„TÁMOP-4.1.2/A/1-11/1-2011-0015 Egészségügyi Ügyvitelszervező Szakirány: Tartalomfejlesztés és Elektronikus Tananyagfejlesztés a BSc képzés keretében”

Kisirodai hálózatok

e-Book

Zrinyi Miklós

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

Tartalom

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

1 Bevezető

Ebben a tananyagban a kis irodai hálózatok kialakításának alapjait, valamint a biztonságos üzemeltetéséhez szükséges ismereteket mutatjuk be. Ma már a legkisebb vállalkozások sem tudnak hatékonyan működni megfelelő informatikai rendszer nélkül. Gondoljunk csak bele, ma már egy egszerű adóbevallás beküldése is megköveteli az internetes kommunikációt. A kisebb vállalkozások nem engedhetik meg maguknak egy bonyolult és költséges informatikai rendszer üzemeltetését.

A tananyag első felében átnézzük azokat az ismereteket amelyeket már korábban megtanultál: megnézzük, hogy hogyan folyik a kommunikáció az interneten.

Áttekintjük, mi az a rétegzett hálózati architektúra. Összehsonlítjuk az OSI és a TCP/IP modelleket. Röviden áttekintünk néhány protokollt, és megnézzük hogyan néz ki a címzés folyamata az internetes kommunikáció során.

A tananyagban bemutatjuk azokat az eszközöket, amelyeket egy kis irodában minden nap használunk. Megnézzük, hogy mikor célszerű vezetékes vagy esetleg vezetéknélküli megoldásokban gondolkodni egy kis irodai hálózat kialakítása során. Áttekinjük, hogy hogyan kapcsható egy kis irodai hálózat az internetre.

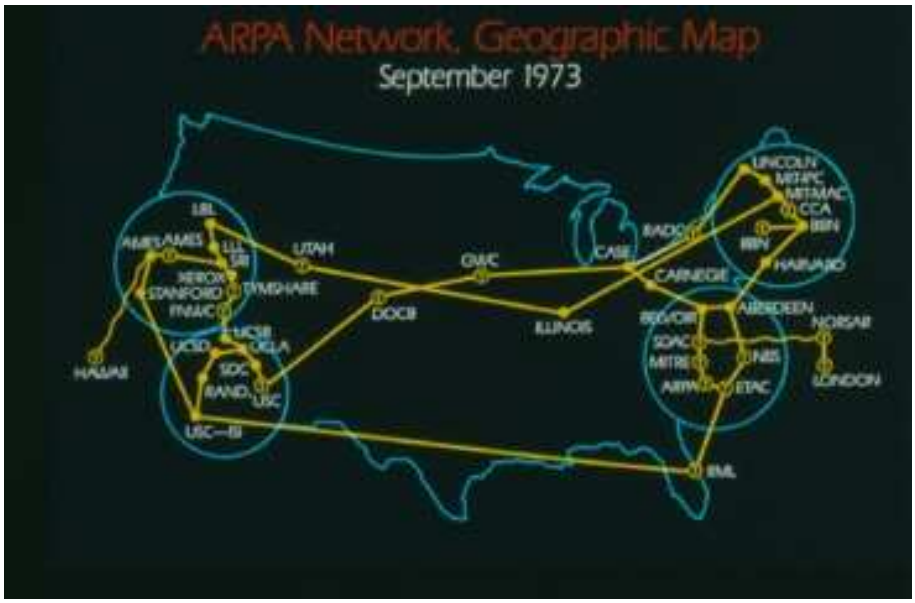
Azonban az internetre csatlakozó kis irodai hálózat, mindenféle rosszindulatú támadásnak ki lehetsz téve. Az ilyen támadások ellen fel kell készíteni a hálózatot. Minden kisvállalkozás rendelkezi olyan információkkal, amiket nem osztana meg másokkal.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

1.1 Számítógép hálózatok története, fejlődésének főbb lépései

Az Internet története az 1960-as évekre nyúlik vissza. 1969-ben az USA Hadügyminisztériuma telefonvonalon egy kísérleti jellegű, csomagkapcsolt hálózatot hozott létre (ARPAnet: Advanced Research Projects Agency Network). A hálózathoz egyre többen kapcsolódtak hozzá (pl. oktatási és kutatási intézmények). Az ARPAnet mellett létrehozták a hasonló technológiával működő MILnet (Military Network) hálózatot, és 1983-ban a két hálózatot összekapcsolták.



1.1. ábra Az ARPANET 1973 szeptemberében

Az ARPANET-hez ezután több hálózat is hozzákapcsolódott; pl. a MInet (a MILnet európai megfelelője), a SATnet és WIDEBAND (műholdas hálózatok), az NFSnet (National Science Foundation Network), a BITnet (Because It's Time Network), a USEnet, stb. Így alakult ki az, amit ma Internet néven ismerünk. Az 1990-es években

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

már a nagy számítógépes kereskedelmi szolgáltató központok (CompuServe, America Online, stb.) is elérhetőek lettek az Interneten keresztül és az üzleti alkalmazások köre azóta is rohamosan bővül. Jelenleg több tízezer különböző számítógépes hálózat érhető el az Interneten, kiszolgálva több tízmillió felhasználót. Az Internet az intézményeken belüli információ szervezésére is hatással van: kialakult az intranet, az Internet technológiáját használó vállalati információs rendszer.

Jelenleg Európát és Amerikát az óceánon át üvegkábelek kötik össze, és műholdon keresztül is lehetséges az adatok átvitele. A jövő lehetséges perspektívái közé tartozik az informatikai, hírközlő, telekommunikációs és szórakoztató iparágak összefonódása és az Internet hálózat egységes kommunikációs közegként történő használata (un. ICE age: Information - Communication - Entertainment). A nagy adatátviteli sebességet (un. sávszélességet) igénylő multimédiás alkalmazások új technológiai megoldások kifejlesztését igénylik, amelyek biztosítják a multimédia információk (pl. hangok, mozgóképek) folyamatos átvitelét, azaz pl. garantálják az átvitelhez szükséges minimális sávszélességet.

1.2 Mi a kis iroda hálózat?

A kis irodai vagy SOHO (Small Office Home Office) hálózat a helyi hálózatok egy fajtája amely a kis irodákban való használatra terveztek.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

1.2. ábra Kis irodai hálózat tipikus felépítése

Helyi hálózatokra jellemzően a kis irodai hálózatokra mind vezetékes mind vezeték nélküli módon kapcsolódnak a számítógépek. Mivel üzleti hálózatról van szó a hálózat szokásos elemi továbbá még a nyomtatók, ritkábban IP telefonok és faxok. A hálózatra kapcsolódó gépek száma általában egy és tíz között van. Az 1.2. ábrán egy tipikus kis irodai hálózat látható.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

2 Az internetes kommunikáció alapjai

2.1 A rétegzett hálózati architektúra

A korszerű számítógép-hálózatok tervezését szigorúan strukturált módon végzik, ami azt jelenti, hogy a hálózat egymásra épülő részeit rétegekbe (layer) vagy más néven szintekbe (level) szervezik. Számuk, nevük, tartalmuk, funkciójuk minden hálózaton más és más. A rétegek csak a közvetlenül alattuk, illetve felettük lévő réteggel tudják tartani a kapcsolatot egy réteginterfész-en (hálózati kártya) keresztül.

Könnyebb érthetőség kedvéért nézzünk meg egy mindennapi rétegzett kommunikációt (2.1. ábra).

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

2.1. ábra Rétegzett kommunikáció

Ahogy az ábra mutatja a kommunikáció mindkét oldalán különböző szintek vannak. Ezek a szintek a másik oldal ugyanezen szintjével kommunikálnak, miközben az alattuk lévő szint szolgáltatására támaszkodnak és a felettük lévőnek szolgáltatást nyújtanak.

A szintek közti kommunikáció szabályait az ábra közepén láthatjuk. Ezeket protokollnak nevezzük.

Tegyük fel, hogy Indonézia minisztere egy gesztust szeretne küldeni a kenyai miniszternek. Ezt kifejti a tanácsadójának, aki megfogalmazza az üzenetet és megkéri a fordítót, hogy fordítsa le. Mikor a fordító elkészül a fordítással azt a titkár legépeli. A gépelt levelet leküldi a postázóba, ahol borítékba teszik, majd a postában bélyeget

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

tesznek rá, végül postazsákba helyezik és elszállítják. A fogadói oldalon ez a folyamat visszafelé játszódik le, ahogy az ábra is mutatja.

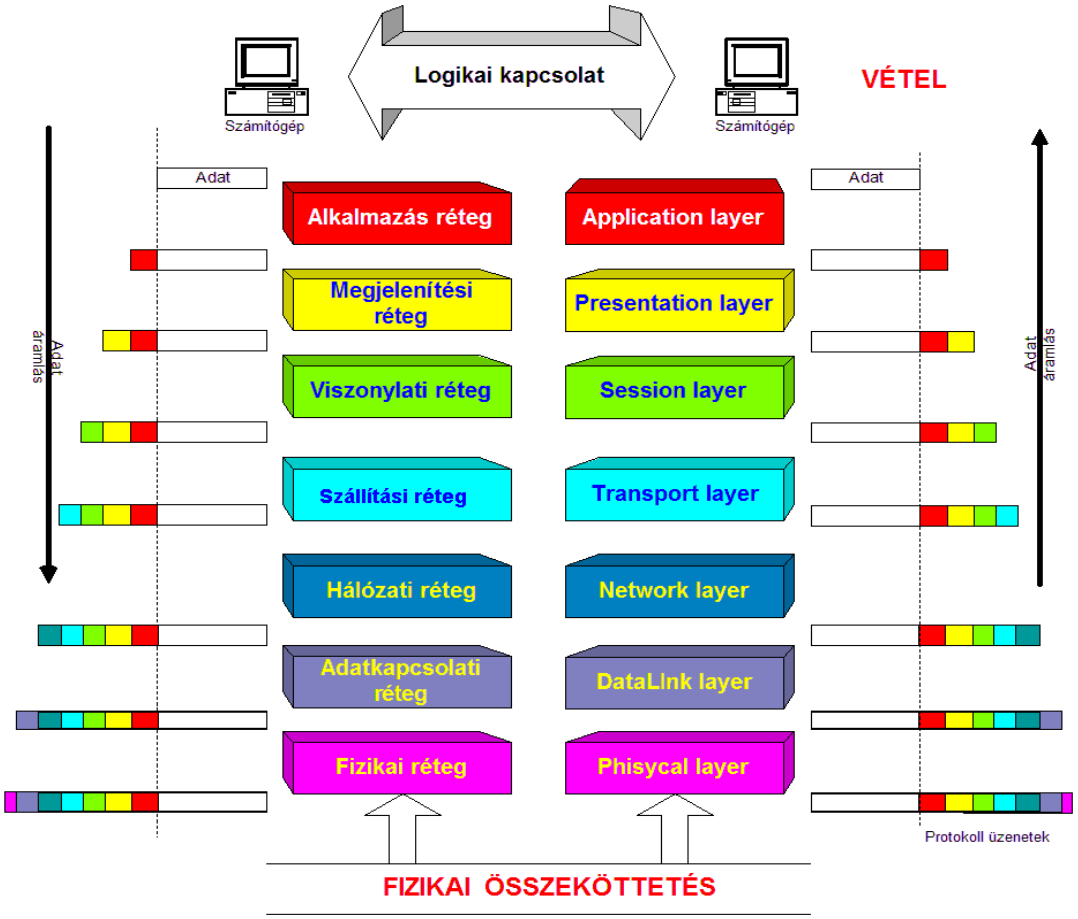
A fenti folyamatban bemutatott kommunikációhoz hasonlóan, a számítógép hálózatok esetén a különböző munkaállomásokon lévő azonos rétegek egymással beszélgetnek, informálják egymást az aktuális adatcsomag paramétereiről (pl.: adathossz, csomag sorszáma stb.). Ezek az információk fejléc formájában hozzácsatolódnak az adathoz, amikor az érintett rétegen halad keresztül. Lejutva a következő rétegbe szintén kap egy információs fejlécet, ennek megfelelően mire az adat a fizikai réteget elhagyja, már valójában jóval nagyobb, mint amikor az elindult. A vevő oldalon a rétegek lecsatolják az információkat, ennek alapján ellenőrzik az adatcsomagokat, és amennyiben hibátlannak bizonyultak, akkor a "megcsonkított" adatcsomagok a következő rétegnek adódnak át immár fölfelé.

2.2 OSI és TCP/IP modell

Az OSI modellje a különböző protokollok által nyújtott funkciókat egymásra épülő rétegekbe sorolja. Minden réteg csak és kizárólag az alsóbb rétegek által nyújtott funkciókra támaszkodhat, és az általa megvalósított funkciókat pedig csak felette lévő réteg számára nyújthatja. A rendszert, amelyben a protokollok viselkedését az egymásra épülő rétegek valósítják meg, gyakran nevezik 'protokoll veremnek' vagy 'veremnek'. A protokoll verem mind hardver szinten, mind pedig szoftveresen is megvalósítható, vagy a két megoldás keverékeként is. Tipikusan csak az alsóbb rétegek azok, amelyeket hardver szinten (is) megvalósítanak, míg a felsőbb rétegek szoftveresen kerülnek megvalósításra.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.



2.1. ábra Az OSI modell

Ez az OSI modell alapvetően meghatározó volt a számítástechnika és hálózatokkal foglalkozó ipar számára. A legfontosabb eredmény az volt, hogy olyan specifikációkat határoztak meg, amelyek pontosan leírták, hogyan léphet egy réteg kapcsolatba egy másik réteggel. Ez azt jelenti a gyakorlatban, hogy egy gyártó által írt réteg programja együtt tud működni egy másik gyártó által készített programmal (feltéve, hogy az előírásokat mindketten pontosan betartották).

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Fizikai réteg

Az OSI modell alján helyezkedik el a fizikai réteg, amely a hálózat fizikai jellemzőivel áll kapcsolatban: milyen kábelek és csatlakozók használhatóak, a kábelek milyen hosszúak lehetnek stb.

A fizikai réteg másik aspektusa a hálózaton továbbított elektronikus jelek leírása, azonban ezeknek a jeleknek a jelentésével nem foglalkozik, csak pl. a logikai 1 és 0 szintjének meghatározására szorítkozik.

A fizikai réteg eszközei közül megemlíthetjük pl. a repeater-t (jelismétlő) és a hálózati csatolókártyát. Az előbbi eszközt akkor használjuk, ha a fizikai réteg által megadott hossznál hosszabb kábelt kívánunk használni a hálózat kiterjesztése érdekében. Működése során a bemenetére érkező jeleket a repeater minden vizsgálat nélkül továbbítja a kimenetére.

Adatkapcsolati réteg

Az adatkapcsolati réteg elsődleges feladata, hogy a hálózat csomópontjai között hibamentes átvitelt biztosítson illetve az adatkeretek kezelése.

Míg a fizikai réteg csak az egyes jelekkel (0,1) foglalkozott, addig az adatkapcsolati réteg a jelek sorozatát ún. adatkeretekben vizsgálja. Az adatkeretek többnyire nx100 byte hosszúságúak. A küldő gép adatkapcsolati rétege a keret tartalmát felhasználva elvégez egy számítást az adatkereten, melynek eredményét hozzácsatolja a kerethez.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

A fogadó gép adatkapcsolati rétege megismétli ezt a műveletet és a kapott eredményt összehasonlítja a kerethez csatolt értékkel, ezzel biztosítva a keretek sérülésmentességének ellenőrzését. Ha a keret sérülésmentes, akkor a fogadó gép adatkapcsolati rétege küld egy ún. nyugtajelet a küldő gép adatkapcsolati rétegének.

Az adatkapcsolati réteg szintjén minden egyes hálózati eszköz egyedi azonosítóval rendelkezik, amelyet az eszköz gyártása során megváltoztathatatlanul rendelnek az eszközhöz. Ez az azonosító az ún. MAC (Media Access Controll).

A MAC magyar fordítása rendszerint Fizikai cím. Ha a Sart/Futtatás-ra klikkelünk, majd a megjelenő ablakba beírjuk a cmd parancsot, a karakteres felületű parancssori ablakban az ipconfig /all parancs kiadásával megjeleníthetjük gépünk bizonyos hálózati adatait.

Hálózati réteg

A hálózati réteg végzi a számítógépes hálózatokban a számítógépek közötti kommunikáció során az adatok útvonalának megválasztását (természetesen ez csak akkor lehetséges, ha több útvonal is rendelkezésre áll az adatok továbbítására). Az itt alkalmazott protokoll feladata tehát az útválasztás és a logikai címzés.

Ahogy az előző fejezetben már említettük, a hálózati eszközök rendelkeznek egy olyan azonosítóval, amelyet az előállításuk során rendeltek hozzá az eszközhöz és amelyet nem tudunk megváltoztatni (MAC). Ha az adatokat többféle úton (esetleg különböző típusú hálózatokon) kell továbbítani, akkor a MAC alapján ez nem lehetséges, mert a MAC nem tartalmaz információt arról, hogy az adott eszköz melyik hálózatban található.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Ha olyan címzési módszert akarunk használni, ahol az eszköz azonosítója információt szolgáltat arról is, hogy az adott eszköz melyik hálózatban helyezkedik el, illetve amelyeknél mi határozhatjuk meg az eszközök azonosítására szolgáló címet, akkor a logikai címzést kell használnunk.

A logikai címzést a hálózati réteg protokolljaival valósíthatjuk meg, (ilyen pl. az IP (Internet Protocol), amelyet rendszerint párban használnak a TCP -vel (Transmission Control Protocol), ezekről részletesebben majd a későbbiekben beszélünk), azaz a hálózati protokoll feladata, hogy a MAC azonosítókhoz hozzárendeljék a megfelelő logikai címet, amely alapján már azonosítható nem csak az eszköz, de az a hálózat is, amelyben az eszköz található.

Szállítási réteg

A szállítási réteg azért felel, hogy az adatcsomagok megbízhatóan és hibamentesen eljussanak az egyik számítógéptől a másikig. Ezt úgy teszi, hogy kapcsolatot teremt a hálózati eszközök között, nyugtázza a csomagok kézbesítését és újra elküldi az elveszett vagy sérült csomagokat.

A szállítási réteg a nagyméretű adatcsomagokat kisebb méretű csomagokká darabolja a hatékonyabb szállítás érdekében. A fogadó számítógép ezeket a csomagokat összeilleszti, és megvizsgálja, hogy minden adatcsomag megérkezett-e?

Bizonyos esetekben a sebesség és a hatékonyság fontosabb, mint a megbízhatóság. Ilyenkor a küldő fél nem foglalkozik az adatok elküldése előtt a kapcsolat felépítésével, csupán elküldi a csomagokat.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Viszonyréteg

A kapcsolati viszony (session) azt jelenti, hogy két számítógép között kiépül a kommunikációs kapcsolat, adatok jutnak el egyik géptől a másikig (szállítási réteg feladata), majd az adatáramlás befejezésével a kapcsolat megszűnik a két gép között.

Megjelenítési réteg

A megjelenítési (prezentációs) réteg felel azért, hogyan jelennek meg az adatok az alkalmazások számára. Pl. a legtöbb számítógép és operációs rendszer (Windows, Unix, Macintosh) ún. ASCII (American Standard Code for Information Interchange) kódolást használ az adatok kódolására. Azonban más számítógépek (pl. IBM mainframe-ek) EBCDIC (Extended Binary Coded Decimal Interchange Code) kódolást használnak. Az ASCII és az EBDIC nem kompatibilisek egymással, ezért ha egy Windows-t futtató számítógép kapcsolódni akar egy IBM mainframe-hez, a megjelenítési réteg feladata az adatkonverzió elvégzése.

A megjelnítési réteg az adatkonverzión túl képes az adatok tömörítésére és titkosítására is.

Alkalmazási réteg

Az alkalmazási réteg (az OSI modell legfelső rétege) a felhasználói programok számára biztosítja a hálózati kommunikációt. Az elnevezés megtévesztő lehet, mert pl. az

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Outlook Express nem része a rétegnek, de a kimenő levelek továbbításáért felelős protokoll (SMTP, Simple Mail Transfer Protocoll) igen.

A TCP/IP egy olyan réteges hálózati modell, amely a világméretű hálózat, az INTERNET alapjául szolgál. Négy rétegből áll:

Hálózat elérési réteg (Network Interface)

Az OSI-modell két alsó szintjének felel meg. Ez biztosítja a kapcsolatot a csomópontok között.

Hálózati réteg (Internet)

Az OSI-modell hálózati rétegének felel meg, a csomagok útvonal kijelölését végzi a hálózatok között. Az üzenetvezérlő protokoll cím meghatározó eljárása az IP (Internet Protocol), a foglalt címet határozza meg. A rétegben előforduló események és hibák jelzésére az Internet Control Message Protocol, az Internet Vezérlőüzenet Protokoll szolgál.

Transzport réteg (Transport):

Az OSI model szállítási-hálózati rétegének felel meg. A létesített és élő kapcsolat fenntartását biztosítja.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

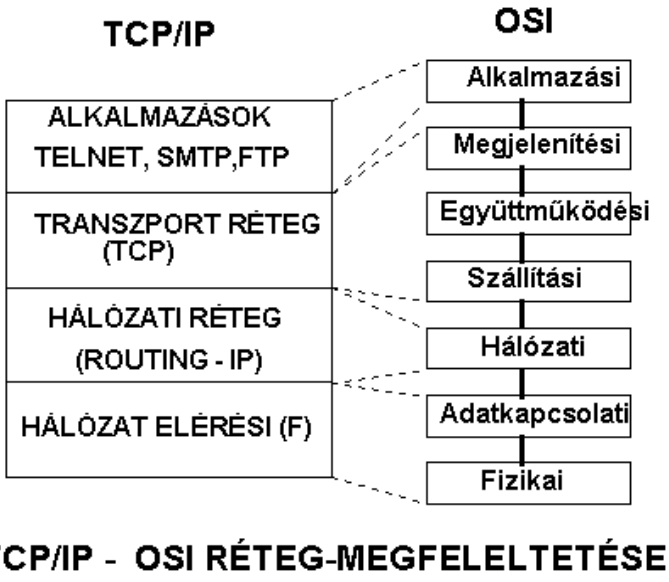
MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Két rétegprotokollból áll:

- a Transmission Control Protocol (TCP), azaz a továbbítást szabályozó eljárásból és
- a User Datagram Protocol (UDP), mint összeköttetésmentes szállítási protokollból

Alkalmazási réteg (Application)

Felhasználói és hálózati kapcsolatot biztosító programok.



2.2 ábra Az OSI és aTCP/IP modell

Minden réteg az adat továbbitása előtt beágyazza a felette levő rétegtől kapott információt. Ez megint egy hétköznapi példával mutatható be: a főnök odaadja a

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

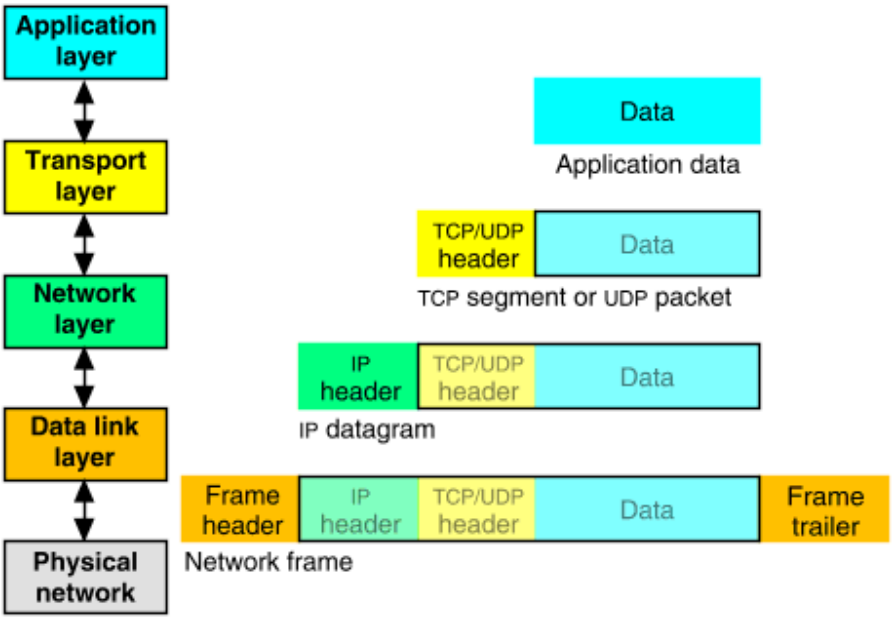
MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

terméket a titkárnőjének hogy küldje el az egyik ügyfélnek. A titkárnő beleteszi egy szatyorba, kikeresi a cimet és odaadja az aszisztensének hogy intézze el a postázást. Az aszisztens szépen becsomagolja, felcimzi, és szól a DHL-nek hogy jöjjön és vigye el a csomagot. A DHL mikor megérkezik kitölti a saját csomagkísérő lapját. A DHL nemzetközi központban a csomagra ráragasztanak néhány cimkét, mely segit a többi nemzetközi központnak illetve a szállitás többi résztvevőjének hogy a Lengyelország az Poland-ot jelent. (Lengyelországot nembiztos hogy más országban tudják hogy mi az…) Lengyelországi központban látják hogy kinek cimezték, kiszállítják, az ottani aszisztens átveszi a csomagot, látja hogy a cégnek küldték, kibontja, majd látva hogy az igazgatónak vagy legalábbis valamelyik management tagnak küldték küldték átadja a tikárnőnek. A titkárnő kiveszi a csomagot a szatyorból, látja hogy az igazgatónak van cimezve, igy átadja az igazgatónak.

Ez a folyamat a beágyazás (encapsulation) illtve a beágyazott csomagok kibontása (decapsulation).

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.



2.3 ábra A beágyazás folyamata

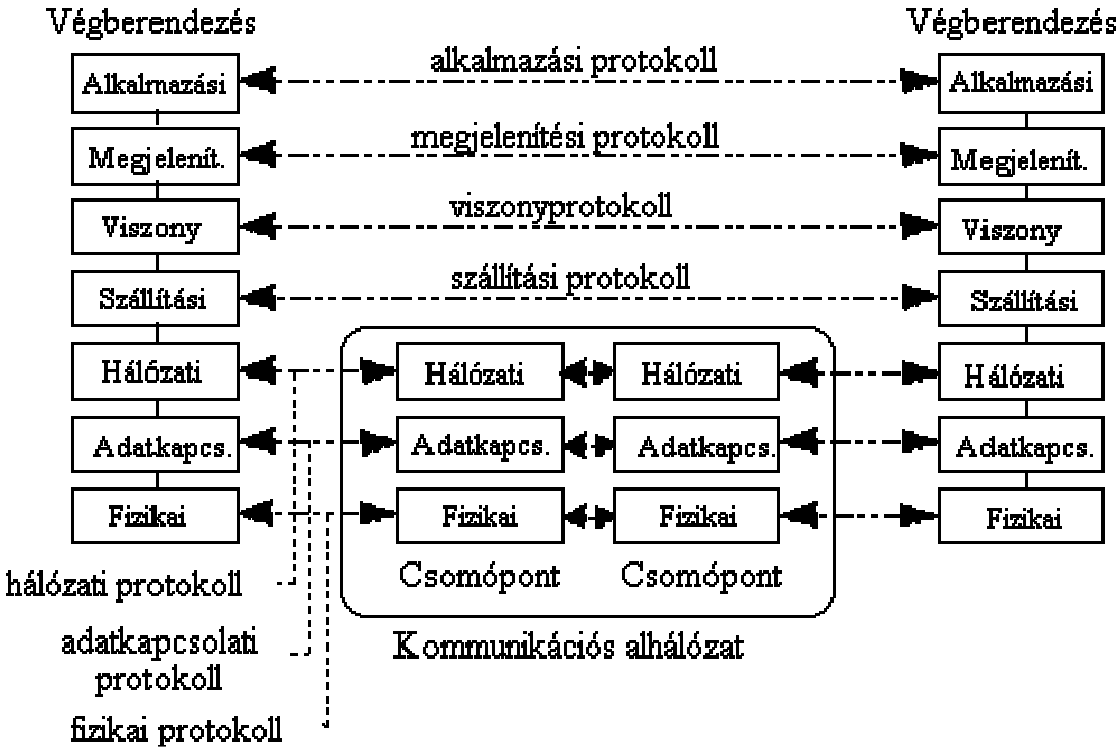
2.3 Protokollok

Az informatikában a protokoll egy egyezmény, vagy szabvány, amely leírja, hogy a hálózat résztvevői miképp tudnak egymással kommunikálni. Ez többnyire a kapcsolat felvételét, kommunikációt, adat továbbítást jelent.

Gyakorlati szempontból a protokoll azt mondja meg, hogy milyen sorrendben milyen protokoll-üzeneteket küldhetnek egymásnak a csomópontok, illetve az üzenetek pontos felépítését, az abban szereplő adatok jelentését is megadja.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.



2.4. ábra Protokollok áttekintése

A protokolloknak igen sok, és teljesen eltérő filozófiájú formája létezik. Vannak olyan protokollok, melyek minden apró részletet definiálnak (például ATM), és vannak, amelyek sok technikai kérdést nyitva hagynak, és rábízzák az implementálóra (például TCP protokollnál implementáció függő a csomagküldés sebességének megválasztása). Az előbbiek főleg a távközlésre jellemzőek, utóbbiakat főleg a kommunikációt informatikai oldalról közelítőkre jellemző. Előbbi előnye a jó kompatibilitás, utóbbié a rugalmasság.

Két eszköz között a kommunikációt általában nem egy, hanem több protokoll valósítja meg. Ezek többnyire egymásra épülnek. Erre jó példa az TCP/IP Ethernet hálózaton.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Ha a wikipedia oldalakat böngésszük, a böngészőnk HTTP protokoll segítségével éri el a kiszolgáló webszervert. A HTTP a web protokollja. Hogy odaérjen, a számítógépünk becsomagolja TCP-protokoll szerint is (a TCP segítségével tud két eltérő számítógépen lévő program beszélgetni). Ezt a számítógépünk tovább csomagolja IP-csomagokba (az IP az internet alapprotokollja), hogy így utazzon át az interneten. Az IP-csomagok, ha helyi hálózaton közlekednek, Ethernet-keretekbe vannak csomagolva, mert Ethernet "nyelven" beszélget egymással két hálókártya. Ez aztán elektromos jelek formájában (amelyeket szintén protokoll ír le) elhagyja a számítógépünket. Miután megérkezett rendeltetési helyére, ott a csomagolási folyamat a másik irányba is megtörténik, és a webszerver megkapja a kérésünket.

2.4 Címzés

Az IP azonos felületet igyekszik adni minden hálózati eszköz felé. Ebben nagy szerepet játszik a címzés felépítése, ami minden fizikai médián logikai cím, és a logikai-fizikai cím közti összerendelést a protokoll végzi el. Megjegyzendő, hogy az IP cím és a hálózati eszköz fizikai címe között nincs összefüggés.

Az IP cím egy 32 bites szám, ami 4 byte-nak felel meg. Írási formája a következő: 192.168.2.1

Ahol két pont között egy byte-nak megfelelő tízes számrendszerbeli szám van. Ez a cím az egész interneten (ill. az intraneten, hogy ha a nagy háló nem elérhető) egyedi. Minden hálózati eszköznek saját címe van, tehát ha egy számítógépben több hálózati eszköz van (több ethernet kártya pl) , akkor az a gép több címen is elérhető.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

A címen kívül a célgépen meg kell neveznünk egy szolgáltatást amit el kívánunk érni. Erre az ún. portcím szolgál, ami egy 16 bites szám. A portcímek egy része előre meghatározott szolgáltatásoknak van lefoglalva, például a 23-as port a telnet, 21-es az ftp, 25-ös pedig a levelezés számára foglalt.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

3 Kis irodai hálózatok felépítése

3.1 Kis irodákban leggyakrabban használt eszközök

A kis irodákban használt eszközök általában a különböző asztali és laptop számítógépek, napjainkban egyre gyakrabban a táblagépek és az okostelefonok. Mindezek mellett elengedhetetlen a nyomtató.

3.1.1 Asztali gépek

Az asztali számítógép általában olyan személyi számítógépet (PC) jelent, amely a hordozható eszközökhöz képest viszonylag kötött helyen (például egy íróasztalon) működik. A mikroprocesszoros rendszerek fejlődésének és világméretű elterjedésének köszönhetően az asztalon elférő számítógépek rendkívül ismertté váltak.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

3.1. ábra Asztali számítógép

Manapság a kifejezés általában a számítógépház formájára, méretére értendő. Az asztali számítógépek külseje ma már széles skálát jelent a hagyományos álló- vagy fekvőházaktól az LCD képernyők hátsó részébe épített minimális súlyú és méretű gépekig. Az asztali számítógép kifejezés (különösen angolszász nyelvterületeken) horizontális orientáltságú házat, rá elhelyezett monitort jelent, ezzel is helyet spórolva az íróasztalon. A legtöbb modern asztali számítógépnek külön monitora és billentyűzete van.

Az asztali számítógépek egyik fő előnye más típusú, nagyobb integráltsággal rendelkező gépek esetén (mint amilyenek a notebookok), az alkatrészek közötti nagyobb fokú szabványosítás, amely adott esetben olcsóbbá teheti az elromlott, vagy elavult részegységek cseréjét. Például, a piac asztali számítógépei közül szinte mindegyik az ATX szabványt használja. Így (egyéb feltételek szempontba vételével) a

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

gépház, az alaplap, és a tápegység szabadon cserélhető. Az asztali számítógépek bővítése újabb egységekkel olyan szabványos bővítőhelyek igénybevételével történhet, mint a PCI, a PCI Express, amelyekből általában több is rendelkezésre áll. Ezzel szemben a hordozható gépek általában egyetlen MiniPCI és PCMCIA bővítőhellyel rendelkeznek. Ez több más szemponttal együtt azt jelenti, hogy az asztali gépek olcsóbban, és egyszerűbben bővíthetőek.

Egy másik előny a hálózati áramforrásról való működés, így nem kell a kritikus szempontok közé emelni az áramfogyasztási kérdéseket.

3.1.2 Mobil eszközök: Notebookok, tabletek, okostelefonok

A notebook és a laptop angol eredetű szavak, és az informatikában a hordozható személyi számítógépeket takarják. Ezek teljes értékű PC-k, az asztali változatokhoz képest a lényegi különbség a kompakt formai kivitelezésben és a hordozhatóságban rejlik.

3.2. ábra Laptop

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Ugyanazokat a funkciókat betöltő alkatrészekből épül fel, ezek azonban jellemzően kisebb méretűek, könnyebbek, kevesebb hőt termelnek, és kevesebb energiát is fogyasztanak, mint az asztali PC-kben megtalálható megfelelőik. Ezt részben korszerűbb anyagokkal, részben a hordozhatóságot szem előtt tartó tervezéssel és gyártástechnológiával érik el. A notebookok ugyanazokat a szoftvereket futtatják, mint az asztali gépek, így a laptopokra ugyanaz a Windows, Linux vagy OS X alkalmazások telepíthetőek. A hordozható számítógépek ma már szinte kivétel nélkül újratölthető akkumulátorral szerelve vásárolhatóak meg, amelyek révén több órát is képesek elektromos hálózat nélkül üzemelni.

A táblagép vagy tablet PC egy hordozható számítógép, amelyet leginkább tartalomfogyasztásra fejlesztettek ki. Az eszköz méretéhez képest nagy kijelző mérettel rendelkezik, - amely növeli a felhasználóélményt -, azonban a kezelhetőséget nehezíti a hiányzó beviteli perifériák tartalomgyártás és szerkesztés esetén. Lényegében tulajdonságai és mérete alapján az ún. marokkészülékek (PDA, okostelefonok) és a billentyűzettel rendelkező netbookok közé helyezhető.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

3.3 ábra Különböző táblagépek

Célja a tényleges hordozhatóság megtartása mellette a kényelmes tartalom felhasználáshoz szükséges (minél nagyobb) kijelző méret elérése. A táblagép elsődleges kezelési felülete a kijelzőként is funkcionáló érintőképernyője, ami a billentyűzettel és egérrel rendelkező számítógépekhez képest eltérő felhasználási, fejlesztési és vezérlési (programozási) filozófiát követel. Leegyszerűsített táblagépekre szabott alkalmazások által egyes alapvető használati funkciók könnyebben vezérelhetőek, mint az ún. „asztali számítógépek” esetén, azonban ezen egyszerű használati módon túllépő igény esetén a lehetőségek erősen korlátozottak.

A táblagépeknél ma már követelménynek tekinthetők az olyan integrált kiegészítők, mint a vezeték nélküli kapcsolatot szolgáló eszközök: wi-fi, bluetooth, mobil net. Valamint olyan hasznos kiegészítők, mint a mikrofon, hangszóró, GPS, kamera, giroszkóp, gyorsulásmérő és a magnetométer.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Okostelefonnak vagy angolul smartphone-nak nevezzük a fejlett, gyakran PC-szerű funkcionalitást nyújtó mobiltelefonokat.

3.4. ábra Okostelefonok

Nincs egyértelmű meghatározás arra, hogy mi az okostelefon. Egyesek szerint okostelefon az a mobil, aminek teljes értékű operációs rendszere szabványosított interface-eket és platformot nyújt az alkalmazásfejlesztők számára. Mások meghatározásában a smartphone egyszerűen egy olyan készülék, ami olyan fejlett funkciókat tartalmaz, mint e-mail, Internet és e-book-olvasó, és/vagy teljes értékű billentyűzet, vagy külső USB-s billentyűzet és VGA csatlakozó. Más szavakkal, egy olyan miniatűr számítógép, ami telefonként is képes működni. Az okostelefon szó továbbgondolásával megjelent a fejlett képességekkel nem rendelkező készülékekre a „butatelefon” elnevezés. A képességeiben e kettő között álló telefonokat angol

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

nyelvterületen feature phone-nak (magyarul elterjedtebb néven: középkategóriás telefonnak) is nevezik.

Az okostelefonokon található operációs rendszerek közé tartozik a Symbian OS, az iPhone OS, a RIM BlackBerryje, a Microsoft Windows Phone, a Linux, a Palm WebOS és a Google-féle Android. Az Android és a WebOS Linux alapra épül, az iPhone OS pedig a Unix-rokon BSD és NeXTSTEP operációs rendszerekből származtatható.

3.1.3 Perifériák, Network Attached Storage (NAS) megoldások

A NAS betűszó a Network Attached Storage, azaz a hálózatra csatolt tároló rövidítése. Magyarul Hálózati adattárolóként is ismerjük.

3.5. ábra NAS szerver alkalmazási lehetőségei

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

A NAS egy fálj szinű adattároló eszköz, amely a számítógépes hálózathoz csatlakoztatva biztosítja az adatok megfelelő menedzselését a felhasználók között legyenek azok akár egy másik földrészen is. Internetkapcsolat segítségével bárhonnan elérhető, a tárolt adatok megoszthatóak, védhetőek a felhasználói engedélyek megfelelő beállításásval.

Jellemzőjük a maximális tárolókapacitás, illetve a többplatformos hozzáférés (OSX, LINUX, Windows). A NAS egységekkel jelentős költségcsökkenés érhető el.

A NAS-ban egy speciálisan elkészített szoftvert és hardvereszközt gyúrtak egybe. Nem egy általános célra összeállított számítógép, amely alkalmas fájl-szerverként is üzemelni. A NAS a legoptimálisabb eszköz, amivel fájlokat (adat és multimédia egyaránt) oszthatunk meg, vagy érhetünk el nemcsak számítógéppel, de akár mobiltelefonnal is.

3.2 Kis irodák hálózati elemei

A kis irodai hálózat elemei a kis irodai router esetleg switch és a acces point. Ezek az eszközök legtöbbször integrálva vannak.

3.2.1 Router, Switch

Router

Az útválasztó vagy router a számítógép-hálózatokban egy útválasztást végző eszköz, amelynek a feladata a különböző – például egy otthoni vagy irodai hálózat és az internet, vagy egyes országok közötti hálózatok, vagy vállalaton belüli hálózatok – összekapcsolása, azok közötti adatforgalom irányítása.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

A számítógépes hálózatok működésének leírására több elméleti modell is létezik, az általánosan elterjedt OSI (Open Systems Interconnection) modell réteges struktúrájában a router a harmadik – hálózati – rétegben helyezkedik el. Útvonalválasztási döntéseinek alapját az ezen rétegbeli – általában IP- – címek adják.

A számítógépes hálózatok forgalma különböző típusú adatcsomagokban zajlik. Ezen csomagok utaznak a feladótól a címzettig, akár több eszközön is keresztül, például az Internet esetében. Útjuk során minden érintett eszköznek ismernie kell, hogy merre továbbítsa a fogadott csomagot, hogy az eljusson a címzettig, és döntéseket kell hoznia amennyiben például több útvonal is ismert. A routerek végzik ezen csomagok megfelelő irányba való továbbítását, és végzik ezen döntéseket. A mai routerek nagy része az IP protokoll-alapú hálózatok forgalmát irányítják, de több más protokoll kezelésére is alkalmasak lehetnek. IP protokoll esetén egymás és a hálózatok azonosítására a harmadik rétegbeli IP-címet alkalmazzák.

3.6. Kis irodai router

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Kisebb cégek illetve otthoni felhasználók Internetre való csatlakozásához használatosak ezen routerek, melyek teljesítménye is ennek megfelelően jóval kisebb. Alapvető feladatuk a belső, saját hálózat Internetre való csatlakoztatása. Egy 2013-as vizsgálat szerint a SOHO routerek nagy részének biztonsága hagy kívánnivalót maga után. A helyi hálózat felül mind a 13 vizsgált készülék feltörhető volt.

Switch

Az adatátviteli kapcsoló vagy switch egy aktív számítógépes hálózati eszköz, amely a rá csatlakoztatott eszközök között adatáramlást valósít meg. Többnyire az OSI-model adatkapcsolati rétegében (2. réteg, esetleg magasabb rétegekben) dolgozik. Magyar jelentése: vált, kapcsol.

A fizikai rétegbeli feladatokat ellátó hubokkal szemben az Ethernet switchek adatkapcsolati rétegben megvalósított funkciókra is támaszkodnak. A MAC címek vizsgálatával képesek közvetlenül a célnak megfelelő portra továbbítani az adott keretet; tekinthetők gyors működésű, többportos hálózati hídnak is. Portok között tehát nem fordul elő ütközés (mindegyikük külön ütközési tartományt alkot), ebből adódóan azok saját sávszélességgel gazdálkodhatnak, nem kell megosztaniuk azt a többiekkel. A broadcast és multicast kereteket természetesen a switchek is floodolják az összes többi portjukra.

Egy switch képes full-duplex működésre is, míg egy hub csak half-duplex kapcsolatokat tud kezelni. Különbség még, hogy a switchek egy ASIC (Application-Specific Integrated Circuit) nevű hardver elem segítségével jelentős sebességeket érhetnek el, míg a HUB nem más mint jelmásoló, ismétlő. A fontos funkciók közé tartozik még a hálózati hurkok elkerülésének megoldása (lásd STP), illetve a VLAN-ok kezelése.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Ethernet switcheken kívül léteznek még például ATM, Frame Relay és Fibre Channel kapcsolók is. Fibre Channel kapcsolók SAN hálózatokban használatosak, általában optikai kábelezéssel.

3.2.2 Vezeték nélküli hozzáférési pont

A vezeték nélküli hozzáférési pont (angolul: Wireless Access Point) egy olyan eszköz amely biztosítja a vezeték-nélküli eszközök vezetékes hálózathoz való hozzáférését. Az hozzáférési pont különálló eszközként a vezetékes routerhez kapcsolódik, de a kis irodai hálózatok esetén gyakran integrált eszközökről beszélünk. A legelterjedtebb szabványok az alábbiak:

802.11a: 5 GHz-es frekvenciasávban működő eszközök; előnye a nagy távolság és sávszélesség, viszont jellemzően csak pont-pont kapcsolatra használják és az ehhez használható eszközök általában drágábbak. Különösen fontos az optikai rálátás a két pont között.

802.11b: 2,4 GHz-es tartományban működő eszközök; hatótávolsága a terepviszonyoktól függően széles skálán mozoghat, lényegesen kisebb, mint a 802.11a, pont-multipont kapcsolatoknál 1 km-es sugarú körön belülre szokták tervezni. Átviteli sebessége max. 11 Mbit/s

802.11g: 2,4 GHz-en működő eszközök, a 802.11b-vel sok tekintetben megegyezik, a routerek nagy része mindkettőt támogatja. Előnye, hogy nagyobb sávszélességet képes átvinni, hátránya pedig, hogy a távolság növekedésével lényegesen romlik a hatásfoka és érzékenyebb az interferenciára. Átviteli sebessége max. 54 Mbit/s.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Felhasználási területek általában

Publikus, nyílt hálózat: bármely wi-fi routerrel kialakítható, az így létrehozott hálózathoz bárki csatlakozhat mindenféle korlátozás nélkül

Privát hálózat: a hálózat saját felhasználásra lett kialakítva, melyet egy titkos jelszó véd, így ahhoz csak a jelszó ismeretében lehet csatlakozni

Publikus, zárt hálózat: egy speciális szoftver gondoskodik arról, hogy a hálózatot csak egy kód ismeretében, korlátozott ideig lehessen használni. Ezt a formát rendszerint éttermek, kávézók használják, ahol az internetelérés fogyasztáshoz van kötve

Publikus, részlegesen zárt hálózat: átmeneti típus a nyílt és egyben publikus hálózatok, illetve a privát hálózatok közt. Két főbb típusa különböztethető meg, így a hozzáférési pont számára elérhető sávszélesség bizonyos, akár igen elenyésző hányadának nyílt, és publikussá tett formája, illetve egy szélesebb kör számára elérhető, publikus, azonban zárt hálózat ismeretes. Céljuk, hogy az internetkapcsolatot ingyenesen használók ne élhessenek vissza, és ne terhelhessék le aránytalanul az adott wi-fi-pontot üzemeltető hálózatát annak terhére. Jelenleg az első, a privát hálózatok és a nyílt hozzáférésű, publikus hálózatok kivitelezése igen körülményes egyszerű felhasználók számára, míg utóbbi hálózatok nem hozzáférhetők mindenki számára, minthogy azokat csak a jelszót ismerő személy, vagy személyek csoportja képes elérni. Ilyen megoldást nyújtanak a Skype, illetve a Google érdekeltségi körébe tartozó FON által kínált olyan wi-fi routerek, melyek az ilyen termékkel rendelkezők számára egymás között elérhetővé teszik az ilyen routereken keresztül megosztott wi-fi hálózatok

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

bizonyos részét, amit egy felhasználói névvel, illetve jelszóval rendelkező - szintén e közösség tagságával bíró személyek - csatlakozhatnak a világ számos különböző pontján elérhető ilyen típusú hálózatok összeséhez. Ezek sávszélességét a tulajdonos határozza meg, egy a közösség tagjai számára részlegesen megosztott 1,5 Mb/s sávszélességű internet kapcsolat 10%-a elegendő, hogy valósidejű, kétoldalú hanghívást bonyolítsunk különböző VoIP-klienseken (Voice Over Internet Protocol) keresztül, mint amilyen a Skype, vagy a Windows Live Messenger.

Kereskedelmi HotSpot szolgáltatás: a vezeték nélküli hálózat csak díjfizetés ellenében, korlátozott ideig használható

3.3 Hálózatra csatlakozás lehetőségei

Kis irodai hálózatunkat általában egy internetszolgáltató cég segítségével kapcsolhatjuk a Világhálóhoz. Az internetszolgáltató cégek – térítési díj ellenében – biztosítják az ehhez szükséges infrastruktúra működtetését. A kapcsolódás fizikailag többféle módon lehetséges – szolgáltatótól és a helyi adottságoktól függően.

3.3.1 Vezetékes megoldások

Otthoni számítógépünket általában egy internetszolgáltató cég segítségével kapcsolhatjuk a Világhálóhoz. Az internetszolgáltató cégek – térítési díj ellenében – biztosítják az ehhez szükséges infrastruktúra működtetését. A kapcsolódás fizikailag többféle módon lehetséges – szolgáltatótól és a helyi adottságoktól függően.

Az egyik leginkább elterjedt lehetőség, hogy a telefonhálózat felhasználásával tudunk kapcsolatba lépni a szolgáltató szerverével. Ehhez a felhasználói oldalon egy telefonos modemre van szükségünk, amely a számítógép LAN, vagy USB portján kimenő jeleket

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

a telefonhálózaton továbbítható jelekké alakítja (modulálja) és viszont (demodulálja). Ez az átalakítás régebben hangokká alakítást jelentett (analóg modemek) manapság valamilyen digitális technológiát (DSL, ISDN). Az otthoni felhasználók a manapság leginkább elterjedt DSL (Digital Subscribe Line) technológiának az aszimmetrikus változatát (ADSL) használják, amelynek jellemzője, hogy az adatátvitel irányától függően eltérő adatátviteli sebesség áll rendelkezésre. (A letöltés sokkal gyorsabban megy, mint a feltöltés.)

Egyes településeken további vezetékes lehetőségek közül is választhatunk, például televíziós kábelen, vagy optikai kábelen keresztül is csatlakozhatunk. Ezekhez a kapcsolatokhoz speciális kábelmodem szükséges, amit általában a szolgáltató cég bocsát rendelkezésünkre.

3.3.2 Vezeték nélküli megoldások

A vezetékes lehetőségeken túl, manapság egyre inkább elterjednek a különféle „mobilinternetes” megoldások, amelyek valamelyik mobiltelefon-szolgáltató rádióhullámú hálózatát használják a kapcsolat felépítéséhez. Az ilyen jellegű kapcsolathoz speciális, SIM-kártyát is tartalmazó, rádiófrekvenciás hálózati eszközt kell csatlakoztatnunk a számítógéphez.

A mobil adatátviteli hálózatokat több generációba sorolják.

1. Generáció (1G)

Ez a hálózat még nem volt felkészítve adatátvitelre csak nalóg jelek átvitelére. Az adatátvitel megoldható volt itt is analóg modem alkalmazásával. Jellemzi az alacsony sávszélesség: 20-30 kb/s.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

2. Generáció (2G)

Általában a GSM (Global System for Mobile Communication) hálózatokat soroljuk ide. Itt már megjelenik az adatátvitel lehetősége, a GPRS (General Packet Radio Service), sávszélesség:172 kb/s, továbbfejlesztve a EDGE (Enhanced Data Rate for Global Evolution), sávszélesség: 474 kb/s. Ez utóbbit gyakran 2.5G-ba szokták sorolni.

3. Generáció (3G)

Ebben a generációban jelenik meg UMTS (Universal Mobile Telecommunicaton System) amelynek sávszélessége (384 kb/s) már alkalmassá teszi a videotelefon szolgáltatásra.

A további fejlesztések után megjelentek a HSDP hálózatok, amelyek 7,2 Mb/s átviteli sebességet biztosítanak. Ez már 3,5 G hálózat.

További fejlesztések után megjelentek a 3,75 G-s hálózatok amelyek 21 Mb/s sebességet biztosítani.

4. Generáció (4G)

Napjainkban néhány helyen már elérhetőek a 4G-s vagy LTE hálózatok. Ezekkel már akár 100 Mb/s átviteli sebesség is elérhető.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

4 Kis irodai hálózatok fenyegetettsége és védelme

A kis irodai hálózatok hasonlóan a nagyvállalati hálózatokhoz különféle veszélyeknek vannak kitéve. Ebben a fejezetben áttekintjük a legfontosabbakat.

4.1 Fizikai veszélyek (túlfeszültség és zavarvédelem)

A fizikai veszélyek általában a kis irodai hálózatunkat fizikailag veszélyeztető veszélyforrások. Ilyenek lehetnek:

- a különböző természeti veszélyforrások, földrengés árvíz stb.
- technikai veszélyforrások, kommunikációs és energiaellátási problémák stb.
- jogosulatlan fizikai hozzáférés, betörés ellenőrzés nélküli behatolás stb.
- elektromágneses veszélyek

Az ilyen jellegű támadások ellen is fel kell készíteni a kis irodánkat. A legtöbb esetben ezek a védekezi mechanizmusok automatikusak, pl. mert a bejárati ajtó védelmével és riasztó felszerelésével az iroda védelmén túl az informatikai rendszert is fizikailag megvédjük.

Nagyon fontos a különböző elektromágneses veszélyek elleni védekezés, azért mert ezek elleni védekezés általában nem oldódik meg egyéb védelmi módok segítségével.

Feszültség - túlfeszültség

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Mindenekelőtt meg kell határoznunk milyen feszültségről is van szó: egy villamos berendezés kapcsán ugyanis számos feszültséget emlegethetünk: üzemi, maximális, próba, névleges stb. Mi itt kizárólag a tranziens, azaz rövididejű, nem ismétlődő, impulzusjellegű túlfeszültségekre korlátozzuk mondandónkat. Nem tartoznak tehát ide az üzemi jellegű túlfeszültségek, melyeknek mind keletkezési mechanizmusa, mind az ellenük való védekezés módja és eszköztára egészen más.

Villám vagy túlfeszültség ?

Sokszor szinte egymás szinonimájaként használják a két szót a védelem kifejezés előtt, holott óriási különbség van a két terület között. A jól működő villámvédelem nem nyújt védelmet a túlfeszültség okozta károkkal szemben, s a túlfeszültségvédelem megléte nem befolyásolja a villámcsapás kockázatát. A két rendszer nem helyettesíti, hanem kiegészíti egymást.

A félreértést az okozza, hogy a túlfeszültségek sok esetben a villámcsapás nyomán jelennek meg hálózatainkban. De vajon csak így keletkezhet túlfeszültség? Nem. Az EMC korábban már említett EMP részterülete tovább osztható a túlfeszültség keletkezési módja szerint.

SEMP

A villamos berendezések, hálózatok ki- illetve bekapcsolása során is keletkeznek rövid idejű jelentős nagyságú túlfeszültségek.

LEMP

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Kifejezetten a villámcsapások által keltett túlfeszültség tartoznak ide. Általában meredekebb felfutású, viszonylag nagy amplitúdójú impulzusok

NEMP

A nukleáris bombák robbanásakor keletkező, rendkívüli elektromágneses tér okozta túlfeszültségek területe. Általában a polgári létesítmények tervezése során figyelmen kívül hagyjuk - érthető okoknál fogva.

A túlfeszültségek hatásai és következményei

A kis energiatartalmú, viszonylag lomha felfutású és kis amplitúdójú túlfeszültségek általában csak múló zavarjelként terhelik a villamos rendszereket. A nagyobb impulzusok azonban már súlyosabb következményekkel járnak.

A kisfeszültségű hálózatokon nagy tömegben előforduló elektronikus készülékek rendkívül érzékenyek a túlfeszültségekre: a rendkívül kis kiterjedésű félvezető átmenetek ugyanis már igen kis energiával roncsolhatók. (Ez a magyarázata, hogy sok esetben semmi látványos nyoma nincs a túlfeszültségnek, csak az elektronika megy tönkre.)

(Meg kell említeni ezen túlmenően azt is, hogy számos esetben a viszonylag kicsi, de többször is ismétlődő túlfeszültség igénybevétel az alkatrész élettartamának rövidülését eredményezheti.)

A védekezés lehetősége

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

A védekezés elve rendkívül egyszerű: vagy nem szabad megengednünk, hogy a túlfeszültség impulzus bejusson villamos rendszereinkbe, vagy ha bejutott már, akkor olyan értékűre kell csökkenteni, hogy készülékeink, eszközeink károsodás nélkül viseljék el jelenlétét.

A bejutás módjai

Alapvetően három módon juthat be túlfeszültség egy villamos hálózatba: kapacitív, induktív vagy galvanikus csatolással (ez utóbbit szokás vezetett túlfeszültségnek is hívni). Létezik egy negyedik mód is, amikor a villám keltette elektromágneses tér közvetíti az energiát a villamos készülék antennaként viselkedő vezető részébe, azonban a rendszerek tervezésénél az első három módot kell figyelembe vennünk.

A védekezés lehetőségei

A kapacitív és induktív csatolás esetében a védekezés módja a megfelelő árnyékolás alkalmazása és a rendszerek vezetékeinek, valamint a villámhárító levezetőinek átgondolt, megfelelő geometriájú elhelyezése.

A vezetett túlfeszültségek "kordában tartására" a túlfeszültséglevezetők szolgálnak. Ezek a villamos készülékek speciális kapcsolóként működnek: nyitott kapcsolóként viselkednek az üzemi feszültségek tartományában, s csak akkor zárnak, ha a megjelenő feszültség meghaladja megszólalási feszültségüket. Ekkor - mintegy

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

rövidzárként viselkedve - kis értékre korlátozzák a védendő berendezés sarkain a feszültséget.

Ezek egy részét az iroda villamos betáplálásához kell elhelyezni, másik részét pedig készülékek betáplálási pontjaihoz.

4. ábra Túlfeszültség levezető megoldások

4.2 Védekezés a logikai veszélyforrások ellen

A pillanattól kezdve, ahogy a felhasználó bekapcsolja számítógépét, rengeteg veszély fenyegeti a rendszert, melyek forrásai az internet. Ezen veszélyforrások lehetnek akár kémprogram támadások, vírusok, trójai falovak, vagy akár hackerek is. Ezeket a veszélyforrásokat nevezzük logikai veszélyeknek.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

4.2.1 Anti-virus megoldások

A számítógépes vírus olyan program, amely saját másolatait helyezi el más, végrehajtható programokban vagy dokumentumokban. Többnyire rosszindulatú, más állományokat használhatatlanná, sőt teljesen tönkre is tehet.

A vírusok manapság jellemzően pendrive vagy e-mail segítségével terjednek, az internetes böngészés mellett.

A számítógépes vírusok működése hasonlít az élővilágban megfigyelhető vírus viselkedéséhez, mely az élő sejtekbe hatol be, hogy önmaga másolatait előállíthassa. Ha egy számítógépes vírus kerül egy másik programba, akkor ezt fertőződésnek nevezzük. A vírus csupán egyike a rosszindulatú szoftverek (malware) számos típusának. Ez megtévesztő lehet a számítógép-felhasználók számára, mivel mára lecsökkent a szűkebb értelemben vett számítógépes vírusok gyakorisága, az egyéb rosszindulatú szoftverekhez, mint például a férgekhez képest, amivel sokszor összetévesztik őket.

Vírusok működése

Bár a számítógépes vírusok lehetnek kártékonyak (például adatokat semmisítenek meg), a vírusok bizonyos fajtái azonban csupán zavaróak. Némely vírus késleltetve fejti csak ki hatását, például csak egy bizonyos számú gazdaprogram megfertőzése után. A vírusok kártékony hatásának legenyhébbje az ellenőrizetlen reprodukciójuk, mely túlterhelheti a számítógépes erőforrásokat, lelassítja a gép működését, elfogyasztja a szabad helyet a merevlemezen. Súlyosabb ártalom, ha a vírus fontos fájlokat töröl a gépről, akár az operációs rendszert megbénítva, hasonlóképp törölhet célzottan dokumentumfájlokat, videofájlokat, programokat. A legsúlyosabb kár a merevlemez

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

teljes tartalmának megsemmisítése vagy elérhetetlenné tétele,[1] vagy a számítógép valamelyik elektronikus alkatrészének szélsőséges túlterhelése révén műszaki meghibásodás, sérülés előidézése.

Napjainkban, az internet térhódításával vírusok már valamivel kevésbé gyakoriak, mint a hálózaton terjedő férgek. Az antivírus szoftverek, melyeket eredetileg a számítógépes vírusok elleni védelemre fejlesztettek ki, mára már képesek a férgek és más veszélyes szoftverek, mint például a kémprogramok (spyware) elleni védelemre is.

2008-ban a Google elindított egy vírus elleni kampányt úgy, hogy megpróbálja elkapni a vírusterjesztő oldalakat, és azt a keresési találatokban vírusos oldalként megjeleníti.

A legtöbb fajta vírusprogram és a legtöbb vírusfertőzés a PC-ken leginkább elterjedt operációs rendszert, a Microsoft Windowst használó számítógépeken figyelhető meg. Sajnálatos jellegzetesség, hogy a vírusok terjedését sokszor csak megkönnyítik az operációs rendszerek és felhasználói programok által kényelmi szolgáltatásnak szánt megoldások. Azok, amikor a program nem terheli a felhasználót esetleg nem érthető kérdésekkel, hanem automatikusan hajt végre műveletsorokat, a program által optimálisnak tartott útvonalon. („Csak egy kattintás...”) Amikor a meghajtóba helyezünk egy DVD-t, akkor automatikusan elindul a rajta levő telepítőprogram, automatikusan megnyílik rajta a fotóalbum vagy a videofájl, a behelyezett pendrive-on levő programok esetében ugyanígy, a megnézett e-mail mellékletei automatikusan megnyílnak, a gépünkre bejegyzett (és bárki által átírható) című kezdőhonlap nyílik meg a böngésző elindításakor, a rendszer külön engedély nélkül letölti és telepíti a Flash-lejátszó program vagy a Java rendszer központi magjának legfrissebb változatát és így tovább. Nem beszélve azokról a biztonsági résekről, amelyek az operációs rendszer vagy a

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

böngésző „túlokosításának” következményeként létrejött speciális, de hozzáértő által a gép védelmeinek kijátszására is kihasználható kerülőutakat jelentik, ezeket a programok gyártói sűrű egymásutánban kibocsátott frissítésekkel, „foltokkal” (patch) próbálják lezárni, utólag, amikor valaki felismer és közzétesz a rendszer szövevényes szerkezetében egy ilyen kerülőutat. A rutinos felhasználó tisztában van ezekkel az eshetőségekkel, és csak annyi automatizmust enged meg a saját rendszerének, amennyinek a kockázatát még elfogadhatónak tartja.

Vírusok fajtái

- Fájlvírusok: csak úgy tudnak szaporodni, hogy egy program állomány belsejébe másolják be magukat.
- Bootvírusok: a floppy vagy merevlemez boot-területeinek egyikébe írják be magukat. Akkor fertőződnek, ha fertőzött lemezről indul a gép.
- Makróvírusok: sok manapság használatos program, mint pl a Word, Excel lehetővé teszik, hogy sablonjaik makrókat tartalmazzanak. A makróvírusok így ilyen dokumentumhoz hozzákapcsolódó öninduló makrók, amik reprodukálódnak, s más dokumentum-állományokhoz fűzik magukat. Fő terjedésük: e-mailek csatolt állományaival.
- Mailvírusok: e-mailekkel terjednek, a levélkiszolgálókat és levelezőprogramokat használják ki terjedésükhöz. Ezek legtöbbször a levelek csatolt állományaival terjednek, de napjainkban már előfordulnak a levéltörzsben speciális karakterekként elrejtve, amik rákényszerítik a levelezőprogramot vagy a levelezőszervert egy speciális feladat végrehajtására.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

A projektek az Európai Unió támogatásával valósulnak meg.

Egyéb rosszindulatú kódok

- Trójai falovak: nem szaporodnak, de a gépbe bekerülve ott valamilyen rendellenességet okoznak, pl. PC-k és a hálózati forgalom lelassítása.
- Kémvírusok: kárt nem okoznak, hanem információkat szolgáltatnak az adott gépről és a hálózatról Interneten keresztül.
- Férgek: „csak” szaporodnak, s emiatt lecsökkentik a háttértár szabad területét, súlyos rendszerhibákat okoznak.

4.2.2 Tűzfalak

A tűzfal célja a annak biztosítása, hogy a hálózaton keresztül egy adott számítógépbe ne történhessen illetéktelen behatolás. Szoftver- és hardverkomponensekből áll. Hardverkomponensei olyan hálózatfelosztó eszközök, mint a router vagy a proxy. A szoftverkomponensek ezeknek az alkalmazási rendszerei tűzfalszoftverekkel, beleértve ezek csomag- vagy proxyszűrőit is. A tűzfalak általában folyamatosan jegyzik a forgalom bizonyos adatait, a bejelentkező gépek és felhasználók azonosítóit, a rendkívüli és kétes eseményeket, továbbá riasztásokat is adhatnak.

A tűzfal megpróbálja a privát hálózatot ill. a hálózati szegmenst a nemkívánt támadásoktól megóvni. Szabályozza a különböző megbízhatósági szintekkel rendelkező számítógép-hálózatok közti forgalmat. Tipikus példa erre az internet, ami semmilyen megbízhatósággal nem rendelkezik és egy belső hálózat, ami egy magasabb megbízhatósági szintű zóna. Egy közepes megbízhatósági szintű zóna az ún. „határhálózat” vagy demilitarizált zóna (DMZ), amit az internet és a megbízható belső hálózat között alakítanak ki. Megfelelő beállítás nélkül egy tűzfal gyakran

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

értelmetlenné válik. A biztonsági szabványok „alapértelmezett-letiltás” tűzfal-szabálycsoportot határoznak meg, amelyben csakis azok a hálózatok vannak engedélyezve, amiket már külsőleg engedélyeztünk. Sajnos egy ilyen beállításhoz részletesen ismerni kell a hálózati eszközöket és azokat a végpontokat, amik a vállalat mindennapi működéséhez szükségesek. Sok vállalatnál hiányzik ez az ismeret, és ezért egy „alapértelmezett-engedélyezés” szabályt alkalmaznak, amiben minden forgalom engedélyezve van, amíg konkrétan nem blokkolják. Az ilyen beállítások kéretlen hálózati kapcsolatokat és rendszer veszélyeket okoznak. A szabálymegszegéseket leszámítva, egy tűzfal funkciója nem abból áll, hogy veszélyeket felismerjen és akadályozzon. Főleg abból áll, hogy a meghatározott kommunikációs kapcsolatokat engedélyezze, a forrás- vagy célcímek és a használt szolgáltatások alapján. A támadások felkutatásáért az ún. behatolás-felismerő rendszerek a felelősek, amelyet akár a tűzfalra is lehet telepíteni, de ezek nem tartoznak a tűzfalhoz.

Csomagszűrés

Az adatcsomagok egyszerű szűrése a cél-port, valamint forrás- és célcím, egy a tűzfal-adminisztrátor által már definiált szabályrendszer alapján történik. Ez minden hálózati-tűzfal alapfunkciója. A vizsgálat eredményeképp a csomagokat megsemmisíti vagy továbbítja. A fejlett tűzfalak csendben dobják el a csomagokat, azaz az érintett kapcsolat egyszerűen nem jön létre/megszakad, de nincs konkrét visszajelzés. Ez egy gyors és univerzális megoldás, viszont jelentős háttérismeretet, a hálózati és alkalmazási protokollok ismeretét igényli. Ez a tűzfalak leggyakrabban használt fajtája,

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

ezekkel az alapvető szűrésekkel rendelkezik manapság a legtöbb router, és vállalati switchek.

Állapot szerinti szűrés

Ez a csomagszűrés egy kibővített formája, ami a 7. OSI-rétegen egy rövid vizsgálatot hajt végre, hogy minden hálózati-csomagról egyfajta állapottáblát hozzon létre. Ezáltal felismeri ez a tűzfal a csomagok közti összefüggéseket és az aktív kapcsolathoz tartozó munkafolyamatokat leállíthatja. Így sikerül ennek felismerni egy kapcsolat felépítése után, hogy a belső kliens a külső célrendszerrel mikor kommunikál, és csak akkor engedélyezi a válaszadást. Amikor a célrendszer olyan adatokat küld, melyeket a belső kliens nem kért, akkor a tűzfal már önmaga blokkolja az átvitelt a kliens és a célrendszer között fennálló kapcsolatnál. Ez különbözteti meg ezt a tűzfalat egy szokásos csomagszűréstől. Egy proxy-val ellentétben a kapcsolat itt önmagában nem befolyásolt.

Alkalmazásszintű tűzfal

Egy alkalmazásszintű tűzfal a tisztán csak a forgalomhoz tartozó, mint a forrás, cél és szolgáltatás adatokon kívül a hálózati csomagok tartalmát is figyeli. Ez lehetővé teszi az ún. dedikált proxy-k alkalmazását is, amik egy specializált tartalomszűrést vagy egy Malware-szkennelést is lehetővé tesznek. Egy népszerű félreértéssel ellentétben egy alkalmazásszintű tűzfal alapszintű feladata nem abból áll, hogy meghatározott alkalmazások (programok) hálózathoz való hozzáférését engedélyezze vagy megtiltsa.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Egyébként egy áramkör szintű proxy-t lehet egy ilyen tűzfalra létesíteni, ami egy protokollfüggetlen port- és címszűrés mellett egy lehetséges hitelesítés a kapcsolat felépítésének támogatásához. E nélkül egy alkalmazás számára nem lehetséges egy külső hálózattal (internettel) történő kommunikálás.

Proxy / Anonymous proxy

Az alkalmazás-szintű tűzfal integrált proxyt használ, ami a munkamenetének helytállósága alapján építi fel a kliensekkel és a célrendszerekkel a kapcsolatot. A szervernek csak a proxy IP-címe lesz látható mint feladó, nem pedig a kliensé. Így a helyi hálózat struktúrája nem lesz felismerhető az Internet felől. Tehát megakadályozza a közvetlen kommunikációt a külső és a védett hálózat között. Közvetítő szerepet játszik a kettő között: a belülről érkező kéréseket feldolgozza, majd azokkal azonos értelmű kérést küld a külső szerver felé, az azokra érkező válaszokat pedig ugyanilyen módon továbbítja a belső hálózat felé. Elég biztonságosnak mondható és általában egyszerűen konfigurálható. Hátránya viszont, hogy kizárólag olyan kommunikációra használható, melynek értelmezésére képes. Magukba foglalhatnak tartalmi gyorsítótárat, így néhány esetben jelentős mértékben csökkenthetik a kifelé irányuló forgalmat. Minden magasabb kommunikációs protokollnak (HTTP, FTP, DNS, SMTP, POP3, MS-RPC, stb.) van egy saját, dedikált proxy-ja. Egyetlen alkalmazás-szintű tűzfalon több dedikált proxy is futhat egyszerre. Anonim proxy: Az eredeti webező identitásának elrejtésére, a webszerver és a böngésző közti kommunikációba harmadik félként beépül olyan módon, hogy valójában ő tölti le a kiszolgálóról a kliens által kért weblapokat. Ezeket továbbítja, így a tényleges kliens identitása (IP címe) a szerver elől rejtve marad.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Tartalomszűrés

Egy tűzfal a tartalomszűrő használatával egy kapcsolat hasznos adatait kiértékelni, ill. az áthaladó adatokat ellenőrizni tudja.

Hálózati címfordítás

(angolul Network Address Translation, NAT)

Lehetővé teszi belső hálózatra kötött saját nyilvános IP cím nélküli gépek közvetlen kommunikációját tetszőleges protokollokon keresztül külső gépekkel. Vagyis, hogy több számítógépet egy routeren keresztül kössünk az internetre. Az elsődleges cél ez esetben az, hogy egy nyilvános IP-címen keresztül több privát IP-című (privát címtartomány: RFC 1918) számítógép csatlakozhasson az internethez. A belső gépekről érkező csomagok feladójaként saját magát tünteti fel a tűzfal (így elrejthető a védett host igazi címe), a válaszcsomagok is hozzá kerülnek továbbításra, amiket – a célállomás címének módosítása után – a belső hálózaton elhelyezkedő eredeti feladó részére továbbít. Egy proxy-val ellentétben itt a csomagokat csak továbbküldik és nem analizálják a tartalmukat.

4.3 Egyéb veszélyek (humán és szervezeti veszélyforrások)

Egy rendszeren belül a legnagyobb veszélyforrást általában a belülről érkező támadások jelentik. Egy szervezeten belül az ilyen támadásokat jellemzően belső munkatársak vagy azok segítségével hajtják végre, ezért rendkívül fontosak azok a

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

technikai védelmeken túlmutató intézkedések, amelyek az úgynevezett humán biztonság megteremtésére irányulnak. Sok esetben ezek egyszerű alapelvek, amelyek betartása adott esetben kényelmetlennek tűnik, de hosszú távon egyértelműen meghozza gyümölcsét.

Kölcsönösen kizáró feladatkörök

A tapasztalat szerint komoly veszélyt jelent, ha egy személynek olyan jogosultságai vannak, amellyel mások engedélye, illetve tudta nélkül végrehajthat visszaéléseket. Ilyenkor aztán akár hosszabb időn keresztül folytatólagosan is elkövethetőek olyan mértékű visszaélések, amelyek sokáig rejtve maradhatnak. Tipikus összeférhetetlen jogkör például egy rendszer fejlesztője – aki módosításokat eszközölhet egy programban – illetve annak üzemeltetője – aki használja az adott rendszert –, ugyanis a program módosításával szinte bármit megtehet a rendszerfejlesztő, bármilyen visszaélés nyomait leplezni képes, ha a működtetést is ő figyeli. Ilyen összeférhetetlen jogkörök továbbá:

- pénzügyi utalványozást előkészítő és azt jóváhagyó;
- hozzáférési jogosultságokat állító adminisztrátor és a rendszer felhasználója;
- adatbázis adminisztrátor és az adatfeltöltő;
- illetve általában egy kritikus műveletet elvégző és az azt jóváhagyó, engedélyező szerepköre.

Bár sok esetben jóval egyszerűbbnek, kényelmesebbnek tűnik, hogy ugyanaz a személy oldjon meg egymásra épülő feladatokat, nem szabad ezt a kompromisszumot

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

megkötni, hanem biztosítani kell, hogy összeférhetetlen szerepköröket különböző személyek lássanak el.

Kötelező szabadságolás, szerepkörök rotálása

Komoly veszélyt jelenthet a szervezetre, ha adott feladatokat csak egy személy képes elvégezni. Ez növeli egyrészt a szervezet sebezhetőségét (munkahelyváltás, baleset stb. esetén komoly kompetencia-hiány alakulhat ki), másrészt megnöveli a visszaélések, csalás valószínűségét. Az ilyen szituációk elkerülésére érdemes rotálni a feladatköröket a megfelelő személyek között, más személlyel helyettesíteni az adott feladatot elvégző személyt, vagy – kritikus esetben – élni a kötelező szabadságolás megoldásával, amely tapasztalatok alapján már sok esetben leplezett le folytatólagosan elkövetett és leplezett visszaéléseket.

„Tiszta képernyő, üres íróasztal” politika

Az „tiszta képernyő üres íróasztal” politika elnevezése arra az alapvető biztonságpolitikai követelményre utal, hogy minden dolgozó pakoljon el az íróasztaláról – a munkavégzés helyéről – a munka befejeztével minden dokumentumot és eszközt a tárolási helyére, ami az adott feladat elvégzéséhez szükséges volt. A munka befejezése itt egyenértékű fogalom a munka felfüggesztésével, szüneteltetésével is, tehát nem csak a munka tényleges befejezését értjük alatta. Az elpakolásba beleértendő a számítógép, fiók le- illetve bezárása, a helység elhagyása esetén a bejárati ajtó bezárása, esetleg riasztó élesítése stb.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Az elnevezésen túl azonban az „tiszta képernyő üres íróasztal” politika egy mélyebb filozófiát takar, nevezetesen azt az elvet, hogy a munka során előkerült és használt információk biztonságáért a munkavégző személy felelős és ezt a felelősséget nem hagyhatja figyelmen kívül, amikor – akár csak öt percre – magára hagyja a munkakörnyezetet.

Az „tiszta képernyő üres íróasztal”politika a gyakorlatban egyszerű és hatásos védelemnek bizonyul a „betekintés” jellegű támadások ellen (például amikor illetéktelen személy hozzáfér egy előhagyott dokumentumhoz), illetve a rendre nevelés révén további jótékony hatása is van. Ezért alkalmazását minden területen javasoljuk.

Social engineering

Social engineering alatt az emberek hiszékenységét/naivitását kihasználni igyekvő támadásokat értjük, magyar szakirodalomban leginkább az angol elnevezést használják.

A sikeres social engineerek többsége rendkívül jó emberi tulajdonságokkal rendelkezik. Kedvesek, udvariasak, szeretetre méltók - ezek azok a jellemvonások, amelyek a gyors kapcsolatépítéshez és a bizalom kalakításához szükségesek. A tapasztalt social engineer megfelelő stratégiával és taktikával gyakorlatilag bármilyen információhoz képes hozzájutni. A hozzáértők szorgalmasan fejlesztik az információbiztonsági megoldásaikat, amelyek minimalizálják a számítógép használatával járó kockázatokat, ám figyelmen kívül hagyják a legsebezhetőbb pontot, az emberi tényezőt. Nem törődünk a fenyegetéssel, ez különösen igaz hazánkban is. Tisztában vagyunk azzal,

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

nem minden ember kedves és őszinte, mégis túl sokszor teszünk úgy, mintha azok lennének. Sok ember hiszi azt, hogy őt nem fogják becsapni/megtámadni, mivel ennek nagyon alacsony a valószínűsége. Egy nagyon egyszerű példa erre az a végtelenül naiv felfogásmód, amivel nap, mint nap találkozhatunk. Tegyük fel, egy jóbarátunk valamilyen online internetes csevegőt használ. Mi utánanézünk ennek a csevegőprogramnak és látjuk, hogyan forgalmazza az üzeneteket. Először eljutnak egy tengerentúli szerverre, aztán visszajönnek, mindeközben akár negyven szerveren is keresztülmennek, ráadásul titkosítatlanul. Abból a negyven szerverből elég összesen egy, ha sebezhető vagy illetéktelen fér hozzá és hallgatózik rajta (sniffel), már tudni fog rólunk mindent, amit csak írogatunk, nem beszélve a tengerentúli központi szerverről, amit szintén egy nagyvállalat üzemeltet, egy vállalatra nézve - ha az éppen munkahelyünk - lehet akár konkurens cég is. A barátunk mit sem törődve ezzel visszakérdez: Ugyan már, miért pont engem hallgatnának le? Ennyire fontos lennék én? Amúgy sem hiszek az összeesküvés-elméletekben.

A támadó nagyon jól ismeri ezt a hozzáállást és kérését olyan természetesen adja elő, hogy nem kelt gyanút, így teljes egészében képes visszaélni az áldozat bizalmával.

4.4 Vezeték nélküli hálózatok védelme

A vezeték nélküli hálózatokon az információ áramlása rádióhullámok segítségével. Ez a lehetőség biztosítja a mobilitást, ugyanakkor a rádióhullámok nem állnak meg a telekhatáron, az épületek falánál, megfelelő árnyékolásuk csak igen költségesen oldható meg. Így az illetéktelen hozzáférés az információkhoz lényegesen könnyebb, mint a vezetékes hálózatok esetén. Ugyanakkor a felhasználók elvárása pedig a vezetékes összeköttetéseket megközelítő biztonság.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

4.4.1 Hozzáférés védelem

SSID Broadcast

A hozzáférést korlátozhatjuk, ha kikapcsoljuk az SSID Broadcast funkciót a hozzáférési pontba. Ez az SSID szétküldését, szétszórását jelenti az Access Point hatótávolságában.

MAC cím szűrés

Ahogy a Routerek beállításaiban általában találkozunk vele: MAC Address Filtering. A MAC (Media-access Control, Eszköz Hozzáférés Ellenõrzés) szűrés annyit jelent, hogy csak azt engedjük a hálózathoz kapcsolódni, akinek az azonosítója szerepel a listánkban. Ezzel korlátozhatjuk az eszközöket, amelyek hozzáférhetnek a hálózatunkhoz.

4.4.2 Titkosítás

Wired Equivalent Privacy

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

A WEP (magyarul kb. a vezetékessel egyenértékű titkosság) volt az első ilyen jellegű szabvány. Létezik 64, 128, 256 és 512 bites változata is. Legelterjedtebb a 64 és a 128 bites WEP.

Nagyon sok oldal tanúskodik arról, hogy még jól beállított eszközök használata mellett is a titkosításhoz használt kulcs hamar (4-5 perc alatt) megfejthető. A WEP titkosítás ugyan védelmet nyújthat az alkalmi próbálkozók ellen, de hamis biztonságérzetet ad, hiszen ingyenes, bárki számára hozzáférhető eszközökkel – mint például az aircrack-ng programcsomag – megfelelő jelerősség esetén nagyon egyszerűen visszafejthető a WEP kulcs. 64bites kulcsot 25 000, 128bites kulcsot 100 000 csomaggal már nagy valószínűséggel lehet törni (A PTW eljárás segítségével, ami az aircrack része). A titkosított csomagok lehallgatása után az aircrack-ng másodpercek alatt megtalálja a használt kulcsot. A szükséges csomagok akkor is kikényszeríthetőek, ha senki se kapcsolódik a hálózatra vezeték nélkül!

Ha eszközünk támogatja a WPA-t, akkor inkább használjuk azt, mert a WEP nyilvánvalóan gyengébb biztonságot nyújt a WPA-hoz képest. Ha a WPA-t nem támogatja eszközünk, akkor lehetőleg minden nap cseréljünk WEP kulcsot, de legalábbis olyan gyakran, ahogy csak tehetjük.

Ezek mellett általánosan ajánlott a hálózati kártyák fizikai címét (MAC) szűrni.

Wi-Fi Protected Access

A WPA (magyarul kb. Wi-Fi védett hozzáférés) egy 2003 óta élő titkosítási szabvány, ma már szinte minden eszköz támogatja – erősen ajánlott használni a WEP helyett. A

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

WPA a TKIP nevű RC4 alapú titkosító algoritmust használja az adatok titkosítására. A TKIP fő előnye, hogy a beállított idő vagy forgalmazott adatmennyiség után új kulcsot generál.

Meg kell jegyezni, hogy igazi biztonságot a WPA is csak akkor nyújt, ha kellően hosszú és összetett jelszót használunk, amivel elkerülhetjük a brute force-támadásokat, illetve a szótár alapú támadásokat.

Az IEEE 802.11i-2004 vagy Wi-Fi Protected Access 2, WPA2 (magyarul kb. Wi-Fi védett hozzáférés 2. generációja) ma már a legtöbb eszköz támogatja, és mivel ez a legbiztonságosabb, ha rendelkezésre áll érdemes ezt használni.

Semmelweis Egyetem
Cím: 1085. Budapest, Üllői út 26.
Telefon: +36 (1) 459-1500
E-mail: hirek@semmelweis-univ.hu
Honlap: http://semmelweis-egyetem.hu

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.