SZÉKELY ZOLTÁN

INFORMÁCIÓS BŰNÖZÉS AZ INFORMÁCIÓS TÁRSADALOMBAN

Bevezetés

Álláspontom szerint az informatikai bűncselekmények megfelelő meghatározáshoz tág fogalomra van szükség. Ez magában foglalja a számítástechnikai bűncselekményeket, amelyeket viszont önálló fogalommal körül kell határolni. Nem véletlenül, hiszen társadalmunk információs társadalommá válásával az annak alapvető feltételeit megteremtő informatikai eszközök használata az élet minden területére kiterjedt. Az emberi természet sajátosságaiból fakadóan, pedig minden területen vannak olyan törekvések, amelyek a társadalom értékrendjével szemben is hajlandóak érvényesítésüket kiharcolni, nem is beszélve arról, amikor a társadalom maga jellemzően nem is ítéli el egyértelműen az egyes bűncselekményeket, különösen a szerzői jog megsértése területén.[274] Be kell látnunk azt is, hogy az informatika egyre nagyobb részesedéssel jelenik meg a „hagyományos" bűncselekmények területén az elkövetést lehetővé tevő, megkönnyítő eszközként. Nem szabad azonban összekeverni a számítástechnikai és az informatikai bűncselekményeket, mert ez a két kategória rész és egész viszonyában áll egymással. Sajnos ebben a tekintetben úgy a nemzetközi, mint a hazai vonatkozásban komoly hiányosságok vannak. Nemzeti jogunk a számítástechnikai bűncselekményeket rendeli büntetni a Btk. 300/C és E szakaszaiban, míg az információs bűncselekmények köre sokkal tágabb ennél. Ezt fel kell ismernünk és az eljövendő anyagi, illetve eljárási szabályokat, megelőző, felderítő intézkedéseket erre figyelemmel kell meghoznunk.

Természetesen nem mellőzöm a történeti visszatekintést sem. Elsősorban az információs társadalom kialakulását mutatom be, hiszen az információs társadalommá válás nélkül az informatikai bűncselekmények megmaradtak volna a hírszerzők eszköztárában. Majd a számítástechnikai eszközök, mint az informatikai bűncselekmények eszközei fejlődésének történetét mutatom be, ugyanis ennek sajátosságainak ismerete a mai helyzet megértéséhez elengedhetetlenek. Az eszközök fejlődése két szempont mentén osztható korszakokra. Egyik az informatikai eszközök elterjedése a mindennapi életben. Ennek révén jutottunk el az állami hírszerzések teremnyi méretű szupertitkos kódfejtő állomásaitól a hétköznapi emberek okos telefonjáig. Másik a nagy kiterjedésű hálózatok megjelenése. Segítségükkel az adatátvitel áttörte térrel és idővel kapcsolatos korlátainak legnagyobb részét. Ha pedig a ma rohamosan terjedő vezeték nélküli vagy mobiltelefon hálózatokra gondolunk, immár látható, hogy rövid időn belül a vezeték nélküli internet elérés teljesen természetes lesz. Rövidesen elfelejthetjük tehát a fizikai hálózati csatlakozás hiányából adódó biztonságot is. Röviden bemutatom az informatikai bűncselekmények elkövetői rétegének kialakulásának folyamatát is, különös tekintettel a számítástechnikai bűncselekmények elkövetőire és kissé bővebben e sajátos szubkultúra hierarchiájának egyes elemeire. Végül, bemutatom az informatikai bűncselekmények legismertebb eszközeinek

[274] Varga Balázs: Informatikai bűncselekmények 2003. www.jogiforum.hu/publikációk, (Letöltés napja: 2007. 09. 01.)

kialakulását, itt is külön kitérve a számítástechnikai bűncselekmények leggyakoribb képviselőjének, a rosszindulatú szoftvereknek az eredetére, valamint napjaink egyik leginkább releváns problémájára, a fájlcserélő hálózatokra, melyek virtuális feketepiacként kiváló hátteret biztosítanak az elkövetők egymásra találásához.

Az informatika mellett azonban még egy igen jelentős területet is meg kell említenünk és ez nem más, mint az adatvédelem. Nagyon sok esetben az információs bűnözés vonatkozásában az adatvédelmi szabályzás tölti ki a büntető anyagi jog keretdiszpozícióit.

Definiálás és tipizálás

Az informatikai és számítástechnikai bűncselekmények viszonyát először is a definíciók párhuzamba állításával kívánom szemléltetni:
Informatikai bűncselekmény: A bűncselekmény, amelynek tárgya vagy eszköze informatikai eszköz.
Számítástechnikai bűncselekmény: A bűncselekmény, amelynek tárgya és eszköze informatikai eszköz.
Informatikai eszköz: Változó jelenség mértékével meghatározott kettes számrendszerű értékekkel ábrázolt információ feldolgozására illetve tárolására alkalmas eszköz.[275]

A két meghatározást nem szabad összemosni, ugyanakkor mindkettőre szükség van. Mindazonáltal tisztában kell lennünk azzal, hogy gyakorlatilag nem minden informatikai bűncselekmény számítástechnikai bűncselekmény.

A tágabb informatikai bűncselekmény definícióra főleg azért van szükség, mert az informatika a hétköznapi élettel egy időben a bűncselekmények jelentős részének is szinte a természetes alkotórészévé vált. Az emiatt fellépő büntetőeljárási sajátosságok majdnem teljesen azonosak valamennyi olyan bűncselekmény esetén, amelyet az általam képviselt informatikai bűncselekmény fogalom magába foglal. Saját definícióm, éppen az informatika mindennapi életben való részvétele miatt igencsak tág. Nem tekinthetek el ettől a meghatározástól. Pont az elterjedtség miatt rengeteg bűncselekményhez használnak informatikai eszközöket és ez azt jeleni, hogy felderítésükhöz, megakadályozásukhoz vagy bizonyításukhoz a számítástechnikai bűncselekmények esetén alkalmazandó eljárásokat, intézkedéseket nagy számban kell alkalmazni. Nyilvánvaló viszont, hogy nem mindegyik kötődik egyformán szorosan az informatikához. Ebből kiindulva típusok felállítása vált szükségessé. A magyar Büntető Törvénykönyvben[276] található, informatikai bűncselekményként értékelhető tényállásokat informatikai eszközökhöz és rendszerekhez való viszonyuk szerint három fő típusba sorolom.
„A" típusú informatikai bűncselekmény (Számítástechnikai bűncselekmény): Informatikai rendszer és eszköz illetve annak védelme ellen irányul (Számítástechnikai rendszer és adatok elleni bűncselekmény).
„B" típusú informatikai bűncselekmény: Elkövetése az információs társadalomban elsősorban az informatikai eszközök révén történik (pl. jogosulatlan adatkezelés, tiltott pornográfia, szerzői jogok megsértése).
„C" típusú informatikai bűncselekmény: Előkészítését illetve elkövetését az informatikai eszközök nagymértékben megkönnyítik (pl. közokirat-hamisítás, kerítés).

[275] A technika mai állásánál az információt hordozó egység a bit amelynek 0 vagy 1 értékét mágneses, elektromos vagy optikai jellemzőkkel adják meg.
[276] 1978. évi IV. törvény a Büntető Törvénykönyvről

Jelen munka csak érinti a „C" típusba tartozó bűncselekményeket, inkább azokra koncentrálok, melyek szorosabb kapcsolatban vannak a számítástechnikával, így elsősorban az „A" illetve a „B" típusú bűncselekményeket, de terjedelmi okok miatt jogszabályi hátterét mélyebben csak a számítástechnikai bűncselekményeknek mutatom be.

Informatikai bűncselekmények a számok tükrében

Megvizsgáltam a 2002 és 2006 között ismertté vált bűncselekményeket és azok informatikai vonzatait és a fenti típusokba sorolva, a dolgozat következő részében rendszerezem azokat, amelyek álláspontom szerint valószínűleg megfelelnek a fogalmamban támasztott követelményeknek. Az informatikai bűncselekmények magas látenciája miatt a véleményem az, hogy a táblázatokban szereplő alacsony értékek messze nem érik el a felderítetlenül maradt, informatikához köthető cselekmények számát. Különösen magas a látencia azon bűncselekmények tekintetében, ahol a társadalmi negatív értékítélet nyilvánvalóan hiányzik. Márpedig nem sok negatív értékítélet kíséri például a szerzői jog megsértésével járó filmek, játékszoftverek és egyéb alkalmazások terjesztését, felhasználását. Számos magánszemély eleve nincs olyan anyagi helyzetben, hogy az eredeti terméket megvásárolja, sőt a jogi személyek egy része sem teszi ezt meg.

Ismertté vált „A" típusú informatikai bűncselekmények számának alakulása Magyarországon 2002-2006

	2002.	*2003.*	*2004.*	*2005.*	*2006.*
Számítástechnikai rendszer és adatok elleni bűncselekmény	206	484	1017	434	217
Számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása	2	246	14	56	315
Összesen:	208	730	1031	490	532

Az ismertté vált „A" típusú bűncselekmények aránya az összes ismertté vált bűncselekmény számához viszonyítva rendkívül alacsony, mindössze 0,14 %. Nem szabad figyelmen kívül hagyni azonban, hogy e területen kiemelkedően magas a látencia.

Az FBI Computer Intrusions Squad részvételével elkészített statisztikák szerint a 1997 és 2002 között az Egyesült Államokban a támadást elszenvedett vállalatok 35 százaléka nem jelentette a támadást akkor sem, miután az a tudomására jutott és a biztonsági rést már befoltozták, amit a vállalatoknak csupán a 70 százaléka tett meg.[277] A magyarországi helyzet még nem ilyen komoly, de rövidesen fel fogunk zárkózni, ha ez még esetleg észrevétlenül nem történ volna meg. Azonban jelentős károkat okoz, és komoly veszély jelentenek a rendszerek működésének megzavarásával vagy jogtalan befolyásolásával kapcsolatos cselekmények is, habár anyagi szemszögből kisebb kárt okoznak. A legjobb példa erre a demokrácia alapköve, a választás és a népszavazás. Az Egyesült Államok 2004. évi elnökválasztásán a szavazók egyharmada már elektronikus választási rendszeren keresztül voksolt. Egy a választás napján tönkretett ilyen rendszer

[277] Computer Security Issues and Trends kiadvány 2002. tavasz. Idézi Varga Balázs: i.m. 86-108. o.

hatalmas károkat okozhat, de még ennél is veszélyesebb az, ha az eredményt észrevétlenül befolyásolják. Másik példaként szeretnék felhozni egy folyamatban lévő ügyet, amelyben 2007. október 27-én emeltek vádat John Escalera és Gustavo Razo amerikai állampolgárok ellen, mert Escalera betört az egyetemük, a Fresco Állami Egyetem adatbázisába, hogy maga és neki anyagi ellenszolgáltatást ígérő társa részére hamis tudományos fokozatot szerezzen. Az egyetem egy belső ellenőrzés során felfedte az esetet, és az elkövetőket feljelentették. Ha bűnösnek találják őket, 20 év börtönre és/vagy 250 ezer USD pénzbírságra számíthatnak.[278] Számos esetben a Számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása bűncselekmény komoly nehézséget okoz az egyéb informatikai bűncselekmények nyomozásában és bizonyításában. Az elkövetők gyakran előbb rosszindulatú szoftver segítségével bejutnak egy harmadik személy számítógépére úgy, hogy például egy ingyenes pornográf tartalmat kínáló oldal a felvételek megtekintéséhez egy program letöltésének szükségességét jelzi, ami valójában egy trójai típusú rosszindulatú szoftver, aminek segítségével a gyanútlan böngésző gépéből pillanatok alatt tiltott pornográf felvételeket megosztó kiszolgáló válik. Ebben az esetben különös szakértelem szükséges a megszemélyesítés kiszűréséhez. Ilyen esetekben általában a harmadik személy válik gyanúsítottá, aki valójában semmilyen bűncselekményt nem követett el. Mégis – különösen, ha ismert közszereplőről van szó – a pedofília bélyegét soha többet nem tudja lemosni magáról. Habár ilyen esetekre a meglátásom az, hogy az információs társadalom fejlődésével megállapíthatóvá válhat e személyek felelőssége is, analógiaként annak a gépjárművezetőnek a felelősségét hoznám fel, aki azért okoz balesetet, mert a gépjárművének a fékberendezése rossz állapotban volt, amiről nem volt tudomása, mivel az indulás előtti ellenőrzést, azaz a kellő gondosságot elmulasztotta. Rövidesen elvárható lesz a gondosság és a használt eszközök ilyen fokú ismerete a társadalom valamennyi tagja részéről, különösen, ha az oktatás ennek megfelelően alakul. Például egy pornográf weblap látogatásakor az átirányít egy másik kiszolgálóra, ahol azonnal megjelenik egy felugró ablak, amely egy ismeretlen forrásból származó Java nyelven írt böngészőbővítmény (applet) letöltését ajánlja fel a látogatónak. A letöltés és telepítés engedélyezésével egy hátsó ajtó (backdoor) nyílik a felhasználó rendszerébe, majd ezen keresztül egy komplex rosszindulatú szoftver kerül telepítésre, ami alkalmas arra, hogy a gépet zombigéppé (bot) tegye.[279]

[278] http://www.cybercrime.gov/escaleraIndict.pdf (Letöltés ideje: 2007.11.05.)
[279] http://www.zdnet.co.uk/talkback/0,1000001161,39115422-39001093c-20057865o,00.htm (Letöltés ideje: 2008.03.24.

Ismertté vált „B" típusú informatikai bűncselekmények számának alakulása Magyarországon 2002-2006					
	2002.	*2003.*	*2004.*	*2005.*	*2006.*
Tiltott pornográf felvételek készítése, felvételekkel visszaélés	144	80	5832	11489	15183
Készpénz helyettesítő fizetési eszköz hamisítás	241	404	50	13	0
Készpénz helyettesítő fizetési eszköz hamisításának elősegítése	0	2	3	3	1
Szerzői vagy szerzői joghoz kapcsolódó jogok megsértése	17532	23269	19046	37401	33446
Szerzői vagy szomszédos jogok védelmét biztosító műszaki intézkedés kijátszása	366	19	11	17	54
Összesen:	18283	23774	24942	48923	48684

A fenti, „B" típusú bűncselekmények már jóval jelentősebb részt képviselnek a bűncselekményekből, az összes cselekmény 8,08 %-át. Szintén rendkívül magas látenciával kell számolnunk, de itt elsősorban nem a módszerek kifinomult volta, hanem a legnagyobb részt képviselő szerzői vagy szerzői joghoz kapcsolódó jogok megsértésével szembeni finoman szólva elnéző társadalmi hozzáállás miatt. Szinte mindenkinek van otthon nem jogtiszta szoftvere, s nyilvánvaló, hogy a nagy többség szándékosan, az eredetének tudtával szerezte be. Nagyon kevés azoknak a száma, akik a szoftverhamisítás áldozatai és tudtukon kívül vásárolnak nem jogtiszta szoftvert. A társadalom túlnyomórészt egyáltalán nem ítéli el a szoftverek jogtalan másolását, a szerzői jogot védő műszaki intézkedés kijátszását, az úgynevezett crackelést azaz törést. Nyilvánvaló azonban az is, hogy a szerzői jog ilyen szigorú törvényi oltalmazása elsősorban a gazdasági szféra nyomására történik, ami arra törekszik, hogy minden terméket minél drágábban, nagyobb haszonkulccsal adhasson el. Az okozott kár valójában sokkal kisebb, mint amit a szerzői illetve főleg a felhasználási jogok tulajdonosai, a kiadó vállalatok peresíteni szeretnének.[280] A szerzői jog szempontjából különösen a külön fejezetben ismertetett fájlcserélő hálózatok jelentenek komoly kihívást, mivel a sejtszerű felépítésükből adódóan szinte elpusztíthatatlanok.

[280] Varga Balázs: op. cit. 5. p.

„C" típusú informatikai bűncselekmények számának alakulása Magyarországon 2002-2006					
	2002.	*2003.*	*2004.*	*2005.*	*2006.*
Magántitok megsértése	2	1	4	0	1
Jogosulatlan adatkezelés	391	732	8	1	0
Visszaélés személyes adatokkal	0	10	1136	503	41
Különleges személyes adatokkal visszaélés	24	380	0	0	0
Visszaélés közérdekű adattal	0	2	2	1	3
Levéltitok megsértése	9	103	67	12	6
Magántitok jogosulatlan megismerése	6	7	38	8	12
Kerítés	99	97	76	39	260
Sajtórendészeti vétség	4	5	8	6	9
Embercsempészés	3639	1481	658	672	525
Államtitoksértés	15	6	14	5	6
Szolgálati titoksértés	5	1	5	1	2
Jogosulatlan titkos információgyűjtés	0	2	2	0	0
Zugírászat	4	7	8	2	1
Közokirat-hamisítás	8754	10650	13537	15016	12224
Magánokirat-hamisítás	19956	18705	18667	19140	22896
Egyedi azonosító jel meghamisítása	4416	4004	4559	4478	3988
Hamis statisztikai adatszolgáltatás	3	4	3	4	9
Üzleti titok megsértése	9	13	7	7	18
Gazdasági titok megsértése	0	0	0	0	6
Banktitok megsértése	4	3	4	4	5
Pénzhamisítás	1105	760	1640	3097	3413
Pénzhamisítás elősegítése	3	1	1	11	2
Bélyeghamisítás	64	33	78	86	52
Bankkártya-hamisítás	17	39	0	0	0
Jogkezelési adat meghamisítása	0	0	0	1	0
Összesen:	38529	37046	40522	43094	43479

Ezen típus informatikához történő kötődése a leglazább, elsősorban az informatikai eszközök azon képességén alapul, amely lehetővé teszi adatok nyom nélküli bevitelét, módosítását, majd újra kinyerését. Gondolok itt különösen az útokmány tekintetében elkövetett közokirat hamisításokra, ahol képbeolvasóval beolvassák, majd a szükséges módosításokat elvégezve nagyfelbontású nyomtatóval az adathordozót leutánozzák, vagy a személyes adatokat tartalmazó okmányokra, felvételekre melyeket a törvényes adatkezelési jog megszűntét követően elfelejtenek letörölni, az illetéktelenül továbbított bizalmas céges adatokat tartalmazó e-mailre vagy éppen a szexuális szolgáltatásokat kínáló személyek hirdetéseit tartalmazó weboldalra.[281] Számos olyan cselekmény is helyet kapott itt, amely az információlopással kapcsolatos joghézag miatt soroltam az informatikai bűncselekmények közé, tárgyuk az adatvédelem. Bizonyos esetekben, pedig a bűncselekmény megszervezésének módja, a végrehajtás megszervezése köti szorosan az informatikai bűncselekményekhez az adott tényállás, mint például az embercsempészet, melyet ma már szinte kizárólagosan az Internet révén szerveznek.[282] Hosszú gondolkodás után végül nem

[281] pl: http://budapestescort.hu/
[282] http://www.espionage-store.com/passport.html

soroltam ide a Terrorcselekményt, habár a terrorista hálózatok nagyfokú konspirációjában komoly szerepet játszik az Internet, napjainkban különösen sok gondot okoznak a titkosított internetes telefon szolgáltatások, például a Skype nevű program titkosításának feltörésével hiába próbálkozott egy lehallgatás során a német rendőrség.[283]

Az információs társadalom kora

A helyzet megfelelő értékeléséhez azonban elengedhetetlen a történelmi háttér ismerete. Nyilvánvaló, hogy az információs társadalom nem jöhetett létre, amíg az egyes tudományágak interdiszciplinaritás révén olyan hatást nem gyakoroltak egymásra, ami lehetővé tette a megfelelő eszközök létrehozását, melyek révén a tudásbeli fölény igazán meg tudott mutatkozni. Kiváló, ámbár igen fájdalmas példa erre az atombomba. Valamennyi kapcsolódó tudománnyal és a kialakulás teljes folyamatával azonban terjedelmi okok miatt nem foglalkozom. Mindazonáltal meg kell említenem, hogy a fizika, a kémia és a matematika nélkül nem alakulhatott volna ki az a két jelenség, amely közvetlen felmenője napjaink számítástechnikájának és ennek révén az információs társadalomnak. E társadalom kialakulása ugyanis szorosan kötődik a számítástechnikai eszközökhöz, melyek először tették lehetővé az ember számára saját képességeit jóval meghaladó információmennyiség kezelését.

Információs társadalom: a társadalom, mely számára az információ előállítása, elosztása, terjesztése, használata és kezelése jelentős gazdasági, politikai és kulturális tevékenység.[284] A megnevezést először Fritz Machlup használta 1933-ban,[285] őt számos elmélet és meghatározás követte, de a fenti, leginkább elfogadott definíció is meglehetősen szubjektív feltételeket szab, ezért ma sincs egyetértés arra vonatkozóan, hogy milyen társadalmat tekintünk információs társadalomnak és milyet nem. Ma a kortárs szociológiának egy külön ága foglalkozik a jelenséggel. A tudományág valamennyi művelője egyetért azonban abban, hogy az 1970-es évektől jelentős átalakulás vette kezdetés. Ennek előidézői pedig nem mások, mint a személyi számítógépek elterjedése és a nagy kiterjedésű hálózatok megjelenése.[286]

Számunkra a 1126/2003. Korm. határozat 1. számú melléklete, a Magyar Információs Társadalom Stratégiája preambulumában leszögezi, hogy *„…első célja annak nyilvánvalóvá tétele, hogy Magyarország számára nincs más alternatíva, mint belépni az információs korba annyira intenzíven és innovatívan, amennyire erőnkből telik.*”[287] A magyar stratégia része az Európai Unió stratégiájának, az eEurope+ programnak és az eEurope 2005 akciótervnek. Sajnos a stratégia végrehajtása sajátosan alakult, erre bővebben a magyarországi információs társadalmat bemutató résznél kívánok kitérni.

A fenti stratégiák azért jöttek létre, mert a harmadik évezred küszöbére nyilvánvalóvá vált, hogy átléptünk az információs társadalom korába. Az információ megfelelő használata kevés tőke befektetésével hatalmas haszon elérését teszi lehetővé. Magyarországon a 2003-as vizsgálatok szerint az elektronikus kereskedelem éves forgalma

[283] http://www.sg.hu/cikkek/56411 Letöltés ideje: 2008-03-24
[284] http://hu.wikipedia.org/wiki/Inform%C3%A1ci%C3%B3s_t%C3%A1rsadalom Letöltés ideje: 2007.11.06.
[285] Fritz Machlup: The Production and Distribution of Knowledge in the United States. Princeton, 1962, Princeton University Press. Idézi: http://www.wikipedia.org Letöltés ideje: 2007.11.08.
[286] Jan Van Dijk: The Network Society. London, 2006, Sage. Second Edition. Idézi: http://www.wikipedia.org (Letöltés ideje: 2007.11.08.)
[287] 1126/2003. (XII.12.) Korm. hat. 1. melléklete - Magyar Információs Társadalom Stratégia, továbbiakban MITS, forrás: www.magyarorszag.hu/jogszabalykereso (Letöltés ideje: 2007.11.05.)

becslések szerint kb. 250-350 Mrd. Ft.[288] amellett, hogy hazánk ilyen szempontból az Európai Unió középmezőnyének végén található. Az információs társadalom fő értékmérőjén, a Tudásgazdasági Indexen (KEI – Knowledge Economy Index) 2007. évben a vizsgált 140 ország közül a 28. helyet foglaltuk el, ami tizenkét év alatt (1995 óta) 4 helyezésnyi előrejutást mutat, ami szerény teljesítménynek mondható. Azonban éppen a haladás miatt az ilyen irányú fejlődésre – azaz az információs társadalomra - veszélyes cselekmények száma természetes módon emelkedik. Emiatt erre fel kell készülni, úgy informatikai szakmai, mint büntetőjogi eszközökkel. Ugyanis az információs társadalomban is megvannak azok a sajátos cselekmények, melyek az adott társadalomra veszélyesek. A büntetőjognak, mint a békés társadalmi együttélés biztosításának végső eszközének feladata éppen ezeknek a cselekményeknek a meghatározása és szankcionálása. Természetesen számos bűncselekmény nem változik, azonban sok átalakul vagy már átalakult és megjelentek teljesen új bűncselekmények is. A kizárólagosan ide köthető, újonnan létrejött cselekményeket nevezzük számítástechnikai bűncselekményeknek, melyeket hatályos büntető anyagi jogunk már tartalmaz. Nagyon sok bűncselekmény ugyanis jelentősen átalakult az információs társadalom hatásának következtében, mivel az kibővítette lehetőségeiket az elkövetés tekintetében és e tényező révén megjelent, „hagyományos" bűncselekmények új arculatát nem hagyhatjuk figyelmen kívül. Szükség van az informatikai bűncselekmény kategória fölállítására és a kapcsolódó anyagi és eljárásjogi jogszabályok megalkotására, valamint az informatikai bűncselekményekkel kapcsolatos alapvető ismeretek oktatására a jogászképzésben.

A számítástechnikai fejlődés szerepe

Számítástechnika az automatizált adatfeldolgozás eszközeivel és azok különböző területeken való használatával foglalkozó elméleti és alkalmazott műszaki tudomány. Az informatikai és számítástechnikai bűncselekmények fogalmát, típusait, továbbá az érvényben lévő szabályzókat később fogom tárgyalni. Most azonban az át- illetve visszatekintést folytatva az információs társadalom kialakulásában kulcsfontosságú tudomány, a számítástechnika keletkezésének főbb stációt és azok szerepét foglalnám össze. Habár a számítástechnika alatt alapvetően a modern számítógépek tudományát értjük, az első számítást megkönnyítő eszközök már időszámításunk előtt megjelentek, mint például az abakusz és a Püthagorasz-féle számolótábla. A középkor módszerei voltak a gelosia-módszert alkalmazó Napier-pálcák és az azokból készített Schickard-számológép. Az első komoly áttörést a logaritmus felfedezése jelentette a XVI. század végén. A logarléc mint számológép ezután 1622-től 1970-ig szinte teljes egyeduralmat gyakorolt a kézi számítástechnikai eszközök területén, annak ellenére, hogy Pascal majd Leibniz is automata számológépet épített a XVII. században. Az első igazi áttörést a számológépek és a számítógépek között a Boole-algebra megjelenése jelentette, ami mind a mai napig az összes számítógéppel végzett művelet alapja. Habár már az 1880-as amerikai választásokon alkalmaztak lyukkártyás adatfeldolgozást Hollerith gépével, akinek 1924-ben alapított cégéből jött létre az IBM.[289] Igazából a robbanásszerű fejlődést a XX. század hozott. A század elején a totalizátorokkal valós idejű valószínűség számítást végeztek, Torres feltalálta a lebegőpontos ábrázolást (1914) és Zuse megépítette az első mechanikus

[288] MITS I.2.1
[289] International Business Machines

adattárolókat (1932), Alan Turing megépítette a digitális számítógépek közvetlen elődjét, a Türing-gépet[290], 1937-re pedig elkészült az első elektronikus számítógép, az Atanasoff-Berry Computer, ismertebb nevén az ABC. Neumann János 1946-ban megépített ENIAC-ja[291] már saját memóriájában tárolta a programokat és az adatokat és feltételes vezérlésátadásra (= a számítógép gondolkodása) is képes volt. Az első kereskedelmi gép az UNIVAC[292] I. volt, majd az első általános kereskedelemben kapható gépet az IBM 360 képviselte 1964-ben.[293] A személyi számítógépek megjelenése 1974-re tehető (Altair 8800), azonban elterjedésüket igazából az 1981-es IBM PC garantálta, amely már a DOS[294] nevű operációs rendszerrel működött. Ezzel a lépéssel kezdődött igazából a számítástechnikai eszközök elterjedése. Ráadásul minél több számítógépet vásároltak az emberek, annál olcsóbbá ált, mert az ipari korszakban a tömeggyártás mindig leviszi egy termék árát, emiatt még inkább elterjedt. Alig több mint 25 esztendővel a PC megjelenése óta már a számítógépek az egész világon elterjedtek. A legtöbb mai hétköznapi használati tárgyban van számítógép: a mobiltelefonban, a televízióban, a CD és DVD lejátszókban, az autókban, mikrohullámú sütőben, zenelejátszóban stb. Nem is beszélve a bonyolultabb eszközökről, mint a repülőgép, az űrsikló, a hajók és tengeralattjárók, a modern fegyverek vagy a robot gyártósorok. A VLSI[295] technológiának köszönhetően rendkívül kis méretűre zsugorodtak a számítógépek, emiatt ma már szinte bármely használati tárgyban elférnek.

Internet: összekapcsolt számítógép hálózatokból álló világméretű számítógép hálózat, a hálózatok hálózata. A számítógépek ilyen elterjedése volt az első lépés, amelyet kis lemaradással követett azok egymással összekötésének gondolata. Az 1966-67-es években létrejött a kaliforniai egyetemen (UCLA[296]) egy hálózati központ, ez volt az ARPANET-nek[297] az első csomóponti berendezése. Később, 1969-ben az UCLA kísérleteket kibővítették és kialakultak a mai Internet hálózathoz hasonló hálózat csírái. A mai Internet egyik fő alkalmazási területét először 1972-ben mutatták be, az ARPANET elektronikus postaként való felhasználásával. Ezzel tulajdonképpen megvalósult egy olyan számítógépes hálózati összeköttetés, amely közvetlen kapcsolatot teremtett a felhasználók között. Az 1980-as években kezdődött el a személyi számítógépeken és a munkaállomásokon alapuló lokális hálózatok elterjedése, ami később, a 80-as évek végén vezetett az Internet mai architektúrájának megalkotásához. Az 1980-as évek végétől beszélhetünk Internetről annak mai formájában. Megjelentek az Internet-szolgáltatók és a világháló széles körben elterjedt a nem kutató vagy fejlesztő környezetben is, vagyis kereskedelmi szolgáltatássá vált. Jelenleg, amikor az elektronikus postai szolgáltatások mellett számos más szolgáltatás is (például home banking, elektronikus kereskedelem stb.) megjelenik a hálózaton, világosan kiütközik az Internet fejlődéséből adódó probléma, nevezetesen, hogy a főleg kutatókra, fejlesztőkre, tehát alapvetően azonos érdekeltségű és motivációjú résztvevőkre épülő Internetet megelőző hálózatoknál a fejlesztők és a felhasználók sem tekintették alapvető kérdésnek a biztonságot.

[290] Markó Tamás: A számítástechnika története, Jegyzet, 1996, PTE
[291] Electronic Numerical Integrator And Computer
[292] UNIVersal Automatic Computer
[293] http://www.wikipedia.org Letöltés ideje: 2007.11.08.
[294] Disc Operating System
[295] Very-large-scale integration *(Rendkívül nagyfokú integráltság)*
[296] University of California, Los Angeles
[297] Advanced Research Projects Agency Network

Az informatikai bűncselekmények elkövetői

Ennek a csoportnak az ismertetésére először is azt ketté kell bontatom. Alapvetően kétféle elkövetői típus van ezen a területen. Az egyik típus informatikában rendkívül képzett, a cselekményt a legnagyobb körültekintéssel és nagyfokú szakmai felkészüléssel követi el, tudásban illetve találékonyságban felveszi a versenyt a legtöbb IT biztonsági szakemberrel. A másik típus egyszerűen csak él vagy visszaél az informatikai eszközök nyújtotta lehetőségekkel.

Professzionális elkövetők

Már az előbb vázolt két jelentős eredmény elérése előtt is követtek el olyan adatokkal kapcsolatos bűncselekményeket, amelyeknek tárgya primitív számítástechnikai eszköz volt. 1820-ban a francia Jacquard-féle lyukkártyával programozható szövőszék megjelenésére a textiliparban dolgozó munkások szabotázsakciókkal válaszoltak, melynek során a lyukkártyákat meghamisították, vagy megrongálták, így páratlan ámde haszontalan textilművészeti alkotások születtek a ruhadarabok helyett.[298] A telefonhálózatok megjelenése után a kézi kapcsolású központokban fiatal mérnökök dolgoztak, akiket a sokak számára misztikus rendszerek működése miatt külön szubkultúrának tekintettek és phreakernek neveztek.[299]

Phreaker: telekommunikációs rendszerek szakértője.

A XIX. század végére már megjelentek a telefonbetyárkodás. Emiatt a néha tréfás kedvű fiatal mérnököket a telefontársaságok többsége betanított, a technológiát mélységében nem ismerő telefonos kisasszonyokra cserélte. Nemsokára persze megjelentek a telefonbetyárkodás komolyabb formái is, mint például a jogtalan vonalhasználat vagy telefonvonal besorolásának illetéktelen megváltoztatása. A telefonbetyárkodás különösen a tizenéves fiúk körében élvezett nagy népszerűséget, akik egyébként is hajlamosak szubkultúrákhoz csatlakozni. A mai veterán black-hat hackerek[300] többsége mind így kezdte. Az egyik legismertebb közülük Kevin Mitnick, akinek egyik kedvenc időtöltése az volt, hogy barátai otthoni előfizetéses telefonvonalának a besorolását utcai telefonfülkés vonalra változtatta, így amikor azok telefonálni akartak, a központ azt hajtogatta nekik, hogy dobjanak be egy érmét a telefonjukba.[301] A hackerek a phreakereket tekintik ősüknek és a mobiltelefonok megjelenésével a nagy előd is feltámadt és most mindkét irányzat jelen van az informatika világában.

Hacker: kiemelkedő informatikai ismeretekkel rendelkező szakember.

A fenti definícióból látszik, hogy téves a közvéleménynek az a felfogása, amely szerint minden hacker számítástechnikai bűnöző. A hackerek nagy tudású szakemberek,

[298] http://cybercrime.planetindia.net (Letöltés ideje: 2007.11.09.)
[299] Varga Balázs: Informatikai bűncselekmények 2003. www.jogiforum.hu/publikációk, (Letöltés napja: 2007.09.01.)
[300] Lásd később
[301] Kevin D. Mitnick – William L. Simon: The Art of Deception – Controlling the Human Elements of Security [A legendás hacker – A megtévesztés művészete] Budapest. 2003. Prefact-Pro, a szerző előszava.

amelyek a rendszereket nap mint nap javítják, tökéletesítik, utat nyitva a társadalom számára az ismeretlenben, ezért is hívják őket hackernek (csákányosnak). A tudást azonban nem csak nemes célra lehet felhasználni.
White-hat Hacker: Számítástechnikai szaktudását a világ jobbá tételére használó szakember.
Black-hat Hacker: Számítástechnikai szaktudását önző módon saját céljaira hasznosító szakember.

A mai köznyelvben hacker alatt csak a black-hat hackert értik, míg a white-hat hackert biztonsági szakembernek nevezik. A két frakció között sok az összetűzés, de az átmenet is. A HACP csoport például saját maga által is bevallottan törvénytelen eszközökkel küzd a gyermekpornó ellen.[302] Az elkötelezett magyar egyenruhás white-hat hackerekből pedig már a Magyar Rendőrségnél is felállításra került az informatikai bűnözők elleni részleg.[303] Nem minden számítógépes bűnöző érdemli meg azonban hacker jelzőt. A laikusok hajlamosak mindenkit hackernek tekinteni, aki egy kicsit is tud bűvészkedni egy számítógéppel. A valódi hackereknél azonban sokkal többen vannak azok, akik csak szeretnék, ha annak tekintenék őket.
Wannabe (tüncike): Magát hackernek beállítani próbáló személy.
Script-kiddie (szkriptkölyök): Hackerek által elkészített programokat vagy azoknak részleteit (scripteket) hackeléshez felhasználó személy.
Cracker: A szerzői jog védelmét biztosító technikai intézkedés kijátszására szakosodott programozó.
Social engineer (szélhámos): A védelmi intézkedéseket a jogosultságokkal rendelkező felhasználók megtévesztésével kijátszó hacker.

A tüncike és a szkriptkölyök kategóriától származik egyébként a céltalan, romboló támadások legnagyobb része, míg a profik sokkal nagyobb károkat okoznak, gyakran észrevétlenül.

Kalóz: Meggyőződésből vagy anyagi haszonszerzés céljából informatikai bűncselekményeket elkövető személy. A fenti definíció takarja a továbbiakban azokat a hackereket, tüncikéket, szkriptkölyköket és social engineereket akik a számítástechnikai bűncselekmények többségét elkövetik. A hacker szó köznapi értelemben vett használatától személy szerint elzárkózom.

Az átlagos informatikai tudású elkövetők

Azonban az informatikai bűncselekmények elkövetői korántsem kizárólag ebből a körből kerülnek ki. Sőt meg kell állapítanunk, még a bűnügyi mutatók látencia által okozott feltehetően igen erős torzulása mellett is, hogy az informatikai eszközökkel elkövetett bűncselekmények nagyobb részét informatikához átlagosan értő személyek követik el. Mindössze a kalózok által elkövetett bűncselekmények nagyobb visszhangot kapnak, mert a társadalom ezeket relatíve nagyobb veszélynek érzékeli, egyébként nem alaptalanul, mint a „közönséges" elkövetők által megvalósított cselekmények jelentős részét. Ugyanis ezek a bűncselekmények sok szempontból valóban veszélyesebbek és egyértelműen nehezebben felderíthetőek, mint a többi informatikai bűncselekmény. Megjelenésük azonban kevéssé találkozott társadalmi előítélettel. Például sokkal inkább elítélünk egy Tiltott pornográf felvételekkel visszaélés bűncselekményt, mint egy Számítástechnikai rendszer és adatok

[302] http://www.szochalo.hu/szochalo-tudomany/hircentrum/article/106789/744/ (Letöltés ideje: 2007.11.10.)
[303] http://broker.origo.hu/vendegszoba/techbazis/20070611netrendor.html (Letöltés ideje: 2007.11.09.)

elleni bűncselekményt, miközben – mindamellett, hogy az előbbit is igencsak szörnyűnek tartom – be kell látni, hogy ha az utóbbi elkövetése révén például egy választás eredményét hamisítják meg, sokkal nagyobb hátrányt okoznak a társadalom egésze számára.

Az informatikai bűncselekmények eszközei

Amikor a fenti szavakat olvassuk, a legtöbbünk fejében sötét, számítógépekkel és furcsa, villogó-zúgó eszközökkel teli rejtekhelyek jutnak az eszünkbe, ahol szemüveges, vézna hackerek éppen feszülten figyelnek egy futó függőleges karaktersorozatot, vagy épp egy folyamatjelzőt, esetleg varázslatos gyorsasággal gépelnek a billentyűzeten. A valóság természetesen egészen más.

A számítástechnikai bűncselekmények eszközei és megjelenési formái

Természetesen a számítástechnikai bűncselekmények eszköztára valamivel bonyolultabb, mint más cselekmények esetén, azonban ott sincs másról szó, mint számítástechnikai eszközökről és a rajtuk futó programokról. Ráadásul ezeknek az eszközöknek is a legnagyobb része teljesen egyszerű operációs rendszer (Linux, Windows, OS/X), annak egy szolgáltatása (Ftp, ping, finger) vagy egyébként kereskedelmi forgalomban található más diagnosztikai szoftver, mint például a SATAN[304] vagy a COPS[305] (ezek persze már elavultak).[306]

Operációs rendszer: programrendszer, amely a számítástechnikai rendszer felhasználását vezérli, például ütemezi a programok végrehajtását, elosztja az erőforrásokat, biztosítja a felhasználó és a számítógépes rendszer közötti kommunikációt.[307] Ezeket az eszközöket eredetileg a biztonsági rések vagy hálózati hibák kiszűrésére használták, de szinte azonnal akadtak olyanok, akik a megszerzett ismeretekkel visszaéltek. A közvélemény figyelmét azonban sokkal inkább lekötik a számítástechnikai bűncselekmények azon eszközei, amelyek látványosan jelentkeznek vagy éppen jól csengő nevet kaptak. Pedig egy portpásztázó vagy egy hálózati csomagfigyelő nagyobb veszélyt jelent egyes rosszindulatú szoftvereknél. Mégis, a leginkább ez utóbbiak ismertek az emberek számára. Viszont nem egészen véletlenül. Az információs társadalom legnagyobb részének éppen ezek okoznak szinte nap, mint nap kellemetlenséget, bosszúságot. A legprofibb kalózok inkább óvakodnak attól, hogy működésüket a felhasználó megtapasztalja, ezt úgy hívják, hogy „megégeti a forrást”, és szakmai kudarcnak számít, kivéve persze, ha pont ez a cél. Attól függetlenül azonban, hogy egy illetéktelenül rendszerünkbe juttatott program tapasztalhatóan vagy rejtve károsítja rendszerünket, egyaránt az alábbi kifejezést alkalmazzuk.

Rosszindulatú szoftver (Malware): a rendszert megzavaró, károsító vagy jogtalan hozzáférést biztosító program. A rosszindulatú szoftvereknek számos típusa van, kialakulásuk szintén hosszas folyamat eredménye. Elméleti alapjukat az angol matematikus, Lionel Penrose fektette le 1959-ben automata önreprodukciós gépekről szóló elméletével. Egyszerű kétdimenziós elméleti modellje már rendelkezett a szükséges tulajdonságokkal,

[304] Security Administrator Tool for Analyzing Networks
[305] Common Open Policy Service
[306] Peter Norton, Mike Stockman: Network Security Fundamentals [A hálózati biztonság alapjairól] Debrecen, 2000. Kiskapu Kft. 43-44. o.
[307] ISO standard definíció önálló magyar fordítása, http://www.iso.org

képes volt aktiválódni, szaporodni, mutálódni és támadni. Röviddel a cikk megjelenése után Frederick G. Stahl megírta a modell alapján épített gépi kódot egy IBM 650-en. Valószínűleg nem rossz szándék vezette őket, a felfedezés megalkotását csak újabb lépésnek szánták az emberiség fejlődésében, csakúgy, mint annak idején a magfizikai elméleteket, melyek alapján később atomfegyvereket építettek. 1962-ben az amerikai BELL telefontársaság laboratóriumában dolgozó ifjú mérnökök, V. Vyssotsky, G. McIlroy és Robert Morris megalkották a Darwin nevű játékot. A játékban egy adott számítógép memóriájának kizárólagos birtoklásáért küzdöttek a felhasználók az általuk megírt programokkal. A cél az ellenséges felhasználó jelenlétének megszüntetése a rendszerben programjainak maradéktalan kiiktatása révén, az egyes programok önállóan képesek voltak a szaporodásra, az ellenfél programjainak keresésére és törlésére. A játék elterjedt és a mai napig játsszák.[308] A hálózatokon is hamar felbukkantak a vírusok, a Creeper az ARPANET gépein terjedt a 1970-es évek elején az akkor használt Tenex operációs rendszeren, a vírus az alábbi szöveget írta ki a képernyőre „I'M THE CREEPER : CATCH ME IF YOU CAN". Az ARPANET felhasználók közül egy mai napig ismeretlen személy darwinista választ adott, megteremtette a Reapert, ami ugyanúgy vírusként terjedt ugyanazon az operációs rendszeren, csak nem szöveget írt ki, hanem ha megtalálta, leirtotta a Creepert.[309] A Rabbit nevű vírus 1974-ben nem tett mást, mint ártalmatlanul szaporodott, igaz, az akkori viszonyokhoz képest eszméletlen ütemben. 1975-ben megjelent az első trójainak tartott játék, a Pervading Animal, ami frissítéskor többszörözte magát, bár nem volt egyértelmű, hogy programozási hibáról vagy szándékosságról volt szó. Rich Skrenta 1982-ben megunta, hogy barátai állandóan tőle kéregetik el a játékprogramjainak lemezeit, és néha elfelejtik visszaadni. A 15 éves srác erre megírta a világ első boot vírusát, az Elk Clonert, ami beírta magát az operációs rendszer indításáért felelős területre és a gép induláskor egy ijesztő versikét írt ki, melynek idézésétől terjedelmi okok miatt sajnos el kell tekintsek.[310] Ez a vírus az akkor népszerű Apple II számítógépre íródott. 1983-ban már veszélyforrásként foglalkoztak az addig csak jó tréfának, játéknak, programozói erőfitogtatásnak tartott vírusokkal. Az első számítógépes virológus Len Eidelmen volt. Az ő munkássága révén került sor egyes definíciók meghatározására is.

Vírus (Virus): más programokba rejtőző, önmaga sokszorosítására és terjesztésére képes rosszindulatú szoftver.

Trójai faló (Trojan): más programokba rejtőző, a felhasználó megtévesztésével futtatását kiváltó vírus.

Az első vírusjárványt az IBM számítógépek elterjedését követve, az azokra 1986-ban írt Brain volt, szerzője két pakisztáni fiatal, a 19 éves Basit Farooq Alvi és öccse Amjad, habár a vírus maga egyebet nem tett, mint hogy a kötetek elnevezését „©Brain"-re változtatta és kiírta a testvérek nevét, címét és telefonszámát. Kárt tehát nem okozott, mégis komoly pánik tört ki miatta a biztonságot eddig elhanyagoló felhasználók körében. Még abban az évben a német Ralph Burger megírta a Virdemet, az első lopakodó vírust, amely képes volt olvasáskor a fertőzött adatok helyett a tiszta adatokat visszaadni és csak futtatáskor aktiválódott. 1988-ban már számos vírus létezett és a vírusfenyegetettség már komoly ellenlépésekre késztette az IBM-et és a többi gyártót, ekkor kezdődött a víruskereső programok készítése.[311] Azonban 1988-ban egy újabb fenyegetés jelent meg. Robert Tappan

[308] http://www.viruslist.com/en/viruses/encyclopedia?chapter=153310910 (Letöltés ideje: 2007.09.01.)
[309] http://www.viruslist.com/en/viruses/encyclopedia?chapter=153310937 (Letöltés ideje: 2007.11.10.)
[310] http://www.sg.hu/cikkek/53734/25_eves_a_szamitogepes_virus (Letöltés ideje: 2007.09.01.)
[311] http://www.viruslist.com/en/viruses/encyclopedia?chapter=153311150 Letöltés ideje: 2007.11.10

Morris Jr., a Cornell Egyetem diákja 1988. november 2-án indította útjára a vírusok új generációját képviselő Morris férget az MIT[312] hálózatán. Tizenkét perc alatt 300.000 számítógépet fertőzött meg, köztük a NASA kutatóközpont gépeit is. A rendszergazdák csak a teljes szegmens leválasztásával tudták a terjedését megakadályozni, magyarán 1988. november 02-án érte az Internetet az eddigi legnagyobb csapás. Az Egyesül Államok törvényhozása ekkor ébredt rá, hogy a jog eszközeivel is cselekednie kell. Morrist 10.000 USD pénzbüntetésre, három év felfüggesztett szabadságvesztésre és közmunkára ítélték. Teremtménye és annak leszármazottai azonban a mai napig csak egyre komolyabb károkat okoznak.[313] Terjedésükhöz ugyanis nincs szükség a fertőzött programok felhasználók által történő átadására, a féreg magától küldi szét magát a fertőzött számítógéppel kapcsolatban lévő gépekre, valamilyen beépített protokollt használva (pl. SMTP[314]).

Féreg (Worm): számítógépes hálózaton önállóan terjedni képes vírus.

A vírusok másik különleges alfajának őse a Melissa volt 1990-ben, amely az első ismert makróvírus és már e-mailen terjedt, a Word biztonsági réseit használva az Outlook címtárából megszerezte a felhasználó postafiókjában található összes címet, amelyekre aztán elküldte magát.

Makróvírus: elektronikus dokumentumok futtatható kódot tartalmazó részébe rejtőző vírus. A legsikeresebb makróvírus azonban a Loveletter volt 2000-ben (nevezik I love you vírusnak is), amely már világszerte milliárdos károkat okozott.

2000-től kezdve egyébként alig van olyan vírus, amely ne az Interneten keresztül terjedne, vagy fejtené ki hatását. Egy részük csupán sokszorosítja magát, de sok komoly károkat okoz a háttértárolókon lévő adatok megsemmisítésével, illetéktelen hozzáférés biztosításával, üzenetek lehallgatásával vagy átirányításával, jelszavak és személyes adatok gyűjtésével. Legveszélyesebbek az észrevétlenül működő, illetéktelen hozzáférést biztosító vírusok, mert ezek segítségével a fertőzött számítógép zombigéppé tehető, melyet aztán támadások kiindulópontjául használhatnak. A zombigépeket botnetekbe szokás szervezni a hatékonyabb támadás érdekében. Az így kivitelezett műveleteket rendkívül nehéz lekövetni vagy megakadályozni, mert egy sok gépből álló botnet jelentős erőt képvisel.

Zombigép (Bot): Valamely kalóz távoli irányítása alatt álló számítógép.

Botnet: Zombigépek összehangoltan működő hálózata.

2004-ben a szakértők szerint hazánkban 120 milliárd forintos kárt okoztak a vírusok[315], miközben az internetszolgáltatók 5-6 ezer támadást védtek ki naponta[316].

A CSI/FBI közös felmérése alapján az Egyesül Államokban 2005-ben a teljes számítástechnikai bűncselekmények okozta kár meghaladta a 130 millió amerikai dollárt, melyből több mint 42,7 millió dollárnyit a vírusok okoztak. [317] Nem szabad azonban figyelmen kívül hagyni a második helyen szereplő illetéktelen hozzáférést, ami a hatályos magyar Btk. 300/C. § (1) bekezdése nevesít és mintegy 31,2 millió USD kárt okoz illetve az információlopást, aminek a tekintetében sajnos hiányzik a megnyugtató mértékű pönalizálás a magyar büntető anyagi jogból, annak ellenére, hogy hazánk csatlakozott a vonatkozó

[312] Massachusets Institute of Technology
[313] http://hu.wikipedia.org/wiki/Sz%C3%A1m%C3%ADt%C3%B3g%C3%A9pes_f%C3%A9reg (Letöltés ideje: 2007.11.10.)
[314] Simple Mail Transfer Protocol
[315] Kaiser László technikai igazgató, SaveAs Kft. 2004.10.15.
[316] Tüdős András, Axelero Internet Rt. 2004.10.15.
[317] CSI/FBI: 2005 Computer Crime and Security Survey, [Számítástechnikai bűnügyi és biztonsági felmérés 2005], s.l., 2005., Computer Security Survey, Fig. 16. Idézi: Adamkó Péter-Szabó Áron: *Vírusok, férgek, kémszoftverek,* Előadás, BME IK 3. dia.

nemzetközi egyezményhez. Mindössze a 178/A. § (1) bekezdésének d) pontja a Magántitok jogosulatlan megismerése bűncselekmény egyik elkövetési magatartásaként nevesíti a másnak számítástechnikai eszközzel továbbított küldemény vagy adat kifürkészését és rögzítését, illetve a 178. § kiterjesztett értelmezése ad bizonyos lehetőségeket. Ez kevés egy olyan veszélyes cselekménnyel szemben, amely 2005. évben 30,9 millió USD kárt okozott az Egyesült Államokban. Hazánkban az adathalászat okozta kárt 200 millió forintra becsülik. Az Egyesült Királyságban tavaly az adathalászat által okozott kár a becslések szerint mintegy 600 milliárd forint.[318] Véleményem szerint ez nagyon súlyos probléma, amellyel mindenképp foglalkozni kell a közeljövőben. Ugyanis azzal, hogy a 300/C. § (1) bekezdés bünteti a rendszerbe történő jogosulatlan belépést, az csak bizonyos esetekben szükséges az információ ellopásához. Erre legjobb példa a lehallgatás, amikor a hálózaton továbbított adatokat a fizikai hordozó megfigyelésével, annak forgalmának rögzítésével szerzik meg. Illetve alapjában tisztázatlan a kérdés, hogy az adatok elfogása megvalósítja a belépést vagy nem.

Lehallgatott átvitel (Interception/wire tapping): az adatok fizikai megjelenésének illetéktelen rögzítése.

Nyitott továbbá az a kérdés is, hogy pontosan mi határolja el jogos belépést a jogosulatlantól. Például szabad-e belépni bármely jelszóval nem védett területre. Különösen jó példa erre a vezeték nélküli hálózatok korában azok, akik jelszóval nem védett vezeték nélküli hálózatokat keresnek abból a célból, hogy az azokon megosztott Internet előfizetést ingyen használják, vagy esetleg a helyi hálózat megosztott mappáiból fájlokat töltsenek le. De immár szinte történelmi példával élve, voltak olyanok is, akik sorra tárcsázták a telefonszámokat, hátha védtelen, modemes kapcsolattal rendelkező hálózatra akadnak.

War dialing: a nyitott modemes kapcsolattal rendelkező hálózatok keresése.

War driving: a nyitott vezeték nélküli hálózatok keresése.

A jogszabály mai állapota látszólag egyértelmű, ha a számítástechnikai rendszer védelmét biztosító intézkedés jelen van, annak kijátszásával történő belépés bűncselekmény. Ha nincs ilyen intézkedés, számítástechnikai bűncselekmény nem valósul meg. Büntetni rendeli viszont a biztonsági rések kihasználásával vagy a számítógéphez jogosulatlanul fizikai kapcsolatba kerüléssel megvalósított elkövetést.

Kiaknázás (Exploit): a rendszer szoftverében található biztonsági rés rosszhiszemű kihasználása.

Betolakodó (Intruder): a rendszerhez jogtalanul fizikailag hozzáférő személy.

Szélhámosság (Social Engineering): a rendszerhez megfelelő jogosultságokkal rendelkező jóhiszemű személy megtévesztése révén történő hozzáférés.

Az információlopásnak számos további módszere van, a legtöbb észrevehetetlen, hiszen egy információ megszerzéséhez az információt hordozó adatnak mindössze az elolvasása szükséges. Ráadásul egy informatikai rendszerből történő információszerzés megtörténhet oly módon is, hogy a social engineer egy bent dolgozó alkalmazottat vesz rá, hogy a szükséges információkat vagy hozzáféréseket részére megszerezze, gyakran úgy, hogy az alkalmazott azt hiszi, a cég egy belső munkatársával beszél.[319] A fenti okok révén kapcsolódik szorosan ezen típusú bűncselekményekhez az adatok védelmének szükségessége. Az információlopás a legkritikusabb pont a vállalatok számára, de ez nem jelenti azt, hogy a kalózok számára látszólag érdektelen információt tároló magánszemélyek

[318] www.uzletihirszerzes.hu, Letöltés ideje: 2007.11.10

[319] Kevin D. Mitnick – William L. Simon: The Art of Deception – Controlling the Human Elements of Security [A legendás hacker – A megtévesztés művészete] Bp., 2003, Prefact-Pro

számítógépei ne lennének veszélyben. Gyakran ugyanis az információ megszerzéséhez vezető első lépés a célszemély otthoni számítógépének megtámadása, hiszen számos ember követi el azt a hibát, hogy azonos jelszavakat használ otthon és a munkahelyén. További kockázatot okoz az adatok nem megfelelő kezelése. Ki gondolná például, hogy az irodában, ahová csak alkalmazottak léphetnek be, biztonsági kockázat, ha jelszavakat vagy más fontos adatokat az asztalán vagy a monitorra ragasztott cetlin tárol?

Kiemelkedő példa a social engineering hatékonyságára a *Stanley Rifkin ügy*, Stanley Mark Rifkin 1978-ban 10 millió USD-t lopott az azóta már megszűnt Security National Pacific Bank Los Angeles-i fiókján keresztül. Stanley egy IT cég szakembereként a bankba telepített, biztonsági másolatot készítő szoftvert ellenőrizte. Munkavégzés közben megfigyelte, hogy a banki alkalmazottak az átutalások kezelésekor önmagukat egy naponta változó kóddal azonosítják, amikor kapcsolatba lépnek az átutalást végrehajtó központtal. Mivel a jelszó naponta változott, ezért a dolgozók megtanulás helyett lejegyzetelték az aznapi jelszót egy cetlire, amit jól látható helyen hagytak. Egyik nap Stanley, miközben az informatikai rendszert ellenőrizte, megtanulta a kódot. Még aznap délután a bank épületéből telefonon felhívta az átutalási központot, magát a kód ismeretében a bank munkatársának adva ki átutaltatott 10.200.000 dollárt egy korábban általa nyitott svájci számlára. Svájcba repült, a pénzt felvette és gyémántokat vásárolt belőle, majd hazautazott az államokba, övtáskájában a gyémántokkal.[320]

A fenti esetnek van még egy nagyon nagy tanulsága. Rávilágít, mennyire könnyen kihasználható kiskaput biztosít bármilyen informatikai rendszerhez a felhasználói támogatás hiánya. Ha a jelszavak és az elérési eljárások túl bonyolultak, túl gyakran változnak vagy a felhasználó nem elég képzettek vagy motiváltak, az megnöveli a biztonsági kockázatot.[321]

A közelmúltban az MI5 kémelhárító szolgálat figyelmeztetett arra is, hogy a kínai hírszerzés az Interneten keresztül próbál információt szerezni az Egyesült Királyság cégeitől, hogy azt piaci manővereknél nagyobb haszon szerzésére használja fel.[322]

A számítástechnikai bűncselekmények megjelenési formái közül még egyet szeretnék kiemelni, amely mind megjelenésében, mind jelentőségében fontos. Olyan cselekményről van szó, amely 2005-ben 7,3 millió USD kár okozásával a negyedik legsúlyosabb számítástechnikai bűncselekmény kategória volt az Egyesül Államokban, továbbá bizonyos esetekben komoly politikai jelentéssel is bír.

Szolgáltatásmegtagadás (Denial of Service): a rendszer működésének jogellenes megzavarása. A DOS típusú támadások vagy célirányos csapások egy-egy kormány, szervezet vagy vállalat ellen indulnak. Egy részük bizonyítani kívánó vagy tudásukat próbálgató kalózok, szkriptkölykök vagy számítógépes bűnözők kísérletei, egy másik, nem elhanyagolható részüket azonban politikai érdekből indítják a kalózok. A kalóz szó használata nem véletlen. Hasonlóan a középkor és kora újkor uralkodói jóváhagyással rendelkező, államilag felszerelt vagy saját elkötelezettségből a hazájukért harcba szálló, de hivatalosan el nem ismert tengeri rablóihoz, az Internet kalózai is meggyőződésből vagy anyagi érdekből cselekszenek. A CIA szakértői szerint évi mintegy négyszázezer ilyen támadás történik. Az 1999-es évtől napjainkig támadások érték és érik a különböző szervereket. Legnépszerűbb célpontok a Fehér Ház, a WTO, a Pentagon, a guantanamo-i bázis, az El-Al légitársaság, a Netvision központi internetszolgáltató, a NASA, a Lockheed-Martin repülőgépgyártó, a RedStone Arsenal katonai bázis és a Sandia National Labs

[320] Uo. 5-6. o.
[321] Peter Norton, Mike Stockman: i.m. 37-38. o.
[322] http://news.zdnet.co.uk/security/0,1000000189,39291239,00.htm?r=1 (Letöltés ideje: 2008.03.24.)

nukleáris kutatóbázis. A támadások mögött különböző kisebb-nagyobb szervezetek révén államok vagy szélsőséges csoportok állnak. Példának megemlíteném a világ jelenlegi társadalmi-gazdasági berendezkedését az Internet segítségével megváltoztatni kívánó Electrohippiket, az iszlám radikális terrorszervezetek internetes szövetségeseit, mint a Gforce Pakistan, a Pakistan Hackerz Club vagy az Iran Hackers Sabotage. A támadások miatt az USA 2006. február 6-10. között egy hasonló támadást szimulált a saját kormányzata ellen, hogy a felkészültséget leellenőrizze és a biztonsági réseket befoltozza (Operation Cyber Storm). A leghíresebb akciók közé tartozik az USA hackereinek Milosevics bankszámlája elleni művelete, a dánok elleni iszlám támadás, amikor 2006. január 30. és február 6. között 578 dán honlapot törtek fel, válaszul a Jyllands-Posten nevű újságban közölt Mohammed-karikatúrákra, vagy a 2007. június 21-i Pentagon elleni roham, amikor a minisztérium 1500 számítógépet „veszített"[323] (gondoljunk bele, mit jelentene ez egy magyar kormányzati szervnek). Sokkal komorabb jóslatokat képviselnek az államok részéről egymás ellen indított támadások. Az első ilyen dokumentált összecsapásra 2000-ben került sor Izrael és Libanon között, összesen 140 ezer támadással 170 kulcsfontosságú gépet bénítottak meg. 2001-ben az USA és Kína csapott össze, eredmények nem ismertek. 2003-ban a II. iraki háború miatt az USA lett a célpontja az iszlám országoknak, több mint 400 weboldalt támadtak eredményesen. 2005-ben hajtotta végre az USA Kína ellen a Titan Rain hadműveletet, elsősorban a katonai hálózatok ellen. 2007-ben Dél-Korea támadta meg a teljes Internetet működtető 13 kulcsfontosságú ún. „root" szervert, hármat sikerült megbénítaniuk egy időre. 2007. áprilisától kirobbant az észt-orosz kalózháború, ami május 18-ig tartott. Utóbbi csak azért nem eszkalálódott tovább, mert a NATO nagylelkűen nem minősítette katonai akciónak az orosz kalózok összehangolt, tervszerű akcióit. Szakértők szerint a jövőben az ilyen támadások esetenként nagyobb anyagi kárt okozhatnak, mint a valódi fegyveres összecsapások.[324]

A magyarországi kalózakciók közül leginkább jellemző a zombigépekről kormányzati szerverek ellen szolgáltatásmegtagadás támadást indító férgek terjesztése. 2004-ben jelent meg a Zafi osztályú nevű féreg, amely a rendszerbe történő beépülése után elárasztás (flood) fajtájú DOS támadást indít a Google, a Microsoft és a Miniszterelnöki Hivatal ellen, miközben megakadályozza a többi alkalmazás működését. Közben a gépen található email-címekre levélben elküldi magát. Néhány vállfaja a levélben szélsőséges politikai üzenetet hordoz.[325]

Informatikai bűncselekmények hétköznapi eszközei

A legtöbb informatikai bűncselekmény elkövetése olyan eszközökön keresztül történik, amelyek semmiben sem különbözik a megszokott saját számítógépünktől. Az abszolút többséget viselő Szerzői vagy szerzői joghoz kapcsolódó jogok megsértése bűncselekményekhez például általában csak egy hordozható háttértárra (lemez, USB kulcs stb.), rögzítő egységre (CD/DVD író) vagy internetkapcsolatra van szükség, a második helyen álló Tiltott pornográf felvételekkel visszaélés bűncselekményhez pedig elegendő egy digitális fényképezőgép vagy egy mobiltelefon. Még a már-már legendás, Szerzői vagy szerzői joghoz kapcsolódó megsértése üzletszerű elkövetéséről híres „warez" szerverek elindításához is elegendő egy személyi számítógép és egy ingyenes kiszolgáló alkalmazás

[323] Természetesen csak képletesen, a számítógépeket „mindössze" egy ideig nem használhatták.
[324] http://nol.hu/cikk/456994 Letöltés ideje: 2007-10-29
[325] Kaiser László technikai igazgató, SaveAs Kft, 2004.10.28.

illetve alapvető webprogramozási ismeret. Sajnos napjainkra az is megszokottá vált, hogy weboldalakon az alkotmányos rend ellen szervezkedjenek vagy gyűlöletbeszédeket tegyenek közzé.

Mindazonáltal egyes bűncselekményekhez valóban speciális, de kereskedelmi forgalomban kapható informatikai eszközöket is használnak, mint például a mágneskártya leolvasók vagy a módosított integrált áramkörök. Például a PlayStationok esetében a házilag írt lemezeket eredetileg nem olvasó meghajtókat „megpatkolják", hogy olvassák az illegálisan beszerzett szoftvereket tartalmazó lemezeket. Szintén ide tartoznak a végtelenített telefonkártyák vagy az utánzott hitelkártya chipek is, csakúgy, mint a közokiratok biztonsági jellegzetességeinek utánzásához használható különleges nyomdatechnikai eszközök.

A fájlcserélő hálózatok problematikája

Warez (kalózszoftver): szerző hozzájárulása nélkül felhasznált alkotás, szó szerint illegális áru. Sajátos megjelenése a társas bűnelkövetésnek az úgynevezett fájlcserélő hálózatok. Az ilyen, két számítógép közötti kapcsolaton alapuló adatcserélő rendszerek egyáltalán nem számítanak újdonságnak, sőt gyakorlatilag a hálózatok első megjelenési formájának tekinthetők, ám igazán akkor terjedtek el, amikor Bram Cohen megírta Python nyelven a BitTorrent nevű programot, amely lehetővé tette fájlcserélő hálózatok működését. A kliensek a fájlokat darabokban töltik le. Minden csomópont megkeresi a hiányzó részhez a lehető leggyorsabb kapcsolatot, miközben ő is letöltésre kínálja fel a már letöltött fájldarabokat. A módszer nagyon jól beválik nagyméretű fájloknál, például videók és nagyobb szoftverek esetében. Ennek az az oka, hogy az ilyen letöltéseknél a szűk keresztmetszetet általában a szerver sávszélessége jelenti. A BitTorrent esetében minél keresettebb egy fájl, annál többen vesznek részt az elosztásában, ezáltal az elosztása gyorsabban megtörténik, mintha mindenki egy központi helyről (szerverről) töltötte volna le. A fájlok darabolásából adódik, hogy a megszakadt letöltések könnyen folytathatóak.[326]

Torrent: megosztott fájl eléréséhez szükséges adatokat tartalmazó kisméretű fájl.

BitTorrent: informatikai protokoll, valamint e protokollt használó p2p alapú fájlcserélő szoftver.[327]

Elérhetőség (availability): A torrent teljes másolatainak száma a kliens számára. Minden seed 1-et ad ehhez a számhoz. Egy csatlakozott peer, amelynek csak töredékek állnak a rendelkezésére, csak egy tört számot ad az elérhetőséghez.[328]

Csomópont (peer): A peer egy másik számítógépen futó kliens, főképp azokat a klienseket értjük ezen, amelyek még nem az egész fájlt, csak részeit birtokolják.[329]

Mag (seed): A seed egy olyan peer, amely már rendelkezik az összes darabkával, és a továbbiakban a fájl töredékei innen is elérhetők.[330]

Szívó (leech): A kifejezést azokra a peerekre használjuk, amelyeknek kifejezetten rossz a feltöltés/letöltés arányuk, vagy elhagyják a bolyt rögtön azután, miután befejezték a

[326] http://hu.wikipedia.org/wiki/Torrent Letöltés ideje: 2008.03.15
[327] loc. cit.
[328] loc. cit.
[329] loc. cit.
[330] loc. cit.

letöltést. Ez az általános BitTorrent etikettel ellenkezik. A téves értelmezés szerint a leech egy olyan peer, amely még nem rendelkezik minden fájltöredékkel.[331]

Boly (swarm): Együttesen az összes peert, ami megosztja a torrent fájlt nevezzük bolynak. Négy peer és két seed hattagú bolyt jelent.[332]

A fájlcserélő hálózatok működtetésével kapcsolatban akár az a kérdés is felmerülhet, hogy a fájlcserélő hálózatban való részvétel bűnszervezetben részvételnek minősülhet-e. E hálózatok alkalmasak arra, hogy a szerzői vagy szerzői joghoz kapcsolódó jogokat különösen nagy vagy különösen jelentős vagyoni hátrányt okozva sértsék meg, mely esetben a lehetséges büntetési tétel eléri, illetve meghaladja az ötévi szabadságvesztést.[333] Továbbá a fájlcserélő hálózatok alapvető feltétele az összehangolt működés, bár az összehangolásra a csoport tagjainak nem kell külön odafigyelnie, elég ha belenyugszanak, mivel azt a program végzi el, amit a számítógépükre telepítenek, illetve elindítanak. Általában a létszám jóval meghaladja a három embert. Láthatóan adva van minden törvényi elem a bűnszervezetté történő minősítéshez.[334] A fájlcserélő hálózatok tagjait a bűnszervezetben történő részvétel joghátrányaival sújtása azonban elképzelhetetlen mértékben kriminalizálná a társadalmat, melynek nagyon súlyos következményei lehetnek.

Azonban a fentiek ellenére is fenntartom, hogy a mainál lényegesen hatékonyabb eljárásokra és keményebb fellépésre van szükség, hiszen jelen pillanatban nem sok eredménye van a hatóságok fellépésének. 2007. november 8-9-én a rendőrség egy akció során lefoglalta a BitHUmen nevű fájlcserélő hálózat több számítógépét. A fájlcserélő hálózat azonban 2007. november 26-án újra száz százalékban üzemelt. Sőt, egyes tulajdonosok még a számítógépüket is visszakaphatták.[335]

A véleményem az, hogy a mainál keményebben kell fellépni a fájlcserélő hálózatok ellen, de figyelemmel kell lenni ennek kockázataira is.

A dolog külön érdekessége, hogy mivel az elérhető fájlok helyét tároló trackerekre fizetés ellenében lehet fellépni, a torrent hozzáférést jelentő felhasználói azonosítók is célpontjává vált a különböző informatikai bűncselekményeknek. Több olyan phishing oldal létezik, amely szimulálja a torrent trackerek belépési felületét, így lopva el a felhasználók hozzáférését.[336]

Torrent Tracker: A torrent tracker egy magas rendelkezére állású szerveren futtatott alkalmazás. Feladata a fájlcserélésben részt vevő végpontok közötti közvetítés.[337]

A trackerek magát a fájlt nem, csak az eléréséhez szükséges adatokat közvetítik a hálózat tagjai között. Általában adatbázissal rendelkeznek a meglévő torrentekből, a felhasználók pedig azért fizetnek, hogy ehhez az adatbázishoz hozzáférjenek. Természetesen vannak nyilvános trackerek is, melyek jelentős népszerűségnek örvendenek.[338]

[331] Uo.
[332] Uo.
[333] 1978. évi IV. törvény 329/A.§
[334] 1978. évi IV. törvény 137. § 8. pont
[335] www.torrentportal.hu (Letöltés ideje: 2008.03.15)
[336] Például http://bithumen.tx.hu
[337] www.torrentportal.hu (Letöltés ideje: 2008.03.15)
[338] Például http://malacka.com

Összefoglalás

Jelen cikk kivonata a szakdolgozatomnak, amelyet egy nagyobb tudományos munka első lépésének szánok. Munkásságom során az információs társadalomhoz kapcsolódó bűncselekményeket kísérlem meg több szempontból is megközelíteni. Elsősorban az információs társadalom kialakulásával és az ezt lehetővé tevő tényezőkkel illetve az informatikai bűnözés megjelenésével, fejlődésével foglalkozom, különös tekintettel a számítástechnikai bűncselekményekre, melyek az informatikai bűnözés, mint jelenség gerincét képviselik. Kitekintek azonban olyan cselekményekre is, melyek átalakultak és mai formájukban már kötődnek az informatikához. Az informatikai bűncselekmények eszközeit és módszereit összefoglalom, a számítástechnikai bűncselekményekéit viszont részletesen tárgyalom, bemutatva az eredményeket és az egyes ellene történő fellépéseket is. Elemzem a témában létrejött magyar és európai uniós jogszabályokat, a nemzetközi szerződéseket, példáimban hazai és külföldi jogeseteket egyaránt bemutatok. Statisztikai adatok tükrében is vázolom a cselekmények állapotát, megoszlását. Reményeim szerint ez a munka is közelebb vihet ahhoz, hogy felhívja a figyelmet az informatikai bűncselekmények súlyára egy információs társadalomban és a jogászképzésben helyet kapjon az informatikai bűncselekmények sajátosságaiknak megfelelő súlyú oktatása.

Bibliográfia

1. Székely Zoltán: Bűnözés az információs társadalomban, Szakdolgozat, PTE ÁJK 2008.
2. Varga Balázs: Informatikai bűncselekmények, Kézirat, 2003.
3. Kevin D. Mitnick – William L. Simon: The Art of Deception – Controlling the Human Elements of Security [A legendás hacker – A megtévesztés művészete] Bp., 2003, Prefact-Pro
4. Peter Norton, Mike Stockman: Network Security Fundamentals [A hálózati biztonság alapjairól], Debrecen, 2000, Kiskapu Kft.
5. Babócsy – Lepenye – Nemetz – Urbanovits: Biztonságos Windows 2003R2 hálózatok Budapest, 2006. NeTeN
6. Adamkó Péter-Szabó Áron: Vírusok, férgek, kémszoftverek, Előadás, BME IK
7. Pintér Róbert (szerk.): Magyar információs társadalom jelentés 1998-2008. Kézirat, ITTK Csoport, Budapest, 2007.
8. http://ap.ohcr.org
9. http://cybercrime.planetindia.net
10. http://eur-lex.europa.eu
11. http://nol.hu
12. www.cybercrime.gov
13. www.harmonet.hu
14. www.iso.org
15. www.its.hu
16. www.jogiforum.hu
17. www.magyarorszag.hu/jogszabalykereso
18. www.origo.hu
19. www.sg.hu
20. www.szochalo.hu
21. www.uzletihirszerzes.hu
22. www.viruslist.com
23. www.wikipedia.org
24. http://www.ipolicy.eu/
25. http://www.zdnet.co.uk/