HADMÉRNÖK

IV. Évfolyam 1. szám - 2009. március

Illési Zsolt
Zrínyi Miklós Nemzetvédelmi Egyetem
illesi.zsolt@proteus.hu

KRIMINÁLTECHNIKA SZEREPE AZ INFORMATIKAI VÉDELEM TERÜLETÉN

Absztrakt

Napjainkban az informatikai védelem fókuszában szinte csak a megelőzés és a javítás áll. A felfedezés, pontosabban az informatikai biztonsági események megfelelő felderítése, az elkövetés körülményeinek kivizsgálása és a bizonyítékok szakszerű és jogszerű gyűjtése jelenleg hazánkban elhanyagolt terület. Pedig az infokommunikáció térhódításával a bűnelkövetések száma is növekszik, és ennek következtében egyre nagyobb társadalmi igény lenne erre. Az informatikai, infokommunikációs rendszerekkel kapcsolatos kriminálltechnikai vizsgálatok alapja a digitális nyom meghatározása. A modern kriminalisztikának feladata továbbá az eljárási cselekmények informatikai környezetre való adoptálása, hogy biztosítsa a jogszerű és szakszerű nyomrögzítést, vizsgálatot és értékelést az informatikai, infokommonikációs rendszerekkel kapcsolatos bűncselekmények esetén. Jelen dolgozat a fentiek fényében az informatikai védelem és a kriminálltechnikai kapcsolatát tárja fel, javaslatot tesz a digitális nyom fogalmára, összefoglalja az informatikai rendszerekkel kapcsolatos eljárási cselekményeket és az azok során elvégzendő tevékenységeket.

In recent times preventive and corrective controls are in the focus of information security. Detection, or to be more precise the adequate exploration of information security events, examination of the circumstances of the perpetration and the professional and lawful collection of digital evidence is a neglected domain in Hungary. However, the spreading of the infocommunication and related technologies increase computer crime and therefore the social demand on this is also increases. The definition of digital evidence could serve as a basis for forensic analysis of investigations of infocommunication related crimes. IT is the duty of the modern criminal science to adopt the general rules of criminal processes to the computerised environment to professional and lawful collection, analysis and valuation of digital evidence for crimes related to computers and infocommunication systems. This paper, in the light of the above, describe the relations between information security and forensics, recommends a definition for digital evidence, summarises the computer linked criminal processes and all the activities to be carry out.

Kulcsszavak: *informatikai védelem, kriminalisztika, kriminálltechnika, digitális nyom ~ information security, forensic science, applied forensics, digital trace*

Bevezetés

Számítógépek vannak mindenhol körülöttünk. A háztartási gépek, a szórakoztató elektronikai eszközök, a mobil telefon, az internet már szerves részesei a hétköznapi emberek mindennapjainak. Az informatikai eszközök számának növekedésével, mintegy annak természetes velejárójaként megjelent, majd elburjánzott az információtechnológiához kapcsolódó bűnözés. Egy-egy „hagyományos" bűncselekmény (pl. csalás, szerzői jog vagy üzleti titok megsértése) megjelentek új elkövetői magatartások, új támadási módszerekkel bombázva a számítógép tulajdonosokat, az internet közösségét, illetve az internethez kötődő szolgáltatásokat nyújtó szervezeteket.

Megjelentek az automatikus károkozók (vírusok, férgek stb.), a más tudásán élősködő script kiddie[1]-k, virágzásnak indultak a (white/grey/black hat) hacker, cracker[2] közösségek. Ennek hatására az internetre kitett számítógépekre leselkedő veszélyek exponenciálisan megnőttek. Először a hálózatokat védték a rendszergazdák egyszerű hálózati forgalomkorlátozással (Access Control List vagy ACL), tűzfalakkal, majd ahogy az informatikai támadások egyre kifinomultabbá váltak úgy jelentek meg a vírusirtók, személyes tűzfalak, virtuális magánhálózatok (Virtual Private Network, vagy VPN), kémprogram felderítő és -írtó programok. Ma már olyan sok automatikus támadás ér egy gépet, hogy nem lehet külön védelmi intézkedések nélkül úgy felinstallálni egy Windows XP-t, hogy valamennyi biztonsági telepítő csomagot letöltsön az internetről mielőtt megfertőzné valamilyen kártékony kód.

Az internetben rejlő lehetőséget nem csak a legális üzleti vállalkozások, hanem az alvilág és a terrorista csoportok is felismerték és egyre nagyobb jártassággal kezelik a XXI. század technológiáját, hogy egymással kommunikáljanak (tervezzenek), pénzt gyűjtsenek, toborozzanak. A „lágy" felhasználás mellett megjelentek az első csírái a „kemény" támadásoknak is, amit a 2007-es észt-orosz konfliktus is jól példáz. A szakirodalom egyre inkább figyelmeztet a kritikus infrastruktúrát fenyegető támadásokra, ami kivitelezhető például az azokat menedzselő/irányító számítógépekre sújtó csapással[3].

A támadások fejlődésével a védelem is egyre nagyobb szerephez jut, a technikai szervezési intézkedések egyre gyakrabban kerülnek előtérbe. Kevés szó esik azonban a sikeres támadásokról – az érintettek sokszor a jó hírnevük védelme érdekében nem is hozzák nyilvánosságra, hogy milyen támadások érték őket és milyen károkat szenvedtek el ezek miatt. A sikeres támadások mellett kevés szó esik arról, hogy milyen módon lehet ezeket vizsgálni, milyen módon lehet az elkövetőtől valamilyen jogorvoslatra szert tenni, büntetőjogi vagy polgári jogi úton elégtételt szerezni.

Az informatikai rendszerek ellen irányuló támadások vizsgálatának akadálya az is, hogy a hagyományos kriminalisztika tudományának központjában a tárgyiasult nyomok állnak, a „virtuális" világ kriminalisztikai vizsgálata hazánkban még gyerekcipőben jár.

A sikeres jogorvoslat, kompenzáció gátja a nem-megfelelő (nem kriminál technikai alaposságú) megközelítés, amelynek „eredményeként"

---

[1] A script kiddie az internetes zsargonban olyan hacker (jelölt), aki még nem rendelkezik elegendő szakismerettel így mások által megírt programok és parancsfájlok (script) segítségével próbál ja az informatikai rendszer védelmét feltérképezni, vagy feltörni.

[2] A cracker az internetes zsargonban a rosszindulatú hacker, aki elsősorban anyagi haszonszerzés miatt tör be informatikai rendszerekbe, vagy hajt végre számítástechnikai bűncselekményeket.

[3] Ld.: Dr. Kovács László: Az információs terrorizmus elleni tevékenység kormányzati feladatai, HADMÉRNÖK 2008:(2) 138-148 (2008) vagy
Dr. Haig Zsolt – Dr. Kovács László: Kritikus információs infrastruktúrák elleni fenyegetések, Kritikus információs infrastruktúrák védelme, In: Szenes Katalin (szerk.), Az informatikai biztonság kézikönyve: 30. aktualizálás, Budapest: Verlag Dashöfer Szakkiadó, 2008. pp. 137-170. vagy
Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme című doktori (PhD) értekezés, Budapest, ZMNE, 2007.

a) nem gyűlik össze elegendő mennyiségű/minőségű bizonyíték
b) nem készül megfelelő dokumentáció
c) a nyomkezelés nem megfelelősége miatt nem megismételhető/
d) hibák keletkeznek az elemzés vagy az értelmezés során.

A dolgozatom célja, hogy

- meghatározzam az informatikai védelem és a krimináltechnika viszonyát,
- definiálja a digitális nyom fogalmát
- javaslatot tegyek a digitális nyomok csoportosítására
- összegezzem az informatikai bűncselekmények helyszíni vizsgálatának főbb jellemzőit.

A krimináltechnika és az informatikai védelem kapcsolata

Informatikai védelem

Az informatikai védelem az informatikai rendszerben tárolt, kezelt, rendszerezett, és továbbított adatot (információt) az informatikai szolgáltatásokat az ezeket biztosító informatikai rendszereket fenyegető tényezők elleni, az informatikai biztonság (mint megkívánt állapot) megteremtésére és fenntartására irányuló humán, technikai (környezeti, fizikai, logikai) és jogi védelmi intézkedések összessége. [1] [2]

A védelmi intézkedések (kontrollok) célja tehát az, hogy az informatikai rendszer fenyegetettségét a nemkívánt események (pl. támadások) valószínűségének vagy hatásának mérséklésével a kívánatos szintre csökkentse ezáltal az informatikai biztonságot a megkívánt szinten tartsa. [3] A fenyegetések bekövetkezésének függvényében a kontrollokat a következőképpen lehet osztályozni:

- ***megelőző kontrollok***, amelyek a fenyegetések bekövetkezésének valószínűségét, vagy a nemkívánatos események által okozott károk hatását csökkentik még mielőtt bekövetkezhetnének (pl. többfaktoros authentikáció, ami csökkenti az illetéktelen behatolás valószínűségét, vagy a rendszeres mentés, ami csökkenti egy adatvesztés hatását);
- ***felfedező kontrollok***, amelyek a nemkívánt eseményeket azok bekövetkezte közben észlelik és ezáltal csökkentik a kárt (pl. hálózat vagy host alapú behatolás-érzékelő rendszerek), vagy az eseményt követő kivizsgálások támogatásával a felelősségre vonás vagy kártérítés során játszanak szerepet a kárcsökkentésben (pl. naplózás);
- ***javító kontrollok***, a melyek az eseményeket követően avatkoznak be, ezáltal csökkentve a közvetlen vagy a későbbiekben esetleg felmerülő károkat (pl. hibajavító kódok, katasztrófa-elhárítási tervek). [4]

Kriminalisztika fogalma, célja, rendszere

A kriminalisztika a "*bűnügyi nyomozástan, azaz a bűnügyi tudományoknak az az ága, amely a bűncselekmények felderítésének és bizonyításának eszközeit és módszereit tárja fel és rendezi elvi és gyakorlati szempontból egyaránt*". {[7] p19}

A kriminalisztkát két fő részre, általános és különös részre osztva tárgyalják. Az **általános rész** öt területre tagolható:

1) ***kriminalisztika történet*** – amely azzal foglalkozik, hogy történelmileg hogyan alakult ki és fejlődött:
   - a bűnüldözés szervezeti rendszere
   - a kriminalisztika módszerei

- a természettudomány, a műszaki- technikai tudományok és a bűnfelderítés kapcsolata

2) ***kriminalisztikai elmélet***, ide tartozik a kriminalisztika egészére érvényes, általános érvényű tételek kidolgozása, amelyek alapvetően befolyásolják e tudományterület valamennyi eredményét.
3) ***kriminál technika***, amelynek célja a bűncselekmények megelőzése, felderítése és bizonyítása érdekében a bizonyítási eszközök felkutatása, rögzítése és vizsgálata technikai módszereivel és eszközeivel, valamint a tárgyi bizonyítási eszközök létrejöttének törvényszerűségeivel foglalkozik". {[8] p63}
   a kriminál technikai tevékenységnek három fő iránya van:
   - büntető eljárások során bizonyítékok felkutatása, rögzítése és szakértői vizsgálata
   - a bűncselekmények megelőzésének előmozdítására technikai eszközök kifejlesztése és alkalmazása
   - tudományos kutató-, fejlesztő munka végzése
4) ***kriminál taktika***, a személyi jellegű bizonyítékszerzéssel, annak főbb sajátosságaival és összefüggéseivel foglalkozik
5) ***kriminál stratégia***, a politika és a jog által meghatározott, a bűnelkövetést megelőző és korlátozó feladatokat (a kriminálpolitikai elveket) közvetíti az igazságszolgáltatáshoz és az államigazgatási szervezetekhez, valamint előírja a megvalósítás átfogó, tervszerű, koordinált közép- és hosszútávú intézkedéseit

A **különös rész** az egyes bűncselekmény kategóriák felderítésére és bizonyítására a szak kriminalisztikákkal foglalkozik, felhasználva a kriminál technika és a kriminál taktika általános eredményeit, így a büntetőjog szerkezetével megegyező struktúrában az egyes bűncselekményfajtáknak megfelelő kriminálmetodikai szabályokat és kriminálmetodikai ajánlásokat tartalmaz.

A kriminál technika az informatikai védelem rendszerében

A korábbi fejezetek figyelembevételével tehát a kriminalisztika tehát az informatikai biztonság rendszerén belül egy olyan felfedező kontroll, ami a természettudomány, a műszaki- technikai tudományok eszközei és módszerei felhasználásával az informatikai rendszereket ért támadások idejének, módjának és forrásának azonosítását szolgálja, továbbá információt nyújt a támadó személyének felderítéséhez.

Nyomok a virtuális világban

Edmond Locard az 1920-as évek kiemelkedő kriminalisztikai szakértője szerint bárki, vagy bármi kerül kapcsolatba egy bűncselekmény helyszínével valamilyen nyomot hagy és valamilyen nyomot tovább visz magával, amikor elhagyja azt, mondta ki.

Ennek az elvnek (Locard Exchange Principle) a következetes vizsgálata vezetett a traszológia (nyomtan) kifejlődéséhez. A traszológia a kriminál technikának az az ága, amely a nyomokkal, azok keletkezésének körülményeivel, a nyomképződés folyamatának elemzésével és a nyomképző objektum (tárgy, testrész) azonosításával foglalkozik a bűncselekmények felderítésére, bizonyítására, megelőzésére és ezek érdekében a nyomok felkutatásának, biztosításának, rögzítésének, vizsgálatának és értékelésének módszereit dolgozza ki.

A nyomtan eredményei az anyagi világban megteremtik az áldozat, terhelt (elkövető) és a helyszín közötti kapcsolatot. [4] [7] A „virtuális” világban is léteznek ilyen nyomok, amelyek hasonló kapcsolatot teremtenek az elkövető, az elkövetésben felhasznált számítógépek és a célpont (a sértett számítógépe) között.

A klasszikus krimináltechnika szerint a nyom keletkezésében három tényező együttesen vesz részt:

- a nyomképző, vagyis az a dolog (tárgy vagy testrész), amely a nyomképződési folyamat során a nyom hordozón nyomot hagy;
- a nyom hordozó, vagyis az a dolog (tárgy, testrész, talajrész), amelyen a nyomképző a nyomképződési folyamat során nyomot hagy;
- a nyomképződési folyamat, vagyis a kölcsönhatás módját meghatározó folyamat, amely meghatározza a nyom egyedi jellemzőit, fajtáját.

A krimináltechnikában a nyom és az anyagmaradvány szorosan összefüggő fogalmak, és sok esetben csak a módszer alapján lehet eldönteni, hogy nyom vagy anyagmaradvány vizsgálata történt-e meg, azonban a két fogalom mégsem azonos, az alábbiak szerint különülnek el:

- ***nyom***, a nyomhordozón a nyomképző érintkező felületének formája (alakbeli sajátosság) a vizsgálat tárgya (pl. harapás)
- ***anyagmaradvány***, a nyomhordozón a nyomképző anyaga rakódik le és ennek elemzése a vizsgálat tárgya (pl. nyál)

Nyom hagyományos kriminalisztikai, traszológiai értelemben

A hagyományos kriminalisztikában a nyomnak tág (kriminalisztikai) és szűk (traszológiai) értelmezéséről beszélhetünk. E szerint:

- *„Kriminalisztikai nyom valamennyi a vizsgált ügy szempontjából releváns objektum kölcsönhatása révén keletkező anyagi jellegű elváltozás (vagyis a nyomok és az anyagmaradványok egyaránt)”.*
- *„Traszológiai értelemben a nyom olyan, a vizsgált ügy szempontjából releváns objektumok kölcsönhatása révén keletkező tárgyiasult elváltozás, amely morfológiai sajátosságai révén információval szolgál a nyomképző objektumról és a nyomképződési folyamatról”.* {[8] p336}

Digitális nyom

A kriminalisztikában és a traszológiában jelenleg használt nyom fogalom központjában az anyagmaradványok és a fizikai elváltozások állnak. A fizikai nyomok (testrészek, eszközök nyomainak, az anyagmaradványok, írás/kézírás, okmány stb.) vizsgálati módszereit a klasszikus kriminalisztika már részletesen feltárta.

A fizikai nyom és az adatmaradvány alapú a szemlélet az informatikai rendszerek belső működésének vizsgálata során alkalmazható, hiszen a fizikai nyomokkal ellentétben a számítógépek adattáraiban, a számítógépek közötti kommunikáció során nincs klasszikus értelemben vett nyom vagy anyagmaradvány; a vizsgálat során adatokat és adatmaradványokat vizsgálnak a szakértők.

Mivel a szakirodalom jelenleg még adós a digitális nyom fogalmának meghatározásával, ezért a továbbiakban áttekintem az informatikai rendszerek működésének főbb jellemzőit nyomtani szempontból, és kísérletet teszek a digitális nyom kriminalisztikai és traszológiai definiálására.

Krimináltechnikai és traszológiai szempontból jelentőséggel bír, hogy az informatikai rendszerek Neumann elvű számítógépekre épülnek, amelyeknek az egyik jellemző sajátossága, hogy az operatív tárban azonos feltételek mellett tárolódnak az adatok és a programok. Az ilyen rendszerekben a rendszerprogram (operációs rendszer), az alkalmazások vagy a felhasználó kezdeményezi a műveletek végrehajtását akár az adatokon akár a programokon. Ennek a sajátosságnak a leírására az informatikai szakirodalom az informatikai rendszerben lévő elemeket két csoportba sorolja:

1) ***Szubjektumok***, olyan entitások a rendszeren belül, amelyek kiváltják a műveletek elvégzését.

„A TOE-n[1] belül többféle szubjektum is létezhet:
- *a) azok, amelyek a jogosult felhasználó nevében intézkednek és szubjektumai a TSP[2] összes szabályának (például UNIX eljárások);*
- *b) azok, amelyek egy bizonyos funkcionális eljárásként viselkednek, viszont egy többszörös felhasználó nevében intézkednek (például a kliens/szerver architektúrákban található funkciók); vagy*
- *c) azok, akik magának a TOE-nak a részeként intézkednek (például bizalmi eljárások).”*

{[11], p15}

2) ***Objektumok***, olyan passzív entitások a rendszeren belül, amelyek információt tartalmaznak vagy fogadnak és amelyen a szubjektumok műveleteket hajtanak végre.

„Az objektumok olyan műveletek céljai, amelyeket a szubjektumok végeznek. Abban az esetben, amikor a szubjektum (aktív entitás) lesz egy művelet célja (folyamatközötti kommunikáció), a szubjektum objektumként működhet.”
{[11], p15}

Az informatikai rendszerekben a nyom keletkezésében résztvevő tényezők:
- a nyomképző, vagyis az a szubjektum (aktív funkció/program, felhasználó stb.), amely a nyomképződési folyamat során adatokat hoz létre, továbbít, tárol, módosít vagy töröl;
- a nyom hordozó, vagyis az objektum (passzív programok, adatok az operatív tárban, háttértárolón vagy valamelyik periférián), amelyen a nyomképző a nyomképződési folyamat során nyomot hagy;
- a nyomképződési folyamat, vagyis a kölcsönhatás módját meghatározó folyamat, amely meghatározza a nyom egyedi jellemzőit, fajtáját.

Az informatikai rendszerekben nem értelmezhető az anyagmaradvány fogalma. A digitális nyom csak adat, vagy az adatokból kinyerhető információ lehet függetlenül az adattovábbítás, -tárolás módjától és az adat megjelenési formájától.

A digitális nyom abban is különbözik a fizikai nyomoktól és anyagmaradványoktól, hogy a fizikaiaktól eltérően a digitális nyomokról (pl. digitálisan aláírt bitsorozat) az eredetivel megegyező másolat készíthető, a vizsgálatok korlátlan számban megismerhetők, és az azok eredménye azonos függetlenül a vizsgálatok számától és attól, hogy az eredeti vagy a másolt adatokon végzik el őket.

A fentiek figyelembevételével az általam javasolt digitális nyom fogalma következő:
- ***Kriminalisztikai értelemben:*** A digitális nyom olyan adat, amely a vizsgált ügy szempontjából releváns informatikai rendszer szubjektumai és objektumai kölcsönhatása révén keletkezett, továbbítódott, tárolt, módosult vagy törlődött.
- ***Traszológiai értelemben:*** A digitális nyom olyan adat, amely a vizsgált ügy szempontjából releváns informatikai rendszer szubjektumai és objektumai kölcsönhatása révén keletkezett, továbbítódott, tárolt, módosult vagy törlődött és ezáltal információval szolgál a nyomképző szubjektumról és a nyomképződési folyamatról.

[1] TOE (Target of Evaluation) az értékelés tárgya, pl. operációs rendszerek, számítógép hálózatok osztott rendszerek, alkalmazások.
[2] TSP (TOE Security Policy) az értékelés tárgyára vonatkozó (biztonsági/működési) szabályok összessége.

Informatikai bűncselekmények krimináltechnikai vizsgálata

Informatikai bűncselekmények sajátossága és osztályozásuk

Mivel a kriminalisztika tárgya a büntetőjogilag minősített magatartásformák felderítése és bizonyítása, jelen dolgozatomban csak az informatikai bűncselekmények sajátosságaival fogok foglalkozni. Véleményem szerint ez a megközelítés lefedi az összes informatikai jellegű támadást is, vagyis azokat a szándékos magatartásokat amelyeknek a célja vagy közvetlenül vagy közvetve az informatikai rendszerek működésének módosítása, blokkolása, adatok illegális bevitele, módosítása és törlése.

Jelenleg a bűncselekmények osztályozásánál a jogi szakirodalom a számítógépes bűncselekményekkel foglalkozik. Mivel azonban az elkövető az informatikai rendszer vagy annak adatainak támadásával végeredményképpen az

- információszerzés;
- információ felhasználás;
- információ előállítás;
- információtovábbítás;
- információt tárolás;
- információfeldolgozás

tevékenységeket sérti helyesebb lenne informatikai bűncselekményekről beszélni. [10] A továbbiakban ezért a „számítógéppel elkövetett bűncselekmény” vagy „számítógépes bűncselekmény” helyett informatikai bűncselekmény megnevezést használom.

Informatikai bűncselekmények sajátossága a

- ***gyorsaság*** – vagyis az eredmények rövid idő alatt, nagy távolságra, jelentős kárt okozva jelennek meg, bár egy-egy bűncselekmény előkészületére az elkövető jelentős időt használ(hat) fel;
- ***magas látencia*** – vagyis az informatikai bűncselekmény bűncselekmények sértettjei nem minden esetben érzékelik közvetlenül az okozott károkat, nem is fedezik fel az ellenük elkövetett bűncselekményt, vagy azokat nem jelentik a hatóságoknak;
- ***nemzetköziség*** – vagyis az informatikai bűncselekmények gyakran átnyúlnak a természetes országhatárokon, így az elkövető, a sértett és az esetleg felhasznált eszközök más-más állam joghatósága alá tartoznak;
- ***intellektuális jelleg*** – vagyis az elkövetők általában jól képzett, intelligens személyek, akik tisztában vannak cselekményük következményeivel és a felderítés elleni védelem szükségességével és annak módszereivel.

A jogi szakirodalom általános felosztása szerint az információrendszer lehet:

- az elkövetés ***célpontja*** – amikor a rendszert vagy annak elemeit, mint eszközt megrongálják, ellopják, vagy egyéb módon kárt okoznak benne;
- az elkövetés ***tárgya*** – amikor a számítógépes környezet szükséges a bűncselekmény megvalósításához;
- az elkövetés ***eszköze*** – amikor az informatikai rendszer a bűncselekmény elkövetését megkönnyítő kellék;
- az elkövetés ***szimbóluma*** – amikor az informatikai rendszerről „csak” szó esik, de az informatikai környezet nem is részese az elkövetésnek (pl. olyan csalás, ahol a sértett számítógépet kíván venni és ezt kihasználva ejtik őt tévedésbe).

Véleményem szerint ez az általános felosztás kiegészíthető még egy további kategóriával, ahol az információrendszer lehet továbbá:

- az elkövetés ***tanúja*** – amikor az informatikai, infokommunikációs rendszer valamilyen módon rögzíti egy bűncselekmény valamely részletét (pl. fénykép, hang formájában).

Az általános felosztás mellett többen (Cornwall, Sieber, Bequai, Waisk stb.) is tipizálták az informatikai bűncselekményeket. Young szerint az informatikai rendszerekkel kapcsolatos jogsértéseket például a következőképpen lehet tipizálni:

- hagyományos lopásszerű jogsértések (ide tartoznak a csalással és sikkasztással rokon tényállások is);
- szellemi tulajdonnal kapcsolatos jogsértések (üzleti, üzemit titkok, vagy szerzői jog megsértése);
- szolgáltatás megzavarása és számítástechnikai eszközök megrongálása (ide tartoznak a DoS és DDoS támadások, de az informatikai rendszer fizikai komponenseinek rongálása is);
- szolgáltatáslopás (informatikai rendszer által nyújtott bármilyen szolgáltatás vagy technikai kapacitás jogosulatlan igénybevétele);
- számítógépes pornográfia és fiatalkorúak kihasználása (pornográf vagy pedofil adatok tárolása, továbbítása, vagy fiatalkorúak elcsábítása pl. az internetes csevegő szoftverek (pl. MS Messenger, Skype) segítségével);
- magánszféra számítógép általi megsértése (természetes személy személyes adataival való visszaélés vagy azok nyilvánosságra hozatala);
- számítógépes kikémlelés (állam ás szolgálati titkok megszerzése az informatikai rendszerben tárolt adatokhoz való illetéktelen hozzáférés által);
- egyéb hagyományos bűncselekmények (ide tartoznak azok a hagyományos bűncselekmények, amelyek megtervezéséhez, kivitelezéséhez informatikai rendszert használnak fel az elkövetők). [6]

Az informatikai bűncselemény nyomainak ismérvei

Digitális nyom keletkezése

Digitális nyomok keletkezhetnek

- emberi (felhasználói) műveletek eredményeként, vagyis a támadó vagy a sértett által használt funkciók hatására (pl. parancsok, alkalmazások),
- automatikusan
  - az informatikai rendszer szubjektumai működésének „mellékhatásaként” (pl. ideiglenes fájlok, szerviz folyamatok működésének eredményei),
  - szubjektumok együttműködésének eredményeként.

A digitális és a fizikai nyom azonban elválaszthatatlan kettőst alkotnak. Az informatikai rendszerek vizsgálatakor közvetlenül nem vagy csak speciális esetekben (pl. biometriai azonosítók alkalmazása esetén) lehet az egyes nyomokat természetes személyekkel összekötni. A digitális nyomok és a természetes személyek összekapcsolásakor ezért minden esetben szükséges az informatikai rendszer fizikai környezetének vizsgálata anyagi nyomok és anyagmaradványok után, hogy a digitális és a fizikai nyomképződés folyamatának zártsága erősítse a nyomozás eredményeit és megfelelő érvrendszert szolgáltasson a bizonyításhoz és a felelősségre vonáshoz.

Digitális nyomok csoportosítása

A digitális nyomokat csoportosítani lehet az adat (digitális nyom)

- élettartam,
- tárolási, megjelenítési helye,
- elkövetés helyéhez való viszonya,
- kódoltsága, rejtettsége

szerint.

A digitális nyomok ***élettartam*** szerint lehetnek rövid, közepes, vagy hosszú élettartamúak. Az élettartam szerinti sorrendre ad példát az RFC3227:

- regiszter és processzorgyorsító tár,
- útvonal irányító tábla, ARP gyorsító tár, kernel statisztika, memória,
- ideiglenes fájlrendszerek
- lemezek
- távoli bejelentkezés és monitor adatok
- fizikai konfiguráció, hálózati topológia
- archív média

[12]

A digitális nyomok ***tárolás, megjelenítés helye*** szerint lehetnek:

- a számítógép operatív tárjában (memóriában) található „futó” programok és azok adatai
- a számítógép adattároló eszközein rögzítve, ezek lehetnek:
  - a rendszer által rögzített technikai adatok, amelyek az informatikai rendszer automatikus működése során jönnek létre, pl.:
    - temporális fájlok,
    - swap fájl/partíció,
    - informatikai rendszer saját technikai adatai (munkafájlok),
    - meta- (pl. kép, hang) és egyéb leíró (pl. registry, ini stb.) adatok,
    - napló állományok (amennyiben azok alapértelmezett rendszerbeállítások mellett készülnek).

  - a felhasználó által tudatosan/akaratlagosan rögzített adatok, amelyek a felhasználó műveletei során, a felhasználó tudtával és akaratával jöttek létre, pl.:
    - adatbázisok,
    - (adat) fájlok (pl. Word, Excel állományok),
    - naplók (amennyiben a felhasználónak kell aktiválnia a naplózási funkciót);

  - adatmaradványok, amelyek valamilyen felhasználói vagy rendszer művelet eredményeként a rendszerben megmaradnak még a művelet sikeres lefutását követően is, ilyenek lehetnek
    - törölt adatok, amelyek lehetnek
      - az operációs rendszer által menedzseltek (pl. MS Windows „kuka”),
      - valós törlés után az adathordozókon maradó adatok,
    - „hulladék” adatok
      - alkalmazások (pl. MS Word) feleslegesen/ellenőrizetlenül rögzített adatai,
      - adatállományok ideiglenes tárhelyein maradó adatok;

  - adathibák, vagy adat rendellenességek (pl. a támadó által szándékosan vagy véletlenül módosított adatok)

  - adathiányok (pl. a támadó által szándékosan vagy véletlenül törölt adatok)

- egyéb helyeken, például ha a vizsgálathoz szükséges adatokhoz
  - képernyőről,
  - hangszóróból,
  - kinyomtatott dokumentumból,
  - digitális vízjelből,
  - hálózati adatcsomagokból,
  - stb.

  lehet hozzáférni.

A digitális nyomokat ***elkövetés helyéhez való viszony szerint*** is lehet csoportosítani, vagyis digitális nyomok találhatók:

- a cél számítógépen (amelyik ellen a támadás irányult),
- a forrás számítógépen (ahonnan a támadás indult),
- kapcsolati számítógép (amelyik valamilyen közvetítő szerepet játszik a cél és a forrás számítógép között)
  - hálózati eszköz (router, switch, tűzfal stb.),
  - fel- (pl. szerver vagy kliens számítógép) vagy kihasznált számítógép (pl. botnet hálózathoz tartozó „zombi”);
- (cserélhető) adathordozón,

A digitális nyomok ***kódoltság, rejtettség szerint*** lehetnek

- nyílt adatok – az adatok az adattárolás helyének megfelelő módon vannak csak kódolva, az elemzést végző az általános informatikai kódolások ismeretében tudja dekódolni azokat;
- titkosított – az adatok valamilyen (szimmetrikus, vagy aszimmetrikus) rejtjelzéssel kódoltak, az elemzést végzőnek nem áll a (titkos) kulcs a rendelkezésére, csak megfejtéssel tudja értelmezni az adatokat;
- (szteganográfiai módszerekkel) rejtett – az adatok valamilyen eljárással valamilyen eljárással el vannak rejtve (pl. a kiterjesztés/név módosításával, vagy az üzeneteket kép vagy hangfájl részeként való kódolásával);
- kombinált – titkosított és rejtett adatok.

Digitális nyomok biztosítása, felkutatása, rögzítése

A nyomozás során gyűlnek össze azok a bizonyítékok, amelyek objektíven támasztják alá a terhelt bűnösségét vagy ártatlanságát. Ennek a folyamatnak lényeges lépése a szemle, ami egyrészt nyomozási cselekmény, másrészt bizonyítási eszköz, hiszen e cselekmény során a helyszínelők a büntetőeljárás (1998. évi XIX. törvény a büntetőeljárásról, vagy röviden Be.) eljárási garanciái mellett észlelik és rögzítik a helyszínen talált állapotot, körülményeket, kutatják fel a feltételezett bűncselekményekkel kapcsolatos nyomokat és azok összefüggéseit.

A szemle célja kettős:

- egyrészt olyan azonnal felhasználható információk nyújtása a nyomozás számára,
- másrészt bizonyítékok gyűjtése úgy, hogy a bizonyítékszerzés jogszerű legyen, megfeleljen a szakmai standardoknak (megismételhetőség, tudományos-technikai megalapozottság, megismételhetőség), a tartalma pedig büntetőjogilag releváns (a perben felhasználható) legyen. [7]

A hatályos Be. szerint a bizonyítási eljárások a következők

- szemle,
- helyszíni kihallgatás,

- bizonyítási kísérlet,
- felismerésre bemutatás,
- szembesítés,
- szakértők párhuzamos meghallgatása.

A továbbiakban a szemle lépéseivel foglalkozom, és megpróbálom összegezni azokat a lényeges pontokat, amelyek biztosítják a jogszerű, szakszerű bizonyítékszerzést, ezáltal a hatékony és eredményes nyomozást.

Helyszín felmérése

Kriminalisztikai szempontból „*helyszínen értjük azt a helyet a hol a feltételezett bűncselekményt elkövették avagy a bűncselekmény részét alkotó vagy azzal összefüggő egyéb részcselekmény, esemény stb. lezajlott*”.{[7] p 174}

Az informatikai bűncselekmények esetében a fenti definíció alapján rendkívül sok lehetséges fizikai és virtuális helyszín alkothatja az elkövetés teljes színterét, magába foglalva a támadó számítógépét és annak környezetét, az érintett internet szolgáltatók kommunikációs eszközeit és azok környezetét, a támadás során felhasznált számítógépeket és azok környezetét, valamint a megtámadott informatikai rendszert és annak környezetét.

A szemlére
- halaszthatatlan
- nyomozás elrendelését követően, nem halaszthatatlan

nyomozási cselekményként kerülhet sor.

A halaszthatatlan nyomozási cselekményként végrehajtott szemlék sajátossága a rövid felkészülés és a gyorsaság. Ennek ellenére a szemlét végrehajtónak ugyanolyan alapos munkát kell végeznie, mint nem halaszthatatlan esetben, mivel a felületesen, hiányosan végrehajtott szemle eredménytelen, nem nyújt elég információt a nyomozás folytatásához, nem biztosít elegendő releváns nyomot a bizonyításhoz.

A szemle eredményességének biztosítása érdekében a nyomozást végzőnek minden esetben fel kell készülnie, és gondoskodnia kell
- megfelelő számú és szakértelmű ember bevonásáról (pl. speciális hardver vagy szoftver ismeret biztosítása érdekében),
- a szükséges tárgyi, műszaki feltételek biztosításáról (nyomkereső, nyomrögzítő műszerek).

A személyi, tárgyi és műszaki feltételek biztosításának az alapja a hatékony felderítés. Előzetes információ hiányában előfordulhat, hogy bár egy jól képzett szakember megy ki a helyszínre, de az ott talált informatikai rendszerhez nincs meg a szükséges kompetenciája, és amíg a megfelelő szakember kiérkezik, addig lényeges adatok vesznek el.

A gyors, hatékony szemlének feltétele a nyombiztosítási, nyom felkutatási és nyomrögzítési módszerek, a dokumentálás (pl. nyomtatványok) szabványosítása.

A helyszín felmérésekor lényeges annak megállapítása, hogy a helyszín:
- valódi – egy megtörtént bűncselekmény tényleges helyszíne,
- koholt (beállított) – egy meg nem történt bűncselekmény „imitációja”,
- megváltoztatott – egy részlegesen beállított (pl. egy valós bűncselekmény végrehajtását részben másnak feltüntetett, az más elkövetőre vagy más elkövetési módszerre utalóvá alakított),
- többes (tagolt) – az elkövető, a felhasznált eszközök és a célpont földrajzilag is széttagoltan található meg (jellemző az informatika bűncselekményekre),

- mozgó – valamilyen közlekedési eszköz felhasználásával végrehajtott bűncselekmény esetén (pl. war driwing), vagy
- élő – működő informatikai rendszerrel kapcsolatos.

A szemlével rokon cselekmény a házkutatás, ami ház, lakás, egyéb helyiség vagy azokhoz tartozó bekerített hely, továbbá az ott elhelyezett jármű átkutatását, illetőleg számítástechnikai rendszer vagy ilyen rendszer útján rögzített adatokat tartalmazó adathordozó átvizsgálását jelenti az eljárás eredményessége érdekében.

Házkutatást alapos gyanú alapján a bíróság, az ügyész, illetőleg ha az ügyész másképp nem rendelkezik, a nyomozó hatóság rendelheti, zárt helyiséggel rendelkező személy akarata ellenére. Azonban ha a zárt helyiség felett rendelkező természetes vagy jogi személy (sértett, terhelt, érintett, pl. ISP) kéri vagy beleegyezik, úgy házkutatás helyett szemlét lehet tartani.

A szemle során lehetőség van arra, hogy dolgokat (pl. eszközöket), számítástechnikai rendszereket, az ilyen rendszerrel rögzített adatokat a hatóság lefoglaljon, ha azok bizonyítási eszközök vagy a törvény értelmében elkobzandók (pl. pedofil képek) vagy amelyre vagyonelkobzás rendelhető el. [7] [9]

Helyszínbiztosítás

A helyszín biztosítása során a cél a változtatások, változások megakadályozása. A helyszín biztosítása történhet passzív, vagy aktív módon. A passzív helyszínbiztosítás során a helyszínelők nem módosítják a helyszínt csak a helyszín körülhatárolásáról, esetleg élőerős védelméről gondoskodnak. Aktív helyszínbiztosítás során a helyszínelők a nyomok megőrzése érdekében olyan intézkedéseket hajtanak végre amelyek bár részben módosítják a helyszínt, de gondoskodnak a releváns nyomok megőrzéséről (pl. külső helyszínen az időjárástól letakarással védik a nyomokat, informatikai bűncselekmények esetén leválasztják a hálózatról a helyszínen lévő számítógépeket. [7] [9]

A helyszínelőnek a biztosítás során gyorsan kell felmérnie, hogy hol vannak a helyszín valódi határai, hol lehetnek olyan érintett számítástechnikai eszközök, amelyek vezetékes vagy vezeték nélküli kapcsolattal csatlakoznak a szűk értelemben vett helyszínen lévő számítógéppel. Informatikai igazságügyi szakértők anekdotáznak arról, hogy a feltételezett helyszínt az elkövető internetes kamerával figyelte és valamilyen távoli kapcsolaton keresztül menedzselte (pontosabban szisztematikusan megsemmisítette) az érintett informatikai rendszer adatait…

Helyszíni szemle lefolytatása

A helyszíni szemle alapvetően egy statikus (összképrögzítő) és egy dinamikus (nyomkereső) szakaszra osztható.

A statikus szakaszban a helyszínelő célja az összkép megfigyelése, az ott lévő valamennyi jelenség és körülmény megfigyelése és rögzítése anélkül, hogy a helyszínen lévő tárgyakat elmozdítaná vagy beavatkozna az ott lezajló jelenségekbe. Célja az elkövetés feltételezett központjának, eszközeinek az azonosítása, illetve információszerzés az elkövetés módjáról. Egy számítógépes munkahely, amely mellett szitázott, de nyers DVD-k sorjáznak támpontot nyújt egy szerzői jogsértés vizsgálatához.

A statikus szakaszban kell arról dönteni, hogy a „fizikai” vagy a „digitális” nyomok felkutatása, rögzítése legyen az elsődleges feladat. Amennyiben az előzetes puhatolás valószínűsíti az informatikai bűncselekmény elkövetését és a gyanú szerint az adatok lényeges elemét szolgáltatják majd a bizonyítási eljárásnak, úgy célszerű először az adatok konzerválására fókuszálni, de eben az esetben különös figyelmet kell fordítani arra, hogy az informatikai szakértő a lehető legkevesebb fizikai nyomot (pl. ujjlenyomat) tegyen tönkre.

A statikus szakasz dokumentálási eszköze lehet a fényképezőgép, videó, diktafon.

A dinamikus szakaszban történik a nyomok szisztematikus keresése, ami kiterjed a helyszínen lévő valamennyi objektumra, eszközre. A helyszínelők célja ebben a szakaszban

az, hogy valamennyi releváns nyom felderítésre és rögzítésre kerüljön, ami bizonyítékul szolgálhat, vagy támpontot nyújt a későbbi nyomozati cselekményekhez és információt szolgáltat az elkövetés idejéről, módjáról, esetleg az elkövető személyéről.

A szemle lefolytatása során az informatikai ügyekkel foglalkozó szakembereknek különösen nagy gonddal kell eljárniuk, hiszen a számítógépek kikapcsolásával esetleg releváns adatok (pl. kapcsolat információk, jelszavak, titkosítási kulcsok) veszhetnek el, a számítógépek izolációja a gép önrombolását, az adattartalom törlését, titkosítását idézheti elő.

A szemle lényeges de el nem hanyagolható feladata a nyomoknak a rögzítése – adatok esetén például digitális aláírással hitelesített, de legalább lenyomattal (hash) ellátott másolat készítésével.

A nyomrögzítés során készül el a bűnjeljegyzék, ami az informatikai eszközök és adathordozók egyedi azonosítását és leltározását jelenti. A bűnjeljegyzékbe az egyes számítógépeket fel lehet venni egységként (a számítógépet és valamennyi beépített alkatrészét), de eben az esetben gondoskodni kell a számítógép szétszerelésének detektálhatóságától (pl. plomba vagy lepecsételt ragasztószalag alkalmazásával).

Összefoglalás

Jelen tanulmány az informatikai védelem és a krimináltechnika kapcsolatát összegzi, illetve az informatikai bűncselekményeken keresztül egyértelműen összekapcsolja ezt a két tudományterületet. Az elemzés alapján megállapítható, hogy az informatikai bűncselekmények tekintetében a kriminalisztika az informatikai védelem része, egy olyan detektív kontroll, amely lehetővé teszi a jogsértések kivizsgálását, segíti az eredmények és hatékony felderítését és alapot szolgáltat a jogorvoslathoz.

Mivel a magyar szakirodalom jelenleg még adós az informatikai bűncselekmények kriminalisztikai nyom fogalmával, ezért a tanulmány javaslatot tesz a fizikai és digitális nyom elkülönítésére és a digitális nyom fogalmának kriminalisztikai és traszológiai definíciójára figyelemmel az informatika sajátos fogalmi elemeire.

A digitális nyom fogalma határozza meg az informatikai igazságügyi szakértők vizsgálatainak tárgyát. A fogalom következetes alkalmazásával különíthetők el a hagyományos kriminalisztikai területek az informatikai bűncselekmények informatikai rendszerben hagyott nyomainak vizsgálatától. A digitális nyom fogalma megmutatja azonban az informatikai rendszeren belüli vizsgálatok korlátaira is fényt vetíthet. Szerintem az egyik ilyen jelentős korlát az, hogy a kizárólag adatok vizsgálatával nem lehet az elkövető személyét minden kétséget kizáróan a bűncselekmény releváns tényezőihez kötni (pl. elkövető→forrás számítógép, elkövető→felhasználói fiók), ehhez a kriminalisztika fegyvertárának egyéb tényezőit is fel kell használni (pl. ujjlenyomat vétel a forrás számítógép billentyűzetéről, tanúvallomás a terhelttől vagy tanútól, a számítógép használati szokásokról).

Ez további megválaszolandó kérdéseket vet fel a bizonyítás elemeinek kapcsolódási pontjaival, illetve az informatikai igazságügyi szakértő által szolgáltatott bizonyítékok kriminál taktikai felhasználásának módjával kapcsolatban.

A dolgozat ismerteti továbbá a digitális nyomok csoportosításának lehetséges szempontjait. A fogalmi meghatározások és osztályozás mellett jelen dokumentum összegzi a digitális nyomok biztosításának, felkutatásának és rögzítésének főbb lépéseit, az ott figyelembeveendő szakmai ökölszabályokat.

Az ismertetett megközelítés megnyit olyan további kutatási területeket, amelyek hosszú távon lehetővé teszik digitális helyszínelés és a digitális nyomok elemzésének szabványosítását, ezáltal a nyomozó- és vádhatóság, a bíróság és az informatikai igazságügyi közösség közös nyelvének kialakítását, hogy az ügyek szempontjából releváns kérdésekre szülessenek szakmailag megalapozott, jó minőségű és érthető válaszok.

Irodalomjegyzék

[1] Munk Sándor: Információbiztonság vs. informatikai biztonság, robothadviselés 7. Tudományos szakmai konferencia, 2007. november 27. http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles7/munk_rw7.html

[2] Vasvári György: Bankbiztonság Műegyetemi kiadó, Budapest, 1995. p6

[3] Touche Ross & Co: Computer Control and Audit, Institute of Internal Auditors, Altaminte Springs, Florida, USA, 1978. p48

[4] Eoghan Casey: Digital Evidence and Computer Crime (second edition), Elsevier Academic Press, 2004.

[5] Balogh Zsolt György: Jogi informatika, Dialóg Campus Kiadó, Budapest-Pécs, 1998.

[6] Micki Krause, Harold F. Tipton: Handbook of Information Security Management, http://www.ccert.edu.cn/education/cissp/hism/ewtoc.html, 1-1-1 fejezet [http://www.ccert.edu.cn/education/cissp/hism/003-006.html]

[7] Tremmel Flórián – Fenyvesi Csaba: Kriminalisztika tankönyv és atlasz, Dialóg Campus Kiadó, Budapest-Pécs, 2002.

[8] Szerkesztette: Dr. Bócz Endre: Kriminalisztika, BM Kiadó, Budapest, 2004.

[9] 1998. évi XIX. törvény a büntetőeljárásról

[10] Dr. Munk Sándor: Katonai informatika a XXI. század elején, Zrínyi Kiadó, 2007.

[11] MSZ ISO/IEC 15408-2:2003

[12] RFC3227 - Guidelines for Evidence Collection and Archiving; h.n.; 2002., www.ietf.org/rfc/rfc3227.txt