BELÜGYMINISZTÉRIUM
ORSZÁGOS KATASZTRÓFAVÉDELMI FŐIGAZGATÓSÁG
„Magyarország szolgálatában a biztonságért!”

Tájékoztató az LRL IBEK feladatrendszeréről

2014. március 10 „Energetikai Szakmai Nap”

DISASTER MANAGEMENT

Dr. Bognár Balázs PhD tű. alezredes
kritikus infrastruktúra koordinációs főosztályvezető
LRL IBEK vezető

- **Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (LRL IBEK)**

LRL IBEK

2013. március 19-én átadásra került a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (LRLIBEK)

BM OKF Országos Iparbiztonsági Főfelügyelőség keretein belül működik

Hálózatbiztonsági feladatai mellett elsősorban iparbiztonsági események kezelésével, gyakorlatok, ellenőrzési akciók koordinálásával
(hóhelyzet, dunai árvíz, DISASTER, ONER)

Folyamatosan bővíti a hálózatbiztonsági szakmai tevékenységet és a bevont rendszerek körét. Kialakítja a működési protokollokat, szabályrendszereket.

Az LRL IBEK feladatkörében:

- **technikai védelmi,**
- **megelőző,**
- **tájékoztatási és**
- **oktatási tevékenységet végez**

Közreműködés infokommunikációs biztonságra, valamint létfontosságú elektronikus információs rendszerek és létesítmények védelmére vonatkozó stratégiák és ágazati szabályozók előkészítésében.

Az LRL IBEK feladatai

• a magyar és nemzetközi hálózatbiztonsági szervezetektől a Központon keresztül kapott **riasztások kezelésére** – a nemzeti létfontosságú rendszerek és létesítmények érintettsége esetén – **számítástechnikai sürgősségi reagáló egységként működik folyamatos rendelkezésre állással,**

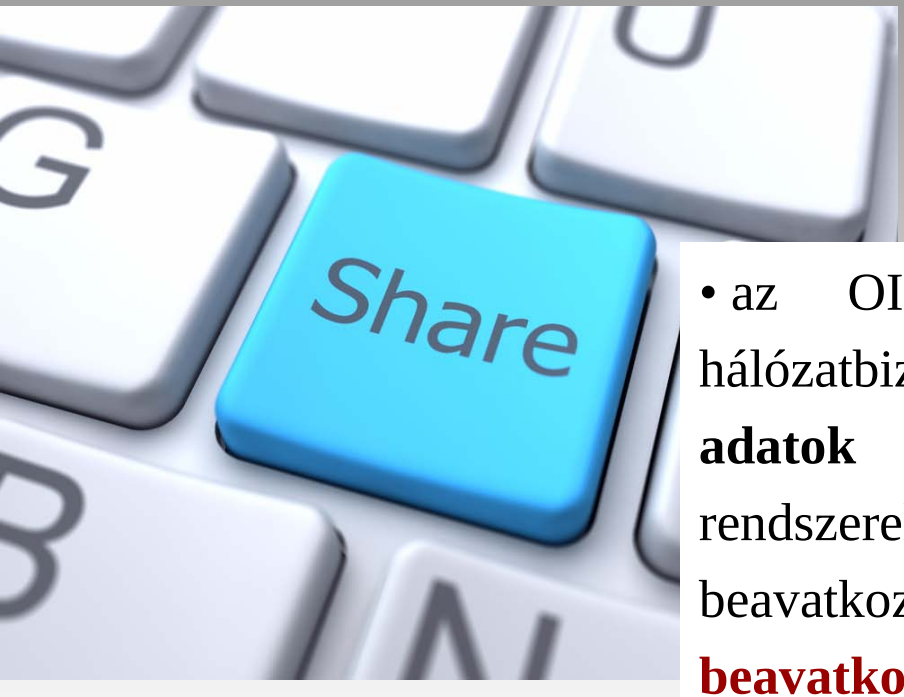
Az LRL IBEK feladatai

•ellátja a **nemzeti létfontosságú rendszerelemként** azonosított informatikai rendszerek és hírközlő hálózatok felé irányuló, a globális kibertérből érkező **beavatkozások elhárításának koordinálását,**

Az LRL IBEK feladatai

•**rendszeres tájékoztatást ad** a nemzeti létfontosságú rendszerelemként azonosított informatikai rendszerek és hírközlő hálózatok felé **a felismert és publikált sérülékenységekről,**

Az LRL IBEK feladatai



• az OIHF-től és a Központtól, vagy más hálózatbiztonsági szervezettől **átvett információk és adatok alapján**, a nemzeti létfontosságú rendszerelemet érintő, a globális kibertérből érkező beavatkozást, és az internet-forgalomba való **beavatkozásra utaló jeleket kiértékeli**, és folyamatos ügyeleti rendszerén keresztül **értesíti a létfontosságú rendszerelem üzemeltetőjét**, valamint az érintett hálózatbiztonsági és létfontosságú **elektronikus információs rendszer és létesítmény üzemeltetőjét**,

Az LRL IBEK feladatai

•tájékoztatási célú, szemléletformáló kampányokat szervez, **hírleveleket** bocsát ki,

• **együttműködik** az informatikai és hálózatbiztonsági, valamint a létfontosságú elektronikus információs rendszerek és létesítmények védelmében érintett **magyar nemzetbiztonsági szolgálatokkal és bűnüldöző szervekkel**, **iparági szereplőkkel**, egyéb **ágazati eseménykezelő központokkal**

Az LRL IBEK feladatai

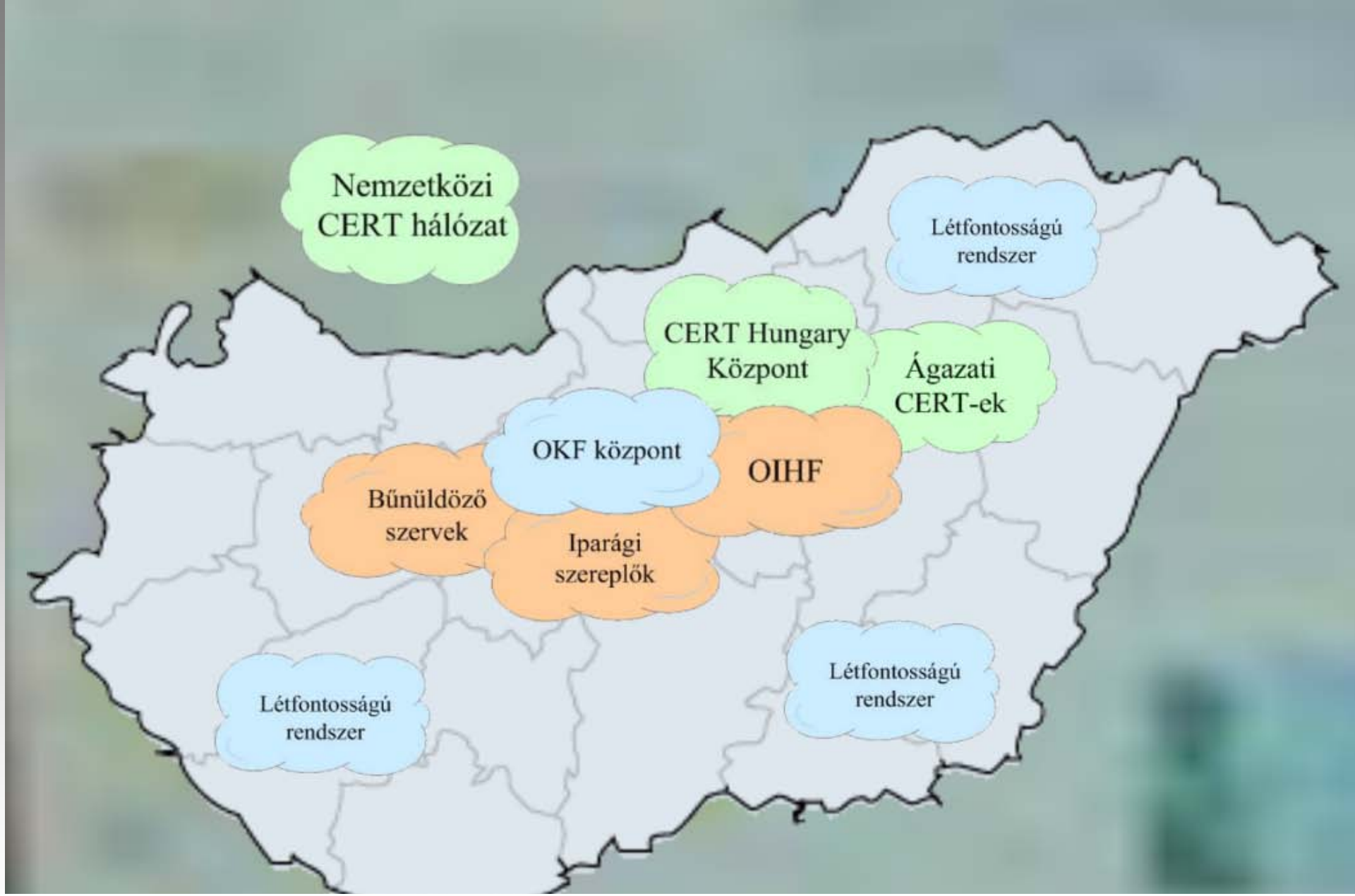
•a **megelőzés érdekében** a szükséges **technikai beavatkozásokat elvégzi**, és

• a **Belügyminisztérium és szervei** érintett informatikai munkatársai részére **képzéseket szervez, tart**.

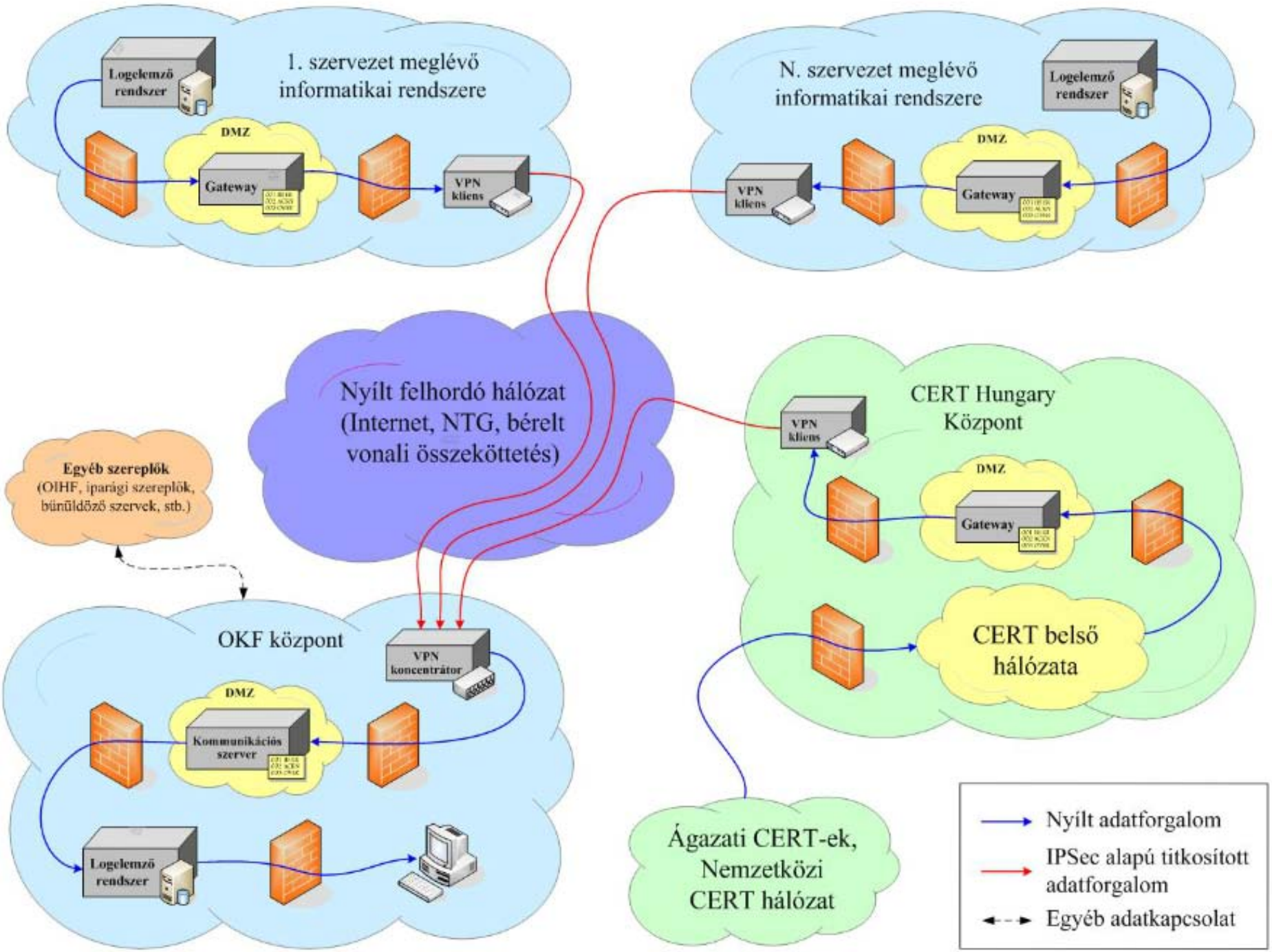
Az LRL IBEK feladatai

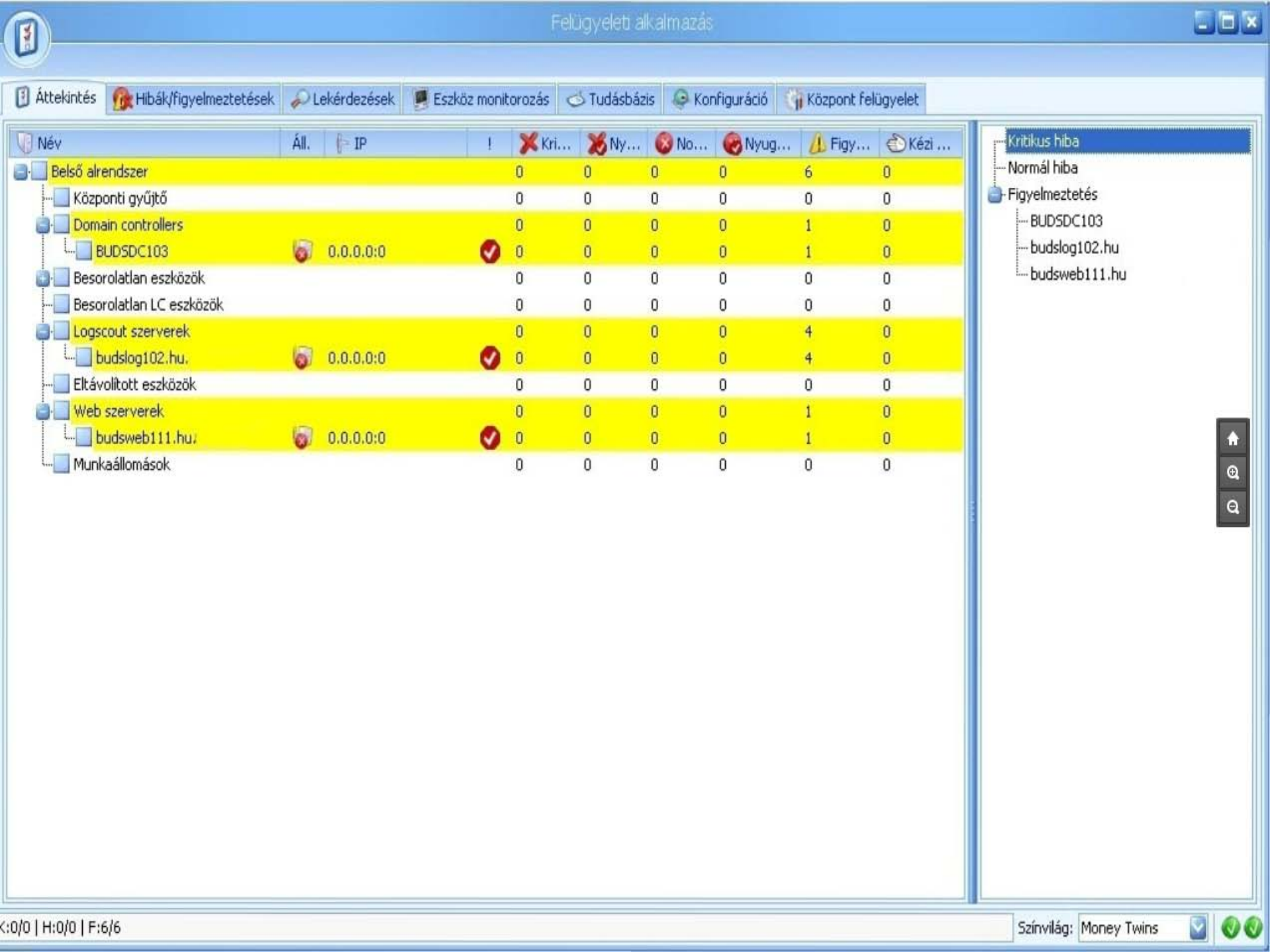
Az LRL IBEK felelős a **hatáskörébe utalt rendszereknél** a **hálózatbiztonság fenntartásának elősegítéséért, fokozásáért**, valamint a GovCERT-től kapott tájékoztatás alapján a hatáskörébe tartozó rendszer biztonságát érintő eseménnyel összefüggésben az **érintett üzemeltető riasztásáért**.

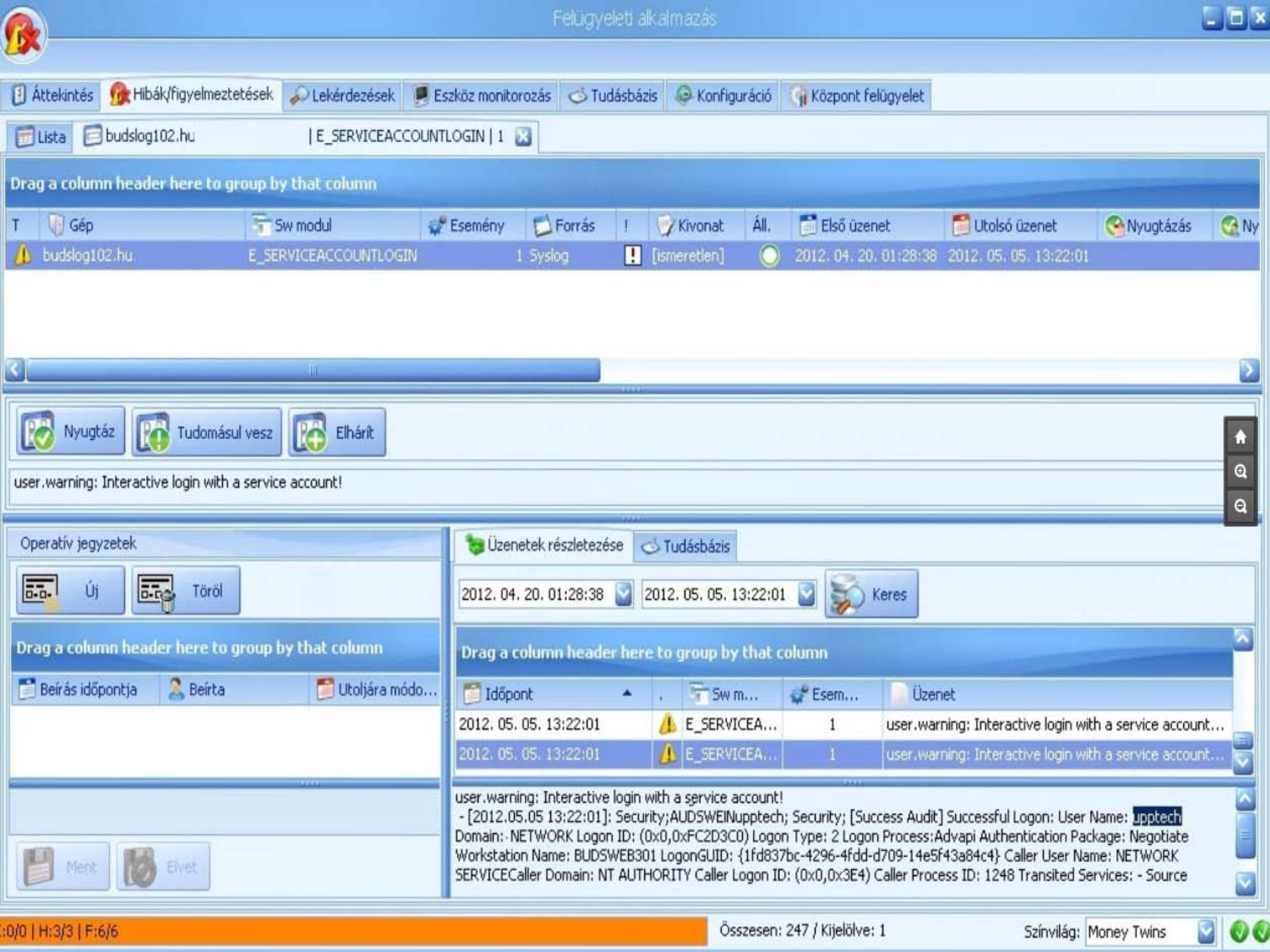
Kritikus sérülékenység estén az LRL IBEK az érintettet **határidő megadásával**, az **elhárításra tett javaslatokkal együtt felszólítja** a sérülékenység megszüntetésére, elhárítására.



Munkája során az LRL IBEK együttműködik az NMHH-val, az OIHF-fel, a Kormányzati Eseménykezelő Központtal, a létfontosságú elektronikus információs rendszert és létesítményt üzemeltető szervezetekkel, hálózatbiztonsági feladatot ellátó más szervekkel (NEIH, NBF).


1. szervezet meglévő informatikai rendszere
Logelemző rendszer
DMZ
Gateway
VPN kliens
N. szervezet meglévő informatikai rendszere
Logelemző rendszer
DMZ
VPN kliens
Gateway
Nyílt felhordó hálózat (Internet, NTG, bérelt vonali összeköttetés)
Egyéb szereplők (OIHF, iparági szereplők, bűnüldöző szervek, stb.)
CERT Hungary Központ
VPN kliens
DMZ
Gateway
CERT belső hálózata
OKF központ
VPN koncentrátor
DMZ
Kommunikációs szerver
Logelemző rendszer
Ágazati CERT-ek, Nemzetközi CERT hálózat
Nyílt adatforgalom
IPSec alapú titkosított adatforgalom
Egyéb adatkapcsolat


Felügyeleti alkalmazás
Áttekintés
Hibák/figyelmeztetések
Lekérdezések
Eszköz monitorozás
Tudásbázis
Konfiguráció
Központ felügyelet
Név
Áll.
IP
!
Kri...
Ny...
No...
Nyug...
Figy...
Kézi ...
Belső alrendszer 0 0 0 0 6 0
Központi gyűjtő 0 0 0 0 0 0
Domain controllers 0 0 0 0 1 0
BUDSDC103 0.0.0.0:0 0 0 0 0 1 0
Besorolatlan eszközök 0 0 0 0 0 0
Besorolatlan LC eszközök 0 0 0 0 0 0
Logscout szerverek 0 0 0 0 4 0
budslog102.hu. 0.0.0.0:0 0 0 0 0 4 0
Eltávolított eszközök 0 0 0 0 0 0
Web szerverek 0 0 0 0 1 0
budsweb111.hu. 0.0.0.0:0 0 0 0 0 1 0
Munkaállomások 0 0 0 0 0 0
Kritikus hiba
Normál hiba
Figyelmeztetés
BUDSDC103
budslog102.hu
budsweb111.hu
K:0/0 | H:0/0 | F:6/6
Színvilág:
Money Twins


Felügyeleti alkalmazás
Áttekintés
Hibák/figyelmeztetések
Lekérdezések
Eszköz monitorozás
Tudásbázis
Konfiguráció
Központ felügyelet
Lista
budslog102.hu
| E_SERVICEACCOUNTLOGIN | 1
Drag a column header here to group by that column
T
Gép
Sw modul
Esemény
Forrás
!
Kivonat
Áll.
Első üzenet
Utolsó üzenet
Nyugtázás
Ny
budslog102.hu
E_SERVICEACCOUNTLOGIN
1
Syslog
[ismeretlen]
2012. 04. 20. 01:28:38
2012. 05. 05. 13:22:01
Nyugtáz
Tudomásul vesz
Elhárít
user.warning: Interactive login with a service account!
Operatív jegyzetek
Új
Töröl
Drag a column header here to group by that column
Beírás időpontja
Beírta
Utoljára módo...
Ment
Elvet
Üzenetek részletezése
Tudásbázis
2012. 04. 20. 01:28:38
2012. 05. 05. 13:22:01
Keres
Drag a column header here to group by that column
Időpont
.
Sw m...
Esem...
Üzenet
2012. 05. 05. 13:22:01
E_SERVICEA...
1
user.warning: Interactive login with a service account...
2012. 05. 05. 13:22:01
E_SERVICEA...
1
user.warning: Interactive login with a service account...
user.warning: Interactive login with a service account!
- [2012.05.05 13:22:01]: Security;AUDSWEINupptech; Security; [Success Audit] Successful Logon: User Name: Upptech
Domain: NETWORK Logon ID: (0x0,0xFC2D3C0) Logon Type: 2 Logon Process:Advapi Authentication Package: Negotiate
Workstation Name: BUDSWEB301 LogonGUID: {1fd837bc-4296-4fdd-d709-14e5f43a84c4} Caller User Name: NETWORK
SERVICECaller Domain: NT AUTHORITY Caller Logon ID: (0x0,0x3E4) Caller Process ID: 1248 Transited Services: - Source
:0/0 | H:3/3 | F:6/6
Összesen: 247 / Kijelölve: 1
Színvilág:
Money Twins

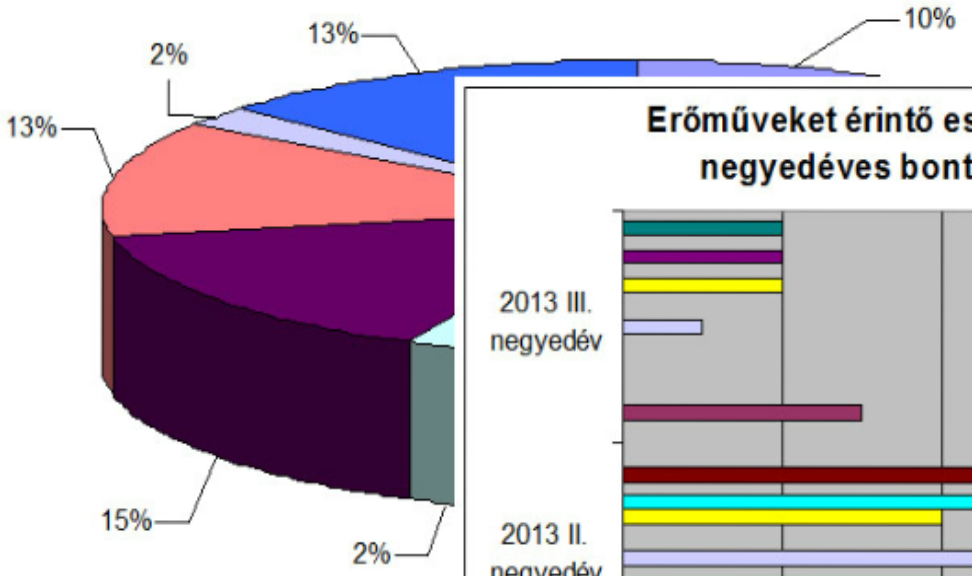
A riportok időtartama: 2012-04-22 - 2012-05-06

Küldés 62/62 (100%) Fogadás 62/62 (100%) Rajzolás 42/42 (100%)

MINDENT lekérdez | AKTUÁLISAT lekérdez | ELAVULTAKAT lekérdez | Nyomtatás

Statisztikák | Tendenciák | Eltérés diagrammok | Eltérés táblázatok | Login statisztikák | Hiba gócok | Fájl hozzáférések

Események megoszlása szektoronként 2012-ben

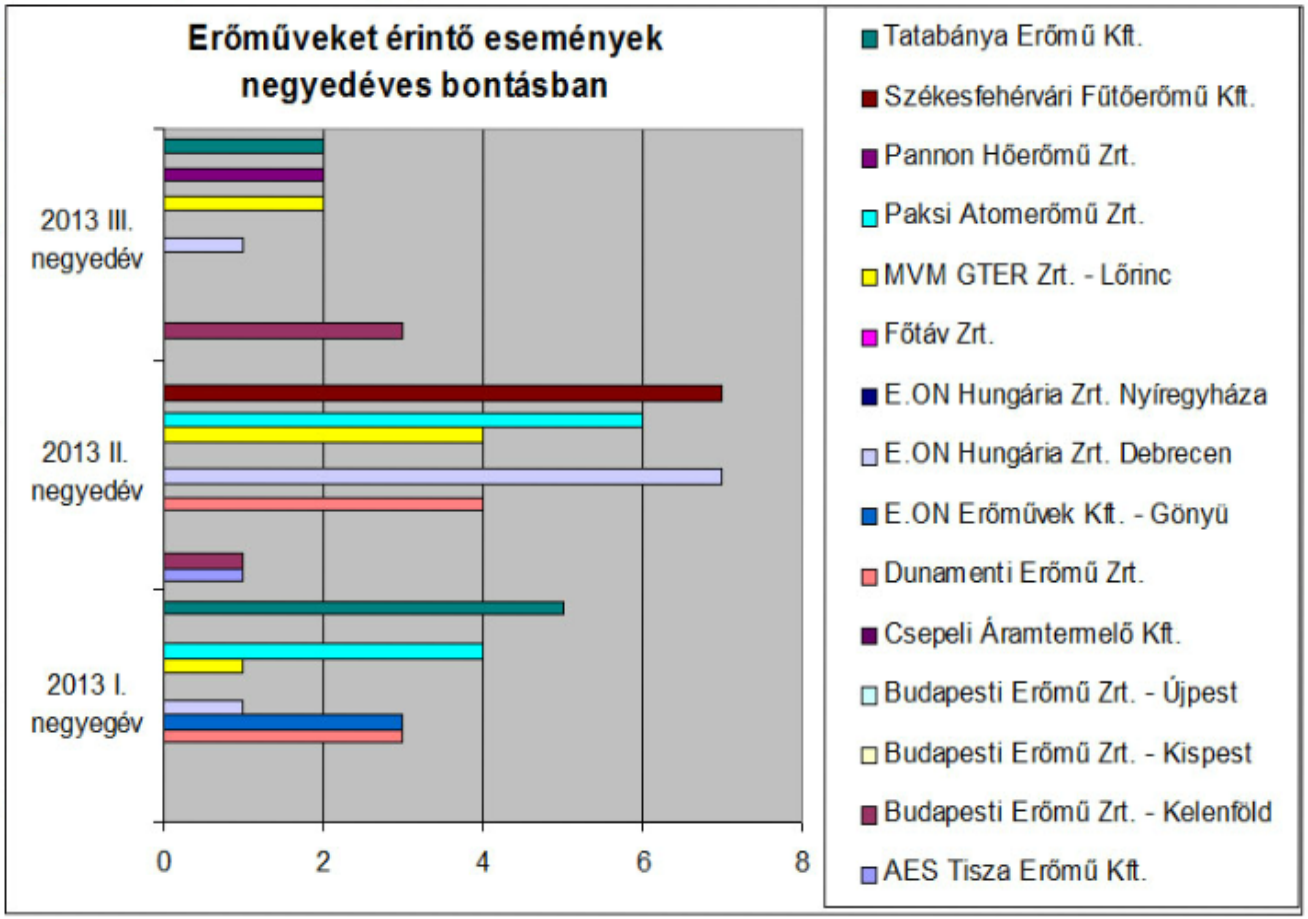


száma

291

74

Erőműveket érintő események negyedéves bontásban



[-] Top-10 sikeres su indító account

Százalékos eloszlá

a0941601 (0%)

Köszönöm a megtisztelő figyelmet!

DISASTER MANAGEMENT

Az előadással kapcsolatos kérdéseiket az

okf.iparbiztonsag@katved.gov.hu e-mail címre várjuk.