**Biztonság és védelem az**

**informatikában**

**7. gyakorlati feladat**

Készítette: Baranyi Gábor  
CRC7FC

2021.04.01.

**Tartalomszűrő tűzfalak**

Egy tűzfal a tartalomszűrő használatával egy kapcsolat hasznos adatait kiértékelni, ill. az áthaladó adatokat ellenőrizni tudja.

**Jellegzetes példái:**

1. az [URL](https://hu.wikipedia.org/wiki/URL)-szűrés és a vírusfigyelés. Mindkét feladathoz többnyire kiegészítő programokra (URL-szűrőre, víruskeresőre) van szükség, a tűzfalak általában nem tartalmazzák ezeket a lehetőségeket
2. a lekért [weboldalakról](https://hu.wikipedia.org/wiki/Weboldal) az [ActiveX](https://hu.wikipedia.org/wiki/ActiveX) és/vagy [JavaScript](https://hu.wikipedia.org/wiki/JavaScript) kiszűrése
3. bizalmas céginformációk kiszűrése (például: Mérleg-adatok)
4. kulcsszavak alapján nem kívánt [weboldalak](https://hu.wikipedia.org/wiki/Weboldal) zárolása
5. nem kívánt alkalmazás-protokollok (például: film megosztás) blokkolása

**Email spamszűrő működése:**



A spamszűrők több kritériumot használnak a beérkező e-mailek értékeléséhez. Olyan gyakori kiváltó szavakat keresnek, amelyek egy nem kívánt e-mailt jeleznek, amely megpróbál eladni valamit, például "ingyenes" és "pénzt keresni".

Ha a feladó e-mailt küld Önnek a kapcsolattartó neve helyett az e-mail címmel, ez kiválthatja a spamszűrőt, mivel a küldő nem szerepel a névjegyekben. Azokat a küldőket, akik olyan tartalmat (például hírlevelet) próbálnak elküldeni Önnek, amelyet Ön nem választott, spamként jelölhetik meg.

Ezenkívül, ha a feladó IP-címét korábban megjelölték spamküldés céljából, akkor valószínűleg ugyanazzal az IP-címmel rendelkező küldő is megjelölésre kerül.

Már maga az e-mail tartalma és kialakítása is kiválthatja a spamszűrőt. A durva nagy betűtípusok vagy a nagy képek a spam két fő elrendezési kiváltó tényezője.

Ha engedélyez egy szoftvert, amely figyeli az adathalász e-maileket, akkor a feltételek kissé eltérnek. Bár a fenti kritériumok mindegyike automatikusan e-mailt adhat a tartalomszűrő radarjára, további piros jelzők adathalász szűrőt váltanak ki.

Az adathalász e-mailek általában linket vagy csatolt dokumentumot tartalmaznak, amely a hálózat feltörésére használt rosszindulatú programokkal van tele. Azok a küldők, akiket korábban megjelöltek rosszindulatú programok küldéséről, beállíthatják az adathalász-szűrőt.

Linkeket vagy csatolt dokumentumokat tartalmazó ismeretlen feladóktól származó e-mailek szintén beállíthatják az adathalász szűrőket.

Az adathalász szűrők általában a megjelölt e-maileket egy másik beérkező levelek mappába helyezik át, néha "Egyéb" címkével. Ebben a postaládában a megjelölt e-maileket „visszatartják”, amíg fel nem engedi, letiltja vagy engedélyezi.

Ha kiad egy e-mailt, akkor az a szokásos postaládájába kerül, hogy megnyíljon, de a jövőben folytatnia kell a küldő e-mailjeinek jóváhagyását. Ha egy e-mailt blokkoltunk, akkor az e-mailt elutasítottuk, és a feladó mostantól le lesz tiltva, hogy jövőbeni e-maileket küldjön Önnek.

Ha egy e-mail megengedett, akkor az a szokásos postaládájába kerül, és a feladó automatikusan jóváhagyja az e-mailek továbbítását közvetlenül a beérkező levelek mappába

**Vírusszűrés:**

Négy különböző módszert alkalmaznak a kártevőirtó programok a rosszindulatú programok szűrésére a számítógépes rendszerben.

Definíciók

A legtöbb anti-malware program a rosszindulatú programok meghatározásának nevezett adatbázist használja, amely megmondja a programnak, hogyan kell felismerni a rosszindulatú programokat és azok hatásait. Ha egy program azonos definíciójú fájlt észlel, potenciális rosszindulatú programként jelöli meg.

Heurisztika

Van egy másik módszer arra vonatkozóan, hogy egy anti-malware program miként képes felismerni a rosszindulatú programokat - heurisztikának nevezett elemzés formájában. Ez a fajta elemzés lehetővé teszi, hogy a rosszindulatú szoftverek felismerjék azokat a rosszindulatú programokat, amelyeket korábban nem észleltek. A definíciókhoz képest a heurisztika viselkedése révén képes azonosítani a potenciális rosszindulatú programokat. Például, ha a számítógépére telepített program úgy van beállítva, hogy eltávolítsa a fontos fájlokat a számítógépes rendszeréből, akkor a kártevőirtó program rosszindulatú programnak fogja tekinteni, mivel egy törvényes alkalmazás nem viselkedik hasonlóan. A heurisztikával azonban az a probléma, hogy néha a törvényes programokat rosszindulatú programként is megjelölheti, annak ellenére, hogy nem - ez a feltétel „hamis pozitív” néven ismert.

Eltávolítás

Ez a módszer elég egyszerű. Ahelyett, hogy csak megjelölné a lehetséges rosszindulatú programokat, eltávolítja azokat a rendszerből. Ez azt jelenti, hogy a rendszerében észlelt minden rosszindulatú program automatikusan törlődik, amint azt észleli. Sajnos néhány rosszindulatú program csak eltávolítás után okoz még további károkat a számítógépén. Ebben az esetben a kártevőirtó program karanténba helyezi a fájlt a számítógép tárolójában, megakadályozva ezzel a károsodást. A karanténban a rosszindulatú fájl nem okozhat kárt a számítógépében, és manuálisan eltávolíthatja.

Sandboxing

Végül van egy sandboxing módszer, amelyben egy rosszindulatú program fut egy sandboxon. A sandbox becsapja a rosszindulatú programot, hogy azt gondolja, hogy képes volt hozzáférni az egész rendszerhez, amikor egy zárt térben fut, miközben figyelemmel kísérik annak viselkedését. Ha a program rosszindulatú viselkedést mutat, akkor az anti-malware program törli; bizonyos típusú rosszindulatú programok azonban felismerhetik, hogy sandbox-ban futnak-e vagy sem. Mint ilyen, csak akkor mutatják be a rosszindulatú viselkedést, ha kiszabadulnak a sandbox-ból.

Források:

<https://ecmanagedit.com/how-malware-filtering-works/>

<https://www.soscanhelp.com/blog/what-is-email-spam-filtering-and-how-does-it-work#how>

<https://hu.wikipedia.org/wiki/T%C5%B1zfal_(sz%C3%A1m%C3%ADt%C3%A1stechnika)>