IT sérülékenység vizsgáló szoftverek összehasonlító elemzése

Készítették:

Törőcsik Marietta, Kozlovszky Miklós

Óbudai Egyetem

Kritikus infrastruktúra védelmi kutatások

TÁMOP-4.2.1.B-11/2/KMR-0001

MAGYARORSZÁG MEGÚJUL

A projektek az Európai Unió támogatásával valósulnak meg.

Incidensek

Érintett szervezet	Becsült kár	Egyéb
Sony	174 millió $	
Citigroup	2,7 millió $	
AT&T	2 millió $	
LinkedIN		6.458.020 jelszó
Kínai kereskedelmi oldal (trade.gov.cn)	1,7 millió $	8000 jelszó
Amerikai haditengerészet (navy.mil)		172 jelszó

Kritikus infrastruktúra védelmi kutatások
TÁMOP-4.2.1.B-11/2/KMR-0001
MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Sérülékenységek

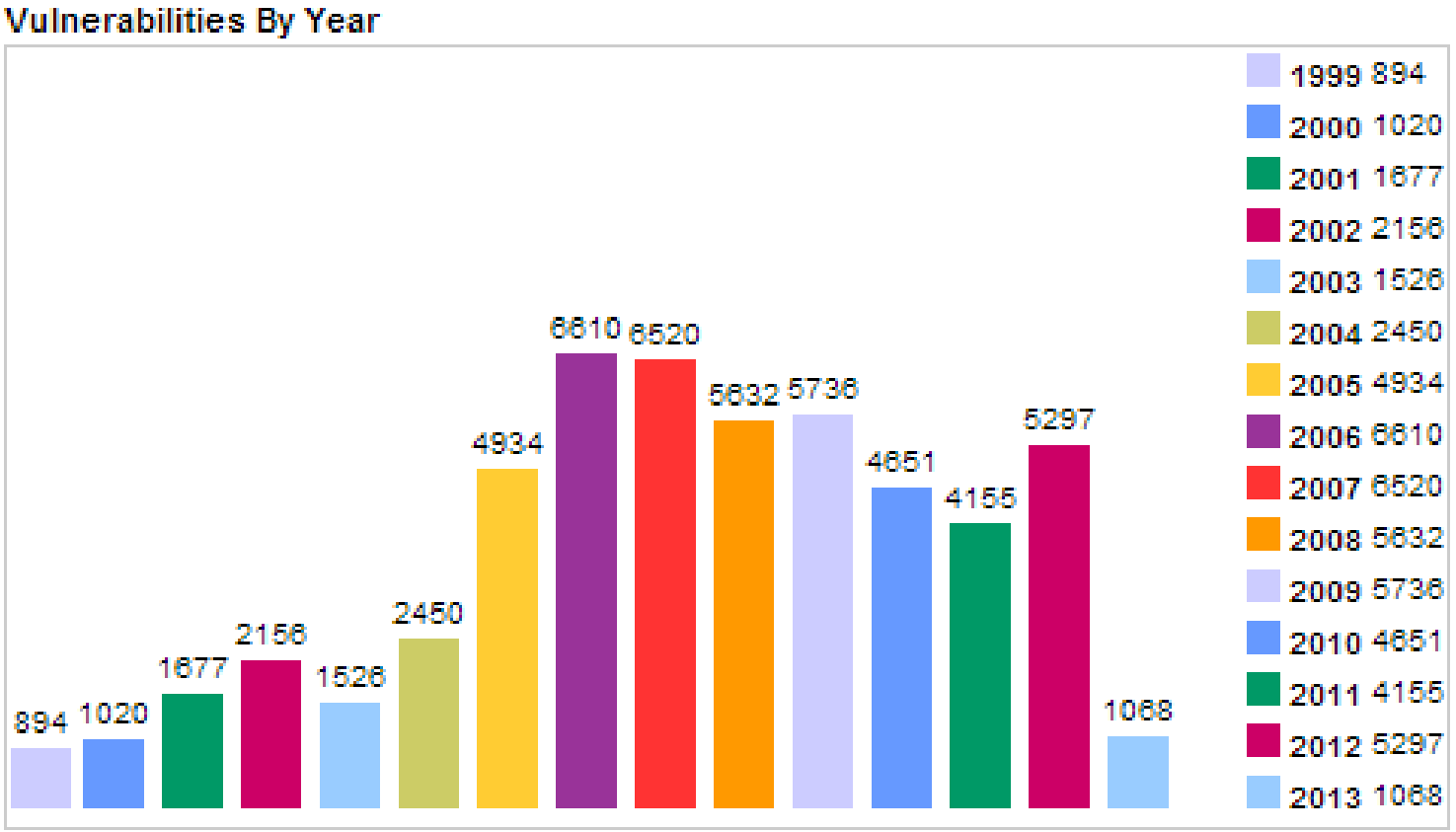
Common Vulnerabilities Exposures (CVE) azonosítóval látják el

Exploit: sérülékenységek kihasználására írt kód mely használatával támadók kárt tehetnek a rendszerünkben.

Kritikus infrastruktúra védelmi kutatások
TÁMOP-4.2.1.B-11/2/KMR-0001

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Sérülékenységek gyakorisága



http://www.cvedetails.com/browse-by-date.php, 2013. 03.19

Kritikus infrastruktúra védelmi kutatások
TÁMOP-4.2.1.B-11/2/KMR-0001

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Informatikai Biztonság problémái

- Esetlegesen bekövetkező esemény ellen védekezünk
  - Költségcsökkentés <=> Profitszerzés
- Már a kockázatok felderítése is költséges

Kockázat csökkentése, elhárítása újabb költségekkel jár

- Folyamatosan napról-napra keletkeznek újabb sérülékenységek
- Általában a funkcionalitás, könnyű használhatóság a fő szempontok a biztonság nincs ezekkel egy szinten

Kritikus infrastruktúra védelmi kutatások
TÁMOP-4.2.1.B-11/2/KMR-0001
MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Védekezés

Megelőzés:

Kockázatmenedzsment:

Kockázatelemzés eredményei alapján elfogadjuk, csökkentjük vagy elhárítjuk a fenyegetéseket

Kockázati tényezők felderítésénél használható a sérülékenység vizsgálat

Egy sérülékenység kockázatát alapvetően meghatározza a sérülékenység kihasználásának valószínűsége, a kihasználásával elérhető erőforrások értéke

Kritikus infrastruktúra védelmi kutatások
TÁMOP-4.2.1.B-11/2/KMR-0001

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Sérülékenység vizsgáló szoftverek

Automatikus vizsgálattal detektálja:
- Szoftveres hibák
- Rossz konfigurációból adódó hibák

A hálózat jelentősebb módosítása nélkül telepíthetők

Külső támadó nézőpontjából tesztelik a hálózatot:
- Hálózat felderítése
- Előre definiált tesztelési mintákkal ellenőrzik a hálózatot

A következő lépésekről (javítás, elfogadás) a felhasználónak kell döntenie, a szoftverek segítséget nyújtanak ebben (hiba prioritása, tudásbázis, ticketek)

Kritikus infrastruktúra védelmi kutatások
TÁMOP-4.2.1.B-11/2/KMR-0001

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Tesztelt sérülékenység vizsgáló szoftverek

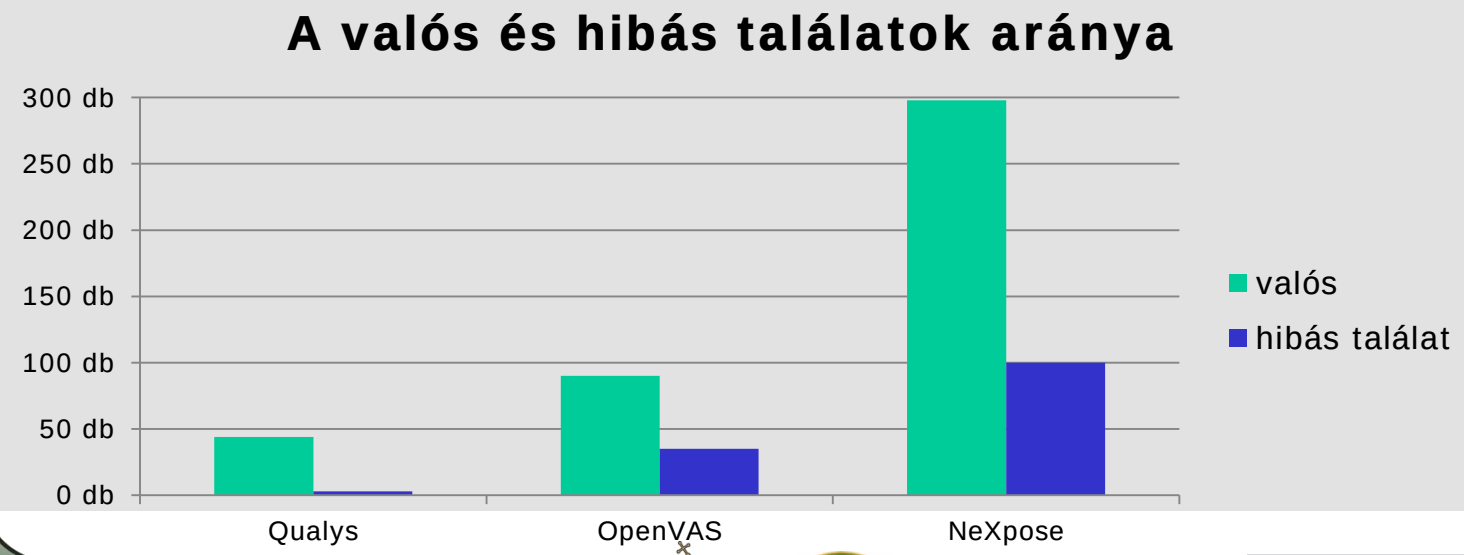
- SC magazin nyertes:
  - QualysGuard
    - Szoftver mint szolgáltatás (SaaS) alapú
- Amerikai kormányzatok és ügynökségek által használt:
  - Nexpose
- Legnépszerűbb nyílt forrású:
  - OpenVAS

Kritikus infrastruktúra védelmi kutatások
TÁMOP-4.2.1.B-11/2/KMR-0001

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Összehasonlítás

- Valós találat: létező sérülékenység
- Hibás találat: szoftver szerint létező sérülékenység, amely nem található meg a hálózatban



Kritikus infrastruktúra védelmi kutatások
TÁMOP-4.2.1.B-11/2/KMR-0001
MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Összehasonlítás

Szempontok	QualysGuard	Nexpose	OpenVAS
Felhasználói felület	bonyolult, sok opció, beállítási lehetőség. jól elkülönült jogosultsági szintek, az egyes felhasználói osztályok a saját feladataiknak megfelelő felületet kapnak	egyszerűen kezelhető webes felület és api	webes felület, kliens alkalmazás, parancssoros környezet Webes felületet használtuk
Dokumentáció, terméktámogatás	felhasználói dokumentációk, videók, kérésre oktatás.	felhasználói dokumentációk	kevés dokumentáció
Adatbázis nagysága	11000 CVE kompatibilis bejegyzés havonta 20-szal nő	28000 CVE kompatibilis bejegyzés	25000 CVE kompatibilis bejegyzés

Kritikus infrastruktúra védelmi kutatások
TÁMOP-4.2.1.B-11/2/KMR-0001
MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

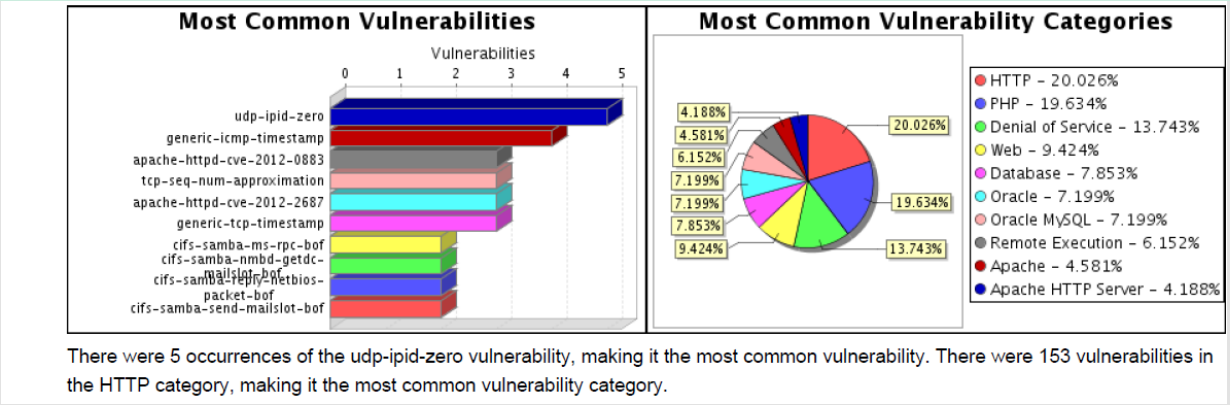
Összehasonlítás

Szempontok	QualysGuard	Nexpose	OpenVAS
Tesztelés időtartama	43 perc	28 perc	32 perc
Rendszer feltérképezése	Az operációs rendszert ritkán határozta meg pontosan	Többnyire felismerte a vizsgált célpont operációs rendszerét	Az operációs rendszert ritkán határozta meg pontosan
Megismételhetőség	A tesztelési paramétereket elmenthetjük, ezeket később, vagy időzítve újra futtathatjuk	A tesztelési paramétereket elmenthetjük, ezeket később, vagy időzítve újra futtathatjuk	A tesztelési beállítást újra meg kell adni, lehetőséget biztosít az időzítésre

Kritikus infrastruktúra védelmi kutatások
TÁMOP-4.2.1.B-11/2/KMR-0001
MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Összehasonlítás

Szempontok	QualysGuard	Nexpose	OpenVAS
Eredmények formája	Több szempont szerint lehet szűrni az eredményeket. szűrés minták létrehozására van lehetőség	Több szempont szerint lehet szűrni az eredményeket	Kevesebb szempont alapján lehet szűrni az eredményeket, az egyik vizsgálat esetében üres PDF riportot generált



There were 5 occurrences of the udp-ipid-zero vulnerability, making it the most common vulnerability. There were 153 vulnerabilities in the HTTP category, making it the most common vulnerability category.

Kritikus infrastruktúra védelmi kutatások
TÁMOP-4.2.1.B-11/2/KMR-0001

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.

Összehasonlítás

Szempontok	QualysGuard	Nexpose	OpenVAS
Bővíthetőség	Előfizetést kell bővíteni, ha belső hálózat, akkor az új hálózatra kell szkennert telepíteni.	A moduláris kialakítás révén egy újabb szkennert kell telepíteni, amennyiben a liszensz eléri a korlátait, új előfizetésre kell bővíteni	A moduláris kialakítás révén egy szkenner szolgáltatást kell telepíteni, amennyiben a hardveres erőforrás kevésnek bizonyul, vagy védett alhálózattal bővült a rendszer.

Köszönetnyilvánítás

- A szerzők ezúton mondanak köszönetet a TÁMOP-4.2.1.B-11/2/KMR-2011-0001 „Kritikus infrastruktúra védelmi kutatások” projektnek a cikkhez végzet kutatások anyagi támogatásáért. A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.
- Szeretnénk megköszönni a Qualys Inc.-nek, valamint az MTA SZTAKI-nak a tesztelésben nyújtott segítségüket, hogy rendelkezésünkre bocsájtották a szoftvereket, illetve az infrastruktúrát.
- Továbbá szeretnénk megköszönni, Kotcauer Péternek, illetve Szenes Katalinnak a témában nyújtott segítségüket.

Köszönöm a figyelmet.

Kritikus infrastruktúra védelmi kutatások
TÁMOP-4.2.1.B-11/2/KMR-0001

MAGYARORSZÁG MEGÚJUL
A projektek az Európai Unió támogatásával valósulnak meg.