Puskás Tivadar Közalapítvány

PTA CERT-Hungary

Nemzeti Hálózatbiztonsági Központ

PTA CERT HUNGARY

NEMZETI HÁLÓZATBIZTONSÁGI KÖZPONT

A CERT-Hungary új, értéknövelt hálózatbiztonsági szolgáltatása (CERT-VAS)

18. HTE Infokommunikációs Hálózatok és Alkalmazások

Konferencia és Kiállítás

2012. október 10-12

Nemzeti Hálózatbiztonsági Központ CERT-Hungary

- **A Puskás Tivadar Közalapítvány (PTA) keretében működő Nemzeti Hálózatbiztonsági Központ (NHBK) a magyar kormány hálózatbiztonsági központja.**
- A közigazgatási hálózatbiztonsági központ felállítása céljából a PTA az Informatikai és Hírközlési Minisztérium (IHM) támogatásával **2004-ben kezdte meg** a CERT-Hungary program beindítását.
- (**CERT** = Computer Emergency Response Team) A külföldi partnerek és szervezetek felé megőrizte a Központ a **CERT-Hungary** nevet!
- A PTA Nemzeti Hálózatbiztonsági Központ indulásakor a MeH-EKK felügyelete alatt állt, jelenleg ezt az **Nemzeti Fejlesztési Minisztérium (NFM)** gyakorolja.
- A PTA NHBK tevékenysége mögött **nonstop (7/24 órás) ügyeleti rendszer** látja el az incidenskezeléssel (megelőzéssel ill. azonnali intézkedéssel) kapcsolatos feladatokat, és **Nemzeti Kapcsolati Pontként** koordinálja a több magyarországi szervezetet érintő incidensek kezelését. (www.cert-hungary.hu)

A PTA CERT-Hungary (NHBK) szerepe

- **Kiemelt feladata: hálózatbiztonsági szolgáltatások nyújtása a támogatott közigazgatási szervek és az üzleti szféra intézményei részére** (felkészítés, megelőzés, információmegosztás, incidenskezelés és koordináció, oktatás, gyakorlatok).
- Az NHBK emellett a **kritikus információs infrastruktúrák védelme** terén is fontos szerepet tölt be: mint közreműködő szervezet látja el (7/24 órás lefedettséggel) a **Nemzeti Média- és Hírközlés Hivatal (NMHH) Országos Informatikai és Hírközlési Főügyelet ügyeleti feladatait.**
- A PTA NHBK egyben szerepet vállal **a hálózati- és információbiztonság szabályozásának előkészítésében is:** részt vesz az elektronikus információbiztonsági törvény előkészítésében és az NFM által szabályozandó kormányzati információbiztonsági feladatokban.
- Az NHBK közfeladatként **az informatikai és hálózati biztonsággal kapcsolatos tudatosság növelését** is felvállalta. (lsd. www.biztonsagosinternet.hu ill. káros tartalom bejelentésére szolgáló hotline felület, 2011. májusától)

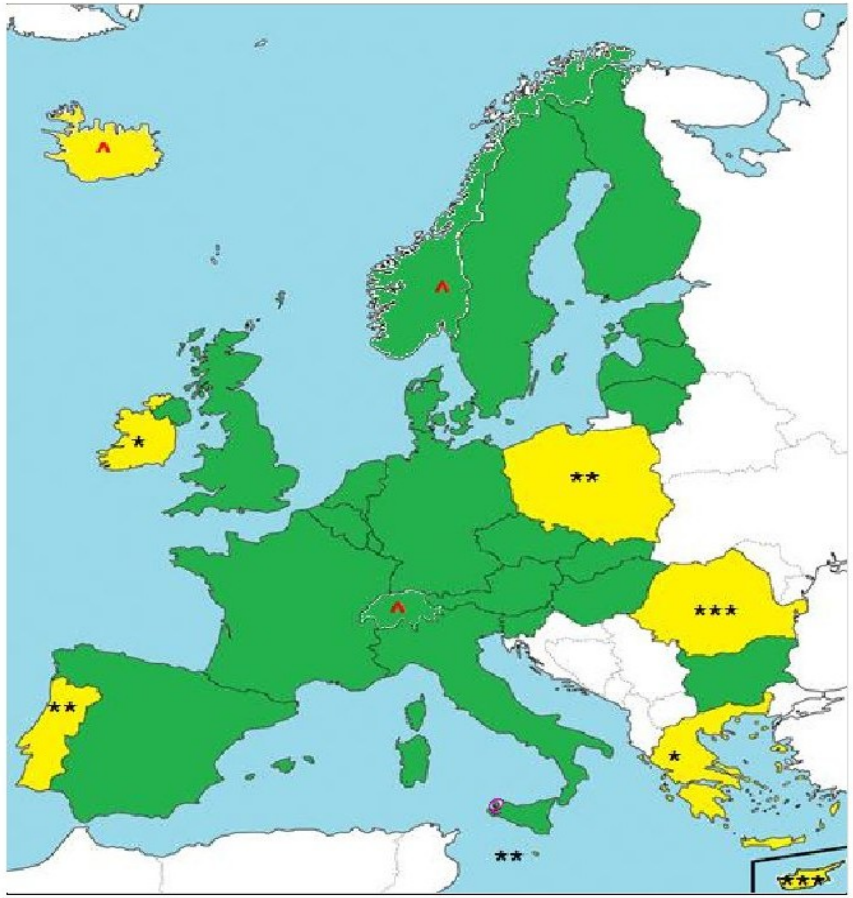
Nemzetközi kapcsolatok – PTA CHK

- A PTA CHK akkreditált tagja az **Európai Kormányzati CERT**-ek Csoportjának (**EGC;** www.egc-group.org).
- Teljes jogú tagja a Magyarország mellett a 14 legfejlettebb állam kormányzati szerveit tömörítő **International Watch and Warning** szervezetnek.
- A CHK nemzetközi elismertségét jelzi, hogy megkapta a hálózatbiztonsági központok világszervezetének (**Forum of Incident Response Teams**) és európai szervezetének (**TF-CSIRT**) akkreditációját (**Trusted Introducer**) is. (www.first.org; www.trusted-introducer.nl)
- A PTA NHBK (CHK) nemzetközi képviselője tölti be az Európai Hálózati és Információ Biztonsági Ügynökség (**ENISA)** alelnöki pozícióját.
- **Nemzetközi gyakorlatok:** CyberStorm (USA, IWWN), Cyber Europe (EU), CMX11 (NATO), Cyber Coalition 2011 (NATO) – 2012 ősz: EU, NATO gyakorlatok!
- **INHOPE** – káros tartalom hotline-ok nemzetközi szervezete

Kormányzati/nemzeti CERT-ek Európában

(ENISA, 2009)

National / Governmental CERTs in the EU and EFTA countries[1]

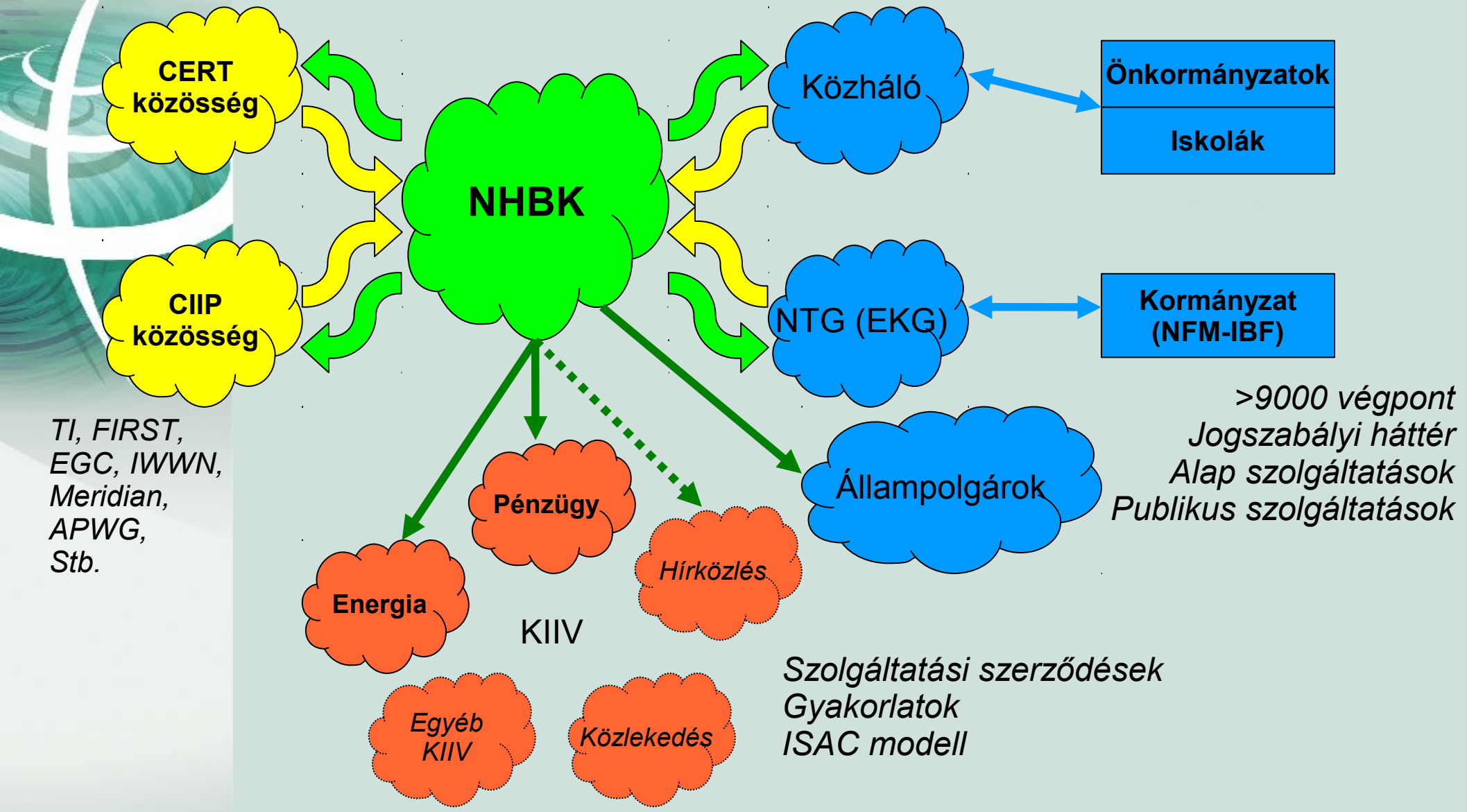


Green:	Official national / governmental CERT.
Yellow:	Either no official national / governmental CERT or national / governmental CERT not fully operational yet
*	no nat/gov CERT
**	national CERT w/o mandate ("de facto national CERT")
***	recently established teams - not fully operational yet
^	EFTA countries

Hazai együttműködések

- **A PTA NHBK kormányzati jellegének köszönhetően egyben nemzeti koordinációs pontként is működik, mely tevékenység keretét a hálózatbiztonság terén működő vagy ahhoz kapcsolódó civil, kormányzati és üzleti szervezetekkel kötött együttműködési megállapodások szabják meg.**
- **Együttműködési megállapodás került aláírásra – többek között - a következő szervezetekkel:** Nemzeti Nyomozóiroda, Pénzügyi Szervezetek Állami Felügyelete (PSZÁF), BME Vírus Kompetencia Központ, eSec.hu konzorcium, MTA SZTAKI, HUN-CERT, ISACA – Információrendszer Ellenőrök Egyesülete, Magyar Bankszövetség, Magyar Nemzeti Bank, Magyar Tartalomipari Szövetség, VirusBuster, Magyar Posta Zrt., MÁV Zrt., Budapesti Művelődési Központ, KEK-KH, Információs Társadalomért Alapítvány, Internet Szolgáltatók Tanácsa; *a káros és illegális tartalommal foglalkozó hot-line működtetése* miatt a bűnüldöző szervezetekkel, NMHH-val, Kék Vonal Gyermekkrízis Alapítvánnyal, a Nemzetközi Gyermekmentő Szolgálattal.

Támogatott szervezetek



TI, FIRST, EGC, IWWN, Meridian, APWG, Stb.

>9000 végpont
Jogszabályi háttér
Alap szolgáltatások
Publikus szolgáltatások

Szolgáltatási szerződések
Gyakorlatok
ISAC modell

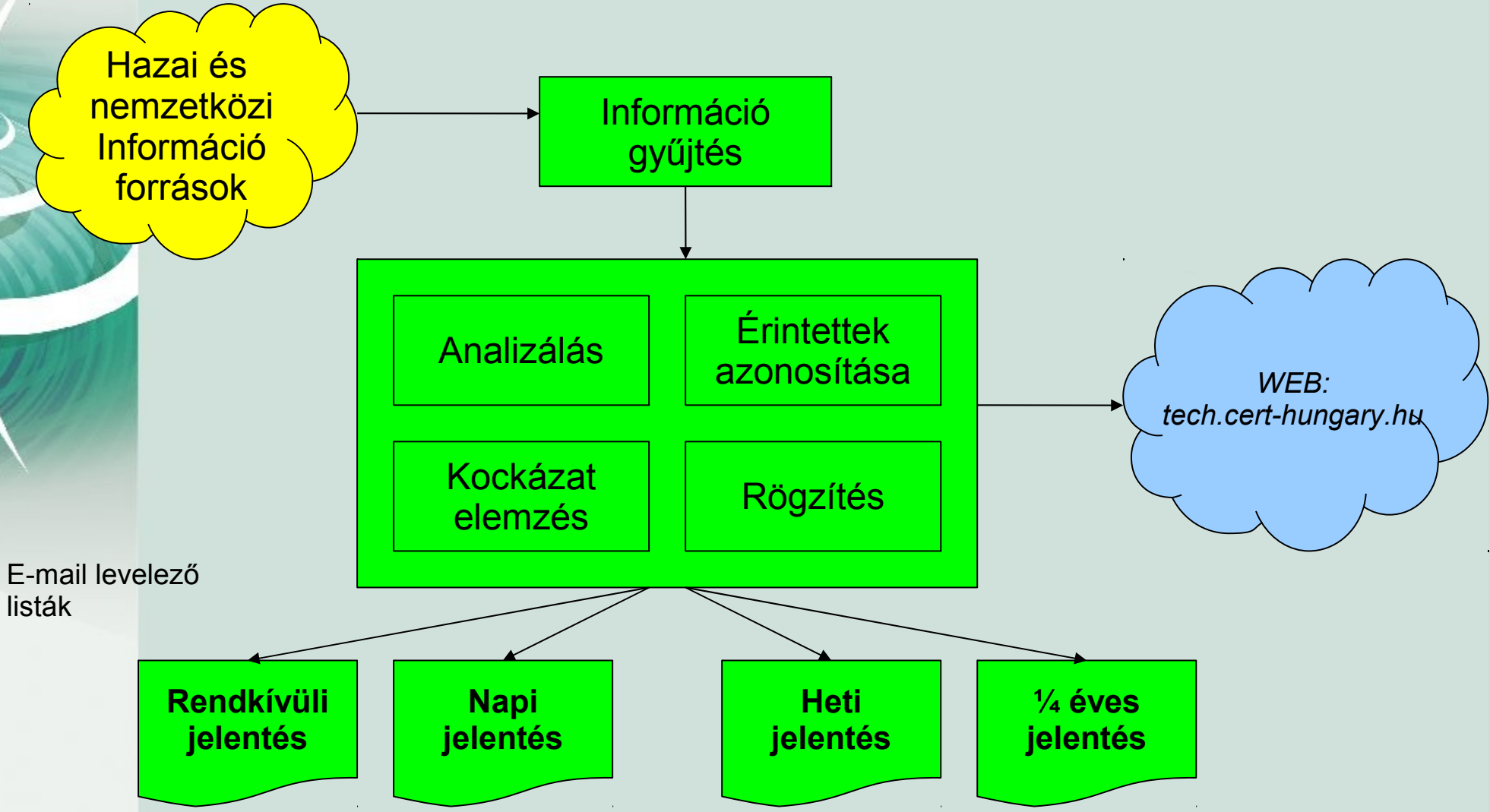
Információ-megosztó és incidens-kezelő munkacsoportok (IKMCS-k)

- **Pénzügyi szektor** (2007 óta) – résztvevők: pénzügyi intézmények, PSZÁF, Bankszövetség, Nemzeti Nyomozó Iroda, Ügyészség. Munkacsoporti ülések (előadások, közös témák megvitatása, aktuális fenyegetettségek, incidensek), közös éves gyakorlatok (COMEX), közös honlap
- **Energia szektor** (2008 óta) – információ megosztás, honlap, ágazatközi gyakorlatokba való bevonás
- **Telekommunikációs szektor** – 2007 óta (lsd. OIHF is), információ megosztás, ágazatközi gyakorlatokba való bevonás
- **Kormányzati IKMCS** – NFM által létrehozva 2011-ben, mintegy 30 intézmény bevonásával – munkacsoporti ülések, portál – hírek, rendkivüli események (CERT által)

Információ-megosztás

- Preventív szolgáltatásként **helyzetértékelések, elemzések készítése,** amelynek keretében nemzetközi hálózatbiztonsági és kritikus információs infrastruktúra védelmi hálózatok hálózatbiztonsági (fenyegetések, sérülékenységek, támadások és ezen kockázatok kezelése) tapasztalatainak, megfigyeléseinek értékelése (lsd.: pl. http://www.cert-hungary.hu/node/171)
- A szolgáltatást igénybe vevő intézmények számára a PTA CERT-Hungary rendszeres időközönként **jelentések formájában** (napi, heti, negyedéves, éves viszonylatban) elemzi és értékeli az internet felől, az intézményeket érintő fenyegetéseket (pl. phishing tevékenység, botnetek, vírusok, trójai programok, stb.) és azok kockázatait.
- **Központi rendszer – logelemzés** (központi rendszert üzemeltetők és felügyelő részére zártkörű információ-megosztás)

Információ-megosztás - jelentések



PTA CHK napi jelentés (napjainkban)

Napi jelentés 2012. február 08.
07:00 és február 09. 07:00 közötti időszakról

Sérülékenységek

CH-6379		***Kockázati besorolás***	2. Alacsony
Publikálva 2012.02.08.	Az IBM Cognos TM1 olyan sérülékenységét jelentették, amelyet a támadók kihasználhatnak cross-site scripting (XSS/CSS) támadások indítására.		
	http://tech.cert-hungary.hu/vulnerabilities/CH-6379		
CH-6378		***Kockázati besorolás***	2. Alacsony
Publikálva 2012.02.08.	Az ISC BIND egy olyan sérülékenységét jelentették, amelyet a támadók kihasználhatnak bizonyos biztonsági szabályok megkerülésére.		
	http://tech.cert-hungary.hu/vulnerabilities/CH-6378		
CH-6377		***Kockázati besorolás***	4. Magas
Publikálva 2012.02.08.	Az Oracle ismertette az Adobe Flash Player sérülékenységeit, amelyet a Solaris tartalmaz. A támadók ezeket a sérülékenységeket kihasználhatják bizonyos biztonsági szabályok megkerülésére és a felhasználó sérülékeny rendszerének feltörésére.		
	http://tech.cert-hungary.hu/vulnerabilities/CH-6377		
CH-6376		***Kockázati besorolás***	3. Közepes
Publikálva 2012.02.08.	A zenon két sérülékenységét jelentették, amelyeket a támadók kihasználhatnak a sérülékeny rendszer feltörésére.		
	http://tech.cert-hungary.hu/vulnerabilities/CH-6376		
CH-6375		***Kockázati besorolás***	3. Közepes
Publikálva 2012.02.08.	Az Avaya Interaction Center sérülékenységét jelentették, amelyet a támadók kihasználhatnak a sérülékeny rendszer feltörésére.		
	http://tech.cert-hungary.hu/vulnerabilities/CH-6375		
CH-6374		***Kockázati besorolás***	2. Alacsony
Publikálva 2012.02.08.	A PHP több sérülékenységét és biztonsági hibáját is jelentették, amelyek közül van egy ismeretlen hatású, a többi sérülékenységet a támadók és rosszindulatú felhasználók kihasználhatják egyes biztonsági szabályok megkerülésére, valamint a támadók szolgáltatás megtagadást (DoS - Denial of Service) is okozhatnak.		
	http://tech.cert-hungary.hu/vulnerabilities/CH-6374		

PTA CHK napi jelentés

CH-6373		***Kockázati besorolás***	3. Közepes
Publikálva 2012.02.08.	Az Apache CXF olyan sérülékenységét jelentették, amelyet a támadók kihasználhatnak bizonyos biztonsági szabályok megkerülésére.		
	http://tech.cert-hungary.hu/vulnerabilities/CH-6373		
CH-6372		***Kockázati besorolás***	2. Alacsony
Publikálva 2012.02.08.	A HP ismertette a HP-UX sérülékenységeit, amelyeket a támadók kihasználhatnak szolgáltatás megtagadás (DoS - Denial of Service) okozására.		
	http://tech.cert-hungary.hu/vulnerabilities/CH-6372		

Káros szoftver

Megnevezés	PWS:Win32/Dofoil.D	***Kockázati besorolás***	2. Alacsony
Publikálva 2012.02.08.	A PWS:Win32/Dofoil.D egy olyan trójai, amely felhasználó neveket és jelszavakat lop el, elsősorban bizonyos FTP alkalmazásokhoz és Microsoft Outlookhoz tartozóakat.		
	http://www.securityhome.eu/malware/malware.php?mal_id=13054849554f321f935991b7.44240791		
	http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=PWS%3AWin32%2FDofoil.D		
	http://www.threatexpert.com/report.aspx?md5=2eab831c64d509a2a84ac9db207f9af0		
Megnevezés	Worm:JS/Depslear.A	***Kockázati besorolás***	2. Alacsony
Publikálva 2012.02.08.	A Worm:JS/Depslear.A egy JavaScript féreg, amely Facebook bejegyzéseken keresztül terjed. A Worm:JS/Depslear.A ellenőrzi a böngésző Facebook web oldalakhoz kapcsolódó cookie-jait. Ha talál ilyet, akkor a cookie-kon keresztül hozzáfér a felhasználó ismerőseinek listájához, majd üzeneteket küld nekik. Ismert még JS/FBspam (AVG) néven is.		
	http://www.securityhome.eu/malware/malware.php?mal_id=12980158564f321f94929bb1.67507609		
	http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3AJS%2FDepslear.A...		
	http://www.avgthreatlabs.com/webthreats/info/js-fbspam/		

A PTA CERT-Hungary Központ értéknövelt alapszolgáltatása - CERT-VAS

CERT-VAS (VAS = value added services)

Adatbázisba szervezett sérülékenységi, fenyegetettségi, káros szoftver, incidens információk; amelyek szervezetekre testreszabottan lekérdezhetők.

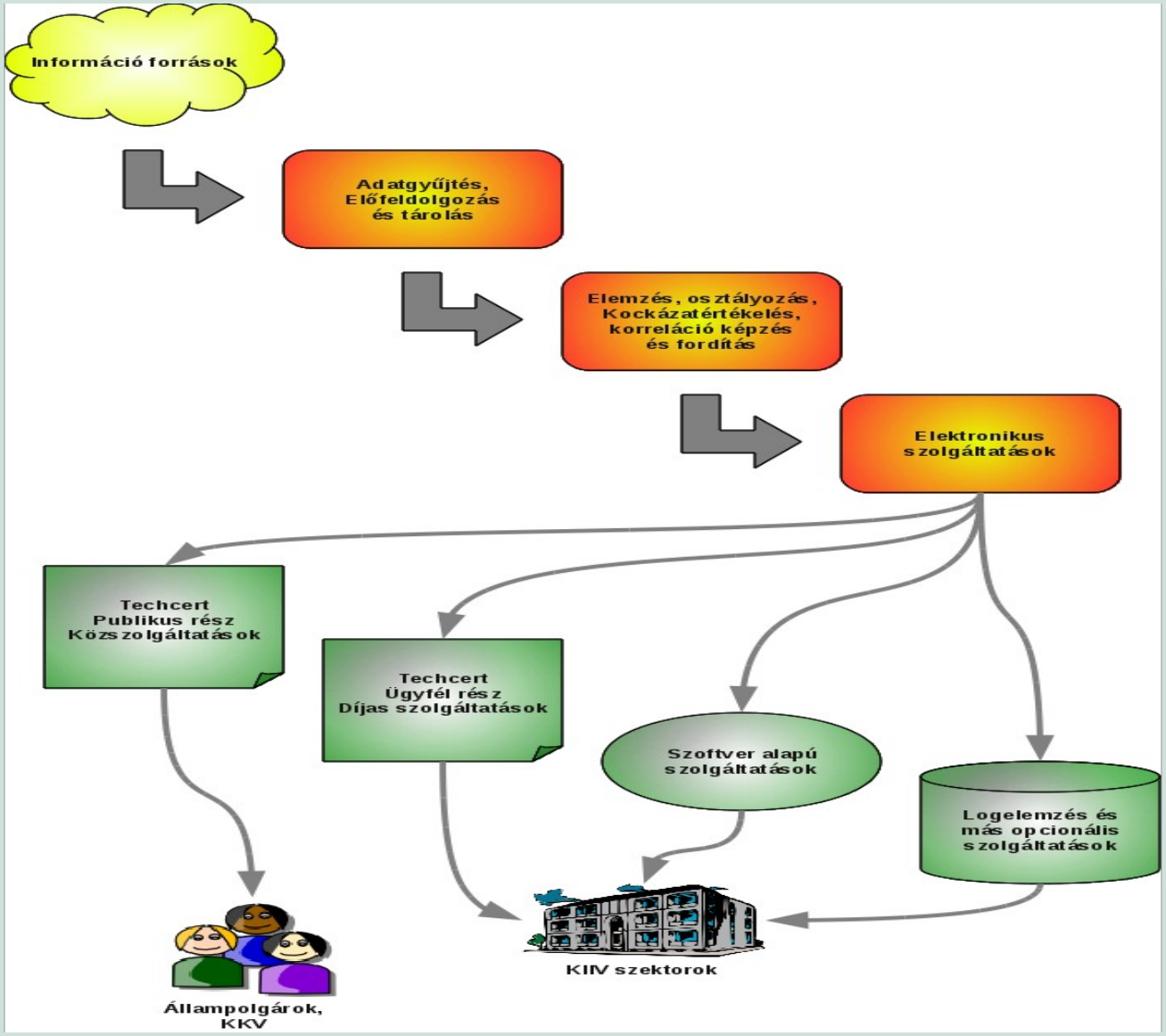
- ***Felhasználói profil készítése*:** Az ügyfél megadhatja a szervezeténél használt szoftvereket és személyre/szervezetre szabott információkat kaphat
- ***Keresés*:** Felhasználói profil nélkül is kereshet az ügyfél a Sérülékenységi adatbázisban
- ***Speciális kockázatértékelés*:** A sérülékenységek elterjedéséhez és kihasználhatóságához kapcsolódó kockázatértékelés (pl. Common Vulnerability Scoring System alapján) – kvázi feladat priorítás!
- ***Speciális jelentések, riportok*:** Az ügyfél az alap szolgáltatásoktól eltérő paraméterű jelentéseket kaphat (pl. figyelt szoftverek)
- ***Analízisek, speciális lekérdezések*:** Bizonyos keretek között lekérdezhető az adatbázis (pl. egy új szoftver beszerzése előtt elemezni lehet a szoftverek sérülékenységi mutatóit és a javításuk gyakoriságát)

IT üzemeltetési és biztonsági integrált és koncentrált naprakész kontroll információk!

2013-tól igénybevehető szolgáltatás!

CERT-VAS szolgáltatási koncepció

Alapelvek:



CERT-VAS rendszer

A teljes szolgáltatási rendszer célja, hogy a PTA CERT-Hungary Központ preventív szolgáltatásait elektronikus szolgáltatásként adja a felhasználók részére. Az elektronikus szolgáltatási felület segítségével kiváltható a nagy mennyiségű, többször a felhasználót nem érintő információ áradat.

A rendszer célja, hogy a felhasználók a rájuk vonatkozó információkat időben, megfelelő kockázatértékeléssel ellátva kapják meg.

A CERT-VAS rendszer az alábbi folyamatokon keresztül valósítja meg a kitűzött cél elérését:

- Információ gyűjtés, előfeldolgozás és tárolás
- Elemzés, osztályozás, kockázat értékelés, korreláció képzés és fordítás
- Elektronikus szolgáltatások

A folyamatok során az információ típusok kerülnek feldolgozásra:

- Sérülékenységek
- Hírek
- Kártékony kódok
- Fenyegetettségek
- Exploitok

CERT-VAS rendszer – információforrás példák

Forrásegyedi sérülékenységek:

- OSVDB (**O**pen **S**ource **V**ulnerability **D**ata**B**ase)
- NVD (National Vulnerability Database)
- CVE (Common Vulnerabilities and Exposures database)

Advisory:

- Secunia
- Security Focus

Malware:

- Kaspersky
- Mc-Afee
- F-Secure
- Sophos

News:

- Team Cymru
- Index tech rovat
- IT Café

Fenyegetettségi adatok:

- Shadow Server Foundatation
- Arakis (lengyel érzékelő)
- Microsoft

A források használata:
szerződések alapján,
együttműködések alapján,
CERT közösségi információk,
publikusak

CERT-VAS rendszer belső folyamatok

Az **információ gyűjtés, előfeldolgozás és tárolás** egy teljesen automatizált folyamat, amelynek során a kijelölt információ forrásokból egy adatgyűjtő eszközrendszer segítségével begyűjtjük az információkat, feltöltjük az információ típushoz tartozó adatsémákat, ahol lehetséges az egyes egyedi rekordokat egymással logikailag összekapcsoljuk és letároljuk az információkat adatbázisban.

Mindezek által a különböző információ típusok egymással való összefüggései is nyomonkövethetővé válnak, illetve a különböző forrásból származó, de egyazon információt leíró adatok összefűzésre kerülnek, így megkönnyítve azok áttekinthetőségét és feldolgozhatóságát a felhasználók számára.

CERT-VAS rendszer belső folyamatok

Az input adatok összegyüjtésével a rendszer leglényegesebb belső (majdnem teljesen automatizált) eljárásai lépnek működésbe az: **elemzés, osztályozás, kockázat értékelés, korreláció képzés és fordítás**.

A két legfontosabb (hozzáadott érték) elem:

Egyes információ típusokhoz (pl. egyedi sérülékenységekhez) beszerezhetők **kockázatértékelések**, azonban az elektronikus szolgáltatás részére átadandó információkhoz a PTA CERT-Hungary Központ a CERT közösség által használt CVSS kockázatértékelési mechanizmusát alkalmazza.

A másik fontos elem a **korreláció képzés**: célja, hogy a különböző információ típusok között a létező kapcsolatok felderítésre, kimutatásra és összekapcsolásra kerüljenek (pl. sérülékenységet, az azt kihasználó exploit kód, az azt felhasználó kártékony szoftver, és az így megvalósult fenyegetettség, illetve az ezekről szóló hírek, leírások).

CERT-VAS rendszer belső folyamatok

Az **elektronikus szolgáltatások** az ügyfél oldali hozzáférés és megjelenítés lehetőségeit és módjait takarja. Így ezen kliens felületen keresztül lehet majd:

- a rendszerbe regisztrálni
- a szervezet informatikai környezetének (szoftvereinek) profilját megadni ill. napra készen tartani; egyedi lekérdezések, jelentések kialakítása
- a management funkciókat kialakítani (feladatok kiadása ill. azok végrehajtásának kontrollja)
- a rendszer információit összekapcsolni (interface-ek által) belső kontroll rendszerekkel

CERT-VAS dashboard

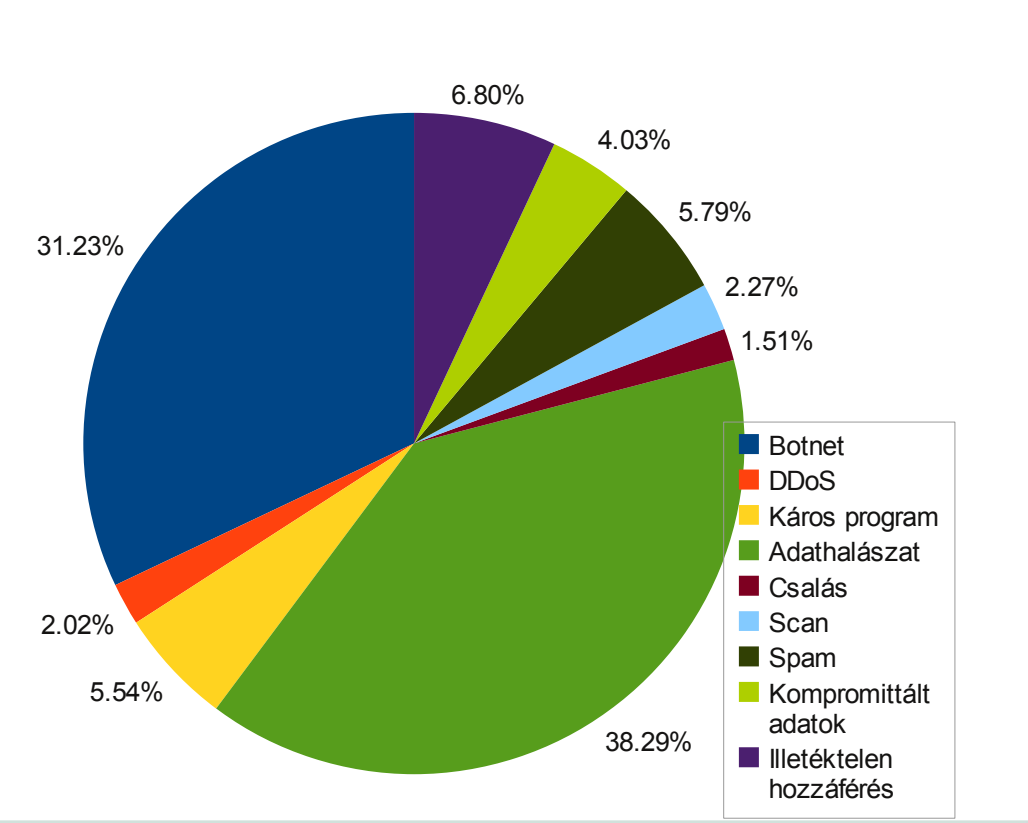
látványterv:

Incidens-kezelés

A PTA CERT-Hungary Központ által kezelt
incidensek eloszlása 2011-ben (zárójelben a 2010. évi adatok)

A PTA CERT-Hungary Központ a 2011. év során összesen **401** (333) **db incidens bejelentést** regisztrált és kezelt, incidenskezelési-koordináció **1754** (654) szálon indult.

Az incidenskezelésbe bevont szolgáltató szervezetek száma: **184** (103).



A PTA CERT-Hungary Központ (NHBK) opcionális szolgáltatásai

Posztaktív, értéknövelt információ- és hálózatbiztonsági, egyedi ill. szervezetre szabott szolgáltatások

- Incidenskezelési folyamat értékelése
- Egyedi (testre/szervezetre szabott) szolgáltatások:
  - a felmért informatikai rendszer tervezésére, fejlesztésére vonatkozó javaslatok kidolgozása
  - Attack and Penetration tesztek
  - Sérülékenységi auditok
- logelemzési szolgáltatás
- incidens analízisek
- információ- és hálózatbiztonsági (incidens-kezelési) szabályozások
- IT biztonsági ill. kibervédelmi gyakorlatok
- oktatások (informatikusok, felhasználók, vezetők)

NEMZETI HÁLÓZATBIZTONSÁGI KÖZPONT

PUSKÁS TIVADAR KÖZALAPÍTVÁNY
CERT-Hungary Központ
(Nemzeti Hálózatbiztonsági Központ)

Elérhetőségeink:

1063 Budapest, Munkácsy M. u. 16.

Levélcím: 1398 Budapest, Pf.: 570.

Tel.: (1) 301-20-30
Fax.: (1) 353-19-37

web: www.cert-hungary.hu

Ügyelet: cert@cert-hungary.hu

Tel.: +36-1-301-2079
Fax.: +36-1-332-3774

www.cert-hungary.hu

tech.cert-hungary.hu

www.biztonsagosinternet.hu