Fehér Krisztián

Kezdő hackerek kézikönyve

avagy informatikai támadások és kivédésük

Fehér Krisztián

Kezdő hackerek kézikönyve

avagy informatikai támadások és kivédésük

BBS-INFO Kiadó, 2016.

A könyv nagyobb mennyiségben megrendelhető a kiadónál:
BBS-INFO Kiadó, 1630 Bp. Pf. 21. Tel.: 407-17-07

ISBN 978-615-5477-44-7

Kiadja a BBS-INFO Kft.
1630 Budapest, Pf. 21.
Felelős kiadó: a BBS-INFO Kft. ügyvezetője
Nyomdai munkák: Biró Family Nyomda
Felelős vezető: Biró Krisztián

TARTALOMJEGYZÉK

ELŐSZÓ

A mindennapjainkat átszövő informatikai megoldásokat sokszor tudatosan használjuk, ám legtöbbször talán nem is gondolunk ebbe bele. Használatuk során információkhoz jutunk és információkat osztunk meg magunkról. Ezt úgy is szokták mondani, hogy **„digitális lábnyomokat"** hagyunk magunk után. Napjainkban az információ sok esetben olyan értéket képvisel, amit közvetlen, vagy közvetett módon pénzzé lehet tenni, vagy más módon hasznot lehet belőle húzni. Ez pedig sajnos történhet rossz szándékkal is.

A korábban csak a televíziók képernyőjén látott „kiberbűnözők" manapság teljesen megszokott szereplőivé váltak a hétköznapoknak, naponta olvasunk, hallunk híreket arról, hogy támadás ért egyik vagy másik weboldalt, számítógépes rendszert. A kiberbűnözők és a védekező oldal állandó versenyfutásban vannak, melyben a támadó oldal van előnyben, mert gyorsabban ki lehet használni egy biztonsági rést, mint kidolgozni és elkészíteni az ellenszerét, különösen úgy, hogy nem is tudunk róla.

A számítógépes bűnözők olyan emberek, akik jogtalanul szereznek és használnak fel információkat. Ők a **crackerek**, támadók, akik a **hackerektől** eltérően többnyire etikátlanul járnak el. A hacker szót tehát valójában tévesen használják gyűjtőfogalomként a „bűnözők"-re. Erre később még visszatérünk.

E könyvben különböző támadási módszereket szeretnénk megismertetni a nagyközönséggel, bemutatva olyan technikákat is, melyeket magas szinten a valóságban is használnak a rossz fiúk. Az ellenük történő védekezésnek ugyanis a megismerés a legbiztosabb alapja. Ez a könyv nem a (potenciális) bűnözőknek szól és nem hivatott senkit sem felkészíteni arra,

hogy törvénybe ütköző cselekedeteket hajtson végre. Éppen ellenkezőleg! Óva intünk ettől mindenkit.

A legáltalánosabb hackelési technikák bemutatása mellett a hétköznapi emberek számára kívánunk tanácsokkal szolgálni. Olyan tanácsokkal, melyek segítségével hatékony válaszokat tud adni a napjainkra egyre inkább terjedőben levő informatikai bűnözés kihívásaira. A védekezés felé megtett első lépés a megértés. Mivel állunk szemben? Mit jelentenek a különböző szakkifejezések? Hogyan férhetnek hozzá adatainkhoz? A megértés teszi lehetővé a védekezési módok meglátását és keresését.

Célkeresztben az információ

Az informatika világában az értéket az információ képviseli. Az információ körül forog minden. Minél több van belőle, annál értékesebb lesz. Ha bizalmas információkról van szó, az tovább növeli az információ értékét. (Nagyon tágan értelmezve, kvázi a bankszámlán lévő pénz is csupán információ.)

Napjainkban két, egymással ellentétes folyamat figyelhető meg a hétköznapokban: az emberek egyre több információt tesznek közzé magukról, miközben egyre nagyobb erőfeszítések szükségesek az információk védelme érdekében. Ebből egyenesen következik, hogy az információkhoz történő jogosulatlan hozzáférések száma is egyre nagyobb lesz.

Gondolatok a személyes adatokról

Könyvünk megírásának kezdetén egy dilemmával találtuk magunkat szembe: hogyan adhatunk tanácsot az embereknek bizalmas adataik védelmével kapcsolatban, hogy közben ne adjunk akaratlanul is ötleteket arra vonatkozóan, hogy hogyan lehet ilyen információkat megszerezni? Stratégiánk az, hogy a különböző módszerek inkább általános, példaszerű leírását és az ellenük történő védekezés lehetőségeit adjuk közre. Az olvasó így ismereteket szerezhet a témában és tudását is gazdagíthatja, anélkül, hogy nagyon el kellene távolodnia a „gyakorlattól”. Az ismeretátadás ezen biztonságos megközelítése alatt értjük annak az ismertetését is, ahogyan egy valódi hacker gondolkodik és dolgozik.

A reklámoknak és a fogyasztás világának köszönhetően az emberek számítástechnikai eszközökkel végzett szinte minden tevékenysége hagy valamilyen nyomot. Ez az ún. digitális lábnyom. Ez lehet egy telefonhívás adatainak rögzítése, egy e-mail elküldése, egy naplófájl, egy elmentett dokumentum, szinte bármi.

A különféle telekommunikációs szolgáltatók, nagy szoftvercégek, hírszerző szervezetek és persze a „szabadúszó" bűnözők is rengeteg információt állítanak össze mindenkiről, aki informatikai eszközöket használ.

Ennek tudatában kell lennünk, mert már a személyes információk keletkezése is szinte észrevétlenül átszövi életünket. Alapvető fontosságú a személyes információk kezelésével kapcsolatos tudatosság kialakítása. Tudnunk kell, hogy személyes adataink csak hozzánk köthetőek, ránk vonatkoznak és senkinek sincsen joga akaratunkon kívül tárolni, vagy felhasználni azokat. Ennek megértése elsősorban a fiatalabb generációk számára fontos, mivel ők már „beleszületnek" egy olyan világba, ahol rengeteg információ keletkezik és kering körbe-körbe a Földön.

A világ mammutcégei számára hatalmas értéket képviselnek a potenciális vásárlóik szokásai. Talán bele sem gondolunk egy webáruház böngészése közben, hogy nagy valószínűséggel minden mozdulatunkat kiértékelik és rögzítik. Hová kattintunk, mennyi időt töltünk egy-egy oldalon, milyen kifejezésekre keresünk rá és még hosszasan sorolhatnánk. Noha ezen statisztikák mérése és kiértékelése elvileg anonimizált módon zajlik, erre kevés a garancia, és ha így is van, az az igazság, hogy az anonimmá tett adatok jelentős része mégiscsak felhasználható konkrét emberek azonosítására, mint azt több kutatás utólag bebizonyította. Ezért aztán könyvünk az információ védelméről is szól és bemutatja az információk jogosulatlan megszerzésére törekvő ellenoldal egyes módszereit is.

Félreértés ne essék: nem paranoiás szemlélet kialakítása a célunk! Ez már a ló túloldalára történő átesés lenne. Ellenben igenis célunk egy egészséges, felvilágosult szemlélet kialakítása

arról, mi történik, és mi történhet adatainkkal ilyen vagy olyan esetekben és hogyan befolyásolhatjuk ezt.

A könyvünkben leírt ismeretanyag továbbá azt a biztonsági tudatosságot is terjeszteni kívánja, ami számos munkahelyen sajnos még manapság is hiányzik.

A könyv felépítése

Könyvünk felépítése messzemenően gyakorlatorientált. A fejezeteket igyekeztünk hétköznapi élethelyzetek köré felépíteni és sok példával illusztrálni. Több esetben szoftvereket is bemutatunk, melyeket a jó és a rossz oldalon álló szakemberek egyaránt felhasználnak védekezésre, ill. támadásra is.

A fejezetek tárgyalásakor a fokozatosság elvét alkalmazzuk. Az első két fejezetben alapfogalmakat tisztázunk és igyekszünk megvetni az alapjait a biztonságtudatos gondolkodásnak.

Miután megismertük azt, hogy miről fog szólni a könyv, a 3-6. fejezetekben biztonsági kockázatokról ejtünk szót, egyszerű, laikusok által is könnyen megérthető formában. Itt már néhány egyszerű gyakorlati példát is mutatunk.

A könyv második fele (7-11. fejezetek) különféle támadási és védekezési módszereket mutat be, melyek már némi számítástechnikai jártasságot igényelnek, de könnyen kipróbálhatóak, mivel lépésről lépésre leírunk mindent. Itt tehát már zömében gyakorlati példákkal találkozhatunk és a példák komplexebbek is lehetnek. Egyre több alkalmazást és módszert, valamint ezek kombinációját mutatjuk be, mely már valóban megközelíti a valódi támadók módszereit.

A könyv végén lévő függelék számos hivatkozást tartalmaz, melyek segítségével tovább bővíthetjük ismereteinket, illetve utat találhatunk egy-egy speciálisabb téma felé is. Szintén a függelékben kaptak helyet olyan információk is, melyek a könyv fejezeteinek sorába nem kerültek bele, de hasznosak, érdekesek lehetnek a könyv témaköreivel történő ismerkedés során.

Nem minden módszert, technikát mutatunk be, ez jóval meg is haladná egy könyv kereteit. Mégis igyekeztünk olyan téma-

kat válogatni, melyekkel hétköznapokban gyakran találkozhatunk, illetve minél több területet lefednek.

A valódi hackerek folyamatosan naprakészen tartják tudásukat és fejlesztik magukat. Erre bíztatjuk olvasóinkat is, és ehhez könyvünk is kiváló ugródeszka lehet. Egy könyv elolvasása után azonban még senkiből nem lesz profi hacker. Ehhez rengeteg gyakorlat, komoly tudás és kitartás szükséges.

A könyvben bemutatott módszerek kipróbálásáról

A könyv példáinak kidolgozásához elszigetelt tesztkörnyezetet, illetve saját hálózatot használtunk. Ezt javasoljuk olvasóinknak is. Óvva intünk mindenkit attól, hogy olyan tevékenységekbe kezdjen, ami külső szolgáltatások megzavarására, vagy egyéb károkozásra alkalmas. Ezekért nem vállalunk felelősséget!

Általánosságban elmondható, hogy saját hálózatunk vagy jelszavaink feltörése tökéletesen elégséges egy-egy módszer működésének a megismeréséhez. Szóval első felbuzdulásunkban ne kezdjük el vadul feltörni a szomszéd vegyesbolt WIFI jelszavát, mert annak rossz vége lehet...

A szerzőről

A szerző veterán szoftvertesztelő, minőségbiztosítási tanácsadó, Magyarországon dolgozik. Gyerekkorában autodidakta módon tanult meg programozni, az évek során számos programozási nyelvvel megismerkedett. Megszerzett tudását előszeretettel használja alternatív, kísérleti alkalmazások készítésére, melyek egy része ingyenesen elérhető, sőt vannak köztük nyílt forráskódúak is. Néhány vonatkozó segédprogramjával ebben a könyvben is találkozni fogunk.

Sok időt fordít saját térinformatikai keretrendszerének fejlesztésére, a ZEUSZ-ra, mellyel a NASA-ig is eljutott.

Az Adobe Flash platform és az AIR keretrendszer, valamint az Android operációs rendszer lelkes híve.

Több könyve is megjelent már a hazai könyvesboltokban. Munkáiról bővebben a **http://feherkrisztian.magix.net/public** weboldalon is lehet olvasni.

1. HACKER TÖRTÉNELEM

1.1. A „hacker” szó eredetéről és értelmezéséről

A „hacker” és az ehhez kapcsolódó kifejezéseket többféleképpen lehet magyarázni.

Maga a hacker szó az angol "hack" igéből képezhető. Pontos fordítása nincsen, de lefektetett szabályrendszerek megkerülését értik alatta, közismertebben a „feltörni”, „behatolni” kifejezéseket.

A „hackerség” kialakulása teljesen független a rosszindulatú tevékenységektől. A számítástechnika hőskorában, évtizedekkel ezelőtt, a felhasználók, akik többnyire hivatásos számítástechnikai szakemberek voltak, gyakorta szembesültek olyan problémákkal munkájuk során, melyet csak az általuk használt rendszerek igen mély ismeretének kiaknázásával, vagy ezen rendszerek nem dokumentált, sokszor csak kerülőutakon elérhető lehetőségeivel tudtak csak megoldani. Nem volt választásuk, egyszerűen rá voltak kényszerítve, ha hatékonyan el akartak végezni bizonyos munkákat. Ezek a szakemberek voltak az első hackerek. (Ide sorolhatóak azok az úriemberek is, akik nem számítógépekkel, hanem telefonhálózatok manipulálásával töltötték szabadidejüket, mely tevékenységek azonban még egyszerűbb formáikban is jócskán átlépték a legalitás határát.)

Az idők során a hackerek öntudatos szubkultúrát alakítottak ki, mely baráti társaságokban, vagy klubszerűen szerveződő közösségekben élt, később pedig hivatalos konferenciákat, összejöveteleket is szerveztek. A mikroszámítógépek aranykorában a hackerek különböző összejöveteleken be is mutatták azon képességüket, hogy maximálisan ki tudták használni a

korabeli számítógépek lehetőségeit ("demo scene" összejövetelek). Ilyen közösségek mind a mai napig léteznek és korántsem idejétmúlt dologról van szó, sőt! A hackerek tudása igen jövedelmező tud lenni és egyre értékesebb is lesz.

Az elterjedt vélemények szerint hackernek senki sem mondhatja magát, ezt a „státuszt" a hacker közösségnek kell elismernie. Egyes megközelítés szerint léteznek ún. **fehér**-, **szürke**- és **fekete** kalapos hackerek, akiket szándékuk szerint lehet megkülönböztetni, és amely elnevezésekre később még ki fogunk térni. Napjaink egyik trendje például pont az ún. **etikus hackerek** foglalkoztatása. Ebben az esetben hackerek legálisan végzett és fizetett tevékenységet végeznek egy munkáltatónál. Fő feladatuk biztonsági kockázatok feltárása. Sőt mi több, még etikus hacker tanfolyamok, workshopok is léteznek.

A köztudatban a hacker szót kizárólag negatív értelemben használják a számítógépes bűnözés elkövetőire. Ez a sajtó felelőtlen nagyotmondóinak köszönhető és kevés köze van a valósághoz. Az ún. **cracker**-ek és a **hackerek** viselkedése között lényegi különbség van, amit egy példával is megvilágítunk:

Vegyünk egy autótolvajt és egy autóriasztókkal foglalkozó szakembert! Mindketten képesek feltörni autókat. Az előbbi meg is teszi, az utóbbi azonban tudását arra használja fel, hogy minél nagyobb biztonságban tudhassák az emberek az autóikat a tolvajoktól. A példában az autótolvaj a cracker, az utós biztonsági szakember pedig a hacker kifejezés megtestesítője. A hacker a tudását károkozás nélkül, sőt annak megelőzésére használja, a cracker saját önös, és/vagy anyagi érdekeinek rendeli alá azt. (Érdekes egyébként, hogy a cracker tevékenységekhez köthető szoftverkalózkodást ugyanaz a sajtó mindig nem hajlandó egyértelműen kriminalizálni.)

A hacker kultúra alapjai évtizedekkel ezelőtt a UNIX számítógépes rendszerek körül alakultak ki. Akkoriban a számítástechnikai szakemberek gyakran önképzéssel sajátítottak el olyan ismereteket, melyek messze az átlagos felhasználó szintje fölé emelték őket szaktudás tekintetében. Ez gyakorta programozással is párosult és ezek a szakemberek képesek voltak olyan megoldásokra, melyekkel a rendszerek rejtett, dokumen-

tálatlan képességeit is ki tudták használni. Ezt a tudást azonban nem visszaélésekre, hanem jobb rendszerek létrehozására használták fel. A nyílt forráskódú közösségi szemlélet kialakulása is abban az időben kezdett kialakulni. Akkoriban a felhasználó és a programozó gyakorta ugyanaz a személy volt, mivel programozói tudás nélkül nem lehetett használni ezeket a gépeket.

1.2. Miért léteznek hackerek?

A hacker jelenséget egy igény és lehetőség szülte. A rendszerek minden részletre történő használatának igénye és a szoftverek sebezhetőségének a lehetősége. A szakmai ismeretek megszerzése, kipróbálása azonban károkozás és bűncselekmények elkövetése nélkül is lehetséges.

A határ a legális és illegális tevékenységek között sokszor nem egyértelmű és az új dolgok kipróbálásának vágya, a hírnév utáni epekedés, vagy beteges vandál hajlamok gyakran ledönthetik a morális gátakat. Problémák valójában ebből keletkezhetnek és sokszor felelőtlen fiatalok csínytevéseiről van csupán szó. De nem minden esetben…

Elfogadható-e például, ha valaki betör egy egészségügyi rendszerbe, pusztán azért, hogy megbizonyosodjon afelől, hogy ez lehetséges? A kérdés még érdekesebb akkor, ha a betörés visszakövethető nyomok és károkozás nélkül elvégezhető.

Egy megközelítés szerint ezzel nincsen semmi probléma, ezen vélemények osztói a „szürke-, vagy árnyékzónába" tartoznak.

Egy másik megközelítés szerint az engedély nélkül végzett tevékenységek nem egyszerűen illegálisak, hanem veszélyesek is, mert potenciálisan kárt, zavart okozhatnak, illetve olyan módon is lehet adatokhoz hozzáférést szerezni, melyet az adatok tulajdonosai nem engedélyeztek. Könyvünkben mi ez utóbbi álláspontot és szemléletet képviseljük.

Az egyetlen elfogadható kivétel az engedély birtokában végzett, megelőző jellegű hacker tevékenység, ami az etikus hackerek világa.

1.3. Miért lehet hackelni?

Jogos kérdés, hogy egyáltalán miért játszhatóak ki az informatikai rendszerek?

Az ok a bonyolultság és a fejlesztések egyre őrültebb tempója, sokszor a profithajhászás jegyében.

Egy modern operációs rendszer forráskódja sok millió kódsort számlál. Ilyen szintű bonyolultság esetén olyan kölcsönhatások érvényesülnek a szoftverek és komponenseik között, hogy a hibák és így a biztonsági kockázatok előfordulása mármár törvényszerű.

Másrészt a programozókat túl gyors munkára kényszerítik, ami sokszor a minőség rovására megy.

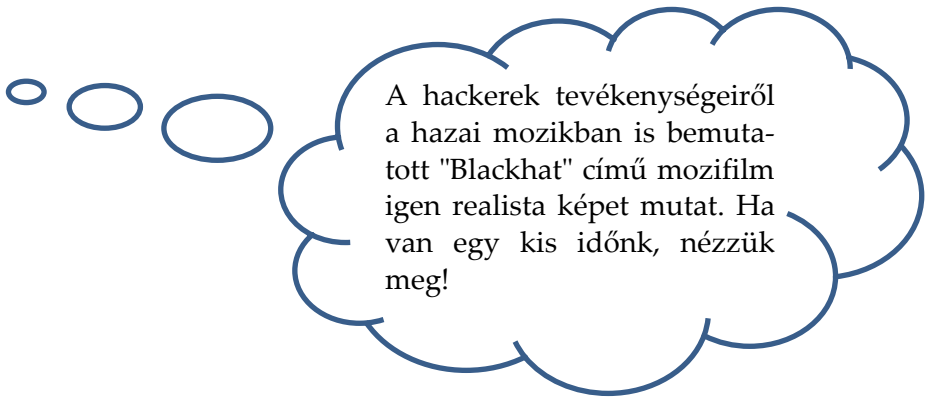
Persze a szakmai hozzánemértés és hanyagság is szerepel az okok listáján.

1.4. A hackerek titkai?

Vajon miért övezi titokzatosság a hackerek tudását? Ennek oka régebben feltehetően az volt, hogy viszonylag kevesen használtak számítógépeket. Ezért a komolyabb hacker tudás érthetetlennek tűnhetett a legtöbb laikusnak.

Napjainkban már szinte mindenki használ számítógépet, de ennél is sokkal fontosabb, hogy mindenki hozzáférhet az internethez és egy olyan tudásbázishoz, melyről korábban álmodni sem lehetett. Az interneten rengeteg fórum, weblap foglalkozik különféle feltörési technikák bemutatásával. Ezért elmondhatjuk, hogy a használható „hackertudás" titkossága ma már inkább mítosz, mint valóság. Ha valakit érdekel a téma és megvan benne a motiváltság mellett a technika iránti érdeklődés is, igen hamar használható „tudásra" és „gyakorlatra" tehet szert.

Ami miatt még manapság is léteznek elit hackerek és hackercsoportok, az az, hogy ezek az emberek kivétel nélkül komoly szakmai képzettséggel rendelkeznek, ami jóval túlmutat néhány internetes leírás áttanulmányozásán. Erre a szintre sok tanulással és munkával, évek alatt lehet csak eljutni.



A köztudatban a kiberbűnözők által használt hardver- és szoftvereszközök egyedileg megírt programokként, vagy szkriptekként jelennek meg. A valóság az, hogy ezek legtöbbje ingyenesen elérhető, sőt sok esetben nyílt forráskódú alkalmazás.

Figyelemre méltó, hogy egyes cégek kereskedelmi szoftvereket és/vagy hardvereket is árusítanak, melyekkel szintén professzionális módon lehet akár támadásokat, feltöréseket, „jelszóvisszaállításokat” kivitelezni.

Az egyik ilyen cég az Elcomsoft: https://www.elcomsoft.com/

1.5. A szoftverkalózkodásról

A szoftverkalózok programokat módosítanak a program készítőinek engedélye nélkül és ezeket a módosított változatokat legtöbbször meg is osztják másokkal. A módosítások általában biztonsági mechanizmusok kiiktatását tartalmazzák, hogy például érvényes liszensz nélkül is használni lehessen egy adott kereskedelmi forgalomban kapható szoftvert.

A szoftverkalózkodás nagyon régi jelenség, már a mikroszámítógépek (Commodore 64 és társai) fénykorában is virágzott.

A kalózok tevékenységüket előszeretettel indokolják azzal, hogy a szoftverek gyártói olyan dologért kérnek el sok pénzt, aminek valójában ingyenesnek kellene lennie. A feltört (módosított) programok terjesztése szerintük lovagias tett, egyfajta Robin Hood történetét idéző cselekedet.

A valóság ezzel szemben az, hogy a feltört szoftverek a módosítások miatt bizonyos fokú sérülést szenvedhetnek, amiből kifolyólag gyakorta lefagynak, nem megfelelően működnek stb. Ráadásul a feltört szoftverek letöltését sokszor valamilyen fizetős szolgáltatással kötik egybe. Így ezek a Robin Hood-ok saját maguk válnak olyanná, akik ellen állításuk szerint fellépnek. Ennél is nagyobb baj azonban maga a tény, hogy a szoftverkalózkodás mások verejtékes munkáját veszi semmibe, ami erkölcstelen.

Sok feltört szoftver „bónuszként" ráadásul kártékony kódot is tartalmaz, melyet előszeretettel használnak kémkedésre, adatlopásra.

A kalózkodás ezen a ponton kapcsolódik könyvünk témájához, de nem központi témája könyvünknek.

1.6. A „tuti" hacker módszerekről

Bizonyára elgondolkodtunk már azon, hogy hogyan lehet feltörni jelszavakat, weblapokat, egyáltalán: hogyan zajlik mindez. Mint könyvünk későbbi fejezeteiben is látni fogjuk, számtalan módszer létezik, melyek alkalmazása azonban hardveres és szoftveres feltételek függvénye.

Éppen ezért komolytalan lenne azt mondani, hogy bemutatható lenne a nagy betűs módszer, amivel minden jelszó feltörhető és minden biztonsági rendszer kijátszható. Ez egyszerűen butaság.

A valódi behatolások sikere éppen abban rejlik, hogy a támadásokat egy adott rendszerre, gépre szabják, tervezik. Ez még annak ellenére is igaz, hogy manapság már igen kényelmes szoftveres eszközök állnak a támadók rendelkezésére.

A felkészülést, tanulást nem lehet megspórolni. Viszont minél többet foglalkozik az ember vele, annál magasabb szintre lehet eljutni.

1.7. A hackercsoportok jövője

A hackercsoportok korábban erősen rendszerkritikus hozzáállást tanúsítottak és tevékenységeiket is ehhez igazították.

Ez a trend valószínűleg mindig is kimutatható lesz, ám a profi hackercsoportok aktivitásában megfigyelhető egyfajta kanalizálódás, illetve fókuszálódás.

Ez kisebb részt üzleti okokra vezethető vissza. Számos nagyvállalat alkalmaz etikus (és kevésbé etikus) hackereket saját rendszereik védelmének erősítésére, illetve a konkurencia figyelésére.

Az információszerzési tevékenységek jelentős részben kezdenek áttevődni a virtuális térbe, így érthető az egyes országok kormányainak érdeklődése is a nemzetbiztonsági érdekű adatszerzési és kibervédelmi tevékenységek iránt. Ez hírszerzési és újabban kifejezetten katonai jelleget kezd felvenni, hiszen egy fejlett ország infrastruktúrája, közműrendszere, kommunikációs csatornái messzemenően támadhatóak informatikai eszközökkel. Ennek pedig konkrét gazdasági, ill. geopolitikai következményei lehetnek.

1.8. Elit hackercsoportok **és a politika**

Számos hackercsoport létezik, melyek kifejezetten politikai berendezkedésekkel szemben, vagy azok mellett foglalnak állást és akcióikat is ennek szellemében hajtják végre. (Az, hogy az egyes kormányok milyen szinten támogatnak egyes csoportokat, könyvünk szempontjából nem fontos.)

Ezek a csoportok igen magas szinten végzik tevékenységeiket. A német Chaos Computer Club például egy klasszikusnak nevezhető hackercsoport, mely néhány évvel ezelőtt egy akciójában Wolgang Schäuble miniszter ujjlenyomatát szerezte meg.

Az alábbiakban néhány további hackercsoportot nevezünk meg. Ezek mind létező, valódi csoportok.

Anonymous nemzetközi hackercsoport

CyberBerkut oroszbarát ukrán hackercsoport

Szíriai Elektronikus Hadsereg (SEA)
szír, kormánybarát csoport

RedHack csoport

2. INFORMATIKAI TÁMADÁSOK MADÁRTÁVLATBÓL

2.1. Gondolatok az adatvédelemről

Mielőtt fejest ugranánk az informatikai biztonság bugyraiba, közelítsük meg a témakört még általánosabban, lefektetve annak a tudatosságnak az alapjait, mely oly gyakran hiányzik napjainkban társadalmi szinten is.

Személyes adataink fontosak számunkra. Nevünk, címünk, bankszámlaszámunk, telefonos előfizetésünk mind-mind olyan adatok, melyek minket, tevékenységeinket írnak le. Ezek kényes adatok, mert visszaélésekre adhatnak lehetőséget, másrészt pedig nem tartozik senki másra.

Lehetséges-e személyes adatainkat képletesen lelakatolni? Ha teljesen őszinték akarunk lenni: a 21. században ez már aligha lehetséges. Mindennapi tevékenységeinkkel szinte nagyüzemben gyártjuk magunkról az adatokat. Ha reggel elindulunk gépjárművünkkel, mobiletelefonunkon keresztül rögzíthetik az általunk megtett útvonalat. Ha bankkártyánkkal vásárolunk, eltárolódik, hogy hol, mit vettünk, mennyit költöttünk. Még hosszasan sorolhatnánk.

Ezek az adatok azért is kényesek, mert időrendben elraktározva, közöttük olyan összefüggéseket lehet megállapítani, melyek nyitott könyvvé tehetik életünket. Nem azért nem szeretjük ezt, mert rejtegetni valónk lenne, hanem azért, mert a magánélethez mindenkinek joga van. Ez sajnos még sincsen így, a következőkben erre mutatunk be pár példát.