# Puskás Tivadar Közalapítvány
# CERT-Hungary Központ

**dr. Angyal Zoltán**
**hálózatbiztonsági igazgató**

**2009**

# PTA CERT-Hungary Központ

- **A Puskás Tivadar Közalapítvány (PTA) keretében működő CERT-Hungary Központ (CHK) a magyar kormány hálózatbiztonsági központja.** ***(CERT = Computer Emergency Response Team)***
- A közigazgatási hálózatbiztonsági központ felállítása céljából a PTA az Informatikai és Hírközlési Minisztérium (IHM) támogatásával **2004-ben kezdte meg** a CERT-Hungary program beindítását.
- A PTA CERT-Hungary Központ a **Miniszterelnöki Hivatal Elektronikuskormányzat-központ (MeH-EKK) felügyelete alatt áll.**
- A PTA CHK CERT tevékenysége mögött **nonstop (7/24 órás) ügyeleti rendszer** látja el az incidens kezeléssel (megelőzéssel ill. azonnali intézkedéssel) kapcsolatos feladatokat. (www.cert-hungary.hu)

# A PTA CERT-Hungary szerepe

- Kiemelt feladata: **hálózatbiztonsági szolgáltatások nyújtása** a támogatott közigazgatási szervek és az üzleti szféra intézményei részére (felkészítés, megelőzés, incidenskezelés, oktatás).
- A CHK emellett a **kritikus információs infrastruktúrák védelme** terén is fontos szerepet tölt be: a 27/2004. (X.6.) számú IHM rendelet 19/2005. (XII.27.) számú módosítása folytán, mint közreműködő szervezet látja el (7/24 órás lefedettséggel) a **Nemzeti Hírközlés Hivatal (NHH) Országos Informatikai és Hírközlési Főügyelet ügyeleti feladatait.**
- A PTA CHK egyben szerepet vállal **a hálózati- és információbiztonság szabályozásának előkészítésében is:** részt vesz a MeH EKK részére az informatikai és információ biztonság terén kiadandó ajánlások kidolgozásában, valamint a PSZÁF internetes bankolás biztonságára vonatkozó ajánlásához szakmai anyagot készít.
- A CHK közfeladatként **az informatikai és hálózati biztonsággal kapcsolatos tudatosság növelését** is felvállalta. (ld. www.biztonsagosinternet.hu)

# Nemzetközi kapcsolatok

- 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 CHK Testület elnöke tölti be az Európai Hálózati és Információ Biztonsági Ügynökség (**ENISA)** alelnöki pozícióját.

# Hazai együttműködések

- **A PTA CHK 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 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, Infomediátor, Magyar Posta Zrt, MÁV Zrt., Budapesti Művelődési Központ.

# A PTA CHK alapszolgáltatásai

- Preventív szolgáltatásként **helyzet értékelések, elemzések készítése,** melynek keretében nemzetközi hálózatbiztonsági és kritikus információs infrastruktúra védelmi hálózatok hálózatbiztonsági (fenyegetések, sérülékenységek, támadások és ezen kockázatok kezelése) tapasztalatainak, megfigyeléseinek értékelését nyújtjuk ügyfeleink részére.
- A szolgáltatást igénybe vevő intézmények számára a PTA CHK rendszeres időközönként **jelentés formájában** (napi, heti, havi, negyedéves, éves viszonylatban) elemzi és értékeli az Internet felől, az intézményeket érintő fenyegetéseket (pl. phishing tevékenység, botnetek, vírusok, trójai programok, stb.) és azok kockázatait.

PTA CERT HUNGARY

# PTA CHK napi jelentés

**Napi jelentés 2009. január 22.**
**07:00 és január 23. 07:00 közötti időszakról**

| Esemény megnevezése | Érintett rendszerek | Kockázati besorolás | Esemény rövid leírása |
|---|---|---|---|
| Joomla BazaarBuilder Shopping Cart Component "cid" SQL befecskendezés sérülékenység | Joomla BazaarBuilder Shopping Cart5.x | Közepes | A Joomla BazaarBuilder Shopping Cart olyan sérülékenysége vált ismertté, melyet kihasználva rosszindulatú támadók SQL befecskendezéses támadásokat tudnak végrehajtani.<br>További információ |
| Cisco Security Manager biztonsági sérülékenység | Cisco Security Manager (CSM) 3.x | Közepes | Egy sérülékenységet jelentettek a Cisco Security Manager programban, amelyet rosszindulatú támadók kihasználhatnak a biztonsági előírások megkerülésére.<br>További információ |
| Apple QuickTime MPEG-2 Playback Component adatbevitel ellenőrzési sérülékenység | Apple QuickTime MPEG-2 Playback Component 7.x | Magas | Egy sérülékenységet jelentettek az Apple QuickTime MPEG-2 Playback Component programban, amit rosszindulatú támadók a rendszer feltörésére használhatnak ki.<br>További információ |
| Sun SPARC Enterprise M4000 / M5000 Server XSCFU biztonsági sérülékenység | Sun SPARC Enterprise Server M sorozat | Közepes | Egy sérülékenységet jelentettek a Sun SPARC M4000 / M5000 szerverekben, amelyet rosszindulatú támadók kihasználhatnak a biztonsági előírások megkerülésére és feltörhetik a sérülékeny rendszert.<br>További információ |

PTA CERT HUNGARY

# A PTA CHK alapszolgáltatásai

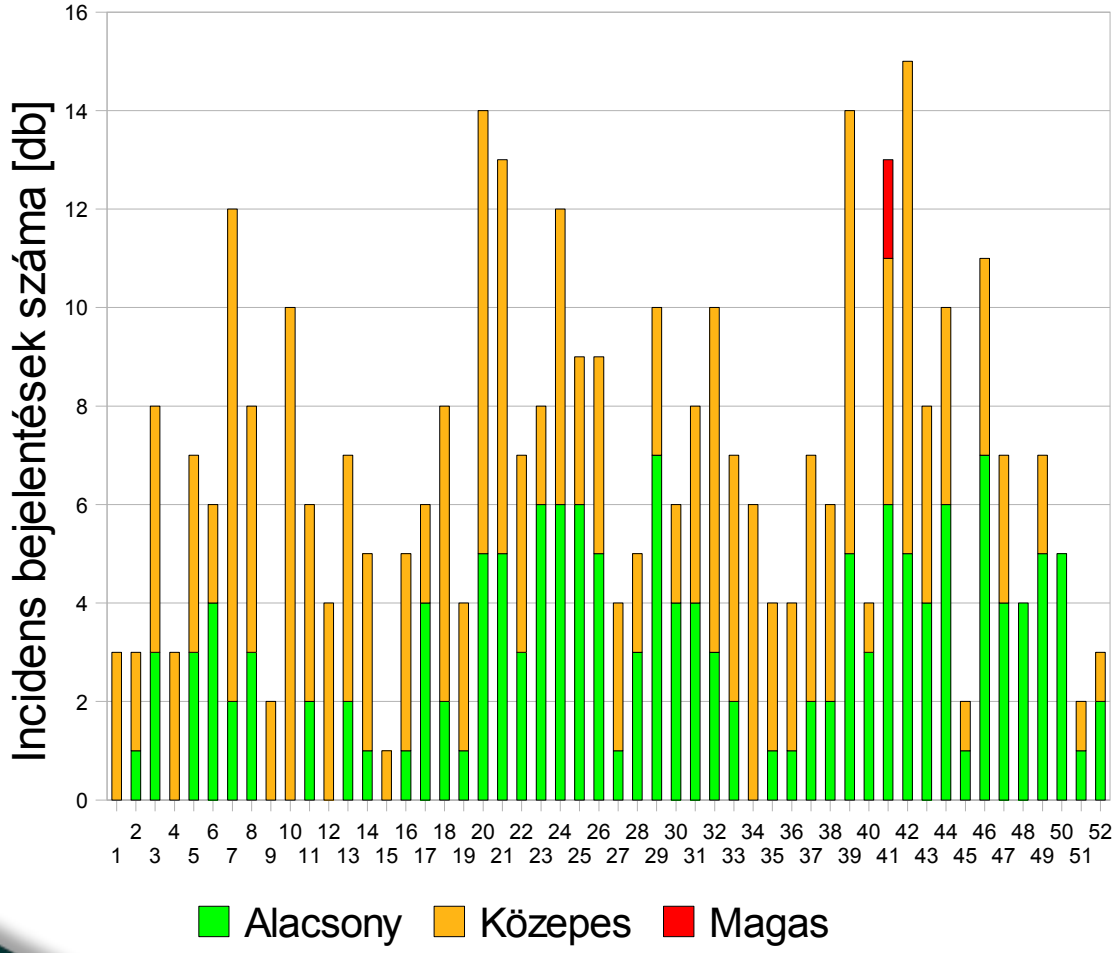
- **Incidens kezelés és koordináció keretében** a szolgáltatást igénybe vevő ügyfél részére a PTA CHK ügyelete az Incidens Kezelési Címjegyzék szerint folyamatos (7/24 órás) rendelkezésre állást biztosít. Az informatikai rendszerének Internet szegmensét ért támadásokat az ügyfél a PTA CHK ügyeleten bejelent(het)i. A PTA CHK ezt a bejelentést fogadja, kezeli és koordinálja a válaszadást.

  Bejelentéskor a PTA CHK incidensnek tekint minden, az ügyfél informatikai rendszerét **az Internet felől fenyegető rosszindulatú megnyilvánulást** (pl. az IT eszközökkel megkísérelt csalásokat, a szolgáltatás megtagadás támadásokat, a behatolási próbálkozásokat, stb.), illetve minden, az ügyfél Internet alapú szolgáltatásainak működését gátló vagy eltérítő próbálkozást (pl. adathalászat, személyiség lopás, stb.).

- **Az Incidens kezelés/koordináció szolgáltatás az ügyféllel kötött szerződés, valamint a PTA CHK incidens kezelési szabályzata alapján történik,** és ez minden esetben dokumentált folyamat. A folyamat dokumentáció alkalmas arra, hogy a PTA CHK bizonyítsa és tanúsítsa, hogy a felek a bejelentés- illetve az incidens kezeléskapcsán a legjobb tudásuk szerint jártak el.

# Incidenskezelés

A PTA CERT-Hungary Központ által kezelt incidensek eloszlása 2008-ban




A PTA CERT-Hungary Központ a 2008. év során összesen **363 db incidens bejelentést** regisztrált és kezelt, ebből :

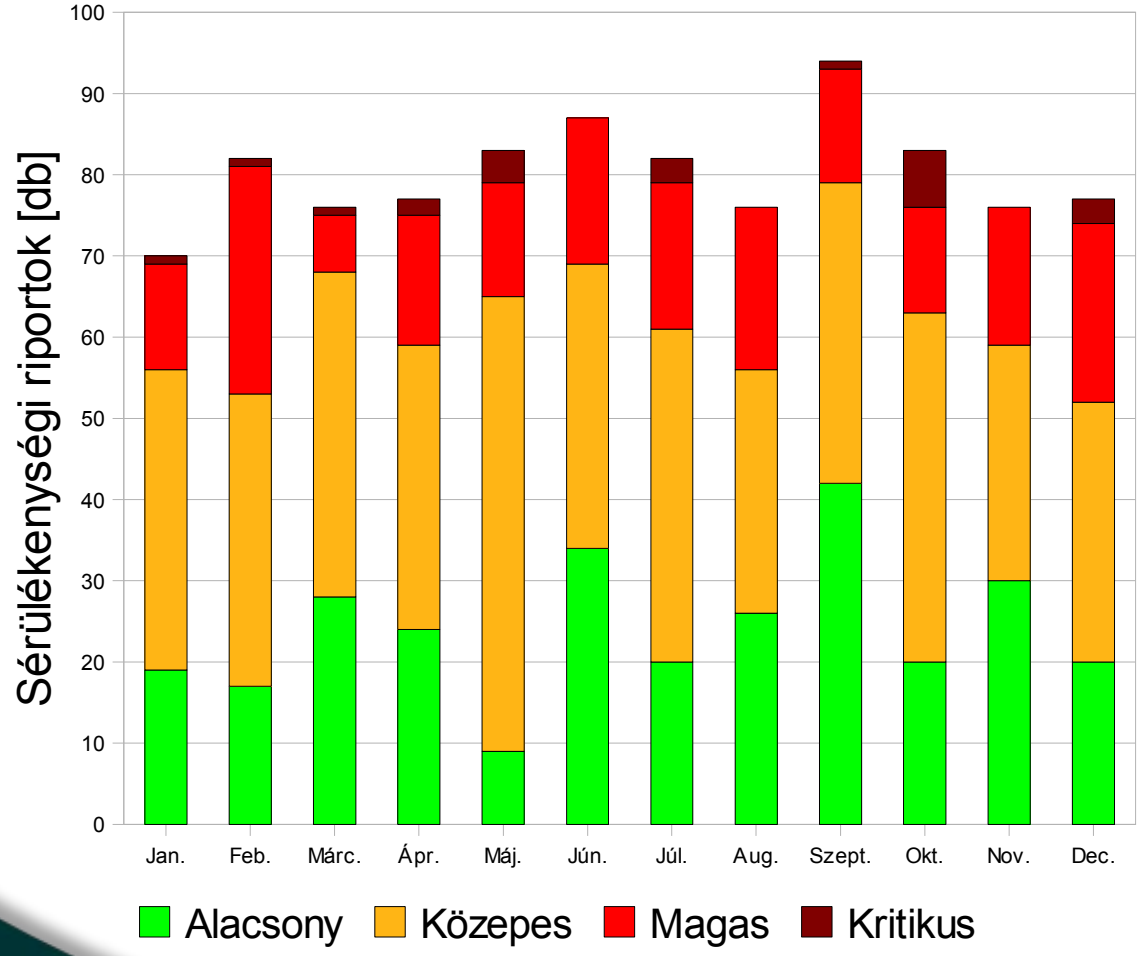
154 db alacsony
207 db közepes és
2 db magas
kockázati besorolású.

# A PTA CHK alapszolgáltatásai

- **A sérülékenység kezelési szolgáltatás keretében** a PTA CHK közhasznú tevékenysége és nemzetközi kapcsolatai révén megbízható forrásokból származó szoftver sérülékenységi információkhoz jut, amelyeket magyarra fordít és saját fejlesztésű adatbázisában helyez el, amit ügyfelei számára elérhetővé és kereshetővé tesz.
- A PTA CHK szerződéses ügyfelei számára titkosított **hozzáférést biztosít sérülékenységi adatbázisához**. A kereső rendszerből az igénylő ügyfél saját informatikai profiljához igazított információkat kap, amelyek hozzá segíthetik saját informatikai rendszere sérülékenységeinek megállapításához.
- A PTA CHK sérülékenységi adatbázisában lévő sérülékenységi információk **kockázati besorolást** kapnak. Ezen kockázatok ismeretében az ügyfél mérlegelni tudja saját informatikai rendszerének fenyegetettségi szintjét. A PTA CHK kockázat értékelését az adott sérülékenység természete, a hozzá kapcsolódó támadási és elterjedtségi mutatók határozzák meg.

# Sérülékenységkezelés

A PTA CERT-Hungary Központ által publikált sérülékenységek eloszlása havi bontásban 2008-ban



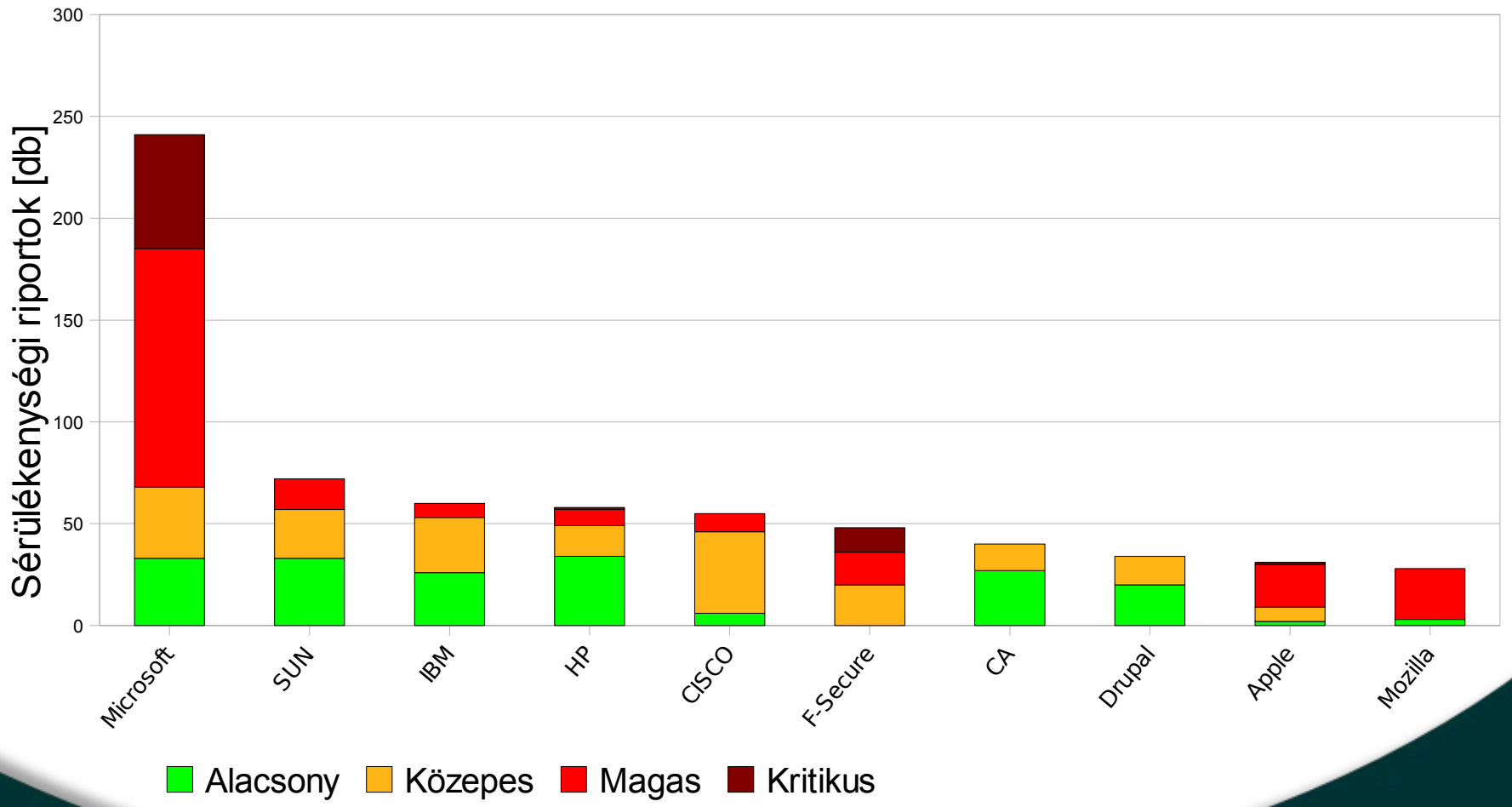

A **PTA CERT-Hungary Központ** a 2008. év során **963 db szoftver sérülékenységi információt** publikált, melyekből:

- 289 db alacsony,
- 451 db közepes,
- 200 db magas és
- 23 db kritikus

kockázati besorolású.

# Sérülékenységkezelés

## Sérülékenységi riportok eloszlása a TOP 10 gyártó termékeit illetőleg 2008-ban



# A PTA CHK alapszolgáltatásai

- **Oktatások, tréningek nyújtásával** a PTA CHK vállalja, hogy évente egy alkalommal „tűzvédelmi oktatás” jellegű, a biztonságos Internet használatát oktató képzést tart az ügyfél munkavállalói részére.
- Biztosítjuk továbbá a PTA CHK-val operatív kapcsolatba kerülő munkavállalók (rendszeradminisztrátorok, operátorok, stb.) részére az együttműködéshez szükséges **szakmai képzéseket** (pl. incidenskezelés, bejelentések, stb.).
- A PTA CHK mindezeken felül lehetőséget biztosít **vezetői szintű részvételre** a PTA CHK által megrendezésre kerülő Incidenskezelési Workshopokon.
- A PTA CHK lehetőséget biztosít **egyéb, bővebb, illetve mélyebb szakmai szintet biztosító képzésekre is**, amiket opcionális szolgáltatásként biztosít.

# A PTA CHK opcionális szolgáltatásai

*Incidens analízis*

- Az incidens analízis szolgáltatás során a PTA CHK **begyűjti** az incidensre vonatkozó információkat (a hazaiakat és a nemzetköziket egyaránt), **kielemzi** őket, majd az eredményeket átadja az ügyfél részére. A PTA CHK a vizsgálatai során feltárt tényekről, a tudomására jutó értesülésekről folyamatosan **tájékoztatja** az ügyfelet — és csak azt.
- Az ügyfél az adatok és az elemzések birtokában megteheti a szükséges lépéseket a hatóságok (pl. Nemzeti Nyomozó Iroda) vagy a társ intézmények felé. A PTA CHK önmagában a bűnüldöző szerveknél semmilyen esetben nem kezdeményez eljárást, mivel ezt csak az ügyfél kezdeményezheti.
- **Javaslatokat tesz** az ügyfél informatikai biztonsági rendszerében szükséges lépésekre. Az incidensek lezárása után incidens jelentést készít az ügyfél részére.

PTA CERT HUNGARY

# A PTA CHK opcionális szolgáltatásai

***Incidens érzékelés***

Az incidens kezelés/koordináció szolgáltatás kiegészítéseként opcionálisan választható az ügyfél internet ki/be járataihoz kapcsolható **érzékelő eszköz** (pl. honeypot/honeynet) telepítése és üzemeltetése. Az ilyen érzékelők alkalmasak a támadási kísérletek észlelésére. Az érzékelő nem az ügyfél belső hálózatára, hanem a publikus hálózati szegmensre kerül telepítésre és technológiájából fakadóan nem vizsgálja az ügyfél hálózati forgalmának információ tartalmát.

Az érzékelő műszaki paraméterei és üzemeltetési eljárásai az ügyfél számára nyíltak, szabadon megismerhetők. Az érzékelő jelzéseit a PTA CHK-hoz továbbítja, a PTA CHK azokat feldolgozza és értékeli. Az ügyfél az észlelésekről és az értékelésről is értesítést kap. A PTA CHK az ügyfél rendelkezésére bocsájtja az érzékelőin összegyűlt adatok összesített és anonimizált információit, amiből megállapítható a hazai internet biztonsági állapota.

Megjegyzés: 2009-től igénybe vehető szolgáltatás

PTA CERT HUNGARY

# A PTA CHK opcionális szolgáltatásai

*Naplóállományok elemzése*

Ebben az esetben nem kerül sor külön, az ügyfél informatikai rendszeréhez illesztett érzékelő eszköz elhelyezésére, hanem ”csak” a PTA CHK-nak átadott, az Internetet és az ügyfél hálózatát elválasztó **„tűzfal”-ról begyűjtött napló(k) adatait elemezzük.**

Mivel a tűzfal napló bejegyzések elemzése utólagos, illetve legjobb esetben is késleltetett, a PTA CHK értékelési lehetőségei is ehhez igazodnak, tehát utólagosak vagy késleltetettek. A PTA CHK jelentései a vészhelyzetet, vagy egy bizonyos fenyegetettségi szint átlépését már bekövetkezett tényként rögzítik — az ügyfélre bízva a feltárt eset és kockázatai kezelését.

# A PTA CHK opcionális szolgáltatásai

***Rendszervédelmi tanácsadás*** keretén belül

- a PTA CHK az ügyfelei részére tanácsadási szolgáltatást biztosít Internet biztonsági, CERT és kritikus információs infrastruktúra védelem témakörében. Tanácsadási szolgáltatásként a PTA CHK a következő tevékenységeket vállalja külön igény és megállapodás alapján:
  - **Incidens kezelési folyamat értékelése és a felmért rendszer fejlesztésére vonatkozó javaslatok kidolgozása**
  - **Attack and Penetration tesztek**
  - **Sérülékenységi auditok**

# A PTA CHK opcionális szolgáltatásai

***Speciális oktatási, tréning szolgáltatások,*** melynek keretén belül:

a PTA CHK vállalja, hogy az ügyféllel egyeztetett keretek között, a **hálózatbiztonsági és internet biztonsági témakörökben egyedi képzéseket** biztosít az ügyfél munkavállalói részére. A képzési forma keretében több szinten (pl. rendszergazdai, felhasználói, fejlesztői, stb.) oktatjuk a nemzetközi tapasztalatok szerinti legjobb szakmai gyakorlatot. Az elvégzett tanfolyamokon megszerzett tudást megállapodás szerint felmérjük és a tanfolyamok elvégzését oklevéllel tanúsítjuk.

PTA CERT HUNGARY

# A PTA CERT-Hungary Központ elérhetőségei

**Puskás Tivadar Közalapítvány  CERT-Hungary Központ**


**<u>Elérhetőségeink:</u>**

**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**

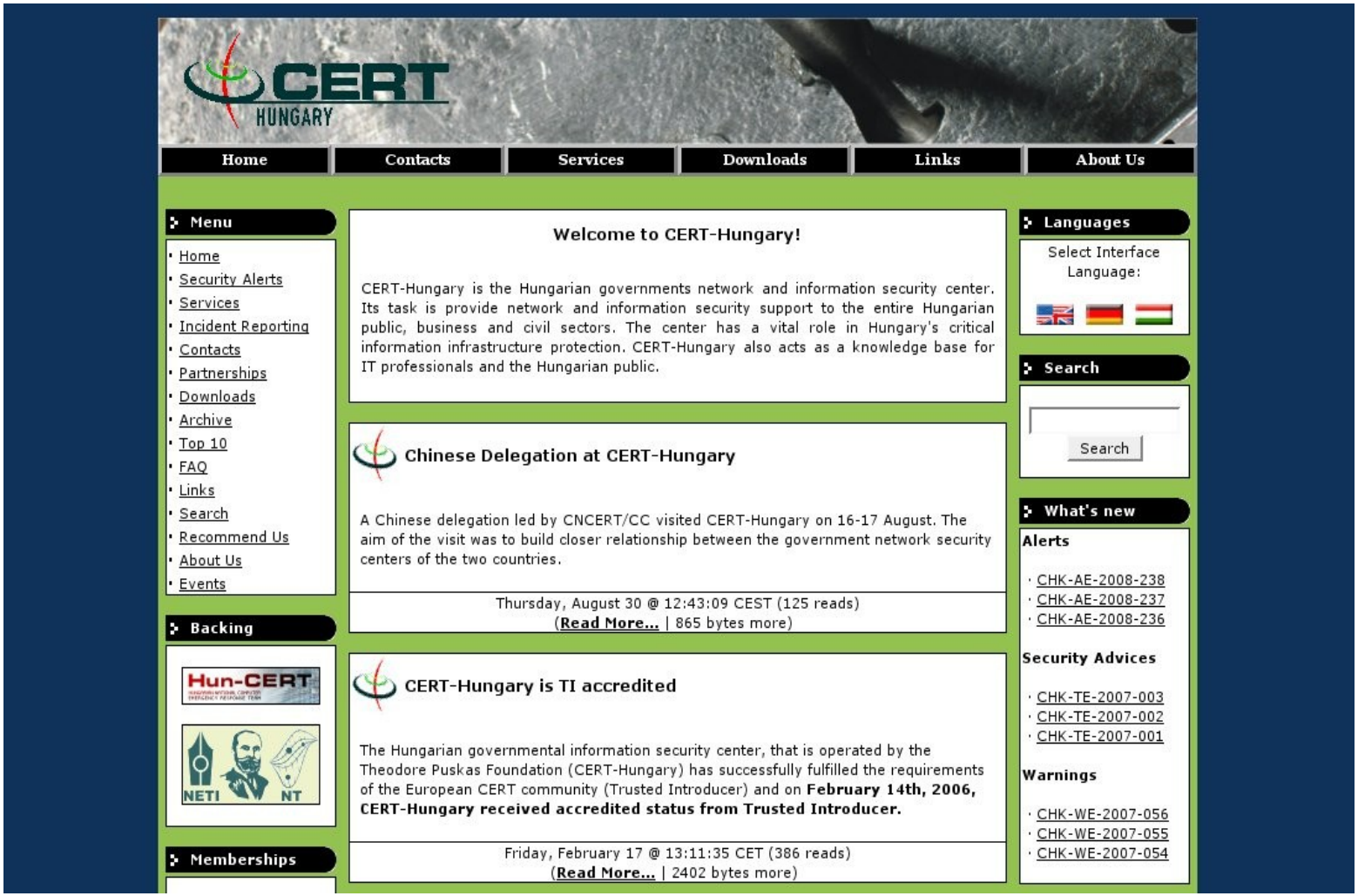
**<u>ügyelet:</u>**

**E-mail: cert@cert-hungary.hu**

**Tel.: +36-1-301-2079**

**Fax: +36-1-332-3774**

# www.cert-hungary.hu




PTA CERT HUNGARY

# www.biztonsagosinternet.hu