HADMÉRNÖK
V. Évfolyam 2. szám - 2010. június

Szegediné Lengyel Piroska
l.piroska@t-online.hu

SZÁMÍTÓGÉPES BŰNÖZÉS AVAGY FIATALOK A CYBER-TÉRBEN

Absztrakt

A cikk az életünkre komoly kihatással bíró informatika és számítástechnika fejlődésének árnyoldalát, a számítógépes bűnözést, a számítógépes hálózatok, az internet segítségével elkövetett támadások potenciális elkövetőit, az indítékokat próbálja bemutatni. Egy-két évtizeddel ezelőtt a számítógépes bűnözés még közel sem jelentett akkora veszélyt, mint manapság, de mára kimondhatjuk, társadalmi problémává nőtte ki magát. Modern korunkban a számítástechnika egyre nagyobb területeket hálóz be, így a kvalifikált, de az átlag ember is, sőt sajnálatos módon a kiskorú vagy kamasz fiatal is – esetleg tájékozatlansága, járatlansága, vagy egyszerűen figyelemkeltés céljából - sokszor tudatosan, sokszor akár akaratán kívül is elkövethet bűncselekményeket. Fontos társadalmi elvárás, tudatosítani a közvéleményben, hogy a technika gyors fejlődésével, a számítógépek, s főleg a hálózatok elterjedésével, a számítógépes bűnözés világméretűvé duzzadt, így mind több és több ember életére van kihatással, ezért komoly veszélyt jelent, amit nem lehet egyetlen kézlegyintéssel elintézni.

The article is to assist the reader to have a look at the shadow side of the development in the informatics and computer techniques, which have a great impact on our daily life; to present the computer based criminalities, the potential transgressors of attacks committed via computer networks, through the world wide web and to show the reasons laying behind the criminalities. One or two decades ago, the computer based criminalities represented far less risks than they do nowadays, as they became a major social problem to the present time. In our modern age, as computer techniques is conquering greater and greater fields, crimes might be committed by people with high qualification and even by average ones or more over, unfortunately, by small children or teenagers – several times in a willful way, but many times without any will – due perhaps to misunderstandings, misproceedings or to actions when someone would simply draw other's attention. It is an important social requirement to make people understand that due to the rapid technical development, to spreading out of computers and computer networks, the computer based criminalities have been pullulated throughout the entire world, thus the criminalities have a major

threatening impact on more and more people's life and this fact can not be neglected by a wave of hand.

***Kulcsszavak**: kritikus infrastruktúrák, cyber–tér, internet, hacker, terrorista, hardver, szoftver, vírus, információbiztonság ~ substantial infrastructures, cyber space, world wide web, hacker, terrorist, hardware, software, virus, security of information*

BEVEZETŐ

Az internet és más információs rendszerek utóbbi években tapasztalt erőteljes fejlődése lehetővé tette az információk, a termékek és a szolgáltatások gyors áramlását a világ országai határain átívelően. Ez nyilvánvalóan számos pozitív hatással jár, ugyanakkor számos új lehetőséget nyit a bűnözők részére. Egyértelműen megfigyelhető olyan újfajta bűncselekmények felbukkanása, amelyeket az internettel vagy információs rendszerek, mint eszközök felhasználásával követnek el. E bűncselekmények folyamatosan fejlődnek, és a jogalkotás, valamint az operatív bűnüldözés nehezen tud lépést tartani velük.

Az elmúlt években a biztonságpolitikával foglalkozó szakemberek által is megerősítést nyert, hogy a társadalom, a vállalkozások és a polgárok számára egyre nagyobb veszélyt jelent a **számítógépes bűnözés. Az aggodalmat** azonban valójában nem **a** számítógépes bűncselekmények erőteljes szaporodása okozza, hanem inkább ezen bűncselekmények kifinomultabbá válása, a számítógépes bűnözés elleni küzdelemmel kapcsolatos koherens politika és jogalkotás hiánya.

A közeli jövőben a társadalom, illetve az oktatási intézmények fontos feladata lesz a számítógépes bűnözés által jelentett veszélyekre való tudatos felkészülés, felkészítés, a számítógépes bűnözés szakismeretének megszerzésére és a védelmi technikai eszközök kifejlesztésére vonatkozó igény erősítése a leginkább érintettek körében.

De kik a leginkább érintettek? A számítógépes bűnözés a társadalom valamennyi területét érinti, így gyakorlatilag mindenhol fellelhető a vele szemben fellépő védekezés igénye. Érintett a közszféra, hiszen a mindennapi életünket kiszolgáló infrastruktúrákat számítógépes hálózatok működtetik és irányítják. De tekintettel arra, hogy ma, a XXI. században már nagyon sok ember használ magánszámítógépet, így a magánszférát is érinti a számítógépes bűnözés elleni küzdelmet célzó kezdeményezés, hiszen a magánszemélyek is potenciális áldozatok lehetnek

És kik a potenciális elkövetők és mik az indítékaik? A potenciálisan szóba jöhető elkövetőket a cyber tér szereplői között kell keresni – hackerek, hacktivisták számítógépes bűnözők, ipari kémek, vállalatok belső szakértői és külső szerződők, terroristák. [1] -, ugyanakkor potenciális elkövető lehet bárki – gyerek, fiatal kamasz, unatkozó felnőtt… -, aki az elkövetéshez szükséges, elegendő számítástechnikai ismeretekekkel és eszközökkel rendelkezik.

A számítógépes bűnözéssel kapcsolatos biztonsági kérdések átfogó jellegűek, így nem kezelhetők pusztán nemzeti szinten. A veszély nemzetközi jellegű, ezért – legalábbis részben – a válasznak is ilyennek kell lennie. A számítógépes bűnözés elleni küzdelem kétségtelenül továbbra is nemzeti szinten lesz a legfontosabb, egyértelműen szükséges azonban a nemzeti erőfeszítések összekapcsolása és esetleges kiegészítése európai szinten.

I. A SZÁMÍTÓGÉPES BŰNÖZÉS JELLEGZETES VONÁSAI

Bár a számítógépek elterjedésével (ami a 70-es évekre tehető) gyakorlatilag „egyidős" a számítógépes bűnözés, kb. a 80-as évekre tehető az a megállapítás, hogy a számítógépes bűnözés általános jelenséggé nőtte ki magát. Közrejátszott ebben a számítástechnika gyors fejlődése, a személyi számítógépek széleskörű elterjedése, az adatátviteli rendszerek robbanásszerű fejlődése, a szoftverkínálat rohamos bővülése, a bankkártyák elterjedése, és végül az, hogy a védelmi rendszerek fejlesztése elmaradt, ráadásul a meglévők is gyorsan „amortizálódtak" a számítástechnika gyors fejlődésének következtében.

A fejlődés okán a számítógépes bűncselekmények száma és típusai is megváltoztak. Megjelentek az adatmanipulálás útján elkövetett számítógépes csalások, számítógépes hamisítások, védett adatbázisok elleni támadások, illegális szoftver-másolás, terjesztés, visszaélés bankkártyával, telefonkártyával stb.

A helyzetet tovább rontotta a számítógépes hálózatok, s főleg az Internet elterjedése, aminek segítségével a bűncselekmények elkövetése gyorsabbá, leleplezésük még nehezebbé vált. Az 1990-es évektől a számítógépes bűncselekményeket egyre inkább az Interneten – mint legjelentősebb hálózaton – követik el, és az utóbbi években ez a tendencia egyre erősödik. Az Internet sajátos jellemzői – **a nyitottság, az interaktivitás, a decentralizáltság, a globalitás** [2] – teszik lehetővé, hogy a bűnözés számára ideális elkövetési területté váljék.

De mit jelent pontosan a számítógépes bűnözés fogalom? Annak ellenére, hogy a napjainkra a számítógépes bűnözés egyre elterjedtebbé, egyre jelentősebbé vált, még nincsen pontos - szakirodalom által egységesen elfogadott - meghatározása. Ennek oka feltehetően a jelenség változékonysága és sokszínűsége: amennyiben megszületik egy pontos definíció, könnyen lehet, hogy már nem sokat mond a jelenségről, annak változásai miatt.

A pontos fogalom-meghatározást talán az is gátolja, hogy nincs egységes álláspontom a szakirodalom a jelenség elnevezése tekintetében sem: **számítógépes bűnözés** vagy **informatikai, adat bűnözés** vagy **hitech bűnözés** vagy **cyber terrorizmus**?

Elnevezéstől függetlenül, egy olyan jelenséggel állunk szemben, amely minden társadalomra nézve veszélyes, mert egyrészt olyan tevékenység, amely számítógépes rendszerekbe történő közvetett, vagy közvetlen behatolással anyagi, illetve szellemi javakban kárt okoz, másrészt az információ-technológiai eszközök, rendszerek, illetve rendszerelemek ellen irányul, illetve ezeket az eszközöket, rendszereket használja a bűncselekmények elkövetésének eszközeként.

A számítógépes bűnözés egyik **fő jellegzetessége** a **gyorsaság**, amely az eredmény realizálódására vonatkozik. A gyorsaság, tehát nem azt jelenti, hogy a bűncselekmények a pillanat szülöttei, bár ez is gyakori eset, de az „akciók" többségére nem ez jellemző, hiszen tudjuk, hogy a legtöbb ilyen bűncselekmény komoly előkészületeket igényel. Az elkövetéseket megelőzi a megfelelő szoftverek beszerzése, azok kezelésének megismerése, biztonsági rendszerek kiismerése, információk beszerzése, gyűjtése és mindezek mellett hosszú tanulás (pl.: főiskolákon, egyetemeken, vagy autodidakta módon), és nem utolsó sorban gyakorlatszerzés.

Modern korunk technológiai, technikai színvonala, az egyre gyorsabb számítógépek, az elkövetők szakmai tudása és rutinja lehetővé teszik, hogy egyre gyorsabban lehet elkövetni a bűncselekményeket. Mindehhez hozzájárul az Internet elterjedése, így már világszerte, nehezen ellenőrizhető módon lehet, nagy gyorsasággal elkövetni számítógépes bűncselekményeket. [3]

A számítógépes bűnözés területét jellemző **magas látenciának** több oka van: Egyik, hogy a bűncselekmények egy része sokszor még a sértett előtt is rejtett marad pl.: betörnek a számítógépére, s másolatot készítenek egyes filekről, de nem észleli azt. A magas látencia másik fő okát egy elég sajátos jelenségben kell keresnünk, abban, hogy az esetek egy részét a sértettek nem jelentik. Ez általában a gazdálkodó szervezetekre és főleg a hitelintézetekre, biztosítókra jellemző, akiknek komoly érdeke fűződik ahhoz, hogy titokban maradjanak az esetek. „…… naponta tapasztaljuk, hogy a médiában bemutatni egy-egy informatikai támadást igen nehéz feladat, ennek következtében számos alkalommal még a sikeres támadásokat és azok következményeit is elhallgatják a megtámadott rendszerek üzemeltetői. Ebben élen járnak a bankok, bár az ő esetükben (is) komoly anyagi veszteséget okozhat – akár közvetett módon, pl. bizalomvesztés miatt – egy-egy ilyen támadás. Így többé-kevésbé érthető, ha nem, vagy nem szívesen ismertetik az ilyen eseteiket. Ugyanakkor azt is el kell mondani, hogy a kritikus ágazatok közül pont a pénzügyi szektor, ezen belül is a bankok azok, amelyek a lehető legtöbb figyelmet fordítják a fizikai védelem mellett az információs rendszereik védelmére". [4] A látenciát tovább fokozza, hogy a tettesek felfedezésének alacsony az esélye, mivel általában nem tartózkodnak az elkövetés helyszínén, az akciókhoz nincs szükségük külső segítőkre, így a kommunikációs csatornákon könnyedén és nyomtalanul eltűnhetnek.

Hangsúlyozni szükséges a számítógépes bűnözés erős **nemzetközi jellegét** is, többek közt azért, mert az elkövetők az Internetet, vagy egyéb más számítógépes hálózatot használnak a bűncselekmények során. Az Internet egy olyan virtuális világ, melyben nincsenek államhatárok, a névtelenség álarca mögé bújhat bárki. Kedvez az elkövetőknek, hogy az Internet hatalmas adatállományát, adatforgalmát nem lehet ellenőrizni, így a visszaéléseket nagyon nehéz nyomon követni.

Mindezek függvényében leszögezhetjük, hogy a számítógépes bűnözés rendkívüli mértékben függ a **technológia, technika fejlettségi szintjétől**, hogy a számítástechnikai eszközök, és azok rohamos fejlődése nélkül elképzelhetetlen lenne a létezése. Megfigyelhető az a tendencia, hogy amint kifejlesztenek egy újabb számítástechnikai vívmányt – hardvert, szoftvert…. – a bűnözők idővel felhasználják azokat az elkövetés során. Ha tehát valaki véget akarna vetni a számítógépes bűnözés fejlődésének, annak az alapot képező technikai fejlődést is meg kellene állítania.

A számítógépes bűnözés **intellektuális bűnözésnek** nevezhető, mert kialakulásához, a technológiai háttér mellett, jól képzett szakemberek *tömeges* megjelenésére és *tömeges* képzésére volt/van szükség. Amennyiben áttekintjük a számítógépes bűnözés fejlődését, észrevehetjük, hogy amíg a technika és a szakképzés nem vált tömegessé, addig nem is ölthetett olyan méreteket, mint napjainkban.

Az elkövetők **általában fiatal, magasan képzett, magas intelligenciájú, számítógépes szakemberek,** akik nem ritkán 2-3 fős csoportokba szerveződve követik el a bűncselekményeket a globalizáció és a technika, elsősorban az Internet felhasználásával. Az esetek többségében sokoldalúan szocializált elkövetőkről beszélhetünk, akik tisztában vannak

a jogaikkal, akik szakképzettségük miatt jó egzisztenciális körülmények között élnek. Természetesen olyan számítógépes bűncselekményekkel is találkozunk, amelyek elkövetése nem igényel magas szakképzettséget, az okozott kár azonban meglehetősen jelentős: vírusok, trójai programok… [5]

Összegezve elmondhatjuk, hogy az internet térnyerésével az emberi közösségek számára kitárult a világ, bárki számára hozzáférhetővé váltak eddig ismeretlen, vagy nehezen hozzáférhető információk, felgyorsult a kommunikáció, on-line üzenetváltások. Az internet hihetetlen lehetőségek tárát nyitotta meg, amely újfajta gondolkodást igényel az emberektől. Mára elmondhatjuk, a bűnözés új ága fejlődött ki, sokkal védtelenebbé téve az embereket, gazdálkodó szervezeteket. Gyermekek, személyes adatok, üzleti, szolgálati és államtitkok kerülnek veszélybe, gyanútlan embereket használnak ki, hatalmas méretű csalásokat hajtanak végre, amivel akár nemzetek gazdaságát dönthetik romba a láthatatlan bűnözők.

II. A SZÁMÍTÓGÉPES BŰNÖZÉS ÉRINTETTJEI

Az információs bázisokon a potenciális elkövetők különböző számítógépes hálózatok működési mechanizmusa után kutatnak. Kiemelt fontosságot képeznek számukra az olyan struktúrák, amelyek:

- közlekedési rendszerek ellenőrzésére szolgálnak, elsősorban a légi és vasúti közlekedés irányítására szolgáló infrastruktúrák
- állami intézmények - kiemelten a katasztrófa-elhárítással és a személyes adatok tárolásával megbízott intézmények, a távközlési hálózatok - igényeit szolgálják ki
- nem állami, de létfontosságú feladatot ellátó szervezetek működését támogatják, mint például a bankok, pénzintézetek vagy az áramszolgáltatók. [6]

Bár a hálózatok általában technikailag igen jól védettek, biztonsági protokollokkal nehezítve az adatokhoz való hozzáférést, mégis a tervezőknek több olyan körülménnyel is számolniuk kell, amelyek áthatolhatóvá teszik az egészen biztonságosnak hitt rendszereket is.

Különös figyelmet érdemelnek a napjainkban egyre jobban elterjedőben lévő számítógépes banki rendszerek, amelyeken pénzügyi tranzakciók sokaságát hajtják végre, így viszonylagos rendszerességgel esnek áldozatul támadási kísérleteknek is. Az elkövetők a rendszereket nemcsak illegális átutalásokra, hanem zsarolásra, üzleti tranzakciók megbénítására is használhatják

Az utóbbi években bizonyosságot nyert, hogy a számítógépes bűnözések tulajdonképpen bárki ellen irányulhatnak, mégis leszögezhető, hogy az elkövetők fő célpontjai. - a bűncselekmények többségében - a vállalatok.

A vállalatok, hivatalok sérelmére elkövetett bűncselekmények közül súlyuknál és számuknál fogva kiemelkednek az adatok megszerzésére, vagy manipulálására irányuló bűncselekmények, valamint az anyagi haszonszerzést célzó bűnelkövetések is. Ezeknél a bűncselekményeknél gyakran a sértettek könnyelműsége vezet oda, hogy áldozattá válnak. Nem vigyáznak kellőképpen jelszavaikra, amit ha, megszereznek az elkövetők, könnyen bejuthatnak a kérdéses rendszerekbe.

Összegezve megállapítható, hogy az Interneten végrehajtott támadások napjainkig egyelőre helyi jellegűek voltak határozott és pontos célokkal, ám a jövőben - szélesebb körű elterjedésükkel - nem zárható ki, hogy több támadás ér majd olyan nyílt rendszereket, amelyek létfontosságú infrastruktúrák, katasztrófavédelmi és pénzügyi létesítmények működését támogatják. Mindez megköveteli, hogy a jövőben kellő hangsúlyt fektessünk a számítógépes bűnözés elleni védekezés oktatására, mivel az emberek csak kellő informáltság mellett képesek felkészülni az ellenük irányuló támadásokra.

III. AZ ELKÖVETŐK

Amikor számítógépes bűnözésről beszélünk, megállapíthatjuk, hogy tulajdonképpen önmagában a technika nem veszélyes, az elkövetők azok, akik nem megengedett, illegális célokra használják.

Legelőször azt érdemes tisztázni ki válhat elkövetővé, milyen feltételeknek kell megfelelni? Véleményem szerint megfelelő szinten kell értenie a technikai eszközökhöz, azok kezeléséhez, olyan helyzetben kell lennie, amely lehetővé teszi számára a számítógép, vagy egyéb számítástechnikai eszköz használatát, aminek segítségével elkövetheti a bűncselekményt.

A tapasztalatok szerint társadalmi helyzetüket, munkakörüket tekintve **az elkövetők többsége magasan képzett, törekvő ember**. Többségük alkalmi haszonszerzés céljából követi el a bűncselekményt. Az elkövetők másik köre nem rendelkezik jelentősebb szakismerettel, olyan emberek, akik talán véletlenül döbbentek rá, hogy mi mindent tehetnek egy számítógéppel, s egyszerűen csak kihasználják az adandó alkalmat.

„Egy adott vállalat életében óriási szerepet játszanak a **szakértők,** akik sok esetben számos helyen - akár több telephelyen - is végzik munkájukat. A szakértők munkájuk elvégzése érdekében általában magas szintű hálózati hozzáféréssel rendelkeznek. Ebből következően adott esetben - pl.: munkahelyi konfliktusok, zsarolás, stb. - igen értékes adatokat tud eltulajdonítani, illetve akár különböző rosszindulatú programok bevitelére is lehetősége van, hiszen a hálózathoz belülről fér hozzá. A **külső szerződők** szintén kaphatnak hozzáférési jogokat a hálózathoz, és természetesen szintén számos igen értékes adathoz férhetnek hozzá, amelyekkel később visszaéléseket követhetnek el.” [1]

Megfigyelhető az is, hogy a számítógépes bűncselekményeket elkövetők gyakran bizalmi pozíciót töltenek be egy adott cégnél, ami nagyban megkönnyíti az elkövetést, hiszen az emberek bizalmával visszaélve könnyen hozzájuthatnak jelszavakhoz, s kijátszhatják a védelmi megoldásokat. A vállalatokat ért támadások közül komoly figyelmet érdemelnek a kívülről jövő támadások, amelyek esetében a támadók a **hackere**k.

„A hacker olyan személy, aki internet segítségével hozzá tud férni védett adatokhoz a számítógépeken. Kezdetben külön fogalmat alkottak a hackerek, akik azért törtek fel rendszereket, weboldalakat, illetve programokat, hogy bizonyítsák azok gyenge pontjait, azonban ezeket a hiányosságokat a rendszergazdák tudomására hozták, azaz általában jóindulatúan jártak el. Ők voltak az úgynevezett fehérkalaposok, azaz a "white hat" csoport tagjai. Az ellentábort azok a fekete kalaposok, "black hat" alkották, akik sokszor

rosszindulatból, vagy valamilyen haszonszerzés reményében hatoltak be egy-egy rendszerbe" [1]

A hackerek motivációik, céljaik elég eltérőek lehetnek: károkozás; védett adatok megszerzése, kíváncsiság, erőfitogtatás, tapasztalatszerzés, de utalva az előbbi meghatározásra, a „jó hackerek" segítő szándékkal törnek be egy rendszerbe. Felhívják a rendszergazda figyelmét a védelmi hiányosságokra, ezáltal segítik a hatékony védelmi rendszer kiépítését, Természetesen a jó szándék ellenére is komoly károkat okoznak, hiszen a rendszer feltörhető, irreleváns, hogy jobbító szándékkal törték-e fel vagy sem.

Napjainkra kialakult egy elkövetői réteg, az ún. **komputerunderground,** amely kategóriába az alábbi elkövetők sorolhatóak: [7]

- **Hackerek, crackerek** (A crackerek annyiban különböznek a hackerektől, hogy jellemzően haszonszerzési céllal törnek be védett rendszerekbe)
- **Phreakek** (Telefonvonalakba, illetve rendszerekbe próbálnak technológiai eszközökkel bejutni.)
- **Vírusírók** (Olyan személyek, akik olyan kódokat írnak, amelyek megpróbálnak behatolni más rendszerekbe, s gyakran mellékhatásokat is produkálnak)
- **Kalózok** (A crackerek közül váltak ki, szoftverek védelmi rendszereit feltörő személyek, akik e tőrt-szoftvereket terjesztik is.)
- **Cypherpunkok** (Olyan programokat terjesztenek, melyekkel bárki adatait erős kódolással láthatja el – nagy teljesítményű számítógépekkel is komoly feladat feltörni az ilyen erősen kódolt adatokat)
- **Anarchisták** (Törvénysértő, vagy legalábbis morálisan kétes megítélésű információkat terjesztő személyek. Olyan személyek, akik minden olyan kísérletet, rendelkezést elutasítanak, amely akadályozná az információ szabad áramlását)

Az elkövetők között meg kell említenünk a **terrorista** szervezeteket is, akik egyrészt propaganda, toborzás, adatszerzés céljából használják a számítógépes rendszereket, másrészt ezeken keresztül rombolnak, erőszakos bűncselekményeket hajtanak végre.

„A tapasztalatok szerint a független csoportok, hacktivisták által elkövetett incidensek előfordulási lehetősége nagy. Különösen igaz ez Magyarország esetében, hiszen a konfliktusokkal teli szomszédságpolitika bármikor elérheti azt a hatást, hogy a kormányoktól független szélsőséges csoportosulások néhány tízezer dollárnyi befektetéssel, mely akár nacionalista vállalkozói rétegtől vagy az alvilágtól is származhat, sikeresen zavarják meg hazánk mindennapos működését. Az országok közötti hasonló konfliktusok bekövetkezési valószínűsége kicsi, ám az informatikai kémkedés valószínűleg mindennapos, így a kritikus információs infrastruktúrák védelme mindenképpen kiemelt fontosságú." [4]

A támadásokat potenciálisan elkövetők típusa, száma igen nagy, és sajnálatos módon erőteljesen növekszik a deviáns, frusztrált, érzelmileg labilis fiatal kamaszok megjelenése a cyber–térben. Véleményem szerint egy átlagos számítástechnikai ismeretekkel rendelkező fiatal képes egy olyan egyszerű programot készíteni, vagy azt - interneten való jártassága miatt - különféle hacker oldalakról „beszerezni", amely, ha eljut egy célszámítógépre, azon automatikusan – a készítő beavatkozása nélkül – kicsomagolja és futtatja magát, majd a futtatás során elkövet valamilyen bűncselekményt, pl.: töröl bizonyos dokumentumokat, avagy lemásolja azokat, s továbbítja a készítőhöz. Az ilyenfajta bűncselekmények rendkívül gyorsan történnek, s a sértett akkor sem észleli, ha éppen a számítógépe előtt ül, s mivel a program minden nyomot megsemmisít, az elkövető biztonságban érezheti magát, hiszen ő

részt sem vett a bűncselekmény tényleges kivitelezésében. További veszélye az ilyen programoknak, hogy hálózatokon, Interneten keresztül, egyszerre juthatnak el rengeteg sértetthez.

Tovább vezetve ezt a gondolatot, egyre jellemzőbb, hogy **fiatal kiskorúak** követnek el számítógépes bűncselekményeket. Például egy előre elkészített programmal „életre hívnak" egy vírust, s azt útnak indítják az Interneten, ami akár jelentős károkat is okozhat. Meg kell azonban jegyeznünk, hogy a kiskorú fiatal elkövetők között inkább a file-cserélés és az illegális szoftvermásolás, terjesztés a jellemzőbb, ami bár enyhébb bűncselekmény, mint a vírusírás, de megfelelő odafigyelést kíván meg. A jelenség azért is aggasztó, mert koruknál fogva ezek a fiatalok nem látják, nem érzik át tettüknek súlyos következményeit.

IV. AZ ELKÖVETŐK INDÍTÉKAI

Az elkövetők motivációi rendkívül sokfélék lehetnek. Gyakori motiváció az **anyagi haszonszerzés,** amely a szoftverek jogosulatlan másolásának, forgalmazásának, a félvezetők tiltott másolásának, kereskedésének hátterében is áll, vagy **a védett személyes adatok, állami, szolgálati, banktitok jogellenes megismerésére irányuló szándék.**

Következő motivációként a **károkozás** emelhető ki. Az elkövetők betörnek rendszerekbe, és védett adatállományokat törölnek, módosítanak, vagy lemásolnak, s így azon túl, hogy komoly károkat okoznak, megsértik az egyes emberek magánszféráját.

Elsősorban munkahelyeken, fiatalok esetében az iskolában gyakori motiváció a **frusztráltság, elismerés hiánya**, vagy ami sokkal veszélyesebb **a bosszú**, de kiskorúak körében gyakran előfordul, hogy az **unatkozá**s, az **unalom váltja ki a** bűncselekmény elkövetését.

Bárkinél, de jellemzően a fiataloknál, további motiváló erőként jelentkezhet az **„Internet-mítosz"** nyújtotta hamis kép is, tehát amennyiben rendelkezik Internet hozzáféréssel, beléphet egy virtuális világba, egy olyan világba, ahol bármit megtehet (akár bűncselekményeket is elkövethet), amely világ teljesen más életformát kínál, mint a valódi, gyorsan a ranglétra legtetejére lehet emelkedni, s ott már szinte korlátlanok a lehetőségek.

"Az új világban mindenki a PC-je segítségével az Interneten keresztül fogja bonyolítani az ügyleteit, így aki nem akar lemaradni, aki modern, up-to-date ember kíván lenni, annak muszáj internetezni. Az igazán modern ember mindent az Interneten csinál ….Ha mindenki részesévé válik az Internet kínálta lehetőségeknek, és aktív felhasználója lesz a rendszernek, akkor bekövetkezik az "információs forradalom", és eljön a világbéke." [8]

A fiatalok számára komoly csábítást jelenthet egy ilyen lehetőség, s minél jobban megtanulják kezelni az Internetet, annál nagyobb lesz a csábítás. Véleményem szerint az Internet-mítosz erős hajtóerőként jelenhet meg azon fiataloknál, akik gyengébb iskolai teljesítményük miatt bizonyítási kényszert éreznek, vagy akik zárkózott, visszahúzódó magatartásuk miatt nehezebben kötnek barátságokat.

A bűnözés intellektuális jellegéből adódóan, a számítástechnika egyre népszerűbbé válásából eredően, sok, számítástechnikában jártas fiatal **szakmai kihívásként is** felfoghatja a bűnelkövetést, míg másokat a **hírnév-szerzés, mások elismerésének a megszerzése, az erőfitogtatás motiválhat**.[9]

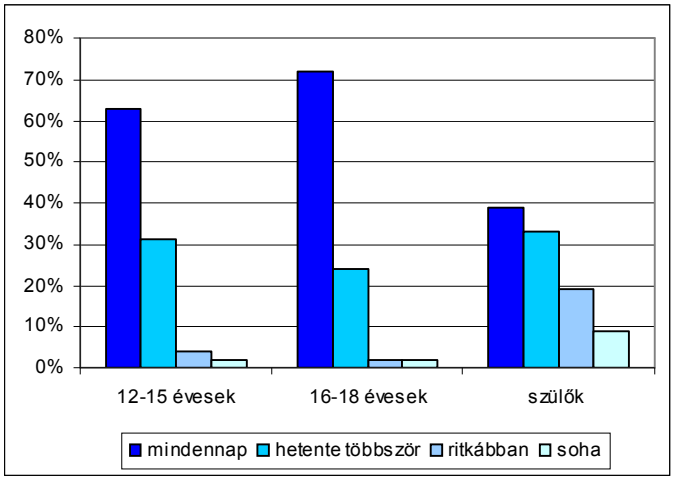
V. FIATALOK A CYBER-TÉRBEN

Az Internet nélkülözhetetlen eszköze a tudás megszerzésének, de a hálózat egyúttal rengeteg veszélyt is rejt. Az internet használata közben véletlenül is váratlan, szokatlan dolgokkal találkozhatunk.

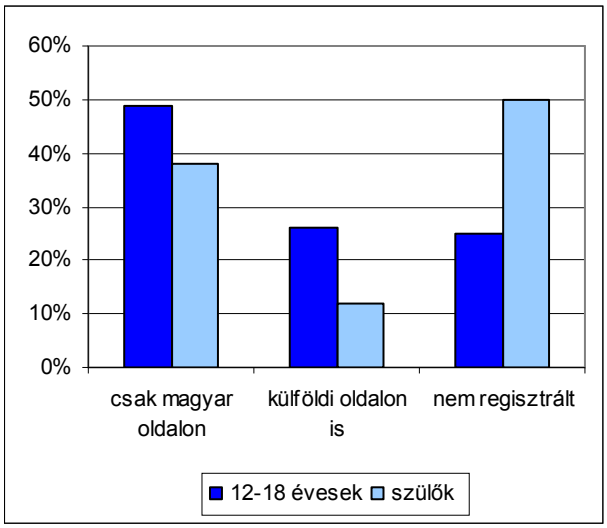
Kellemetlen tény, hogy bárkiből lehet elkövető és áldozat egyszerre. Az interneten barangoló személy gépe bármikor beleütközhet egy olyan szoftverbe, mely önmagát letölti a gépre és telepíti, vagy a rosszindulatú támadás áldozata lesz. Az ilyen gépeket a tulajdonos tudta nélkül képesek felhasználni bármire: fontos információt tölthetnek le a fertőzött gépről, képesek nem kívánt üzenetek (spam) ezreit szétküldeni onnan, de fel tudják használni akár más számítógép megfertőzésére is.

A tapasztalatok szerint a legsérülékenyebb és legveszélyeztetebb korcsoport a fiatal kamaszok, hiszen az internethasználat mára már életük részévé vált. Õk általában zenét töltenek le, azonnali üzenetküldõ (IM) programokat használnak, leveleznek, és on-line játékokat játszanak. Gyakran használnak keresõmotorokat is, hogy ráleljenek az általuk keresett információra. Többségük felkeresett már csevegõszobákat, és elképzelhetõ, hogy részt vettek felnõtt témájú csevegésben is. A tizenéves fiúk fegyelmezetlenebbek, róluk képzelhetõ el inkább, hogy véres vagy szexuális tartalmú honlapokra látogatnak, vagy szerencsejátékokba kezdenek. A lányok esetében inkább az a veszély fenyeget, hogy szexuális zaklatások érik õket.

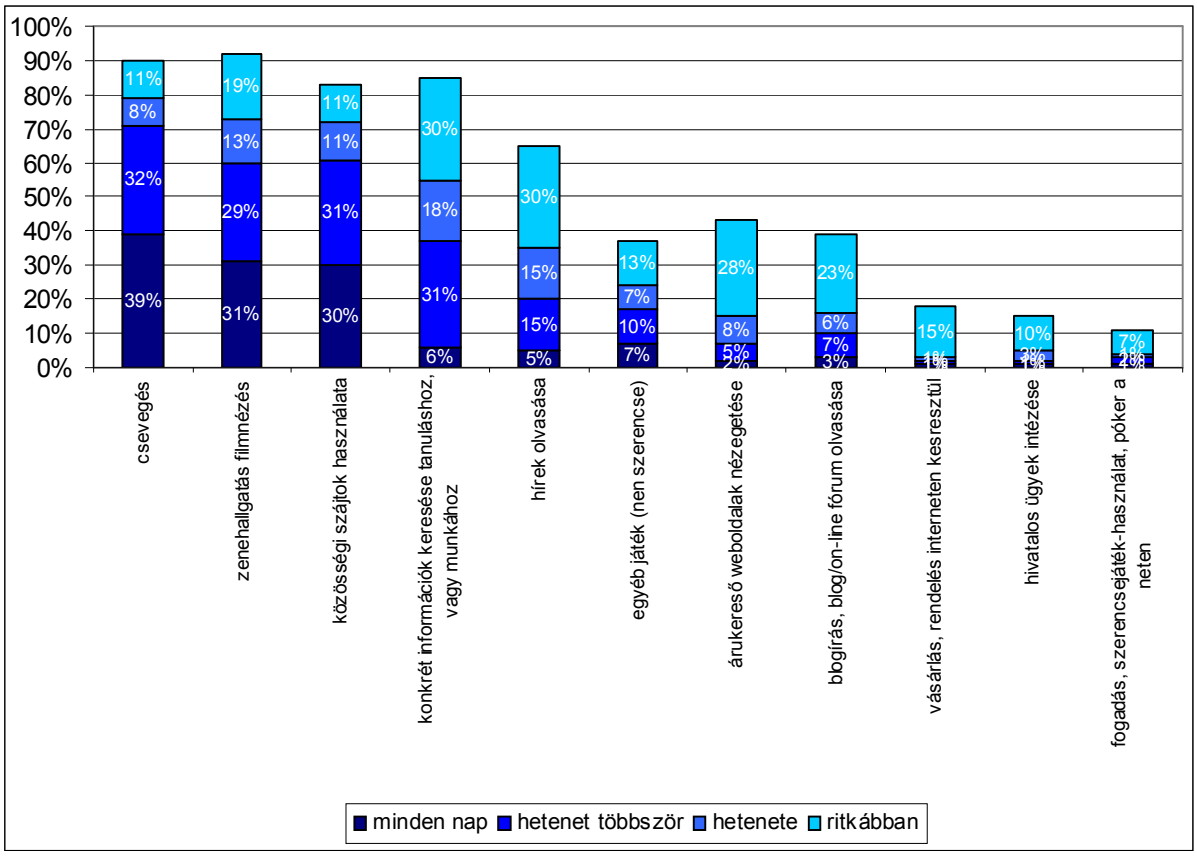
Egy 2009. évi felmérés szerint a 12-18 évesek 93 százalékának van Internet-hozzáférése, 86 százaléknak otthon is. A számítógép előtt hétköznaponként átlagosan 2 órát, hétvégeken közel 3 órát töltenek el



1. ábra. Otthoni Internet-használat, akiknek van otthoni internet hozzáférésük [Forrás: MEDIÁN, 2009]



2. ábra. Regisztrálás névvel, jelszóval [Forrás: Medián, 2009]



3. ábra. Mire használják a fiatalok az Internetet [Forrás: Medián, 2009]

A kamasz fiatalok - életkorukra való tekintettel -, az adaptív kockázatkeresés korszakában vannak, amit az evolúciós pszichológia „fiatal férfi szindrómának” nevez. Az „együttes élmény” hiánya a szülővel, vagy barátokkal, fokozza a magány, a depresszió, az unalom érzését, ami növeli az internet függőség kockázatát. Lehetnek olyan időszakok ebben a korban, amikor valamilyen érzelmi, hangulati vagy impulzus-kontroll probléma miatt erős függőséget mutat egy fiatal, vágyik felfedezni önmagát, elkívánkozik a szülői felügyelet alól, és a családon kívül keres új kapcsolatokat. A névtelenség látszata alatt szívesen vállal

kockázatot anélkül, hogy teljesen tisztában lenne a lehetséges következményekkel. Aggodalomra ad okot, hogy az interneten elérhető tengernyi információ - számtalan eset mutatja - csak súlyosbítja a fiatalok aggodalmait személyes problémáikkal kapcsolatban

Hosszasan lehetne sorolni az internet negatív hatásait, de emellett hangsúlyoznunk kell az áldásos oldalát is, azokat a lehetőségeket, amelyeket a fiatalok számára, a tudományos ismeretszerzéséhez nyújt. Elég arra gondolnunk, hogy az érdeklődő fiatal majdnem minden hírportálon találkozhat tudományos hírekkel, amelyekkel szélesítheti látókörét, bővítheti általános műveltségét. A használható nyelvtudással rendelkezők válogathatnak a világ vezető tudományos oldalainak kínálatából, de akár egészen speciális témákról is találhatnak hasznosítható anyagot.

Egyes fiatalok szakmai ambícióból, míg mások csak hobbiból, szeretnek elmélyedni egyes tudományágakban, így - a mai információ és kommunikáció alapú világunkban meghatározó szerepet betöltő - informatikában is. A világháló ehhez minden lehetőséget felkínál: az informatikának szinte minden ismerete megtalálható az interneten. Bármilyen szinten áll az érdeklődő, óriási támogatás és tudásanyag áll rendelkezésére a további fejlődéshez. Motivációval és kitartással komolyabb szintű szaktudás is szerezhető autodidakta módon.

Azon fiatalok, akik kutatói ambíciókkal rendelkeznek, vagy csak mélyebben szeretnének megismerni egy-egy speciális területet, szintén kihasználhatják a világháló nyújtotta lehetőségeket. A speciális szakmai oldalakon megismerhetik szakterületük új eredményeit, felfedezéseit.

Annak igazolására, hogy a mai fiatal nemzedék jó néhány csoportja kellő szakmai ismerettel rendelkezik, hogy - az internetről szerzett vagy saját ötletek alapján - anyagi haszonszerzés, de inkább, csak „egy jó hecc, egy jó balhé” kedvéért törvényellenes cselekményt kövessen el, nézzünk meg néhány esetet:

1. eset
2000. március 9-én jelent meg az a sajtó-hír, amely nyilvánosságra hozta, hogy a Rendőrség felderítette, elfogta és büntetőeljárás alá vonta azt a magyar hacker-társaságot, amely januárban kétszer is feltörte az Elender szervereit. A rendőrség kiemelt ügyként kezelte a bűncselekményt, mert a nyomozás során gyorsan felismerte, hogy nem egyszerű "piaci lopásról" van szó, hanem az internetre kapcsolódó számítógépes hálózatok ellen elkövetett olyan bűntényről, amely nemcsak a szolgáltatóknak okozhat károkat, hanem adott esetben a közszolgálati, a kormányzati, sőt a titkos adatbázisokat is veszélyeztetheti. A nyomozás során kiderült, hogy a fiataloknak nem volt az Elender Rt. alkalmazásában álló segítőjük. A számítógépes csalás bűntettével vádolt 15 és 19 éves fiatal hackerek vallomásukban azt állították, hogy **unaloműzésként** törték fel az Elender szerverét, és az ehhez szükséges speciális ismereteket autodidakta módon sajátították el. Arra nem gondoltak, hogy noha nem nyereségvágyból törtek be a szolgáltató szervereire, mégis több tízmilliós kárt okoztak a cégnek.[http://www.jogiforum.hu/publikaciok/75]

2. eset
Egy ismeretlen személy 2003. október 28-án az Országgyűlés Hivatala, a BRFK, valamint több kereskedelmi tévécsatorna e-mail címére fenyegető tartalmú levelet küldött, amelyben a Parlament és a Nemzeti Bank felrobbantásával fenyegetőzött. A Nemzetbiztonsági Hivatal

megállapította, hogy az e-maileket egy dunaújvárosi szakközépiskola számítógépéről küldték. Az iskola számítógépes nyilvántartási rendszerében végzett kutatás során beigazolódott, hogy az e-mailt egy ötödéves - stúdiókezelő feladatokat is ellátó - hallgató küldte, más felhasználói névvel belépve a rendszerbe. A Hivatal tájékoztatta az ORFK illetékes szervét, amely soron kívül végrehajtotta a diák meghallgatását. A fiatal a cselekmény elkövetését beismerte, tényleges végrehajtását nem tervezte, azt **"diákcsínynek"** szánta. [http://www.nbh.hu/oldpage/evk2003/terror.html]

3. eset

„Kétszáz óra közhasznú munkára ítélte egy brit bíróság azt a fiatalembert, aki még a tavalyi év során tört be egy amerikai részecskekutató intézetbe, és bénította meg annak működését napokra. Az ifjú hacker személyes zene- és filmgyűjteményének tárolására használta fel az intézet közel másfél tucat számítógépét, miután saját gépének merevlemezén már nem fértek el a nagyméretű médiaállományok.

A 18 éves James McElroy még 2002. májusában nyert illetéktelen hozzáférést az amerikai kormányzat által üzemeltetett Fermi Nemzeti Gyorsítóhoz, ahol a részecskekutatással és nukleáris kutatásokkal foglalkozó intézet 17 számítógépét kerített hatalmába. A több száz gigabájtnyi adatot illegálisan feltöltő fiatal többek között barátaival történő fájlcserélgetésre használta az áldozatul esett gépeket. McElroy a bíróság előtt azzal védekezett, hogy **fogalma sem volt** arról, hogy a megtámadott gépek kormányzati kutatólaboratóriumhoz tartoznak. A betörés által okozott zavarok következtében a részecskegyorsító működése három napig szünetelt, közel 21 ezer fontnyi kárt okozva az intézetnek." – olvashattuk a hírt az interneten is. [http://pcforum.hu/hírek/?qnid=2101&nfr=1&auth= f149 b6a885fa]

4. eset

Richter Csabát 3 év börtönre ítélték 2005-ben azért, mert feltörte az Ericsson informatikai rendszerét, és az onnan ellopott információkat **pénzért akarta eladni** a cégnek. A svéd titkosszolgálat tartóztatta le, mert fontos, bizalmas adatokhoz fért hozzá. Saját bevallása szerint hozzáfért telefon-szoftverek forráskódjához, radar förmverekhez, a Gripenek radarrendszerének rajzához, valamint adminisztrátori jogosultságot szerzett több rendszerben. [http://www.origo.hu/techbazis/internet/200504043ev.html]

5. eset

2004. áprilisában söpört végig Magyarországon, azután Európában is a Zafi névre keresztelt vírus, amely nevét erősen politikai töltetű tartalma miatt a hazafi szóból kapta, és amely hosszú hónapokig a legfertőzőbb kártevők közé tartozott. A vírus törzse szerint a pécsi SNAF Team készítette a kódot.[http://itcafe.hu/hir/zafi_a_virus_egy_igazi_hungarikum.html]

Összegezve elmondhatjuk, hogy a világ, így Magyarország informatikai rendszereit is folyamatosan támadások érik, érhetik, ezért a képzett fiatalok, a jó hackerek jó szolgálatot tennének az ország informatikai piacának és biztonságának is. Meg kell becsülnünk azokat a fiatalokat, akik rengeteg energiát fektetnek a rendszerek megismerésébe, és szaktudásukat a jó cél érdekében használják fel. Oktatási intézményeinkkel szemben fontos elvárás a jövőben, hogy a fiataloknak egyrészt magas szintű, az üzleti életben is hasznosítható informatikai ismereteket oktassanak, másrészt, hogy kiemelt hangsúlyt fordítsanak az **információbiztonsági ismeretek** oktatására.

Fontos elvárás továbbá a szülőkkel szemben, hogy ismerjék gyermekeik internetezési szokásait, hogy ismerjék azokat a játékokat, amivel a gyerekük játszik, hogy próbálják meg ésszerűen korlátozni gyermekük internet-használatát, hogy figyeljenek oda arra, gyermekük

mivel foglalkozik az interneten, és próbálják meg irányítani a „barangolásukat”. Véleményem szerint a fiatalok számára a legkézenfekvőbb és leghatékonyabb védelmet a jól funkcionáló családok biztosíthatják a cyber-térben.

ÖSSZEGZÉS

Az Internet elterjedése következtében a számítógépes bűnözés az egész világon elterjedt jelenséggé vált. Manapság kellő szakértelemmel és egy Internet hozzáféréssel rendelkező számítógép segítségével rendkívül gyorsan hatalmas károkat lehet okozni másoknak.

A jelenség jellemzőinek számbavételekor láthattuk, hogy a jelen kor, egyik veszélyes bűnözési formájával állunk szemben, veszélyességének egyik legfőbb forrása, hogy igazából bárki lehet elkövető, csak a szükséges technikai felszereltség (ami manapság már viszonylag olcsón beszerezhető) és némi szaktudás szükségeltetik, szemben mondjuk egyes hagyományos bűncselekményekhez, amelyekhez akár erős fizikum, drága felszerelések kellenek.

Ami a jövőt illeti, hangsúlyozni szükséges, hogy az információs társadalom térhódításával együtt a számítógépes bűnözés jelentősége s egyben veszélye is csak nőni fog. Az információs társadalom jövőképe a tudástársadalom: egy új minőségű, tudásközpontú, hálózati jellegű társadalom, ahol rendkívül fontos szerepe lesz az információnak, és a számítástechnikának. Egy információs társadalomban, ahol mindenki a mainál sokkal jobban függ a számítógépektől, számítógépes rendszerektől, s azok működőképességétől, illetve, ahol az információ s annak biztonságos megőrzése társadalmilag fontos tényező, igen komoly veszélyt jelent a számítógépes bűnözés.

A fiatalok közül a 12-18 éves korcsoport intenzíven használja a digitális technológia áldásait, és ezzel nagyobb kockázatot is vállalnak más korcsoportoknál. A biztonságos internetezés tudatosításának ezért elsősorban erre a korosztályra kell összpontosítania, különös tekintettel a közösségi oldalak használatában rejlő veszélyekre. Tudatosítani kell a fiatalokban az internet, az email, az üzenetváltó programok és a fizetős oldalak használatában rejlő veszélyeket.

Figyelemre méltó kezdeményezés a gyerekekre káros internetes tartalmak kiszűrését támogató **Biztonságos Böngészés Program (BBP),** amelyhez már több száz iskola csatlakozott, illetve több ezer munkaállomás tagja a programnak. Az iskolák számítógépeire olyan szoftvert telepítenek, amelyek képesek megvédeni a gyerekeket a káros vagy nem nekik való tartalmaktól és az internetes zaklatástól. A biztonságos böngészés program olyan szűrőszoftverek telepítését ajánlja, amelyek segítségével a pedagógus (otthon a szülő) maga állíthatja be és szabályozhatja, hogy a gyerekek milyen adattartalmat érhetnek el a világhálón, illetve, milyen, a számítógépre feltelepített programokat használhatnak.

Folyamatban van továbbá a **Magyarország Internetes Gyermekvédelmi Stratégia** kidolgozása, többek között az Országos Kriminológiai Intézet, a Symantec és a Biztonságos Böngészés Program az ORFK és a BRFK bűnmegelőzési szakembereinek együttműködésében, ami további bizakodásra adhat okot.

A védekezési lehetőségek közül fontos megemlíteni egyrészt a nemzeti és a nemzetközi együttműködést, a tapasztalatok átadását, a számítógépes és szoftveripar szoros kapcsolatát, illetve el az erőszakszervek és az igazságszolgáltatás bűnözőkkel szembeni határozott fellépését, másrészt a családok szerepét, a szülők felelősségét, hiszen a mikrokörnyezet, a család támogatása nélkül egyetlen program, egyetlen kezdeményezés sem lehet sikeres.

Felhasznált irodalom

[1] Kovács László: Az információs terrorizmus eszköztára http://hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html (letöltés: 2010. április 07.)

[2] Mezey Nándor: A számítógépes bűnözés http://www.jogiforum.hu/publikaciok/307 (letöltés: 2010. április12)

[3] Csepeli György: Veszélyesen élni? http://74.125.77.132/search?q=cache:LKlua6Imj8IJ:de.njszt.hu/files/kockazatkonf/01_Csepeli_Gyorgy_Veszelyesen_elni.ppt+sz%C3%A1m%C3%ADt%C3%B3g%C3%A9ps+szabot%C3%A1zs&cd=2&hl=hu&ct=clnk&gl=hu/www.zmne.hu/kulso/mhtt/hadtudomany/2008_e_2.pdf (letöltés: 2010. április 10.)

[4] Kovács László - Krasznay Csaba: Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság, III. évfolyam. 1. szám. 2010. február ISSN 1789-5286 p.: 44-56.

[5] Dr. Balogh Zsolt György: Jogi informatika, Dialog Campus Kiadó, Budapest-Pécs, 1998, 264-265. o.

[6] Dr. Sárkány Tamás: Támadási lehetőségek távközlési hálózatok ellen, Híradástechnika, LVIII. évfolyam, 2003/5. szám

[7] Steven Mizrach: Létezik-e „hackeretika" a 90 –es években, Replika 2000. 41-42; 303-305. oldal

[8] Tarr Dániel: Internet mítosz http://mek.niif.hu/01400/01437/html/kod03_2.htm#5 (letöltés: 2010. április 12.)

[9] Flammich Mariann: Hackerek http://krono.inaplo.hu/index.php/inter/recenzio/282-hackerek- (letöltés: 2010. április 05.)