CSIRT

Computer Security Incident Response Team

Fejlesztési tervek (CSIRT-es Automata)

http://www.niif.hu/hu/csirt

Rőczei Gábor

NIIF Intézet

roczei@niif.hu

Bevezetés

Miről is lesz szó?!

- NIIF's AUP - http://www.niif.hu/aup
- Incidensek fajtái
- Fejlesztési tervek
  - MOT2, RIPE DBs update
  - CSIRT-es Automata

NIIF's AUP- http://www.niif.hu/aup

Az informatikai és hírközlési miniszter

20 /2004. (VI.21.) IHM rendelete

a Nemzeti Információs Infrastruktúra Fejlesztési Program

Felhasználói Szabályzatának

közzétételéről

A Nemzeti Információs Infrastruktúra Fejlesztési Program működtetéséről szóló 95/1999. (VI. 23.) Korm. rendelet (a továbbiakban: Kormányrendelet) 9. §-ának (4) bekezdésében foglalt felhatalmazás alapján az alábbiakat rendelem el:

NIIF's AUP- http://www.niif.hu/aup

Felhasználók:

a) "NIIF felhasználók": a NIIF tagintézményekben a NIIF hálózat használói.
b) "NIIF Iroda": a Kormányrendelet 2. §-ának (3) bekezdése alapján a NIIF Program végrehajtására alapított teljes jogkörrel rendelkező önállóan gazdálkodó központi költségvetési szerv.

c) "NIIF szolgáltatások": a Kormányrendelet 9. §-ának (3) bekezdése alapján a NIIF Iroda illetve a NIIF tagintézmények között létrejött csatlakozási és szolgáltatási szerződés vagy megállapodás keretében meghatározott, a NIIF tagintézményeknek nyújtott hálózati csatlakozás, hálózati és információs szolgáltatások, valamint a szolgáltatásokhoz a NIIF Iroda vagy szerződéses partnerei által biztosított infrastruktúra.

d) "NIIF tagintézmények": felső- és közoktatási intézmények, kutató-fejlesztő helyek, közgyűjtemények és egyéb oktatási, tudományos és kulturális szervezetek, amelyek a Kormányrendelet 9. §-ában meghatározott módon NIIF tagintézményekké váltak.

NIIF's AUP- http://www.niif.hu/aup

A felhasználók kötelességei

8. §

A NIIF felhasználók kötelesek jelen Szabályzat megismerésére és megtartására.

9. §

Az a felhasználó, aki a NIIF hálózaton keresztül más hálózati szolgáltató szolgáltatásait is igénybe veszi, az idegen hálózatra érvényes szabályokat is köteles megtartani.

10. §

A NIIF felhasználó a polgári jog általános szabályai szerint felel minden általa - a NIIF Irodának vagy harmadik félnek - okozott kárért.

11. §

A NIIF felhasználó köteles a NIIF Irodát, illetve a NIIF tagintézményeket a Szabályzat megsértése és az esetleges káresetek kiderítésében, valamint lehetőség szerint a bekövetkezett károk következményei felszámolásában segíteni.

NIIF's AUP- http://www.niif.hu/aup

A Szabályzat betartatása, a Szabályzat megsértésének szankcionálása

13. §

A NIIF tagintézmények kötelesek a Szabályzat több intézményt érintő súlyos megsértése esetén a NIIF Irodát tájékoztatni. Az ilyen esetet a NIIF Iroda és az érintett NIIF tagintézmény közösen vizsgálja ki. Amennyiben a Szabályzat több intézményt érintő súlyos megsértése más hálózatot is érint, akkor annak illetékeseivel a NIIF Iroda és az érintett NIIF tagintézmény együttműködni köteles.

14. §

A NIIF Irodának a Szabályzat súlyos megsértése esetén joga van a NIIF tagintézmény hálózati hozzáférését azonnal korlátozni. A hálózathoz való hozzáférés korlátozása esetén a NIIF tagintézményt kártérítési igény nem illeti meg, ugyanakkor a NIIF Iroda a korlátozás okáról az érintett NIIF tagintézményt a lehető legrövidebb időn belül tájékoztatni köteles.

NIIF's AUP- http://www.niif.hu/aup

A Szabályzat betartatása, a Szabályzat megsértésének szankcionálása

15. §

A NIIF Iroda a Szabályzat megsértéséből eredő károkozás megelőzésére és a bekövetkezett károk következményeinek mielőbbi és minél eredményesebb felszámolására törekszik, illetve a Szabályzat megsértése esetén - amennyiben annak feltételei fennállnak - a polgári jog szabályai szerint felelősségre vonást kezdeményez.

16. §

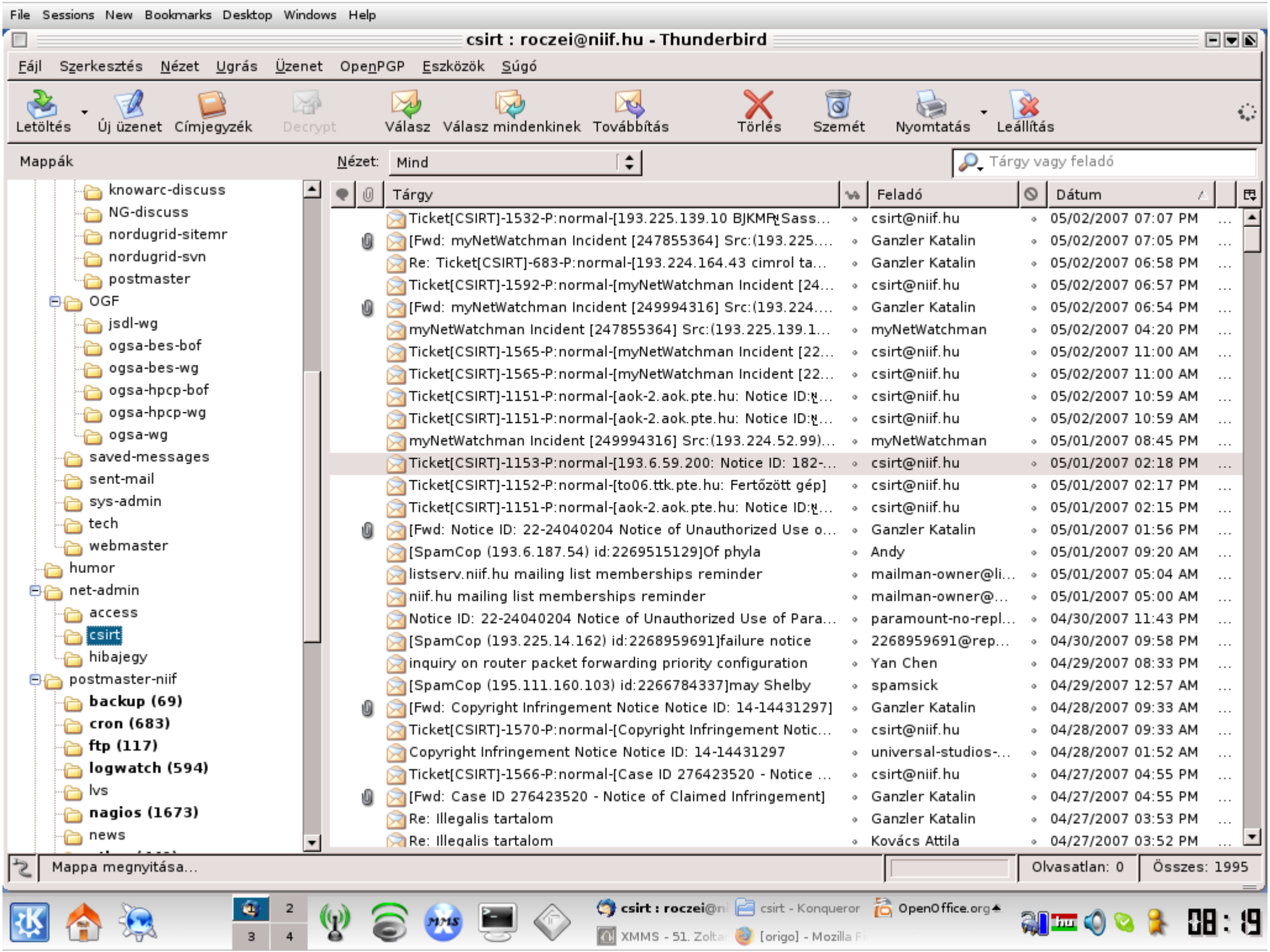
A NIIF Iroda és a NIIF tagintézmények a mindenkori műszaki lehetőségeknek megfelelően törekednek arra, hogy a hálózaton áthaladó, illetve a hálózaton elérhető információkhoz, adatokhoz illetéktelenek ne férjenek hozzá.

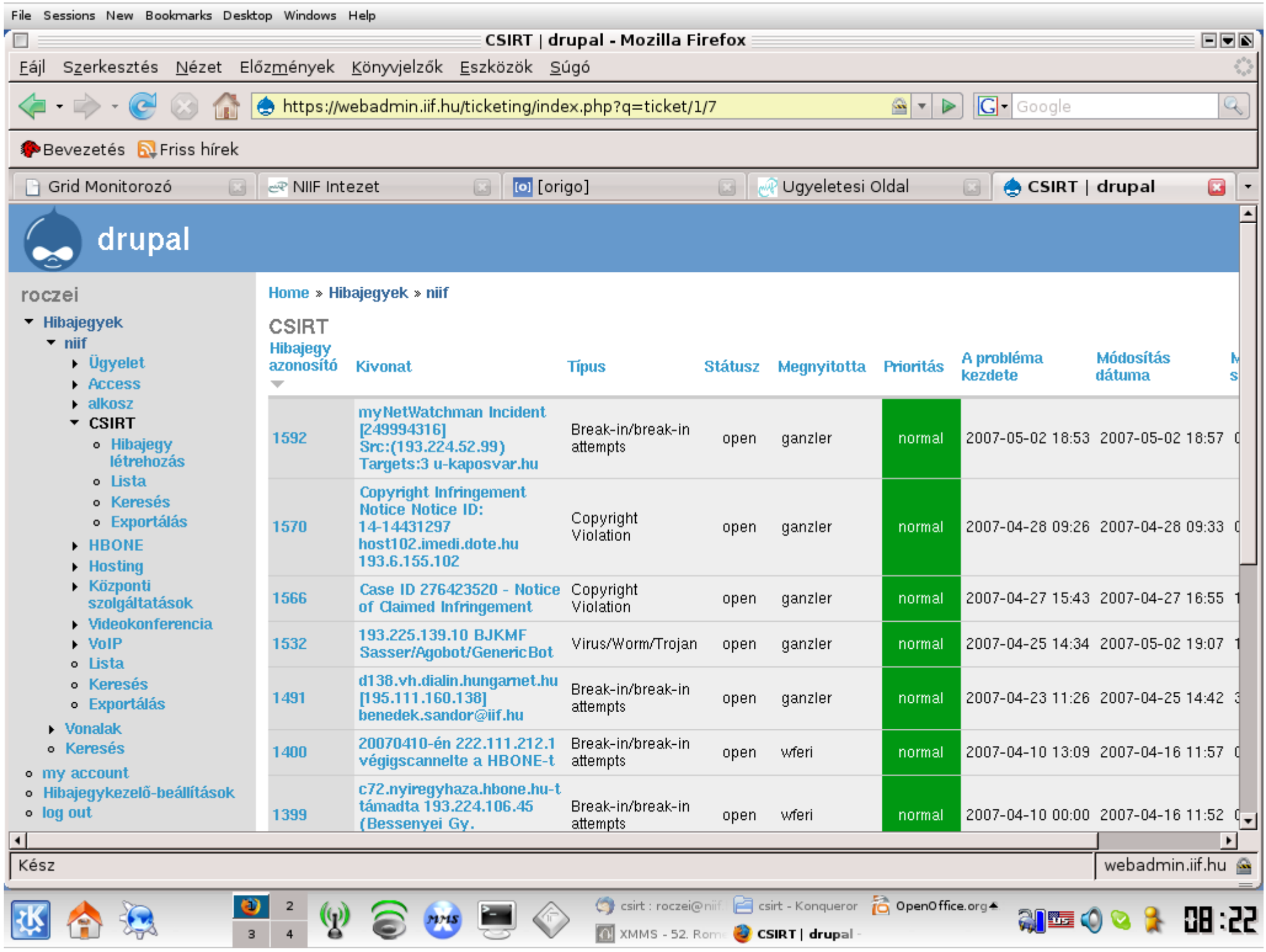
NIIF's AUP- http://www.niif.hu/aup

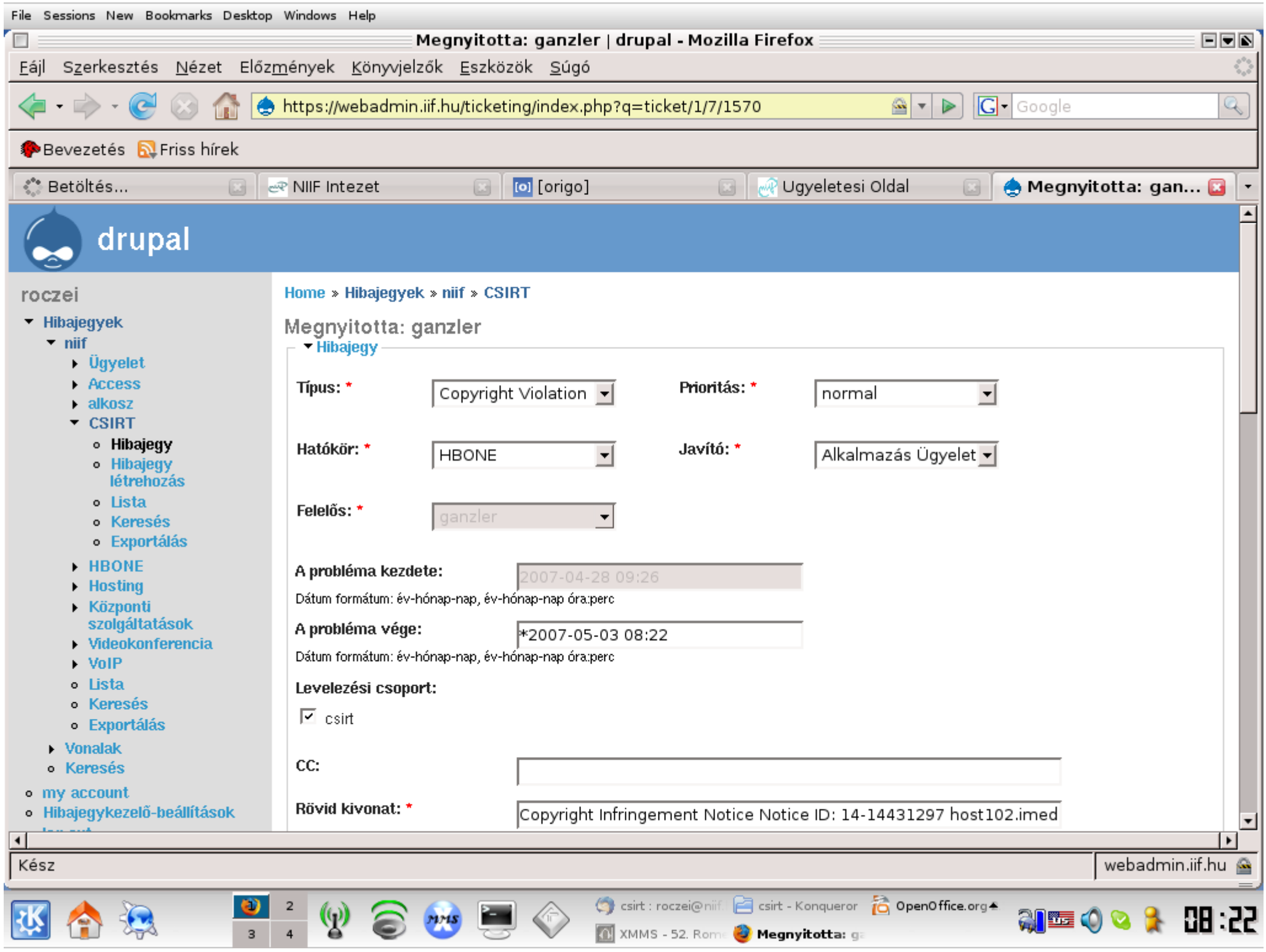
A Szabályzat betartatása, a Szabályzat megsértésének szankcionálása

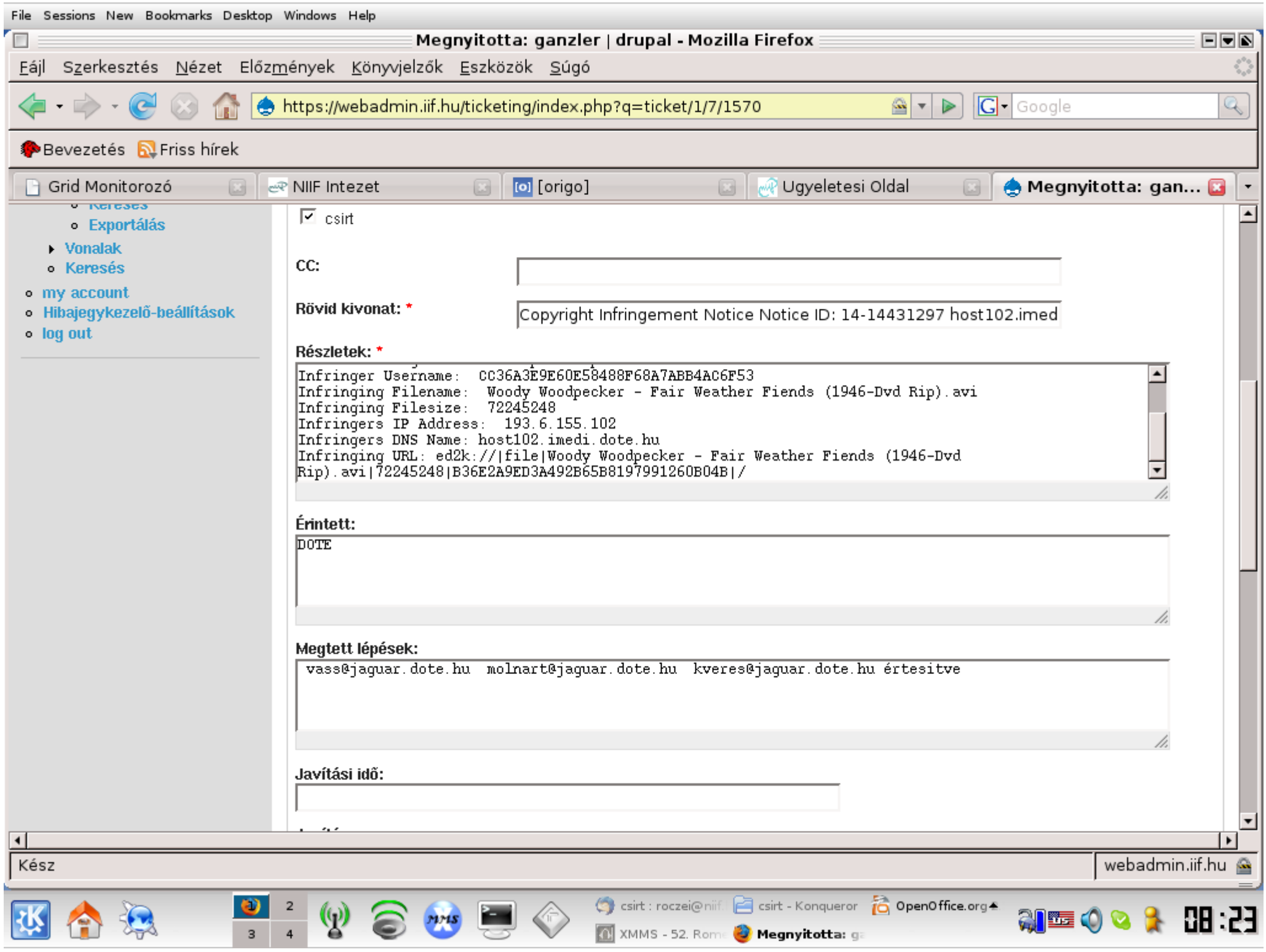
18. §

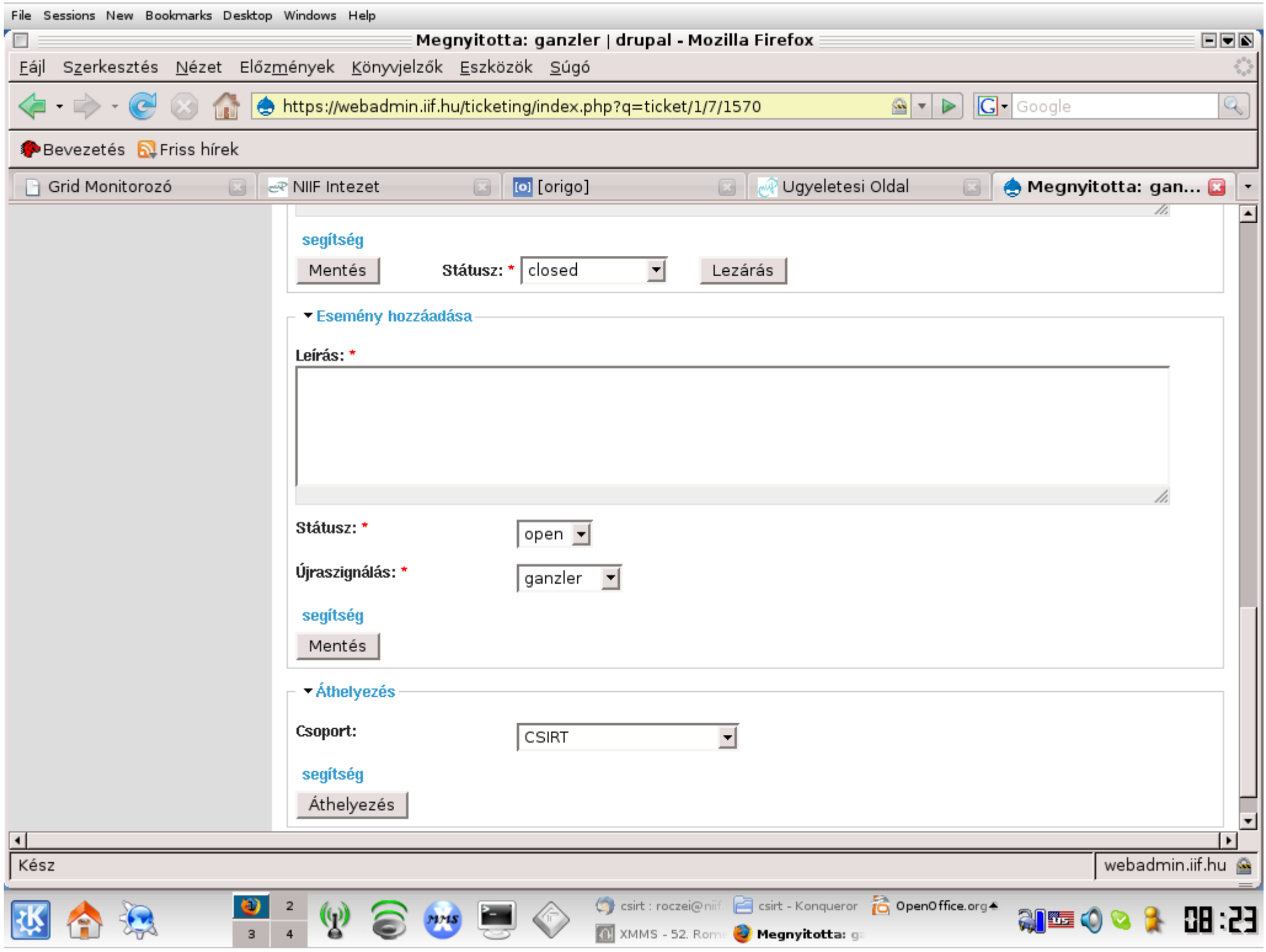
A NIIF Műszaki Tanács által létrehozott NIIF Etikai Bizottság a NIIF Iroda, a NIIF tagintézmény vagy a NIIF felhasználó kérésére állást foglal a Szabályzatot érintő vitatott kérdésekben. Az Etikai Bizottságnak nem feladata a konkrét esetekben hozott döntések felülvizsgálata.


File Sessions New Bookmarks Desktop Windows Help
csirt : roczei@niif.hu - Thunderbird
Fájl Szerkesztés Nézet Ugrás Üzenet OpenPGP Eszközök Súgó
Letöltés
Új üzenet
Címjegyzék
Decrypt
Válasz
Válasz mindenkinek
Továbbítás
Törlés
Szemét
Nyomtatás
Leállítás
Mappák
Nézet: Mind
Tárgy vagy feladó
knowarc-discuss
NG-discuss
nordugrid-sitemr
nordugrid-svn
postmaster
OGF
jsdl-wg
ogsa-bes-bof
ogsa-bes-wg
ogsa-hpcp-bof
ogsa-hpcp-wg
ogsa-wg
saved-messages
sent-mail
sys-admin
tech
webmaster
humor
net-admin
access
csirt
hibajegy
postmaster-niif
backup (69)
cron (683)
ftp (117)
logwatch (594)
lvs
nagios (1673)
news
Tárgy
Feladó
Dátum
Ticket[CSIRT]-1532-P:normal-[193.225.139.10 BJKMPﾝSass... csirt@niif.hu 05/02/2007 07:07 PM
[Fwd: myNetWatchman Incident [247855364] Src:(193.225.... Ganzler Katalin 05/02/2007 07:05 PM
Re: Ticket[CSIRT]-683-P:normal-[193.224.164.43 cimrol ta... Ganzler Katalin 05/02/2007 06:58 PM
Ticket[CSIRT]-1592-P:normal-[myNetWatchman Incident [24... csirt@niif.hu 05/02/2007 06:57 PM
[Fwd: myNetWatchman Incident [249994316] Src:(193.224.... Ganzler Katalin 05/02/2007 06:54 PM
myNetWatchman Incident [247855364] Src:(193.225.139.1... myNetWatchman 05/02/2007 04:20 PM
Ticket[CSIRT]-1565-P:normal-[myNetWatchman Incident [22... csirt@niif.hu 05/02/2007 11:00 AM
Ticket[CSIRT]-1565-P:normal-[myNetWatchman Incident [22... csirt@niif.hu 05/02/2007 11:00 AM
Ticket[CSIRT]-1151-P:normal-[aok-2.aok.pte.hu: Notice ID:ﾝ... csirt@niif.hu 05/02/2007 10:59 AM
Ticket[CSIRT]-1151-P:normal-[aok-2.aok.pte.hu: Notice ID:ﾝ... csirt@niif.hu 05/02/2007 10:59 AM
myNetWatchman Incident [249994316] Src:(193.224.52.99)... myNetWatchman 05/01/2007 08:45 PM
Ticket[CSIRT]-1153-P:normal-[193.6.59.200: Notice ID: 182-... csirt@niif.hu 05/01/2007 02:18 PM
Ticket[CSIRT]-1152-P:normal-[to06.ttk.pte.hu: Fertőzött gép] csirt@niif.hu 05/01/2007 02:17 PM
Ticket[CSIRT]-1151-P:normal-[aok-2.aok.pte.hu: Notice ID:ﾝ... csirt@niif.hu 05/01/2007 02:15 PM
[Fwd: Notice ID: 22-24040204 Notice of Unauthorized Use o... Ganzler Katalin 05/01/2007 01:56 PM
[SpamCop (193.6.187.54) id:2269515129]Of phyla Andy 05/01/2007 09:20 AM
listserv.niif.hu mailing list memberships reminder mailman-owner@li... 05/01/2007 05:04 AM
niif.hu mailing list memberships reminder mailman-owner@... 05/01/2007 05:00 AM
Notice ID: 22-24040204 Notice of Unauthorized Use of Para... paramount-no-repl... 04/30/2007 11:43 PM
[SpamCop (193.225.14.162) id:2268959691]failure notice 2268959691@rep... 04/30/2007 09:58 PM
inquiry on router packet forwarding priority configuration Yan Chen 04/29/2007 08:33 PM
[SpamCop (195.111.160.103) id:2266784337]may Shelby spamsick 04/29/2007 12:57 AM
[Fwd: Copyright Infringement Notice Notice ID: 14-14431297] Ganzler Katalin 04/28/2007 09:33 AM
Ticket[CSIRT]-1570-P:normal-[Copyright Infringement Notic... csirt@niif.hu 04/28/2007 09:33 AM
Copyright Infringement Notice Notice ID: 14-14431297 universal-studios-... 04/28/2007 01:52 AM
Ticket[CSIRT]-1566-P:normal-[Case ID 276423520 - Notice ... csirt@niif.hu 04/27/2007 04:55 PM
[Fwd: Case ID 276423520 - Notice of Claimed Infringement] Ganzler Katalin 04/27/2007 04:55 PM
Re: Illegalis tartalom Ganzler Katalin 04/27/2007 03:53 PM
Re: Illegalis tartalom Kovács Attila 04/27/2007 03:52 PM
Mappa megnyitása...
Olvasatlan: 0
Összes: 1995
csirt : roczei@ni
csirt - Konqueror
OpenOffice.org
XMMS - 51. Zoltar
[origo] - Mozilla Fi
08:19


File Sessions New Bookmarks Desktop Windows Help
CSIRT | drupal - Mozilla Firefox
Fájl Szerkesztés Nézet Előzmények Könyvjelzők Eszközök Súgó
https://webadmin.iif.hu/ticketing/index.php?q=ticket/1/7
Google
Bevezetés Friss hírek
Grid Monitorozó
NIIF Intezet
[origo]
Ugyeletesi Oldal
CSIRT | drupal
drupal
roczei
Hibajegyek
niif
Ügyelet
Access
alkosz
CSIRT
Hibajegy létrehozás
Lista
Keresés
Exportálás
HBONE
Hosting
Központi szolgáltatások
Videokonferencia
VoIP
Lista
Keresés
Exportálás
Vonalak
Keresés
my account
Hibajegykezelő-beállítások
log out
Home » Hibajegyek » niif
CSIRT
Hibajegy azonosító
Kivonat
Típus
Státusz
Megnyitotta
Prioritás
A probléma kezdete
Módosítás dátuma
1592
myNetWatchman Incident [249994316] Src:(193.224.52.99) Targets:3 u-kaposvar.hu
Break-in/break-in attempts
open
ganzler
normal
2007-05-02 18:53
2007-05-02 18:57
1570
Copyright Infringement Notice Notice ID: 14-14431297 host102.imedi.dote.hu 193.6.155.102
Copyright Violation
open
ganzler
normal
2007-04-28 09:26
2007-04-28 09:33
1566
Case ID 276423520 - Notice of Claimed Infringement
Copyright Violation
open
ganzler
normal
2007-04-27 15:43
2007-04-27 16:55
1532
193.225.139.10 BJKMF Sasser/Agobot/GenericBot
Virus/Worm/Trojan
open
ganzler
normal
2007-04-25 14:34
2007-05-02 19:07
1491
d138.vh.dialin.hungarnet.hu [195.111.160.138] benedek.sandor@iif.hu
Break-in/break-in attempts
open
ganzler
normal
2007-04-23 11:26
2007-04-25 14:42
1400
20070410-én 222.111.212.1 végigscannelte a HBONE-t
Break-in/break-in attempts
open
wferi
normal
2007-04-10 13:09
2007-04-16 11:57
1399
c72.nyiregyhaza.hbone.hu-t támadta 193.224.106.45 (Bessenyei Gy.
Break-in/break-in attempts
open
wferi
normal
2007-04-10 00:00
2007-04-16 11:52
Kész
webadmin.iif.hu
csirt : roczei@niif
csirt - Konqueror
OpenOffice.org
XMMS - 52. Rom
CSIRT | drupal -
08:22


File Sessions New Bookmarks Desktop Windows Help
Megnyitotta: ganzler | drupal - Mozilla Firefox
Fájl Szerkesztés Nézet Előzmények Könyvjelzők Eszközök Súgó
https://webadmin.iif.hu/ticketing/index.php?q=ticket/1/7/1570
Google
Bevezetés Friss hírek
Betöltés... NIIF Intezet [origo] Ugyeletesi Oldal Megnyitotta: gan...
drupal
roczei
Hibajegyek
niif
Ügyelet
Access
alkosz
CSIRT
Hibajegy
Hibajegy létrehozás
Lista
Keresés
Exportálás
HBONE
Hosting
Központi szolgáltatások
Videokonferencia
VoIP
Lista
Keresés
Exportálás
Vonalak
Keresés
my account
Hibajegykezelő-beállítások
Home » Hibajegyek » niif » CSIRT
Megnyitotta: ganzler
Hibajegy
Típus: *
Copyright Violation
Prioritás: *
normal
Hatókör: *
HBONE
Javító: *
Alkalmazás Ügyelet
Felelős: *
ganzler
A probléma kezdete:
2007-04-28 09:26
Dátum formátum: év-hónap-nap, év-hónap-nap óra:perc
A probléma vége:
*2007-05-03 08:22
Dátum formátum: év-hónap-nap, év-hónap-nap óra:perc
Levelezési csoport:
csirt
CC:
Rövid kivonat: *
Copyright Infringement Notice Notice ID: 14-14431297 host102.imed
Kész
webadmin.iif.hu
csirt : roczei@niif
csirt - Konqueror
OpenOffice.org
XMMS - 52. Rom
Megnyitotta: g
08:22


File Sessions New Bookmarks Desktop Windows Help
Megnyitotta: ganzler | drupal - Mozilla Firefox
Fájl Szerkesztés Nézet Előzmények Könyvjelzők Eszközök Súgó
https://webadmin.iif.hu/ticketing/index.php?q=ticket/1/7/1570
Google
Bevezetés Friss hírek
Grid Monitorozó
NIIF Intezet
[origo]
Ugyeletesi Oldal
Megnyitotta: gan...
Exportálás
Vonalak
Keresés
my account
Hibajegykezelő-beállítások
log out
csirt
CC:
Rövid kivonat: *
Copyright Infringement Notice Notice ID: 14-14431297 host102.imed
Részletek: *
Infringer Username: CC36A3E9E60E58488F68A7ABB4AC6F53
Infringing Filename: Woody Woodpecker - Fair Weather Fiends (1946-Dvd Rip).avi
Infringing Filesize: 72245248
Infringers IP Address: 193.6.155.102
Infringers DNS Name: host102.imedi.dote.hu
Infringing URL: ed2k://|file|Woody Woodpecker - Fair Weather Fiends (1946-Dvd Rip).avi|72245248|B36E2A9ED3A492B65B8197991260B04B|/
Érintett:
DOTE
Megtett lépések:
vass@jaguar.dote.hu molnart@jaguar.dote.hu kveres@jaguar.dote.hu értesitve
Javítási idő:
Kész
webadmin.iif.hu
csirt : roczei@niif
csirt - Konqueror
OpenOffice.org
XMMS - 52. Rom
Megnyitotta: g
08:23


File Sessions New Bookmarks Desktop Windows Help
Megnyitotta: ganzler | drupal - Mozilla Firefox
Fájl Szerkesztés Nézet Előzmények Könyvjelzők Eszközök Súgó
https://webadmin.iif.hu/ticketing/index.php?q=ticket/1/7/1570
Google
Bevezetés Friss hírek
Grid Monitorozó
NIIF Intezet
[origo]
Ugyeletesi Oldal
Megnyitotta: gan...
segítség
Mentés
Státusz: * closed
Lezárás
Esemény hozzáadása
Leírás: *
Státusz: * open
Újraszignálás: * ganzler
segítség
Mentés
Áthelyezés
Csoport: CSIRT
segítség
Áthelyezés
Kész
webadmin.iif.hu
csirt : roczei@niif
csirt - Konqueror
OpenOffice.org
XMMS - 52. Rom
Megnyitotta: g
08:23

Incidensek fajtái

- DoS: Szolgáltatásmegtagadási támadás távoli gépek ellen, beleértendő a szándékos rongálást is.
- Rosszindulatú kód: Vírus, worm, trójai, spyware, dialer
- Problémás tartalom: SPAM, gyalázkodás
- Jogvédett tartalom hozzáférhetővé tétele
- Törvénysértés: pl. gyermekpornográfia, terrorizmus stb.
- Információgyűjtés: scanelés, sniffelés, megtévesztés (social engineering)

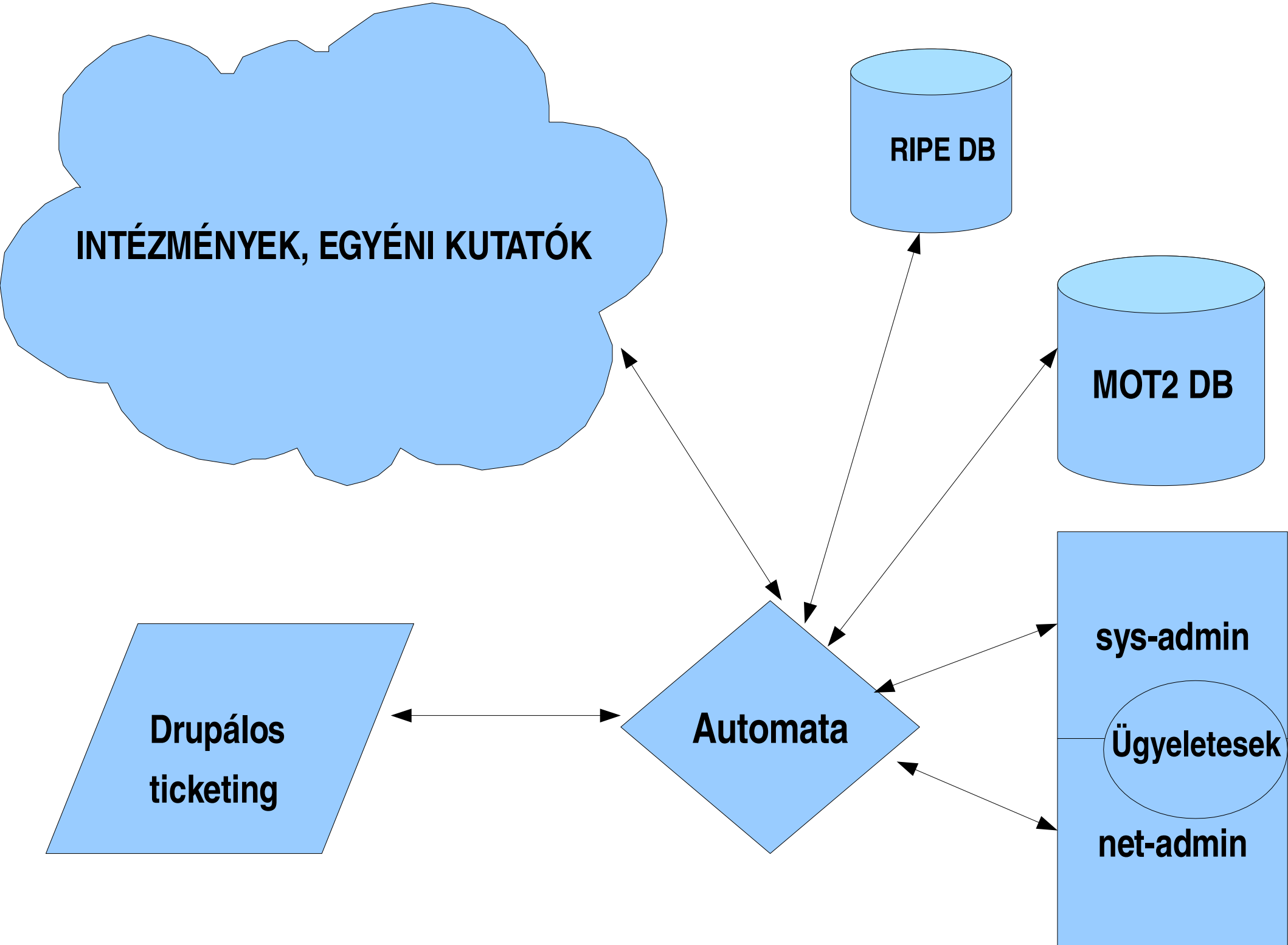
Incidensek fajtái

- Betörési kísérlet: ismert sérülékenységek (buffer overflow, Cross-site-scripting, hátsó ajtó stb), jelszó kitalálás, ismeretlen sérülékenységek utáni kutatás
- Betörés: jogosulatlan adminisztrátori, vagy nem adminisztrátori jogok szerzése, alkalmazás hibáinak kihasználása
- Egyéb

csirt@niif.hu

E-mail típusok (tárgy):

- Spam complaint from UOL [1MDEPFtpKh6MKsj06mI] (SPAM)
- Notice ID: 182-7140742 ESA Foreign Notice (jogi dolog)
- [SpamCop (195.111.160.22) id:2250480033]leatherback seltzer (SPAM)
- myNetWatchman Incident [246585666] Src:(193.225.18.45) Targets:1
- Vad web letoltes (valaki ír a csirt-es listara)
- Copyright Infringement Notice Notice ID: 14-12057294 (jogi dolog)
- Reported spam originating from 193.225.135.134
- Ticket[CSIRT]-1400-P:normal-[20070410-én 222.111.212.1 végigscannelte a HBONE-t]
- NetFlow-s email
- NIIF-es egyéni felhasználó: a hálózati ügyeletestől kell érdeklődni
- Etc.


INTÉZMÉNYEK, EGYÉNI KUTATÓK
RIPE DB
MOT2 DB
sys-admin
Ügyeletesek
net-admin
Drupálos
ticketing
Automata

Fejlesztési tervek

- RIPE DB, MOT2 DB update
- Nagyobb intézmények, csirt-es levlista, minimum 3 taggal
- Automata megtervezése, implementálása, bevezetése

Automata

Mi a célunk vele: ***kevesebb csirt-es munka***

- Az alkalmazás ügyeletesnek 10-ből 8-szor annyi dolga legyen, hogy lezárja a drupálos ticketet
- Automatikus e-mail fogadás, továbbítás, analizálás, TILTÁS
- Rossz e-mail címek kezelése ---> RIPE módosítás, Ganzler Kati értesítése
- Ticketing feature, a visszaeső intézmények fekete listára küldése (szényen fal)

Automata működési elve

E-mail típusok (tárgy):

- Spam complaint from UOL [1MDEPFtpKh6MKsj06mI] (SPAM)
- Notice ID: 182-7140742 ESA Foreign Notice (jogi dolog)
- [SpamCop (195.111.160.22) id:2250480033]leatherback seltzer (SPAM)
- Etc.

Automata:

- Mesterséges intelligencia (szakértőrendszeres motor)
- Fuzzy logika alkalmazása
- Több feltétel analizálása egy adott e-mail esetén, ha ezek AND kapcsolatban igaz értéket adnak akkor a végeredmény TRUE
- Ticketing <-----> Automata <----> MOT2/RIPE DB

Az AUTOMATA bevezetésének a lépései (6 hónapos terv)

Lépések:

- MOT2, RIPE DB update, 3 hónap
- AUTOMATA implementálása, 1 hónap
- Tesztelés, AUTOMATA PILOT rendszer bevezetése, 2 hónap

Köszönöm a figyelmet!

KÉRDÉS?!

http://www.niif.hu/hu/csirt

Rőczei Gábor

NIIF Intézet

roczei@niif.hu