Pedagógusok versus hackerek, vírusok és hasonló férgek

Pšenáková Ildikó[1], Szabó Tibor[2]

[1]ildiko.psenakova@truni.sk, [2]szabo.tibor@ukf.sk
[1]Trnavská univerzita v Trnave, [2]Univerzita Konštantína filozofa v Nitre, SK

Absztrakt. A számítógépen tárolt adatok védelme és a számítógép-biztonsága napjaink egyik legnagyobb problémái közé tartoznak. Az Internet, a számítógép hálózatok és az infokommunikációs rendszerek, egyre nagyobb teret nyújtanak a számítógépes támadásoknak. A számítógép felhasználók többségét a számítástechnikában kevésbé járatos felhasználók közé sorolhatjuk, ezért nem ismerik a veszélyforrásokat és a lehetséges védekezési módokat sem. Ha támadás éri számítógéprendszerüket viselkedésük sokszor kiszámíthatatlan, és gyakran a probléma növekedését idézi elő. Ezért szinte elengedhetetlen, hogy elsajátítsák legalább a legszükségesebb tudást, hogy kellőképpen biztosítsák számítógépes rendszerüket.

Kulcsszavak: kártékony szoftver, hacker, vírus, számítógép biztonság, pedagógusképzés

1. Bevezetés

A számítógép és információs biztonság legtöbb kérdéseire és problémáira az informatikusok és számítógépekhez értő szakemberek tudnak válaszolni és állást foglalni, de vannak bizonyos készségek, amelyek szükségesek, sőt nélkülözhetetlenek még egy egyszerű, az információs és kommunikációs technológiák terén nem hivatásos felhasználónak is. [1] Minél előbb elsajátítják a laikus felhasználók a szükséges tudást és megfelelő készségeket, annál eredményesebben tudják majd biztosítani saját és mások számítógépének biztonságát.

Ma már az alapiskolai képzésben is szerepel az informatika oktatása és a diákok rendszeresen használják az infokommunikációs eszközöket a tanuláshoz is, így a pedagógus az, akinek át kell adni a diákoknak a szükséges tudást és megismertetni velük a megfelelő jártasságokat. Ehhez azonban elsősorban a tanároknak kell elsajátítani a számítógép biztonságos használatát. Ezért is indokolt és szükséges a számítógépes biztonság oktatása a pedagógusoknak, ill. a leendő pedagógusoknak is.[2]

2. A számítógépes vírusok születése

A vírusszerű programok az 1980-as években jelentek meg a számítógépeken. A mai modern számítógépes vírusok céljai azonban nem azonosak azokkal, amelyekre a vírusok készültek eleinte. Eredetileg a vírusok célja elsősorban az volt, hogy a programozó megvédje a programját a kalózkodás ellen[1]. 1988 előtt a legtöbb vírus csak zavaró volt és gyakorlatilag ártalmatlan.

Egyes források[2,3] szerint a számítógépes vírusok őse 1983. november 10-én „született meg". A Dél-kaliforniai Egyetem számítógép-tudományi doktorandusz hallgatója Fred Cohen, kb. nyolc óra

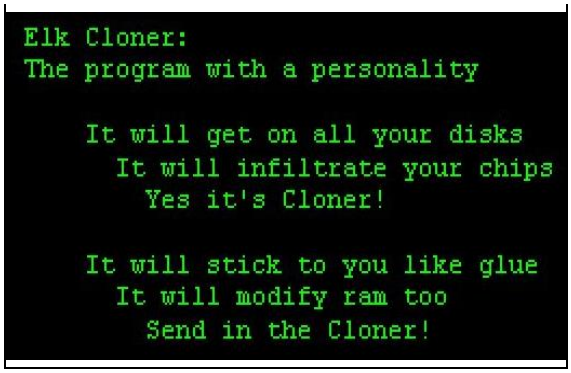
[1] https://us.norton.com/internetsecurity-malware-when-were-computer-viruses-first-written-and-what-were-their-original-purposes.html

[2] http://www.delmagyar.hu/szorakozas/30_eves_az_elso_szamitogepes_virus/2356981/

[3] https://mno.hu/tudomany/harminc-eve-jelent-meg-a-legyozhetetlen-virus-1194354

alatt írta meg és egy számítógép-biztonsági szemináriumon mutatta be tanárának Leonard Adlemannak a programot, amelyet egy grafikai alkalmazásba rejtett. A kódot a professzora nevezte el vírusnak, mert az úgy terjedt szét a számítógépeken, hogy kihasználta a felhasználók hozzáféréseit a hálózatba kötött gépek között, tehát olyan, mint az emberi vírus, fertőző és hajlamos a szaporodásra.

Mások szerint[4,5] a számítógépes vírus már korábban jelent meg és „szülőatyja" a 15 éves Richard Skrenta pittsburghi diák volt, aki 1982-ben fejlesztette az „Elk Cloner" nevű programot. Skrenta az Apple II operációs rendszeren futó számítógépekre írt játékprogramokat, s az egyik játékot megtoldotta az általa írt rövid kóddal. A program hajlékony mágneslemezeken villámgyorsan terjedt és a játék minden ötvenedik indításakor egy üzenet jelent meg a képernyőn (lásd. 1. ábra).



1. ábra: Az „Elk Cloner" üzenete.

Skrenta több számítógépes játékot és hasznos programot is írt, de hírnevét mégis az „Elk Cloner" kódjának köszönheti.

1986 januárjában fedezték fel az első MS-DOS operációs rendszerre írt vírust a „Brain"-t, melyet két pakisztáni programozó Basit Farooq Alvi és bátyja Amjad Farooq Alvi fejlesztettek ki, akik akkoriban csak 17 és 24 évesek voltak. A testvérek tudomására jutott, hogy a kalózok egy általuk létrehozott programot engedélyük nélkül terjesztenek, ezért kifejlesztették a „Brain" programot[6]. A kalóz szoftver felhasználója egy üzenetet kapott, amely azt állította, hogy számítógépe vírussal van fertőzve és azonnal lépjen kapcsolatba a testvérekkel a vírus eltávolítása miatt és megadta a testvérek címét és három telefonszámot:

```
Welcome to the Dungeon © 1986 Brain & Amjads (pvt). BRAIN
COMPUTER SERVICES 730 IZANAMI
   BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE:
430791,443248,280530. Beware of this VIRUS.... Contact us
for vaccination...
```

A testvérekkel szemben semmilyen jogi eljárás nem indult. Jelenleg Pakisztán legnagyobb internetszolgáltatójának a BrainNet-nek tulajdonosai.

A „Brain" vírus hatására 1987-ben az IBM programozói létrehozták az első víruskereső szoftvert.

[4] http://docplayer.hu/3544901-Bevezetes-az-elet-jatekaiba.html

[5] https://antivirus.comodo.com/blog/computer-safety/short-history-computer-viruses/

[6] https://m.thevintagenews.com/2016/09/08/priority-brain-first-computer-virus-created-two-brothers-pakistan-just-wanted-prevent-customers-making-illegal-software-copies/

3. Hackerek, vírusok és hasonló férgek

Skrenta programja nem okozott kárt a felhasználó számítógépén, inkább csak viccesnek számított. „Brain" is az illegális szoftvermásolás ellen védett. A mai vírusok alkotói már nem ilyen tapintatosak, ellenkezőleg kártékony, rosszindulatú programjaikkal - vírusaikkal csalni, ártani, kárt okozni akarnak más számítógépes felhasználóknak.

A rosszindulatú szoftvereken kívül, sajnos, más fajta számítógépes támadásokkal is találkozhatunk a gyakorlatban.

3.1. „Kalapos" hackerek

A „hacker" szóval már nagyon fiatalon találkoznak a gyerekek, sokszor nem is ismerve értelmét. Lehet sokan közülük a mesebeli boszorkányokkal és sárkányokkal helyezik őket egy „kosárba", mert tudják, hogy rosszak. De lehet a mai modern gyerkőcök inkább Darth Vader-ként képzelik el őket, vagy a birodalom támadóinak. De félre a viccet, kik is igazán a hackerek?

A „hacker" szó, klasszikus értelmében, olyan szakember megnevezésére szolgál, aki kivételes technikai ismeretekkel és programozási készséggel rendelkezik és ennek köszönhetően nem szokványos módon is képes megoldani a felmerülő problémákat. Ez a mai napig is igaz, de sajnos, a szót inkább a tudását *negatív* módon felhasználó, tipikusan számítógépes rendszereket feltörő szakemberek megnevezésére használják.

A hackerek tevékenységüket számos pozitív és negatív okból végzik, mint például a nyereség, a tiltakozás vagy a kihívás. De léteznek jóindulatú hackerek is. A másik végletet pedig a bűnügyi hackerek alkotják, akik bűncselekmények elkövetése érdekében hoznak létre rosszindulatú programokat. Az egyes hacker típusokat különböző színű kalapos néven is szokás nevezni.

Fehérkalapos hackerek[7] az „etikus hackerek" néven is ismertek. A tudásukat kizárólag pozitív és legális célokra használják fel. Ők a számítógépes biztonsági szakértők, akik tipikusan biztonsági cégek alkalmazásában dolgoznak, és kizárólag a tulajdonosok megbízásából kutatnak. Elsősorban a cég informatikai rendszerei vagy szoftverei sebezhetőségét vagy más gyenge pontjait keresik, azzal a céllal, hogy megelőzzék a rosszindulatú behatolásokat.

Szürkekalapos hackerek néha törvényesen járnak el, néha jó szándékkal, néha pedig nem. Általában nem pusztítanak, nem keresnek személyes hasznot, nincs ártó szándékuk. Miután megtalálták a rendszer vagy szoftver gyenge pontját, nem kezdenek vele semmit; vagy felajánlják például a „meghackelt" oldal tulajdonosának, hogy kijavítják a hibát, vagy figyelmeztetik, hogy javítsák meg a rendszerüket.

Feketekalapos hackerek[8],[9] tudásukat és megszerzett ismereteiket negatív, legtöbbször illegális célokra, anyagi vagy más előny szerzésére használják fel. Számítógépeket használhatnak arra, hogy megtámadják a rendszereket nyereségért, szórakozásért, politikai motivációkért vagy társadalmi okokból. A különböző számítógépes rendszereket azok tulajdonosainak engedélye nélkül, legtöbbször annak érdekeivel ellentétes módon manipulálják, „törik fel". Az ilyen behatolás gyakran magában foglalja az adatok módosítását és/vagy megsemmisítését, de a feltört rendszerből megszerzett bizalmas információkkal (pl. személyes adatok, hitelkártyaszámok, jelszavak, stb.) visszaéléseket is elkövethetnek.

Egyszerű példája a „hackerkedésnek" az az eset, amikor az ELTE Informatika karán a diákok a SignalR kliens oldali JavaScriptes részleteinek átírásával törtek be a rendszerbe. [3]

---

[7] https://home.mcafee.com/virusinfo/glossary#G

[8] https://pcforum.hu/szotar/feketekalapos+hacker

[9] https://home.mcafee.com/virusinfo/glossary#G

3.2. Malware

Mára már a vírus programok megjelenése szinte mindennapossá vált. Folyamatosan változik a formájuk, egyre nagyobb károkat tudnak okozni, sőt már saját magukat is tudják modifikálni, ezért a hagyományos vírus elnevezés már nem tartalmazza mindazt, ami az egyes kártékony programokra jellemző és nem felel meg minden tekintetben. Ezért ma inkább a *malware* elnevezés használatos.

„***Mal****icious soft****ware***" - „rosszindulatú szoftver" olyan programokat jelent, melyeknek célja kárt okozni a számítógépben, információkat, kényes adatokat gyűjteni.

Jellemzői [2]:

- általában ártó szándékkal készültek;
- a felhasználó tudta nélkül jutnak be a rendszerbe;
- rejtetten működnek;
- gyakran időzítve tönkretesznek más fájlokat;
- egyre fejlettebb intelligenciával rendelkeznek, például változtathatják saját kódjukat és aktivitásukat.

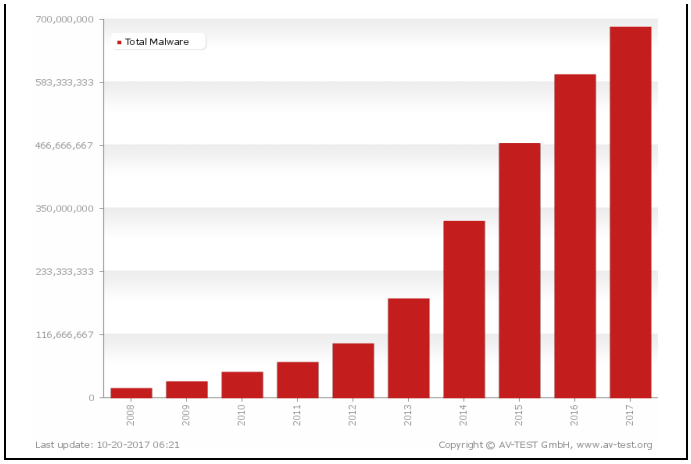
A rosszindulatú szoftverek közé sorolhatjuk:

Rosszindulatú szoftverek	
Computer viruses	Vírusok
Worms	Férgek
Trojan (Trojan horse)	Trójai faló
Spyware	Kémprogram
Adware	Reklámprogram
Browser hijacker	Böngésző eltérítő
Rootkits	Rootkitek
Keylogger	Billentyűzetfigyelő
Ransomware	Zsarolószoftver
Hoax	Láncievél
Spam	Kéretlen levél
Mail bomb	Mail bomba
Malvertising	Rosszindulatú hirdetés

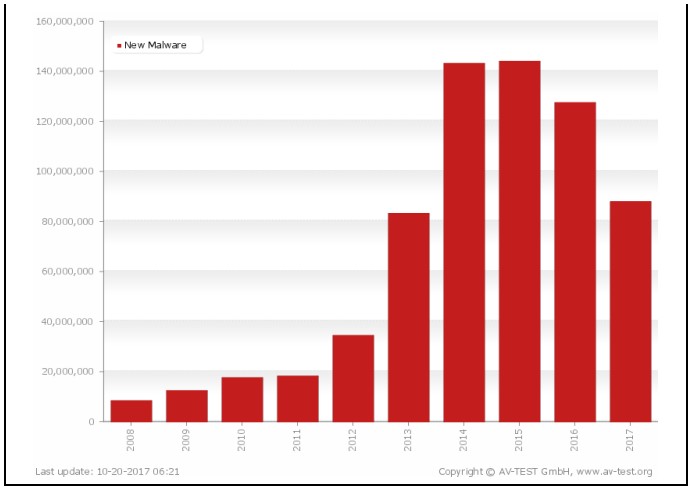
Sok kártékony szoftverfajta nevének nincs is magyar nyelvű megnevezése, mivel a mindennapi használatban az eredeti megnevezés nagyon gyorsan elterjed és megszokottá válik.

Az AV-Test[10] az egyik legismertebb Anti-Malware termékkel foglalkozó intézet, amelynél világszerte az egyik legnagyobb malware gyűjtemény található. Az intézet naponta regisztrálja az új rosszindulatú programokat. Statisztikákat készítenek és közzéteszik az új malware fájlok számát. A következő ábrákon látható, hogy a malware fájlok száma az utóbbi 10 évben egyre növekszik (2. ábra), de az új rosszindulatú programok száma az utóbbi két évben csökkent (3. ábra). De ennek ellenére a több mint 7 millió malware őrült nagy szám.

[10] https://www.av-test.org/en/statistics/



2. ábra: A malware példányok száma[11].



3. ábra: Az új malware példányok száma[12].

De a kártékony szoftverek ma már nem csak a számítógépeket támadják, hanem a mobil telefonkészülékek is veszélyben vannak. Mivel az Android operációs rendszer dominál a mobil piacon, elsősorban rá irányulnak a támadások. A G DATA biztonsági szakértői több mint 750 000 új Android malware alkalmazást fedeztek fel a 2017. év első negyedévében. Ez mindössze 8 400 új malware példányt jelent naponta. Az Android operációs rendszerrel működő okostelefonokkal és tabletokkal rendelkező felhasználók veszélyeztetettségi szintje így nagyon magas.[13]

3.3. Social Engineering

Social Engineering magyar megfelelője a „pszichológiai manipuláció" olyan kifejezés, ami a nem technológiai jellegű behatolásokra vonatkozik. Ez azt jelenti, hogy aki pszichológiai manipuláció útján akar

[11] https://www.av-test.org/en/statistics/malware/

[12] https://www.av-test.org/en/statistics/malware/

[13] https://www.gdatasoftware.com/blog/2017/04/29712-8-400-new-android-malware-samples-every-day

információt szerezni, általában az emberi természet tulajdonságait igyekszik kihasználni. Mivel a legtöbb ember segítőkész, igyekszik segíteni annak, aki segítséget kér, és így például bizalmas információkat mond el annak, aki kérdezi.

A pszichológiai manipuláció sokféle formát ölthet, történhet akár közvetlen személyi kapcsolattartással vagy kommunikációs eszközzel (telefon, posta...) online vagy offline formában. Lényege ugyanaz, más emberek becsapásával jogosulatlan személy bizalmas adatokhoz jut.

A Social Engineering technikái közé tartoznak például:

Social Engineering (pszichológiai befolyásolás)	
Phishing	Adathalászat
Spear phishing	Szigonyozás
SMiShing	SMS-alapú adathalászat
Vishing	Telefonos adathalászat
Pharming	Átirányítás hamisított weblapra
Spoofing	Becsapás
Typosquatting	Typosquatting
Whaling	Bálnavadászat
Dumpster driving	Kukabúvárkodás
Pretexting	Pretexting
Eavesdropping	Hallgatózás
Shoulder surfing	„Váll szörfözés“

Mivel a gyerekek könnyen manipulálhatóak, megtéveszthetőek, a veszélyeztetett kategóriába sorolhatjuk őket.

4. A védelem leggyengébb láncszeme a felhasználó!

A Social Engineering típusú támadások sikere főként a kiszemelt felhasználó döntésein múlik. De hasonlóan a rosszindulatú szoftverek terjedése is nagyban múlhat rajtuk. Ezért a védelem leggyengébb láncszeme a felhasználó, mivel naivitása („gyenge” jelszavak), sokszor gondatlansága (működő számítógép felügyelet nélkül) ismerethiánya (hiányzik a védelemhez szükséges tudás), csökkenti a rendszer biztonságát. Felmérések szerint az okozott károk többségét a felhasználók viselkedése rovására írható.[2]

Nagyon jó példa a felhasználók viselkedésének jellemzésére a WannaCry zsarolóvírus (Ransomware), mely 2017-ben nagyon rövid idő alatt világszintű fertőzést okozott. A vírus az MS17-010 kódú hibajelenséget használta ki. [4] Szinte teljesen a felhasználók hanyagságán múlott az egész folyamat, hiszen elegendő lett volna az MS Windows operációs rendszer folyamatos frissítését elvégezni. A 2017-es év „gazdag” volt a Ransomware támadások számát tekintve, a WannaCry zsaroló Trójain kívül a Petna sem tétlenkedett, így több nagyvállalatnak jelentős veszteségeket okoztak.

Gyakori eset a kalóz szoftverek használata folyamán történő fertőzés. Ugyan a telepített víruskereső szoftver gyakran jelezheti, hogy rosszindulatú kódot talált a kalóz szoftverben, de ezt a felhasználók több esetben ignorálják. Természetesen valójában a találat lehet hamisan kiértékelt, de mi történik, ha nem? A felhasználó fontos jelszavai, érzékeny adatai veszhetnek el, esetleg kerülhetnek a támadó birtokába, vagy egy zombi hálózat részévé válik a számítógépe, vagy más infokommunikációs eszköze.

A védekezés alapja, hogy a felhasználónak tudnia kell, mi ellen kell védekeznie, milyen veszélyekkel kell szembe néznie. A gyakorlatban nincs olyan egzakt módszer, amely minden esetben tökéletes védelmet nyújtana. Vannak azonban általános elvek, melyek betartásával minimálisra csökkenthető a támadás kockázata. [2]

Összegezve a felhasználóknak tisztában kellene lennie bizonyos szabályokkal, melyek betartásával sok felesleges gond és probléma megelőzhető. Megoldás lehet a megfelelő oktatás, mely felkészíti a felhasználót ilyen helyzetekben való helyes eljárásokra. Természetesen az oktatás sem garantálhatja teljes mértékben a veszély elhárítását, de mindenképpen nagy előrelépést jelenthet.

A gyakorlatban még nagyon sok más veszély és támadás is létezik, és folyamatosan újak és újabbak látnak napvilágot. Ezért is nagyon fontos, hogy ez a problémakör teret kapjon az oktatásban.

5. Oktatás

Szlovákiában az oktatás tartalmát minden iskolai szinten oktatási szabvány határozza meg. A szabványok az Állami pedagógiai intézet (Štátny pedagogický ústav) web oldalán mindenkinek elérhetőek *http://www.statpedu.sk/*. Az Intézet közvetlen a Szlovák Köztársaság Oktatási, tudományos, kutatási és sportminisztériuma (Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky) által irányított költségvetési szervezet.

Az oktatási szabvány nemcsak a teljesítményt és a tartalmat határozza meg, hanem a tanulók egyéni tanulási lehetőségeinek fejlesztését is lehetővé teszi.

A teljesítményszabvány az általánosan megfogalmazott kognitív fokozatú teljesítmény átfogó rendszere. A teljesítményt a tanár további tanulási célok, tanulási feladatok, kérdések vagy tesztelemek formájában pontosabban részletezheti, konkretizálhatja és fejlesztheti, természetesen figyelembe véve a tanuló aktuális kognitív képességeit.

A tanár az oktatási szabványban megadott tananyag tartalmát az iskolai tanterv keretén belül az egyes osztályok szerint módosíthatja.

Az oktatási szabvány úgy van kialakítva, hogy a tanár ne csak kész ismereteket nyújtson a tanulóknak, hanem megfelelő feltételeket teremtsen az aktív tanulásához. Olyan teret hozzon létre, amely lehetővé teszi a diákok számára, hogy konkrét tárgyakkal manipuláljanak, megfigyeljék a jelenségeket, mérjenek, kísérletezzenek, megbeszéljék egymás között a teendőket, nyitott gyakorlati és elméleti problémákat oldjanak. A felfedezés, kutatás és feltárás olyan alapvető módszerek, melyek a diákoknak nemcsak lehetőséget adnak az új ismeretek megszerzéséhez, hanem a tudományos munka alap készségeit is elsajátíthatják.

Az oktatási szabvány az iskolákat évfolyamok szerint három szintre osztja:

- általános iskola első szintje: 1. - 4. osztály
- általános iskola második szintje: 5. - 9. osztály
- 4 és 5 évfolyamos gimnázium.

Az egyes szinteken belül oktatási területek vannak definiálva, amelyek tartalmazzák az egyes tantárgyak tartalmát.

Az Informatika tantárgy a Matematika és munka az információkkal (Matematika a práca s informáciami) oktatási területbe van besorolva.

5.1. „Vírusok” az informatika tantárgy tartalmában

Az oktatási szabvány szerint az informatika oktatásának a feladata az, hogy irányítsa a tanulókat azoknak az alapfogalmaknak, eljárásoknak és technikáknak a megismerésére és megértésére, amelyek a számítógépes rendszerekben az adatokkal és információáramlással kapcsolatosak. Ezzel információs

kultúrát épít, mivel arra neveli a tanulókat, hogy hatékonyan használják az információs eszközöket, tiszteletben tartva az információs technológiák és termékek használatának jogi és etikai elveit.

Az informatika tantárgyban két elem található. Az egyik elem célja, hogy a tanulók konkrét tapasztalatokat és készségeket sajátítsanak el a számítógépekkel és alkalmazásokkal való munkához. A második komponens a számítástechnika és informatika alapjainak elsajátítására koncentrál, elsősorban a problémák számítógépen való megoldására. Ugyanakkor az informatika oktatása felkészíti a tanulókat arra is, hogy helyesen használják a megszerzett készségeket és ismereteket más tantárgyakon is.

Minket az érdekel tartalmaznak-e a szabványok olyan részeket, melyek a vírusokkal, vagy a számítógépes biztonsággal foglalkoznak. Ezzel azt próbáltuk illusztrálni, menyire van beépítve a tantárgyba ez a tematika.

Az első oktatási szinten nincs jelen az informatika oktatásában ez a témakör. A második szinten a 6. és 8. osztályban a következő témakörök és követelmények szerepelnek[14]:

Szoftver és hardver - munka a vírusok és kémkedés ellen[15]	
Teljesítményszint követelmény	**Tartalmi követelmény**
Az általános iskola 6. osztályának a végén a diák tudja/képes: ✓ hogy nem szabad ismeretlen, kétes alkalmazások letölteni és futtatni.	*Jellemzők és kapcsolatok*: vírus, mint rosszindulatú szoftver; kémkedés, mint a szoftver vagy weboldalak jogosulatlan tevékenysége

Információs társadalom - biztonság és kockázatok	
Teljesítményszint követelmény	**Tartalmi követelmény**
Az általános iskola 6. osztályának a végén a diák tudja/képes: ✓ beszélgetni az internetes a kockázatokról, ✓ alkalmazni az adatok és alkalmazások biztonságára (az e-mail-re is) irányuló szabályokat a jogosulatlan használat elleni védelemre, ✓ beszélgetni a számítógépes bűnözésről, ✓ megvitatni a weben található információk hitelességét.	*Jellemzők és kapcsolatok*: vírus, mint rosszindulatú szoftver; a megszerzett információk hitelessége; az internet és a szociális hálózatok kockázatai *Folyamatok:* a számítógépes vírusok és spamek terjedése; biztonságos és etikus viselkedés az interneten; a hackerek tevékenysége

A 8. osztályban bővül a tartalom és a követelmények is kicsit komolyodnak, de túl nagy előrehaladást nem látni a tananyag bővítésében.

Szoftver és hardver - munka a vírusok és kémkedés ellen	
Teljesítményszint követelmény	**Tartalmi követelmény**
Az általános iskola 8. osztályának a végén a diák tudja/képes: ✓ hogy nem szabad ismeretlen, kétes alkalmazásokat letölteni és futtatni.	*Jellemzők és kapcsolatok*: vírus, mint rosszindulatú szoftver; kémkedés, mint a szoftver vagy weboldalak jogosulatlan tevékenysége;

[14] http://www.statpedu.sk/files/articles/dokumenty/inovovany-statny-vzdelavaci-program/informatika_nsv_2014.pdf

[15] Megjegyzés: A táblázat ilyen formában szerepel a honlapon is, természetesen szlovák nyelven.

✓ a vírusok felderítésére és eltávolítására szolgáló mechanizmusokkal dolgozni.	vírusirtó, mint szoftver a rosszindulatú szoftver felismerésére és eltávolítására és a rosszindulatú tevékenységek blokkolására; a vírusirtó programok korlátozottsága (a vírusirtó is csak program, és nem mindig találja meg a legújabb rosszindulatú szoftvert) *Folyamatok:* a számítógépen futhat vírusirtó és ellenőrizhet (majdnem) mindent, amit csinálunk
Információs társadalom - biztonság és kockázatok	
Teljesítményszint követelmény	**Tartalmi követelmény**
Az általános iskola 8. osztályának a végén a diák tudja/képes: ✓ megvitatni az internetes a kockázatokat, ✓ értékelni, mely információkat szükséges védeni a visszaélésektől, ✓ alkalmazni azokat a szabályokat, melyek bebiztosítják az e-mail, a közösségi oldalak és magát a számítógépet a jogosulatlan használat ellen, ✓ felmérni a fertőzött számítógépen folytatott munka kockázatait, ✓ beszélgetni a számítógépes bűnözésről, ✓ megvitatni a weben található információk hitelességét, ✓ megvitatni a bűncselekményekkel és illegális tartalmakkal járó kockázatokat.	*Jellemzők és kapcsolatok*: vírus, mint rosszindulatú szoftver; spam, mint kéretlen levél; vírusirtó program, mint eszköz a vírusok elleni védekezésre; a jelszavak minősége, mint a biztonság mechanizmusa; a megszerzett információk hitelessége; az internet és a szociális hálózatok kockázatai *Folyamatok:* a számítógépes vírusok és spamek terjedése; biztonságos és etikus viselkedés az interneten; a hackerek tevékenysége

Az Informatika tantárgy oktatása a 4 és 5 évfolyamos gimnáziumokban, sajnos, csak egy iskolai évre csökkent. Ezt a legtöbb iskolán az első évfolyam tantervébe iktatják be. Érdemes megemlíteni, hogy a gimnáziumokban is lehet informatikából érettségizni. Azok a diákok, akik ezt választják, a következő évfolyamokban csak, mint választható tantárgy, ill. szakkörön belül foglalkozhatnak informatikával.

Informatika - 4 és 5 évfolyamos gimnázium	
Szoftver és hardver - munka a vírusok és kémkedés ellen	
Teljesítményszint követelmény	**Tartalmi követelmény**
A diák tudja/képes: ✓ kihasználni a rosszindulatú programok észlelésére és eltávolítására szolgáló eszközöket.	*Jellemzők és kapcsolatok*: vírus, mint rosszindulatú szoftver; kémkedés, mint a szoftver vagy weboldalak jogosulatlan tevékenysége; vírusirtó, mint szoftver a rosszindulatú szoftver felismerésére és eltávolítására és a rosszindulatú tevékenységek blokkolására; a vírusirtó programok korlátozottsága (a vírusirtó is csak program, és nem mindig találja meg a legújabb rosszindulatú szoftvert)
Információs társadalom - biztonság és kockázatok	
Teljesítményszint követelmény	**Tartalmi követelmény**

A diák tudja/képes:	*Folyamatok:*
✓ megvitatni a fertőzött számítógépen folytatott munka kockázatait, ✓ alkalmazni azokat a szabályokat, melyek bebiztosítják az e-mail, a közösségi oldalak és magát a számítógépet a jogosulatlan használat ellen, ✓ bebiztosítani saját adataikat és kommunikációjukat a visszaélésekkel szemben, ✓ értékelni a weben található információk hitelességét, ✓ felismerni a számítógépes bűnözést, ✓ megkülönböztetni a jogellenes tartalmakat.	a számítógépes vírusok és spamek terjedése; biztonságos és etikus viselkedés az interneten; a hackerek tevékenysége; személyes adatok az interneten nem publikálandók

5.2. „Vírusos" a leendő pedagógusok képzése?

A rosszindulatú szoftverek elleni védelem és a számítógép biztonságos használatának oktatására a leendő pedagógusok számára nincs az egyetemeinken a jelenleg akkreditált tantervekben kijelölve külön tantárgy. Az sincs megszabva, hogy melyik tantárgy tartalmába és mennyi óraszámban kellene, ill. lehetne beilleszteni az oktatásba. [2]

Sajnos, még a leendő informatika tanárok képzésében sincs erre a témakörre irányuló tantárgy. Ez nemcsak hogy nagyon furcsa, de szerintünk helytelen is, mivel ha az általános iskolai képzésben megjelenik a tematika, akkor a pedagógusoknak is el kell sajátítani a megfelelő tudást, hogy ne érje őket a probléma felkészítetlenül a gyakorlatban. Ezért a feltett kérdésre akár igennek is felelhetnénk.

A probléma kezelésére a leendő informatika tanárok képzésében azonban van lehetőség, mivel több tantárgy tartalmába be lehet illeszteni a számítógépes biztonság kérdéseit. Például a „Számítógép architektúrák", „Operációs rendszerek", „Számítógép hardvere" témakörei között szerepel a fizikai biztonság, memória védelem, operációs rendszer szintű biztonság, felhasználó hitelesítés, jogosultságkezelés és a hozzáférés védelem módszereinek részletes tárgyalása.

A programozás oktatására irányuló tantárgyak tartalmába is megfelelő módon beilleszthetőek a problémához tartozó elemek, pld. víruskódok elemzése.

A számítógépes biztonság és a rosszindulatú szoftverek elleni védelemmel kapcsolatos tudás nemcsak az informatika tanárok számára fontos, ezért szükséges lenne az összes pedagógus képzésébe beiktatni a tematikával foglalkozó tantárgyat, ill. a meglévő informatika alapjaival foglalkozó tantárgy tartalmát ezzel kibővíteni. Sajnos, a tantárgy jelenlegi terjedelmébe (egy vagy két óra hetente - egyetemtől függő) nagyon nehéz a tartalomba beiktatni.

6. Befejezés

Ahogy már említettük, az egyetemeinket jelenleg az aktuális pedagógusképzés tanterveiben nem jelenik meg a rosszindulatú szoftverek, hackerek és más kártevők elleni védelem kérdése. Tanulmányunkkal megpróbálunk rámutatni a problémakör fontosságára és illusztrálni hogyan próbáljuk orvosolni a hibát a képzésben, mivel fontosnak tartjuk a jövőbeli, vagy akár az aktív pedagógusok képzését ezen a téren.

Természetesen nem csak a pedagógusokra gondolunk kizárólag, ugyanis meggyőződésünk, hogy nagyon sok vállalatnál, intézménynél előnyös lenne legalább olyan szinten beiktatni, mint mondjuk a tűzvédelmi vagy munkavédelmi oktatást.

Meggyőződésünk, hogy a felhasználók megfelelő tudásszintje a problematikáról, ha nem is teljes mértékben szüntetne meg a különböző biztonsági incidensek és vírusfertőzések gyakoriságát, de mindenképpen csökkenthetne azok számát.

Irodalom

1. I. Pšenáková, T. Szabó: *Niektoré aspekty potreby kurzu počítačovej bezpečnosti pre neprofesionálov*. In: Science for Education - Education for Science - II.volume = Veda pre vzdelanie-vzdelanie pre vedu - II. zväzok: zborník z 3. ročníka medzinárodnej konferencie, Nitra 26. - 27. apríla 2013. 1. vyd. Nitra: UKF, (2014) ISBN 978-80-558-0555-9, p. 311-317
2. I. Pšenáková. *Számítógépes biztonság oktatása a leendő tanároknak*. In: A magyar tannyelvű tanítóképző kar 2017-es tudományos konferenciáinak tanulmánygyűjteménye. Subotica: University of Novi Sad, Hungarian Language Teacher Training Faculty, (2017) ISBN 978-86-87095-76-2, 1022-1031
3. V. H. Bakonyi, ifj. Z. Illés, Z. Illés: *Első lépések a hallgatói saját eszközök felhasználására az ELTE Informatika Karán*. In: Informatika a Felsőoktatásban 2017 Konferencia, Debrecen (2017) 117-122
4. Microsoft Security Bulletin MS17-010 – Critical (2017) https://technet.microsoft.com/en-us/library/security/ms17-010.aspx