Jegyzőkönyv

Biztonság és védelem az informatikában c. tárgy

7. feladat

Készítette:

Csomor Bence, TVIK4I

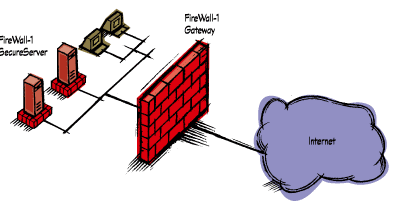
2021.04.01.

**Tartalomszűrő tűzfalak**

A tűzfal (angolul firewall) célja a számítástechnikában annak biztosítása, hogy a hálózaton keresztül egy adott számítógépbe ne történhessen illetéktelen behatolás. Szoftver- és hardverkomponensekből áll. Hardverkomponensei olyan hálózatfelosztó eszközök, mint a router vagy a proxy. A szoftverkomponensek ezeknek az alkalmazási rendszerei tűzfal szoftverekkel, beleértve ezek csomag- vagy proxyszűrőit is. A tűzfalak általában folyamatosan jegyzik a forgalom bizonyos adatait, a bejelentkező gépek és felhasználók azonosítóit, a rendkívüli és kétes eseményeket, továbbá riasztásokat is adhatnak.

A számítástechnika során a tűzfal olyan hálózati biztonsági rendszer, amely felügyeli és szabályozza a bejövő és kimenő hálózati forgalmat előre meghatározott biztonsági szabályok alapján.

A tűzfal jellemzően akadályt képez egy megbízható belső hálózat és egy bizonytalan külső hálózat között.

**Tűzfalak fajtái:**

* Csomagszűrés
* Állapot szerinti szűrés
* Alkalmazásszintű tűzfal
* Proxyk
* Tartalomszűrés
* Behatolásfelismerő és -megelőző rendszerek
* Hálózati címfordítás
* Internet Connection Firewall (ICF)
* Átjáró (Gateway)
* Demilitarizált zóna (DMZ)
* Intranet
* Port szűrés, port kezelés

**A tartalomszűrő tűzfalak szerepe:**

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

Jellegzetes példái:

* az URL-szűrés és a vírusfigyelés. Mindkét feladathoz többnyire kiegészítő programokra (URL-szűrőre, víruskeresőre) van szükség, a tűzfalak általában nem tartalmazzák ezeket a lehetőségeket
* a lekért weboldalakról az ActiveX és/vagy JavaScript kiszűrése
* bizalmas céginformációk kiszűrése (például: Mérleg-adatok)
* kulcsszavak alapján nem kívánt weboldalak zárolása
* nem kívánt alkalmazás-protokollok (például: film megosztás) blokkolása

**E-mail szűrő tűzfalak:**

E-mail azaz Spam szűrő tűzfalak elengedhetetlenek manapság, a sok reklámok és kéretlen értesítések és üzenetek világában. Ezek szűrésére is van pár hasznos alkalmazás, mint például a SpamAssassin Spam Filter vagy a Vade Secure levelezőrendszer védelmi spamszűrő.

SpamAssassin:

A SpamAssassin spam szűrő azonosítja a spam üzeneteket a Plesk szerveren tárolt postafiókokba küldött e-mailek között.

A SpamAssassin bekapcsolási szakaszában megtudhatja, hogyan kapcsolja be és konfigurálja a spam védelmet.

A kívánt spamvédelem elérése érdekében a Plesk lehetővé teszi számos SpamAssassin beállítás konfigurálását, nevezetesen: Spamszűrő érzékenység.

A spam üzenetek azonosításához a SpamAssassin számos különféle tesztet hajt végre az egyes üzenetek tartalmán és tárgysorán. Ennek eredményeként minden üzenet számos pontot kap. Minél nagyobb a szám, annál valószínűbb, hogy egy üzenet spam. Például egy üzenet, amely a „VIAGRA VÁSÁRLÁSA ALACSON ÁRON !!!” szöveget tartalmazza a Tárgy sorban, és az üzenet törzse 8,3 pontot ér el. Alapértelmezés szerint a szűrő érzékenysége úgy van beállítva, hogy az összes, legalább 7 pontot elért üzenet spamnek minősüljön. Ha a felhasználók továbbra is az alapértelmezett érzékenységű spamüzeneteket kapják, akkor növeljék kisebb érték, például 6 érték beállításával. Ha a SpamAssassin az érvényes üzeneteket spamként jelöli, akkor magasabb érték beállításával csökkentse az érzékenységet.

Vade Secure:

A VadeSecure Cloud az internet felől érkező levelezést az Ön levelezőrend-szere előtt fogadja, így a belső rendszernek nem kell biztonsági kérdésekkel foglalkoznia és a rendszer, vagy a szűkös internetkapcsolat túlterhelése is kizárható. Beállításoktól függően a levélszemét, a reklámlevelek, a marketing célú hírlevelek, a káros csatolmányok és vírusos levelek rögtön törlésre kerülhetnek vagy karanténba helyezhetők, esetleg a tárgy megjelölésével továbbadhatók.

Vírusszűrő tűzfalak:

* Webroot Antivirus
* ClamXav
* ESET NOD32

Webroot Antivirus:

A Webroot víruskereső szoftvere alacsony áron kínál alapvető védelmet, és a legfelső két szint magában foglalja az e-kereskedelem és a banki védelmet, a személyazonosság-lopás néhány ellenőrzését és a jelszókezelést.

ClamXav:

A ClamXav távol tartja a fenyegetéseket, és megerősíti a Mac biztonságát. Egy adott fájlt fájlt vagy a teljes merevlemezt is megvizsgálhatja vele.

ESET NOD32 Antivirus:

Az a vírusirtó olyan szoftvert használ, ami felismeri, blokkolja és el is távolítja a vírusokat, kém- és zsarolóprogramokat, botokat, trójaiakat, rootkiteket és adathalász programokat. Ezenkívül megakadályozza, hogy olyan weboldalra kattints, amely veszélyt jelenthet adataid biztonságára.

A felsorolt vírusszűrők mind nagyon hatásosak a vírusok elleni védelemben.

A NOD32 minden nagyobb operációs rendszerre több verziója is elérhető.



A ClamXav külön csomagot kínál különböző felhasználásra specializált védelmeket, például otthoni használatra, tanulásra vagy üzleti felhasználásra.

A Webroot Antivirus a legjobb és leg biztonságosabb vírusszűrők között van manapság.

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

<https://docs.plesk.com/en-US/obsidian/administrator-guide/mail/antispam-tools/spamassassin-spam-filter.59432/>

<https://hu.joecomp.com/discuss-top-free-firewalls-for-windows-10>

<https://eutuzfal.hu/portfolio/vade-secure/>

<http://servira.com/fogalomtar/95.tuzfal>

<https://www.webroot.com/us/en/home/affiliates/wsc-29?sc=70161000000TRru&rc=8200>

<https://www.clamxav.com/>

<https://eset_nod32_antivirus.hu.downloadastro.com/>