftvert a gépünkről.

SZOFTVEREK CSOPORTOSÍTÁSA:

1. Szoftverek csoportosítása funkciójuk szerint:

1. Operációs rendszerek
2. Segédprogramok
3. Felhasználói programok:
 - Szöveg és kiadványszerkesztők
 - Adatbázis és táblázatkezelők

Grafikai programok

- Prezentáció-készítő programok
- Tervezői rendszerek
- Kommunikációs programok
- Játékok
- Egyéb programok

1. BIOS

BIOS (Basic Input/Output System)

A számítógép megvásárlásával az alapvető funkciókat biztosító programot is megkapjuk, a BIOS-t (alap be- és kiviteli rendszert). Mivel e nélkül a számítógép működésképtelen, ezért ez a program egy ún. ROM-ban (Read Only Memory, azaz csak olvasható memória) foglal helyet, amit az alaplapha beültetve kapunk meg. E program feladata a számítógép egységeinek ellenőrzése, alapfunkcióinak irányítása, a gépi szintű folyamatok vezérlése, valamint az ember és a gép közötti kapcsolatot megteremtő program keresése.

Az operációs rendszerek feladatai:

Az ISO nemzetközi szabványosítási szervezet definíciója szerint, az operációs rendszer:

„Olyan programrendszer, amely a számítógépes rendszerben a programok végrehajtását vezérli: így például, ütemezi a programok végrehajtását, elosztja az erőforrásokat, biztosítja a felhasználó és a számítógépes rendszer közötti kommunikációt.”

A számítógép részegységeinek összehangolt működtetése,
Erőforrások kihasználásának ütemezése,
A számítógép adatforgalmának lebonyolítása,
A kiadott parancsok értelmezése, végrehajtása,
Hiba esetén a hiba javításának megpróbálása, ha nem megy: hibajelzés,
Több felhasználó egyidejű munkájának megszervezése,
Több számítógép együttműködésének megvalósítása,
Adatvédelem, hozzáférési jogok ellenőrzése

2. Szoftverek csoportosítása a felhasználói jog szempontjából:

1. **Kereskedelmi szoftverek:** kereskedelmi céllal készültek, azaz mindig pénzbe kerülnek és meghatározott feltételekkel alkalmazhatók. Általában társul hozzá valamilyen dokumentáció is, amiben részletesen elmondják a használatát a programnak. A kereskedelemben értékesített programok előnye, hogy a vevő a boltban meg is nézheti, az eladó pedig azonnal a pénzhez jut.
2. **SHAREWARE szoftverek:** szabadon terjeszthetők, kipróbálhatók, de a szoftverrel együtt járó szerződés szerint a próbaidő letelte után már fizetni kell. Ha a felhasználó nem fizet a próbaidő lejárta után a szoftver használata jogtalanak minősül. A shareware verzió gyakran nem teljes, tudatosan le van butítva, de bemutatja a program előnyös oldalait. A regisztráció után küldik el a teljes verziót.
3. **FREWARE szoftverek:** Szabadon felhasználható és terjeszthető szoftverek, ha elismerjük a gyártó céget, mint a szoftver egyedüli létrehozóját. Nem szabad visszafejteni a forráskódot. Ez azt jelenti, hogy a programot nem adhatjuk tovább, mint saját termékünket és azt nem változtathatjuk meg. Azaz a szerzői jogok ezen szoftverekre is érvényesek.

4. **Trial:** általában kipróbálásra adják ki. Hasonlóak a shareware programokhoz, de fontos eltérés az, hogy nem terjeszthetők szabadon.
5. **Demo szoftverek:** bemutatóprogramok, azaz olyan szoftverek, amelyek egy program bemutatására, megismertetésére szolgál, de annak szolgáltatásait, teljes mértékben nem veszi át.
6. **Public domain:** olyan program, amelyet a programozó ajánl fel tetszőleges felhasználásra. Gyakran letölthető forráskód is, amellyel szerkeszthető, módosítható.
7. **E-MAIL-ware** (Postcard-ware): Ingyenes programok, a programozónak E-mailben kell küldeni egy minősítést a programról.
8. **Szabad szoftverek:** ingyenes, szabadon használható és terjeszthető szoftverek, a forráskód megismerhető, ezáltal módosítható.
9. **Félig szabad szoftverek:** Valamilyen felhasználási célra, kedvezőbb vásárlási feltételekkel kerülnek forgalomba, például, ha az oktatásban alkalmazzák.

1. Programcsomagok

A szoftver nemcsak elektronikus memóriatartalomként realizálódik, hanem életciklusának megfelelően többféle formában jelenik meg, fogalma következő megvalósulási formákra is kiterjed, így a szoftver fogalmába tágabb értelemben beletartozik

- az összes fejlesztési dokumentáció (mint például a forráskód);
- az összes felhasználói dokumentáció (mint például a felhasználói kézikönyv);
- az összes kereskedelmi dokumentáció (mint például a licenc);

illetve az ezek bármelyikét tartalmazó adathordozók (mint például a telepítő CD vagy a nyomtatott számla). Az összetett feladatok elvégzésére kifejlesztett, egymással szoros kapcsolatban álló, önállóan is működőképes, de együttesen hatékonyabb és teljesebb támogatást nyújtó, éppen ezért teljes életciklusuk során együtt kezelt szoftverek csoportját **programcsomagnak** nevezzük.

2. Szoftverfejlesztés

A szoftver egy gyűjtőnév a számítógépes programokra és adatokra. A dokumentáció is a szoftver szerves részét képezi, bár ez nincs benne, a programban.

A szoftvertervezés részei:

A megoldandó probléma meghatározása, felmérése a majdani felhasználók igényei alapján, specifikáció készítése

Valamely programtervezési módszerrel a programszerkezet megalkotása és a használandó eszközök kiválasztása. (Hardver platform, nyelvek, adatok stb.)

Forrásprogram elkészítése (kódolás)

A kész program tesztelése

Dokumentáció készítése, mely tartalmazza a szoftvertervezés fázisaiban keletkezett adatokat (felhasználói leírás, igényfelmérés, programtervek, algoritmusok, forráskód, tesztelési jegyzőkönyvek stb.), fő célja a szoftver későbbi fejlesztésének elősegítése.

3. Forráskód (angolul Source Code):

Ezalatt az informatikában egy programozási nyelv utasításainak sorozatát értik. A szoftverek elkészítésének fontos eleme, amikor az ember által olvasható utasításokból futó program lesz. Ennek a folyamatnak az egyik lépését a fordítóprogram (compiler) végzi, aminek a bemenete (forrása) a fent említett utasítássorozat, kimenete pedig általában egy köztes kód. A forráskódot legtöbbször féltve őrzik a fejlesztők, de van amikor ezt hozzáférhetővé teszik, ezt nevezik Nyílt forráskódnak (bővebben lásd itt: Nyílt forráskód).

Nyílt forráskód (angolul Open Source):

A nyílt forráskód kifejezést általában olyan számítógépes programok esetén használjuk, melyeknek a forráskódja vagy közkinccs, vagy gyakoribb esetben a szerzői jogok tulajdonosa egy nyílt forráskódú licenc alatt terjeszti. Az ilyen licenc előírhatja azt, hogy a forráskódot a programmal együtt kell terjeszteni, és hogy az szabadon módosítható. A nyílt forráskódú licencek nem feltétlenül követelik meg azt, hogy a program, vagy a forráskódja ingyen és szabadon publikálásra is kerüljön (az interneten), noha a legtöbb nyílt forráskódú projekt ilyen.

4. A szoftverek funkciójuk szerint

A programvezérelt gépek célszerű működését a szoftverek több rétege biztosítja. Aszerint, hogy egy szoftver specifikusan mennyire inkább a gép pusztán működtetését, avagy az ember által igényelt feladatmegoldást segíti elő, a következő funkcionális csoportokat különböztetjük meg.

indítóprogram vagy alapszoftver – a felhasználó által a legkevésbé manipulálható, a gépüzemszerű működését beállító program(ok), ide tartozik a firmware is;

rendszoftverek – a gép és perifériái kommunikációját lebonyolító programok, beleértve a felhasználó oly mértékű kiszolgálását, amely lehetővé teszi a számára más szoftverek elkészítését és üzembe helyezését is;

alkalmazói szoftverek vagy alkalmazások – a felhasználót a számítógép használatán túl mutató céljainak elérésében támogató specifikus programok

5. Biztonsági állapot ellenőrzése a Windows Biztonsági központ használatával

A Biztonsági központ megnyitásához kattintson a Start gombra, kattintson a Vezérlőpult parancsra, ezután kattintson a Biztonság segédeszköze, majd kattintson a Biztonsági központ gombra.



2. ábra. Biztonsági központ

Tűzfal. A tűzfal segít megvédeni a számítógépet attól, hogy támadók vagy rosszindulatú szoftverek hozzáférjenek.

Automatikus frissítés. A Windows rendszer szabályos időközönként megkeresi a számítógéphez megjelenő frissítéseket, és automatikusan telepíti azokat.

Kártevő programokkal szembeni védelem. A vírusvédelmi szoftverek meg tudják védeni a számítógépet a vírusoktól, férgektől és más fenyegetésektől. A kémprogram-elhárító szoftverek meg tudják védeni a számítógépet a kémprogramoktól és egyéb nemkívánatos szoftverektől.

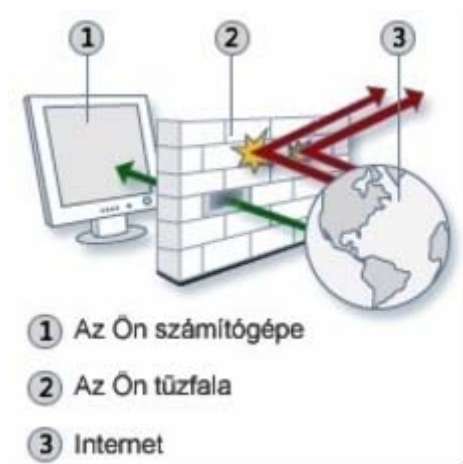
Mik azok a biztonsági figyelmeztetések?

Ha a Windows felfedezi, hogy a számítógépnek valamelyik biztonsági területen – tűzfal, automatikus frissítés, rosszindulatú programokkal szembeni védelem vagy más biztonsági beállítások – jobb védelemre van szüksége, akkor minden bejelentkezésnél megjelenik egy értesítés, egészen addig, amíg meg nem oldja a problémát. Az értesítések az értesítési területen jelennek meg a tálcán.

6. Tűzfal használata

A tűzfal olyan szoftver vagy hardver, amely ellenőrzi az internetről vagy hálózatról érkező információkat, és a tűzfal beállításaitól függően vagy elutasítja, vagy továbbengedi azokat a számítógépre. A tűzfal így segít megakadályozni, hogy a támadók vagy rosszindulatú szoftverek hozzáférjenek a számítógéphez.

A Windows tűzfal be van építve a Windows rendszerbe, és automatikusan bekapcsolódik.



3. ábra. Tűzfal

Ha olyan programot futtat, amelynek működéséhez adatok fogadására van szükség az internet vagy az intranet felől (ilyen programok például az azonnali üzenetküldő szolgáltatások vagy a több résztvevős hálózati játékok), a tűzfal megkérdezi, hogy engedélyezi, vagy blokkolja a kapcsolatot. Ha a kapcsolat blokkolásának feloldása mellett dönt, akkor a Windows tűzfal létrehoz egy kivételt így a tűzfal, többet nem jelzi, ha a programnak információt kell fogadnia.

Az alapértelmezett tűzfalbeállítások használata ajánlott:

A tűzfal be van kapcsolva.

A tűzfal be van kapcsolva az összes hálózati helyhez (Otthon vagy munka, Nyilvános hely vagy Tartomány).

A tűzfal be van kapcsolva az összes hálózati kapcsolathoz.

A tűzfal blokkolja a bejövő kapcsolatokat, amelyek nem felelnek meg egyetlen kivételnek sem.

7. Vírusvédelem használata

A vírusok, férgek és trójai alkalmazások olyan, támadók által létrehozott programok, amelyek az internetet használják a sérülékeny számítógépek megfertőzéséhez. A vírusok és férgek képesek számítógépről számítógépre terjedni, míg a trójai alkalmazások egy ártalmatlannak tűnő programba, például egy képernyővédőbe, rejtve jutnak be a számítógépre. A pusztító vírusok, férgek és trójai alkalmazások információkat tudnak törölni a merevlemezeiről, vagy teljesen működésképtelenné is tehetik a számítógépet. Más ilyen programok nem okoznak közvetlen károkat, de rontják a számítógép teljesítményét, és instabillá teszik azt.

A vírusvédelmi programok képesek a számítógépen található e-mail üzenetekben és más fájlokban a vírusokat, férgeseket és trójai alkalmazásokat megkeresni. Ha találják őket, akkor a vírusvédelmi program vagy karanténba zárja (elkülöníti), vagy törli a rosszindulatú programot, még mielőtt az kárt tudna tenni a számítógépében vagy fájljaiban.

A vírus olyan program, amely önmagát sokszorozítja. Terjedése érdekében egy számítógépen lemásolja magát vagy programokba és az operációs rendszer fájljaiba, illeszt be számítógépes kódot. A vírusok nem minden esetben okoznak kárt a fájlokban vagy a számítógépben, de általában befolyásolják a számítógép teljesítményét és stabilitását. Ahhoz, hogy egy vírus megfertőzhessen, egy számítógépet vagy terjedhessen, általában valamit tennie kell, például, meg kell nyitnia egy fertőzött e-mail mellékletet.

A féregvírus olyan számítógépes kód, amely a felhasználó beavatkozása nélkül terjed. A legtöbb féreg e-mail mellékletként születik meg, amely megnyitásakor megfertőzi a számítógépet. A féreg a fertőzött számítógépen olyan fájlokat keres, mint például a címjegyzékek vagy ideiglenes weblapok, amelyek e-mail címeket tartalmaznak. A féreg arra használja a címeket, hogy fertőzött e-mail üzeneteket küldjön, és gyakran lemásolja (vagy meghamisítja) a „Feladó” címét az e-mail üzenetekben, így úgy tűnhet, mint ha a fertőzött levél ismerőstől érkezne. Ezután a férgek automatikusan terjednek e-mail üzeneteken, hálózatokon vagy az operációs rendszerek részein keresztül,

8. Mit jelent az operációs rendszer frissítése?

Az operációs rendszerfrissítések olyan új szoftvereket tartalmaznak, melyek segítenek naprakészen tartani számítógépét.

A frissítések között vannak szervizcsomagok, verziófrissítések, biztonsági frissítések, vezérlők és más jellegű frissítések.

A fontos és sürgős frissítések a számítógép biztonsága és megbízhatósága vonatkozásában nélkülözhetetlenek. Ezek teszik lehetővé a legújabb jelentkező rosszindulatú online tevékenységek elleni védekezést.

Minden programot frissíteni kell, beleértve a Windows-t, Internet Explorer-t, Microsoft Office-t, és másokat is.

9. A szoftver, mint fogalom

A szoftver szó az angolból átvett software magyar változata. Alatta, olyan szellemi terméket értünk, amely valamilyen alkalmas eszközt (gépet, gépegységet, gépcsoportot), meghatározott algoritmusok alapján fizikai megvalósításra utasít

Ahhoz, hogy valamire használni lehessen, tartalmaznia kell valamilyen hordozón (leggyakrabban: CD, DVD) magát a telepíthető programot, használatára vonatkozó leírást, kézikönyv, esetleg elektronikus formában, használat közben segítségnyújtást (súgó). Nyílt forráskód esetén tartalmaznia kell a fejlesztési dokumentációt is. Az elektronikus kézikönyv elérése, legyen telepítéstől független. Vannak szoftver-fejlesztők és szoftver-forgalmazók, akik nem tartják be teljes mértékben az előbbi megkötéseket. Ettől függetlenül, az adott szoftver egyszerűség estén lehet (jól-) használható is. Összetettebb, drágább szoftver esetén mindenképpen ragaszkodjunk az összetevők meglétéhez, vagy keressünk alternatívát.

Assembly: legközelebb áll a gépi kódhoz hardverillesztő szoftver, operációs rendszer programozására használatos alkalmazása időigényes, költséges cserébe leggyorsabb futásidejű.

C, C++, Pascal, COBOL: gépi kódra fordított programot állítanak elő, amelyet az operációs rendszer közvetlenül képes futtatni objektumorientáltság függvényében költség-hatékony, a futásidő növekedik.

Java: köztes kódra fordított programot állít elő, amelyet a Java virtuális gép (JVM) JIT fordítója futás közbeni gépi kódot állít elő szükség szerint módosítás nélkül alkalmazható különböző platformokra, operációs rendszerekre kizárólagos objektumorientált nyelvnek számít.

BASIC, JavaScript, PHP: nem állít elő gépi kódot, futtatásához külön futtató környezet szükséges módosítás nélkül alkalmazható különböző platformokra, operációs rendszerekre általában internetes alkalmazások fejlesztésére használatos támogatják az objektumorientáltságot.

10. Lemeztöredezettség-mentesítés

A sok merevlemezre való másolástól és törléstől előbb utóbb széttöredeznek a fájlok. Ez gyakorlatilag minden fájlrendszerre érvényes, káros mellékhatás. Védekezni ellene a célnak megfelelő programokkal lehet. DOS-tól kezdve ezek megvoltak minden operációs rendszerben. Az XP-ben a grafikus megvalósítás mellett parancssorból – és ennek következtében batch fájlból, szkriptekből, programból – való töredezettség-mentesítés lehetősége is adott.

11. Hálózatok csoportosítása

Területi kiterjedés alapján

LAN (Local Area Network) – kis kiterjedésű hálózat. Jellemzője az egyedi kábelezés, és az ebből következő gyors adatátvitel. Mérete: 1 szobától kezdve néhány kilométerig.

MAN (Metropolitan Area Network) – városi méretű hálózat. Egy város nagyságrendjét lefedő hálózat.

WAN (Wide Area Network) – nagytávolságú hálózat. Kiterjedése pár kilométertől kezdve az egész Föld nagyságáig terjedhet.

Topológia alapján

Bus (sin) – a gépek egy közös átviteli közegre csatlakoznak

Gyűrű – a gépek egy gyűrűre vannak felfűzve

Fa – Bármely két összekötött gép között csak egy és csak egy út van

Csillag – Minden gép csak a központi géppel (vagy eszközzel) van összekötve

Teljesen összefüggő – minden gép minden géppel egyedileg össze van kötve

Részben összefüggő – a teljesen összefüggőből elhagyunk néhány ágot

12. Az ISO–OSI modell

Adatátvitellel foglalkozó rétegek

A fizikai réteg (physical layer): a bitek kommunikációs csatornára való kibocsátásáért felelős. Ide tartozik a csatlakozások elektromos és mechanikai definiálása, átviteli irányok megválasztása

Az adatkapcsolati réteg (data link layer) – feladata egy hibátlan adatátviteli vonal biztosítása a "szomszéd" gépek között. Az adatokat adatkeretekké (data frame) tördeli, továbbítja, a nyugtát fogadja, hibajavítást és forgalomszabályozást végez.

A hálózati réteg (network layer) – a kommunikációs alhálózatok működését vezérli, feladata az útvonalválasztás a forrás és a célállomás között. Ha az útvonalban eltérő hálózatok vannak, akkor fregmentálást, protokoll-átalakítást is végez. Az utolsó réteg, amely ismeri a hálózati topológiát.

A szállítási réteg (transport layer) – feladata a végpontok közötti hibamentes átvitel biztosítása. Már nem tud a hálózati topológiáról, csak a két végpontban van rá szükség. Feladata lehet például az összeköttetések felépítése és bontása, csomagok sorrendhelyes elrendezése, stb.

Logikai összeköttetéssel kapcsolatos rétegek

A viszonyréteg (session layer) – lehetővé teszi, hogy két számítógép felhasználói kapcsolatot létesítsen egymással. Jellemző feladata a logikai kapcsolat felépítése és bontása, párbeszéd-szervezés. Elláthat szinkronizációs funkciót ellenőrzési pontok beépítésével.

A megjelenítési réteg (presentation layer) – az egyetlen, amelyik megváltoztathatja az üzenet tartalmát. Tömörítést, rejtjelezést, kódcserét (ASCII – EBCDIC) végezhet el.

Az alkalmazási réteg (application layer) – széles körben igényelt szolgáltatásokat tartalmaz. Ilyen alapvető igényt elégítenek ki például a file-okat tetszőleges gépek közötti másolását lehetővé tevő file transfer protokollok.

13. A hálózatok részelemei

A hálózatok részelemei a hálózat típusától, felépítésétől függnnek.

hálózati kártyák: olyan vezérlő egység, amely a számítógépbe építve a hálózat és a gép kapcsolatát biztosítja. Típusát meghatározza a hálózati architektúra és a kábelezés. Sok fajta hálózati kártya kapható, de árban, megbízhatóságban és minőségben eltérnek egymástól.

HUB: passzív hálózati eszköz, mely a szegmensek kapcsolatát biztosítja. Mivel jelerősítést nem végez, az előírt kábelhosszt nem léphetjük túl.

repeater: olyan elektronikus eszköz, amely az adatátvitel során, a csillapítás következtében torzult jelek felismerését, helyreállítását és újraidőzítését végzi.

router: egy intelligens eszköz, amely meghatározza a hálózaton áramló adatcsomagok útvonalát.

bridge: azonos architektúrájú, de különböző protokollok segítségével működő hálózatok össze kapcsolását teszi lehetővé.

switch: olyan szerkezeti elem, amely útvonalszegmensek időleges egymáshoz rendelésével épít fel kommunikációs útvonalat.

modem: olyan eszköz, mely telefonvonalon keresztül teszi lehetővé az adatátvitelt.

14. A hálózati operációs rendszerek biztonsági rendszerei

A korszerű hálózati operációs rendszerek mindegyike legalább négy szintű biztonsági rendszerrel rendelkezik. Ezek:

- bejelentkezési védelem
- jogosultságok védelmi rendszere
- attribútumok védelmi rendszere
- szerver (kiszolgáló) védelem

Hálózatok kezelése (távoli erőforrások, telefonos hálózati elérés használata, csatlakozás az internethez, elektronikus posta használata), az operációs rendszer megvédése a programhibáktól, az illetéktelen beavatkozásoktól.

Nyomtatószerver (Print Server):

A nyomtatószerver a hálózat valamennyi állomása számára lehetővé teszi, hogy egy vagy több nyomtatót használjon. Így a munkaállomásokon úgy használhatjuk a nyomtatót, mintha az közvetlenül a mi gépünkhöz lenne kötve. A nyomtatószerver azt is lehetővé teszi, hogy a nyomtatóra akkor is kiküldhessünk adatokat, amikor a nyomtató éppen foglalt.

A szerver operációs rendszerének jellemző többletfunkciói.

- bejelentkezés szabályozása
- fájlmegosztás
- nyomtatók megosztása
- web – szolgáltatás (webszerver)
- levelező–szolgáltatás (levelező szerver)
- FTP, Proxy, tűzfal

15. Telnet: távoli terminál

A távoli terminál alapvető célja, hogy hálózaton keresztül távoli belépési lehetőséget és virtuális terminált (billentyűzetet és képernyőt) nyújtson a felhasználók számára. Más szavakkal, bárhol is legyen egy az. A gép előtt ülő felhasználó, mindenhol oly módon használhassa a B gépet, mintha előtte ülne, annak terminálját használná, feltételezve, hogy A és B gépek között létezik hálózati összeköttetés. Eredetét tekintve a távoli terminál a soros vonali terminál–hozzáférés (dialup terminal connection) megfelelője a hálózati környezetben.

A távoli belépés egyik megvalósítása a Telnet (teletype network) protokoll, mely a TCP/IP protokollcsalád része, illetve a protokollt használó Telnet program. A fejezet további részében e rendszeren keresztül ismertetjük a távoli terminál elérés legfontosabb tulajdonságait. (Napjainkban a Telnet protokoll helyett az SSH protokoll használata javasolt, amely a távoli terminál–elérést titkosított hálózati kommunikációval, oldja meg.)

16. Az FTP–parancsértelmező

Az FTP–rendszerben a felhasználó alapértelmezésben a parancsértelmezőt használja helyi és távoli feladatok megoldására, illetve a fájlvitelre.

A parancsok alapvetően három nagy kategóriába sorolhatóak: helyi (kliens) parancsok, távoli (szerver) parancsok, és adatátviteli parancsok. Az átviteli mód meghatározására szolgáló ascii és binary parancsok kiadása után a cd paranccsal beállíthatjuk a távoli, illetve az lcd paranccsal a helyi munkakönyvtárat. Ezek után a put vagy get parancsok segítségével bonyolítható le a kívánt fájlvitel, majd a quit paranccsal szakíthatjuk meg a kapcsolatot és léphetünk ki az FTP kliensprogram parancsértelmezőjéből.

17. Szoftver, hardver műveletek

Az operációs rendszer telepítése.

Az adott operációs rendszert egy adathordozón (floppy, CD, DVD) kapjuk meg. A gépen ekkor csak a BIOS fut, amiben az adott adathordozónak megfelelőre kell állítani az elsődleges boot–forrást, mivel innen fogjuk indítani a telepítést. A Windows XP esetén a telepítés lényegesen leegyszerűsödik. Először a partíciókat kell meghatároznunk, azokat formatálni, elosztani. Ezek után csak követni kell a telepítőben leírt lépéseket, majd a Windows települése után telepíteni kell a drivereket, amiket az alaplaphoz, a hangkártyához és a videokártyához kaptunk, internet kapcsolat esetén azt is szükséges telepíteni.

Hardver eszközök üzembe helyezése, beállítása (konfigurálása), eltávolítása.

A hardver eszközök (billentyűzet, egér, nyomtató, új CD-meghajtó, scanner, pen drive stb.) csatlakoztatása a megfelelő portra a legelső lépés (PS/2, soros, USB, PCI-E, AGP stb.). Amennyiben ez megtörtént, az operációs rendszer felismeri, hogy új eszközt csatlakoztattunk a géphez. Ha van a hardverhez driverünk, tehát vezérlőprogramunk, akkor annak telepítésével és konfigurálásával végeztünk is. Amennyiben ez hiányzik és nem is szükséges, akkor a vezérlőpultban az Új hardver hozzáadását választjuk és értelemszerűen itt is lehet a hardvert eltávolítani.

A szoftverek telepítése, beállítása, eltávolítása.

A szoftvereket általában egy futtatható állomány (pl. setup.exe) segítségével telepíthetjük a gépünkre, amiben pusztán a telepítési varázsló lépéseit kell követnünk. Kiválaszthatjuk, hova szeretnénk telepíteni az adott szoftvert, esetleg hogy milyen verziót szeretnénk (telepítse-e az összes adott komponenst, vagy csak a szokásosat, esetleg egyénileg választjuk ki), vagy hogy akarunk-e reklámokat, sidebar-t a böngészőbe, ikont az Asztalon, gyorsikont a Tálcán stb. Elolvashatjuk a licencszerződést, amit el kell fogadnunk, hogy a program feltelepüljön. Néhány program már a telepítés során felajánlja, hogy konfiguráljuk, azaz beállítsuk a legfőbb jellemzőit, de általában létezik egy alapértelmezett beállítás, és ha meg akarjuk változtatni, azt már az első indítás után kell eszközölnünk. A szoftverek szakszerű eltávolítása a Vezérlőpultban történik (Windows oprendszer esetén természetesen), a Programok hozzáadása/eltávolítása címszó alatt, ami általában elindítja a programhoz mellékelt uninstallt, ami törli a szoftvert a gépünkről.

TANULÁSIRÁNYÍTÓ**1.feladat**

Szoftverek témakörében látogassanak el a www.szoftver.hu honlapra vagy a témakörrel kapcsolatban, a keresőben keressenek a szoftverekkel kapcsolatos leírásokat tanulmányokat.

2.feladat

Beszélgessenek, vitassák meg a gyakorlatban megvalósítható és az alkalmazott szoftvervédelmet s azok hatékonyságát.

3.feladat

Számítógépen mutassanak egymásnak szoftver beállításokat, példákat.

4.feladat

Fogalalkozásokra tervezzenek időt.

ÖNELLENŐRZŐ FELADATOK**1. feladat**

Írja le a szoftver fogalmát.

2. feladat

Sorolja fel az operációs rendszerek feladatai az ISO nemzetközi szabványosítási szervezet definíciója szerint

3. feladat

Írja le a Nyílt forráskód (Open Source) definícióját.

4. feladat

Írja le a vírus fogalmát.

5. feladat

Az ISO–OSI modell Logikai összeköttetéssel kapcsolatos rétegeket fogalmazza meg.

MEGOLDÁSOK

1. feladat

A szoftver a hardver egységeket működtető, vezérlő programok összessége. A szoftver (software) mesterséges szó, azokat a szellemi javakat hívják összefoglalóan így, amelyekkel kihasználhatjuk a hardverben rejlő teljesítményt és lehetőségeket. A szoftvert egyrészt a gépet működtető programok, másrészt a számítógéppel való feldolgozásra előkészített adatok alkotják.

2. feladat

A számítógép részegységeinek összehangolt működtetése,
Erőforrások kihasználásának ütemezése,
A számítógép adatforgalmának lebonyolítása,
A kiadott parancsok értelmezése, végrehajtása,
Hiba esetén a hiba javításának megpróbálása, ha nem megy: hibajelzés,
Több felhasználó egyidejű munkájának megszervezése,
Több számítógép együttműködésének megvalósítása,
Adatvédelem, hozzáférési jogok ellenőrzése

3. feladat

A nyílt forráskód kifejezést általában olyan számítógépes programok esetén használjuk, melyeknek a forráskódja vagy közkinccs, vagy gyakoribb esetben a szerzői jogok tulajdonosa egy nyílt forráskódú licenc alatt terjeszti. Az ilyen licenc előírhatja azt, hogy a forráskódot a programmal együtt kell terjeszteni, és hogy az szabadon módosítható. A nyílt forráskódú licenc nem feltétlenül követeli meg azt, hogy a program, vagy a forráskódja ingyen és szabadon publikálásra is kerüljön (az interneten), noha a legtöbb nyílt forráskódú projekt ilyen.

4. feladat

A vírus olyan program, amely önmagát sokszorozítja. Terjedése érdekében egy számítógépen lemásolja magát vagy programokba és az operációs rendszer fájljaiba illetve be számítógépes kódot. A vírusok nem minden esetben okoznak kárt a fájlokban vagy a számítógépben, de általában befolyásolják a számítógép teljesítményét és stabilitását. Ahhoz, hogy egy vírus megfertőzhessen egy számítógépet vagy terjedhessen, általában valamit tennie kell, például meg kell nyitnia egy fertőzött e-mail mellékletet.

5. feladat

Logikai összeköttetéssel kapcsolatos rétegek

A viszonyréteg (session layer) – lehetővé teszi, hogy két számítógép felhasználói kapcsolatot létesítsen egymással. Jellemző feladata a logikai kapcsolat felépítése és bontása, párbeszéd szervezés. Elláthat szinkronizációs funkciót ellenőrzési pontok beépítésével.

A megjelenítési réteg (presentation layer) – az egyetlen, amelyik megváltoztathatja az üzenet tartalmát. Tömörítést, rejtjelezést, kódcserét (ASCII – EBCDIC) végezhet el.

Az alkalmazási réteg (application layer) – széles körben igényelt szolgáltatásokat tartalmaz. Ilyen alapvető igényt elégítenek ki például a file-okat tetszőleges gépek közötti másolását lehetővé tevő file transfer protokollok.

MUNKANYAG

ADATVÉDELEM

ESETFELVETÉS – MUNKAHELYZET

Munkahelyén azt a feladatot kapta, hogy vizsgálja felül a szoftverállományt és az adatvédelem állapotát.

A szoftvervizsgálat terjedjen ki a szoftverek típusára, eredetére, továbbá arra, hogy a felhasználásuk legális vagy illegális, és különösen a licencszerződésekre vonatkozóan

A vizsgálat célja kideríteni, hogy a szoftverek eredetiek vagy másoltak.

Az adatvédelem ellenőrzése, felülvizsgálata terjedjen ki az adatok védelem struktúrájára, megbízhatóságára és a módszerekre

Az adatvédelem módjára, eszközeire, biztonságára, megbízhatóságára, jogosultságokra

Jelen tananyag alapvető célja összefoglalni azokat a szoftver és adatvédelmi alapismereteket melyek alkalmazásához, a munkahelyi struktúrába, rendszerbe való alkalmazáskor, a megfogalmazott munkahelyzet megoldása során nélkülözhetetlenek.

SZAKMAI INFORMÁCIÓTARTALOM

ADATVÉDELEM

1. Adatvédelmi alapfogalmak

Az **adatvédelem** szűkebb értelemben a személyes jellegű adatokat védi attól, hogy illetéktelen személyek megismerjék, kiértékeljék, vagy megváltoztassák azokat.

A Magyar Köztársaságban mindenkit megillet a jó hírnévhez, a magánlakás sérthetlenségéhez, valamint a személyes adatok védelméhez való jog.

(Magyar Köztársaság Alkotmánya 59..)

Adatvédelem

Az adatvédelem szűkebb értelemben a személyes jellegű adatokat védi attól, hogy illetéktelen személyek megismerjék kiértékeljék vagy megváltoztassák azokat.

Adatbiztonság

Az adatbiztonság magában foglalja az adatok és a programok műszaki eredetű, vagy hanyagságból eredő vagy célzatos megváltoztatása ill. törlése ellen foganatosított összes védőintézkedést. Ide tartozik az illetéktelen hozzáféréssel szembeni biztonság is.

Az adatokra leselkedő veszélyek

A legfontosabb veszélyforrások a következők:

- illetéktelen hozzáférés,
- a számítógép, vagy az adathordozó meghibásodása, sérülése,
- vírusok,
- túlfeszültség, áramszünet

Illetéktelen hozzáférés

A számítógép tárolt adatokhoz sajnos azok is hozzáférhetnek, akikre pedig nem is tartoznak. Nem árt bizonyos óvintézkedéseket megtenni. (Felhasználói jogok, jelszavak használata.)

A jogilag tiszta szoftver előnyei

- A gyártók a programra garanciát vállalnak.
- Ha regisztráljuk a szoftvert, annak továbbfejlesztett változatához az új ár töredékért juthatunk hozzá.
- Az eredeti programhoz teljes dokumentáció jár.
- A vírusmentességet a gyártó garantálja.
- Nem kell tartanunk a szoftver-rendőrség ellenőrzésétől.

Adatvédelmi fogalmak

Adatvédelem

BSA (Business Software Alliance, magyarul Üzleti Szoftverszövetség):

A szervezet szerint a BSA „...a biztonságos és jog-tiszta digitális világ érdekében tevékenykedő, legjelentősebb világszervezet. A BSA feladata, hogy a fogyasztóknak a szoftvergazdálkodásról, a szerzői jogi védelemről, a biztonságról, a kereskedelemről, az e-kereskedelemről és az internettel kapcsolatos egyéb témakörökről adjon tájékoztatást...” A közhiedelemmel ellentétben a BSA NEM „szoftver-rendőrség”, azaz nincs semmilyen hatósági jogosítványa, ugyanakkor a rendőrséggel valósan együttműködik. Ennek oka, hogy tagjai gyakran vesznek részt házkutatásokon és bírósági eljárásokban kirendelt szakértőként; illetve a számukra gyanús cégek ellen névtelen bejelentést tesznek.

Illegális szoftverhasználat és következménye

A szoftver előnye, a nagyfokú reprodukciós képessége egyben legnagyobb hátránya is. A másolás egyszerű, így az illegális felhasználás, a szerzői jogok sérelme magas szintű. A szoftver illegális lemásolásakor, vagyis lopásakor – az igazi lopással ellentétben – nem keletkezik hiány, az eredeti példány megmarad. A szoftvernek ezt a tulajdonságát kihasználva, a számítástechnika térhódítását követően kialakult egy új, jövedelmező bűnözési forma, a szoftverkalózkodás. Az illegális szoftverhasználat – illegális programok terjesztése és felhasználása – mára világméretű problémává vált.

A nyílt forráskódú licenc olyan licenc, mely biztosítja a licencelt dolog – ami legtöbbször egy számítógépes program vagy szoftver – forráskódjának nyitottságát. Egy licencet általában akkor tekintünk nyíltnek, ha azt az Open Source Initiative jóváhagyta, a Nyílt forrás definíció alapján. A közkincként terjesztett programok (vagyis azok, melyeket nem korlátoz a szerzői jog) is megfelelnek a követelményeknek, amennyiben a teljes forráskód elérhető, és így jogosultak az OSI "service mark" (szolgáltatási védjegy) használatára.

2. Adatvédelmi alkalmazások

Adatok védelme

Az informatikai rendszerben működő alkalmazások, és a hozzájuk kapcsolódó adatok fenyegetettségét a legszélesebb körben a következőkkel lehet jellemezni:

- a bizalmasság elvesztése,
- a sértetlenség elvesztése,
- a hitelesség elvesztése,
- a rendelkezésre állás elvesztése,
- a funkcionalitás elvesztése.

A továbbiakban a fenti fogalmakat alapfenyegetettségeknek nevezzük. Az adatok bizalmassága, sértetlensége és hitelessége logikailag erősen kapcsolódik az informatikai rendszerben kezelt (feldolgozott, tárolt és továbbított) információk **(adatok) védelmének** fogalmköréhez és sok esetben egymáshoz is, mert például a bizalmasság sérülése együtt járhat a sértetlenség és/vagy a hitelesség sérülésével és viszont. A továbbiakban az információvédelem fogalmát abban az értelemben használjuk, hogy a bizalmasság, a sértetlenség és a hitelesség védelmét együttesen tartalmazza.

Informatikai rendszer teljes életciklusa

Az informatikai rendszer teljes életciklusában figyelembe kell venni a biztonsággal kapcsolatos szempontokat. Az életciklusra jellemző szakaszok az alábbiak:

- az informatikai rendszer tervezése;
- az informatikai rendszer fejlesztése;
- az informatikai rendszer bevezetése, illetve üzembe helyezése;
- az informatikai rendszer üzemeltetése, fenntartása;
- az informatikai rendszer megszüntetése, felszámolása vagy rekonstrukciója.

Információvédelem

az azonosítás és a hitelesítés folyamatának kialakítása,
a hozzáférés rendszerének felépítése
jogosultság kiosztás (alanyok eszközök meghatározása, attribútumok rögzítése, hozzárendelések – megengedő, illetve tiltó módszer a szigorodó követelményekre),
a hozzáférés-ellenőrzés rendszerének megvalósítása – jogosultság ellenőrzés,
a hitelesség garantálása
a sértetlenség garantálásának kiépítése,
a bizonyítékok rendszerének és folyamatának kialakítása.

Megbízható működés

a hibaáthidalás folyamatának kialakítása,
az újraindítási képesség megvalósítása,
a rendszer funkcionalitásának biztosítása.

4. Adatvédelem fogalma

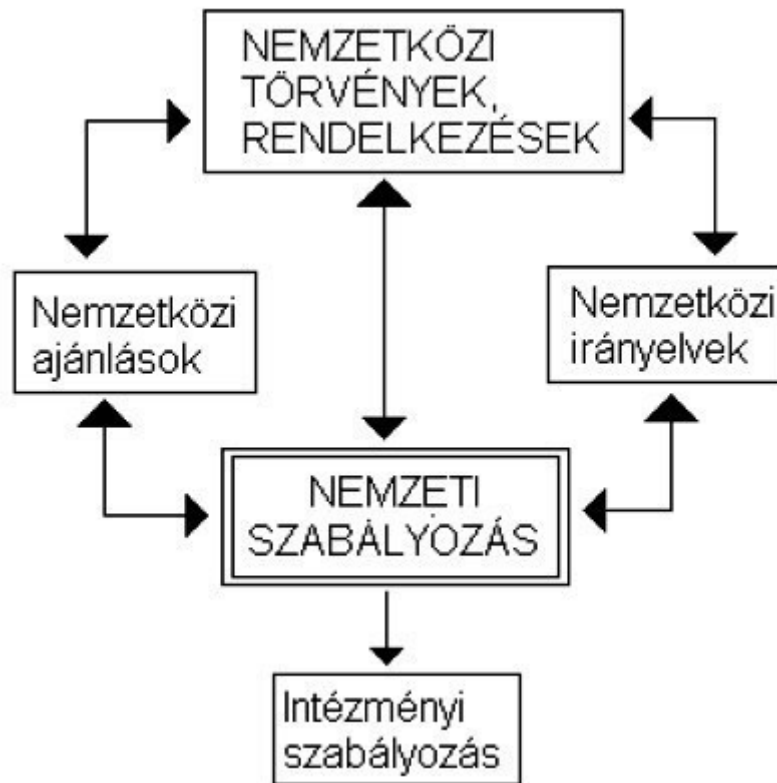
Az adatvédelem egy sokféleképpen definiálható fogalom. Talán ez az oka annak, hogy téves értelmezésekből adódóan gyakran keverik össze az adatbiztonsággal. Míg az adatbiztonság valamennyi adat különböző negatív hatások elleni védelmét, biztosítását jelenti, addig az adatvédelem tárgyát a személyes adatok képezik.

Feladata, hogy mindenki számára biztosítsa a saját adataival való szabad rendelkezést, így az adatokon keresztül az érintett személyt védi. Ezt különböző törvények, jogszabályok, és ajánlások segítségével oldja meg.

A védelem akkor megfelelő, ha általa a személyes adatok a magántulajdonnal közel azonos elbírálás alá esnek, azaz mindenki szabadon választhatja meg, hogy a saját adatait mely személyeknek és szervezeteknek adja át, ezáltal lehetővé teszi számukra azok kezelését. Valamint a jogszabályoknak biztosítani kell azt is, hogy ezek az adatkezelők a tudomásukra jutott személyes adatokat harmadik személynek nem adhatják tovább az érintett személy beleegyezése nélkül.

Ezt a védelmet nem szabad egy-egy ország területére korlátozni, hanem biztosítani kell a jogszabályok folytonosságát az országhatárokon kívül is.

AZ ADATOK VÉDELME



4. ábra. Adatvédelmi szabályozás

3. Fogalmak pontos meghatározása

Személyes adat: meghatározott személlyel kapcsolatba hozható adat, amelyből az érintettre vonatkozó következtetéseket lehet levonni (egy személy akkor tekinthető azonosíthatónak, ha őt közvetlenül, vagy közvetve – név, azonosító jel, illetve – fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet);

Különleges adat: faji eredetre, nemzeti és etnikai hovatartozásra, politikai véleményre, világnézetre, szervezeti tagságra, egészségi állapotra, kóros szenvedélyre és szexuális véleményre vonatkozó adat. Valamint ide sorolhatók még a bűnügyi személyes adatok;

Közérdekű adat: közfeladatot ellátó szerv vagy személy kezelésében lévő adat,

Közérdekből nyilvános adat: minden olyan adat, melynek nyilvánosságra hozatalát a közérdekében, törvény rendeli el;

Hozzájárulás: az érintett személy önkéntes és határozott nyilatkozata, amellyel beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez;

Adatkezelő: adatkezelés fogalma alá tartozó tevékenységeket végző személy (lehet természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet);

Adatkezelés: alkalmazott eljárástól függetlenül a személyes adatokon végzett bármely művelet, vagy műveletek összessége, úgymint gyűjtés, felvétel, rögzítés, rendszerezés és tárolás, megváltoztatás, felhasználás, összekapcsolás, zárolás és törlés; (Adatkezelésnek számít a továbbítás és a nyilvánosságra hozatal is.)

Adattovábbítás: meghatározott harmadik személy az adatokhoz való hozzáféréseinek engedélyezése;

Nyilvánosságra hozatal: az adat mindenki számára hozzáférhetővé tétele;

Adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy azok visszaállítása nem lehetséges;

Adatzárolás: az adatok továbbításának, megismerésének, nyilvánosságra hozatalának, átalakításának, megváltoztatásának, megsemmisítésének, törlésének, összekapcsolásának és felhasználásának végleges vagy ideiglenes megakadályozása;

Adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (függetlenül az alkalmazott eszköztől és módszertől);

Adatfeldolgozó: az adatkezelő megbízásából az adatfeldolgozást végző személy.

4. Biztonsági alapfunkciók listája a következő

Azonosítás és hitelesítés,
Hozzáférés-vezérlés,
Jogosultság ellenőrzés, elszámoltathatóság,
Biztonsági vizsgálat,
Biztonságos adatcsere,
Biztonságos kezelési funkciók,
A rendelkezésre állás biztosítása,
A biztonságos rendszer-visszaállítás biztosítása,
A funkcionalitás biztosítása.

5. Hozzáférés-vezérlés

Hozzáférési jogok:

írás,
olvasás,
programvégrehajtás.

A hozzáférési jogok megadhatók:

egyedi fájl tulajdonosnak,
csoport fájl tulajdonosoknak,
"mindenki más" fájl tulajdonosoknak.

A jogok érvényesülésének prioritási sorrendje.

A rendszer objektumaihoz (fájlok, eszközök, processzek közötti kommunikációs csatornák) egyedi, illetve csoport tulajdonosok rendelődnek az objektum létesítésekor. A hozzáférés-vezérlés a szubjektumokhoz (felhasználók, processzek) rendelt jogok és az objektumokhoz rendelt tulajdonosok és jogaik összevetése alapján történik.

Az érintett személy jogai és érvényesítésük

Az információs önrendelkezési jog mellett biztosítani kell az állampolgároknak, hogy tudomást szerezhessenek arról, hogy személyes adataikat ki, hol, milyen célból kezeli, és azokhoz milyen forrásból jutott hozzá. Így minden adatkezelőnek az általa kezelt adatok alanyaival szemben tájékoztatási kötelezettsége van.

Informatikai biztonság

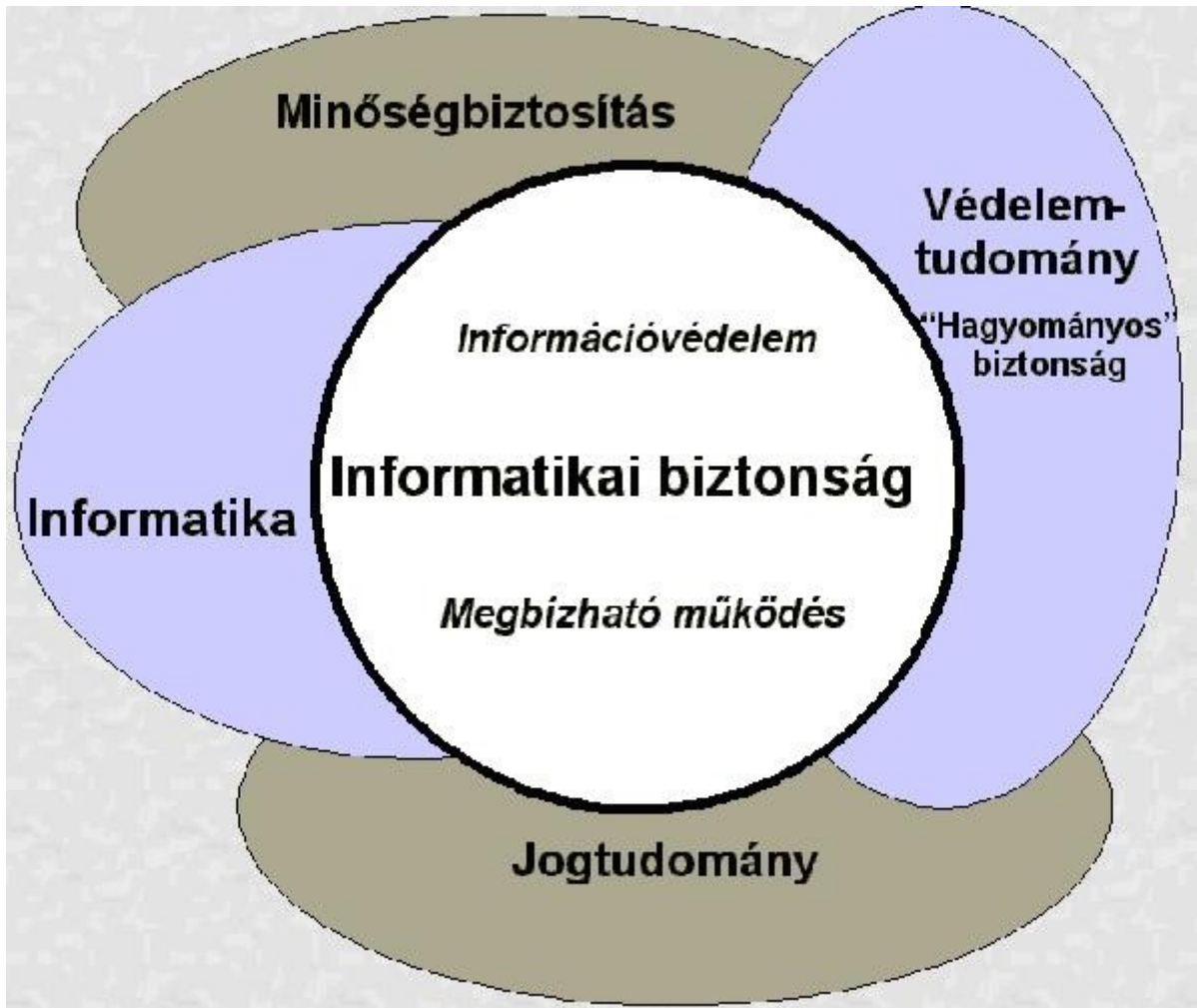
Az informatikai biztonság az informatikai rendszerek által az ott tárolt adatok védelmét jelenti, ez a védelem két alapterületre osztható
Egyrészt biztosítani kell az adatok rendelkezésre állását, azaz a rendszer működéséhez szükséges erőforrásokat és a tárolt adatok fizikai sérülés elleni védelmét. Ezt nevezzük a továbbiakban megbízható működésnek.
Másképp az adatok által hordozott információk sérthetlenségnek, hitelességének és bizalmasságának elvesztését kell megakadályozni, ezt nevezzük információvédelemnek.



5. ábra. Adat védelme

6. Az informatikai biztonság

Az informatikai biztonsággal kapcsolatban gyakran említésre kerülnek a hagyományos biztonság, a minőségbiztosítás, az informatikai rendszerek auditálása, jogtudomány.



6. ábra. Informatikai biztonság kapcsolata

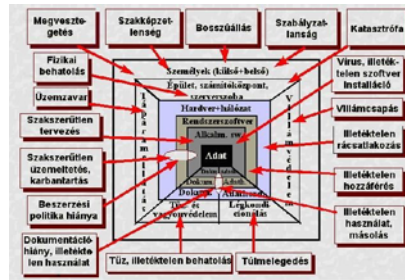
A védelemtudomány elemei az informatikai rendszerek védelmében "hagyományos biztonság" jelennek meg, míg az adatminőség biztosítása az adatok sértetlenségének, hitelességének, rendelkezésre állásának és funkcionalitásának biztosítása területén jelentkezik.

7. AZ INFORMATIKAI BIZTONSÁG

Informatikai biztonság

adatvédelem,
 adatbiztonság,
 információbiztonság,
 információvédelem,
 informatikai biztonság,
 megbízható működés, stb.

Jellemző fenyegetések



7. ábra. Az adat jellemző fenyegetettségei

Az informatikai biztonságot úgy határozhatjuk meg, hogy az az állapot amikor az informatikai rendszer védelme a rendszer által kezelt adatok bizalmassága, hitelessége, sértetlensége és rendelkezésre állása, illetve a rendszer elemek rendelkezésre állása és funkcionalitása szempontjából – zárt, teljes körű, folyamatos és a kockázatokkal arányos.

Az informatikai biztonság két alapterületet foglal magába: **Információvédelem**, amely az adatok által hordozott információk sértetlenségének, hitelességének és bizalmasságának elvesztését hivatott megakadályozni. **Az informatikai rendszer** megbízható működése területét, amely az adatok rendelkezésre állását és a hozzájuk kapcsolódó alkalmazói rendszerek funkcionalitását hivatott biztosítani.

Az adatvédelmi nyilvántartás tartalmazza:

- az adatkezelés célját
- az adatok fajtáját és kezelésük jogalapját
- az érintettek körét
- az adatok forrását
- a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját
- az egyes adatfajták törlési határidejét
- az adatkezelő nevét és címét (székhelyét), valamint a tényleges adatkezelés helyét

8. Információs önrendelkezési jog védelme – magyar szabályozás

A Polgári Törvénykönyv 83. §-ának (1) bekezdése főszabályként azt mondja ki, hogy a számítógéppel vagy más módon történő adatkezelés és adatfeldolgozás a személyhez fűződő jogokat nem sértheti.

A szakasz (2) bekezdése szerint a nyilvántartott adatokról tájékoztatást – az érintett személyen kívül – csak az arra jogosult szervezetnek vagy személynek lehet adni. A (3) bekezdés értelmében pedig, ha a nyilvántartásban szereplő valamely tény vagy adat nem felel meg a valóságnak, az érintett személy a valótlan tény vagy adat helyesbítését külön jogszabályban meghatározott módon követelheti.

A személyes adatok védelméhez való jogot az Alkotmány 59. § (1) bekezdése alapvető emberi jogként deklarálja. Az Alkotmánybíróság egy alapvető jelentőségű határozatában a személyes adatok védelméhez való jogot nem hagyományos védelmi jogként értelmezte, hanem annak aktív oldalát is figyelembe véve, információs önrendelkezési jogként.

Az Alkotmány 59. §-ában biztosított személyes adatok védelméhez való jognak eszerint az a tartalma, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról. Személyes adatot felvenni és felhasználni tehát általában csakis az érintett beleegyezésével szabad; mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát.

Az információs önrendelkezési jog gyakorlásának feltétele és egyben legfontosabb garanciája a célhoz kötöttség. Ez azt jelenti, hogy személyes adatot feldolgozni csak pontosan meghatározott és jogszerű célra szabad. A célhoz kötöttségből következik, hogy a meghatározott cél nélküli, „készletre”, előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés és -tárolás alkotmányellenes. A másik alapvető garancia az adattovábbítás és az adatok nyilvánosságra hozásának korlátozása.

Az Alkotmánybíróság szerint személyes adatot az érintetten és az eredeti adatfeldolgozón kívüli harmadik személy számára hozzáférhetővé kell tenni – s eszerint adatfeldolgozási rendszereket egymással összekapcsolni – csak akkor szabad, ha minden egyes adat vonatkozásában az adattovábbítást megengedő összes feltétel teljesült. Ez tehát azt is jelenti, hogy az adattovábbítás címzettjének (az adatkérőnek) vagy konkrét törvényi felhatalmazással kell rendelkeznie ahhoz, hogy a továbbított adatokat feldolgozhassa, vagy az érintett beleegyezését előzetesen meg kell szereznie. 117/2004. (IV. 28.) Korm. rendelet

A szerzői jogról szóló 1999. évi LXXVI. törvény 38. §-ának (5) bekezdésében szabályozott szabad felhasználás esetében a nyilvánosság egyes tagjaihoz való közvetítés és a számukra történő hozzáférhetővé tétel módjának és feltételeinek meghatározásáról.

a) olyan biztonságos műszaki megoldást alkalmaz, amely megakadályozza a gyűjtemény hozzáférhetővé tett elemeinek módosítását, többszörözését (bármely hordozón való rögzítését), illetve az igénybe vevőként meghatározott személyek körén kívülre irányuló közvetítését, ideértve a nyilvánosság számára történő hozzáférhetővé tételt is;

(3) A 2. § (1) bekezdésének a) pontja és a 3. § (2) bekezdésének a) pontja alkalmazásában biztonságosnak kell tekinteni azt a műszaki megoldást, amely megfelel a külön jogszabályban meghatározott informatikai biztonsági tanúsítvány kiadásához szükséges feltételeknek.

9.A Windows rendszer a számítógépen található adatok biztonsági mentésére

Ha biztonsági másolatot készít a saját adatairól, ezt egyszerű másolással és beillesztéssel megteheti. Vagy a Windows Vista, illetve a Windows XP operációs rendszer használata esetén a biztonsági mentésre szolgáló eszköz használatával néhány kattintással elvégezheti ezt a műveletet.

Miután eldöntötte, melyik fájlokról készít biztonsági másolatot, és hol tárolja ezeket, a cikkben leírt pontokat követve biztonsági másolatot készíthet a fontos adatokról.

Biztonsági másolat és visszaállítás központ. Automatikus biztonsági mentés, amely csak a fájlokról és adatokról készít biztonsági másolatot vagy Komplet PC biztonsági mentés, amely a számítógépen található összes objektumról biztonsági másolatot készít, beleértve az operációs rendszert és az alkalmazásokat is.

Biztonsági másolat és visszaállítás központ elérése:

1. Kattintson a **Start gombra**, majd mutasson a **Vezérlőpult parancsra**.
2. Kattintson a **Rendszer és karbantartás** lehetőségre, majd válassza a **Biztonsági másolat készítése** a számítógépről parancsra.

10. A szerzői jog fogalma

A szerzői jog a szellemi tulajdonjog azon területe, amely a szerzői művek, azaz bármely, az alkotó szellemi tevékenységből fakadó, az irodalom, a tudomány és a művészet területén létrehozott egyéni, eredeti alkotás – függetlenül attól, hogy az adott alkotás milyen műtípusban testesül meg – szerzőinek és az ún. szerzői joghoz kapcsolódó jogok jogosultjainak védelmét szabályozza.

A szerzői joggal kapcsolatos alapvető szabályokat a szerzői jogról szóló 1999. évi LXXVI. törvény (Sztj.) tartalmazza, de számos egyéb jogszabály 156/1999. (XI. 3.) Korm. rendelet a Szerzői Jogi Szakértő Testület szervezetéről és működéséről; 158/2000. (IX. 13.) Korm. Rendelet, a reprográfiára szolgáló készülékek körének meghatározásáról; 16/1999. (XI. 18.) NKÖM rendelet a szerzői és a szomszédos jogok közös kezelését végző egyesületek nyilvántartásának szabályairól is rendelkezik szerzői jogot érintő kérdésekről.

A SZOFTVER SZERZŐI JOGVÉDELEM TÁRGYA

A szoftver szintén tárgya a szerzői jognak akár forráskódban, akár tárgykódban vagy bármilyen más formában rögzített minden fajtája, A szoftverhez annak dokumentációja is hozzáértendő a szerzői jogi védelemben. A szoftver keretein belül védett a felhasználói program és az operációs rendszer is a szerzői jog rendszerében.

Személyhez fűződő jogok

A személyhez fűződő jogokat csak a szerző gyakorolhatja. Ezek a következők:

A mű nyilvánosságra hozatalához való jog

E jog alapján a szerző kizárólagosan jogosult eldönteni, hogy művét nyilvánosságra hozza-e vagy sem.

A névjog

A szerzőt minden körülmények között megilleti az a jog, hogy nevét a művének bármely felhasználása esetén feltüntessék, természetesen attól függően, hogy mi a felhasználás konkrét módja.

A mű egységéhez, torzításmentességéhez fűződő jog

E joga alapján a szerző felléphet bárkivel szemben, aki olyan változtatásokat eszközöl a művén, ami az ő becsületére vagy hírnevére sérelmes.

TANULÁSIRÁNYÍTÓ

1.feladat

Adatvédelem témakörében látogassanak el a www.magyarország.hu honlapra vagy a témakörrel kapcsolatban, a keresőben keressenek jogszabályokat.

2.feladat

Beszélgessenek, vitassák meg a gyakorlatban megvalósítható, alkalmazott szoftver és adatvédelmet s azok hatékonyságát.

3.feladat

Számítógépen mutassanak egymásnak szoftver és adatvédelmi beállításokat, példákat.

4.feladat

Fogalalkozásokra tervezzenek időt.

ÖNELLENŐRZŐ FELADATOK**1. feladat**

Fogalmazza meg az adatvédelem fogalmát

2. feladat

Sorolja fel a hozzáférési jogokat.

3. feladat

Írja le a személyes adatok védelméhez való jogot

4. feladat

Fogalmazza meg az Alkotmány 59. §-ában biztosított személyes adatok védelméhez való jogot.

5. feladat

Írja le, hogy az adatvédelmi nyilvántartás tartalmazza?

MEGOLDÁSOK

1. feladat

Az adatvédelem egy sokféleképpen definiálható fogalom. Talán ez az oka annak, hogy téves értelmezésekből adódóan gyakran keverik össze az adatbiztonsággal. Míg az adatbiztonság valamennyi adat különböző negatív hatások elleni védelmét, biztosítását jelenti, addig az adatvédelem tárgyát a személyes adatok képezik.

2. feladat

írás,
olvasás,
programvégrehajtás.

A hozzáférési jogok megadhatók:

egyedi fájl tulajdonosnak,
csoport fájl tulajdonosoknak,
"mindenki más" fájl tulajdonosoknak.

Ez egyben a jogok érvényesülésének prioritási sorrendje.

A rendszer objektumaihoz (fájlok, eszközök, processzek közötti kommunikációs csatornák) egyedi, illetve csoport tulajdonosok rendelődnek az objektum létesítésekor.

A hozzáférés-vezérlés a szubjektumokhoz (felhasználók, processzek) rendelt jogok és az objektumokhoz rendelt tulajdonosok és jogaik összevetése alapján történik.

3. feladat

A személyes adatok védelméhez való jogot az Alkotmány 59. § (1) bekezdése alapvető emberi jogként deklarálja. Az Alkotmánybíróság egy alapvető jelentőségű határozatában a személyes adatok védelméhez való jogot nem hagyományos védelmi jogként értelmezte, hanem annak aktív oldalát is figyelembe véve, információs önrendelkezési jogként.

4. feladat

Az Alkotmány 59. §-ában biztosított személyes adatok védelméhez való jognak eszerint az a tartalma, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról. Személyes adatot felvenni és felhasználni tehát általában csakis az érintett beleegyezésével szabad; mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát.

5. feladat

az adatkezelés célját
az adatok fajtáját és kezelésük jogalapját

az érintettek körét
az adatok forrását
a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját
az egyes adatfajták törlési határidejét
az adatkezelő nevét és címét(székhelyét), valamint a tényleges adatkezelés helyét

MUNKANYELV

IRODALOMJEGYZÉK

FELHASZNÁLT IRODALOM

<http://www.szoftver.hu> 2010-08-26

<http://www.jogforum.hu> 2010-08-17

117/2004. (IV. 28.) Korm. Rendelet.

A Polgári Törvénykönyv

<http://www.szerzoijog.net/SZOFTVER-SZERZOI-JOG/SZOFTVER-SZERZOI-JOG.php>

AJÁNLOTT IRODALOM

Hajós Ferenc-Eperjesi Zsuzsanna Jogi és vállalkozási ismeretek

MUNKANYAG

A(z) 1180-06 modul 013-as szakmai tankönyvi tartalomeleme felhasználható az alábbi szakképesítésekhez:

A szakképesítés OKJ azonosító száma:	A szakképesítés megnevezése
55 481 01 0000 00 00	Általános rendszergazda
55 481 02 0000 00 00	Informatikai statisztikus és gazdasági tervező
55 481 03 0000 00 00	Telekommunikációs asszisztens
55 481 04 0000 00 00	Web-programozó
55 810 01 0010 55 01	Energetikai mérnökasszisztens
55 810 01 0010 55 02	Építettkörnyezetmérnök-asszisztens
55 810 01 0010 55 03	Faipari terméktervező
55 810 01 0010 55 04	Faipari termelészservező
55 810 01 0010 55 05	Gépipari mérnökasszisztens
55 810 01 0010 55 06	Hálózati informatikus
55 810 01 0010 55 07	Kohómérnök asszisztens
55 810 01 0010 55 08	Könnyűipari mérnökasszisztens
55 810 01 0010 55 09	Mechatronikai mérnökasszisztens
55 810 01 0010 55 10	Műszaki informatikai mérnökasszisztens
55 810 01 0010 55 11	Vegyész mérnökasszisztens
55 810 01 0010 55 12	Vegyipari gépészmérnök-asszisztens
55 810 01 0010 55 13	Villamosmérnök-asszisztens

A szakmai tankönyvi tartalomelem feldolgozásához ajánlott óraszám:

15 óra

MUNKANYAG

A kiadvány az Új Magyarország Fejlesztési Terv
TÁMOP 2.2.1 08/1-2008-0002 „A képzés minőségének és tartalmának
fejlesztése” keretében készült.

A projekt az Európai Unió támogatásával, az Európai Szociális Alap
társfinanszírozásával valósul meg.

Kiadja a Nemzeti Szakképzési és Felnőttképzési Intézet
1085 Budapest, Baross u. 52.
Telefon: (1) 210-1065, Fax: (1) 210-1063

Felelős kiadó:
Nagy László főigazgató