



IT ADVISORY

Biztonság a felhőben

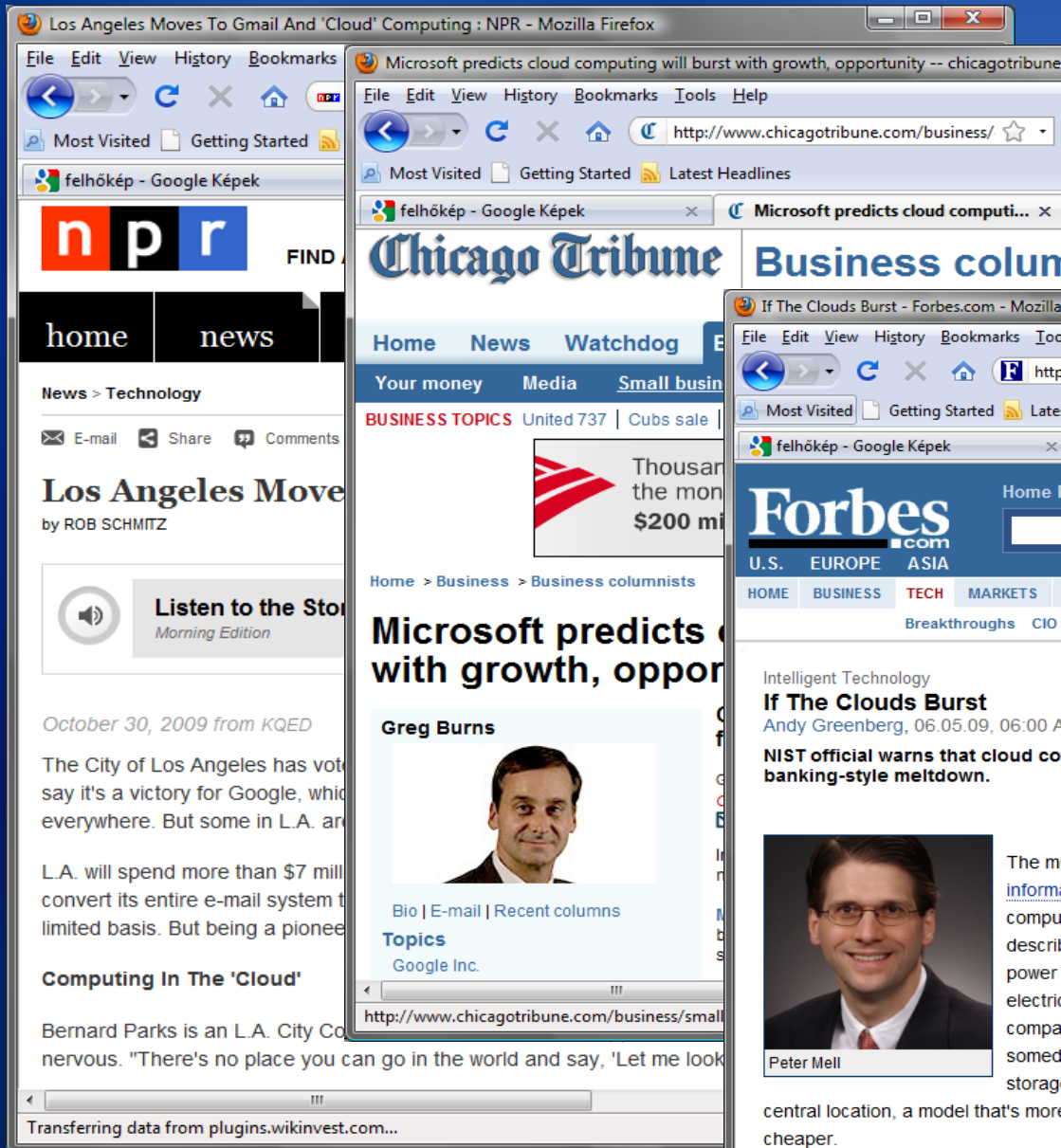
Gaidosch Tamás
CISA, CISM, CISSP

2010. január 20.

Tartalom

- Cloud hype
- Mi micsoda?
- Szempontok
- Előnyök és kockázatok

Hype



Los Angeles Moves To Gmail And 'Cloud' Computing : NPR - Mozilla Firefox

Microsoft predicts cloud computing will burst with growth, opportunity -- chicagotribune.com

Chicago Tribune Business column

Home News Watchdog

Your money Media Small business

BUSINESS TOPICS United 737 | Cubs sale |

Thousar the mon \$200 mi

Forbes.com U.S. EUROPE ASIA

HOME BUSINESS TECH MARKETS

Breakthroughs CIO

Intelligent Technology

If The Clouds Burst
Andy Greenberg, 06.05.09, 06:00 A

NIST official warns that cloud computing could bring banking-style meltdown.

The me inform comput descri power electric compa somed

Greg Burns

Bio | E-mail | Recent columns

Topics
Google Inc.

http://www.chicagotribune.com/business/small

Transferring data from plugins.wikinvest.com...



Cloud computing to burst in next year - Mozilla Firefox

http://cloudcomputing.spunje.com/2009/11/cl

Most Visited Getting Started Latest Headlines

Cloud computing to burst in next year

CLOUD COMPUTING SPUNJE
CONSTANTLY UPDATED ONLINE SOURCE OF NEWS & DEVELOPMENTS IN CLOUD COMPUTING - SOAK IT UP!

HOME ABOUT DIRECTORY SUBSCRIBE

Cloud computing to burst in next year
By Cloud Computing Spunje Published: November 5, 2009
Posted in: Cloud Solutions, Hosting, Opinions & Explanations
Tags:



Comments [0] Digg it! Facebook

Speaking at Gartner Symposium ITxpo in Cannes, Gartner vice president David Cearley said that by 2012, 20% of businesses would be using cloud computing for part of their IT infrastructure — a figure which contrasts sharply with the build-up surrounding the concept of on-demand, elastic computing services.

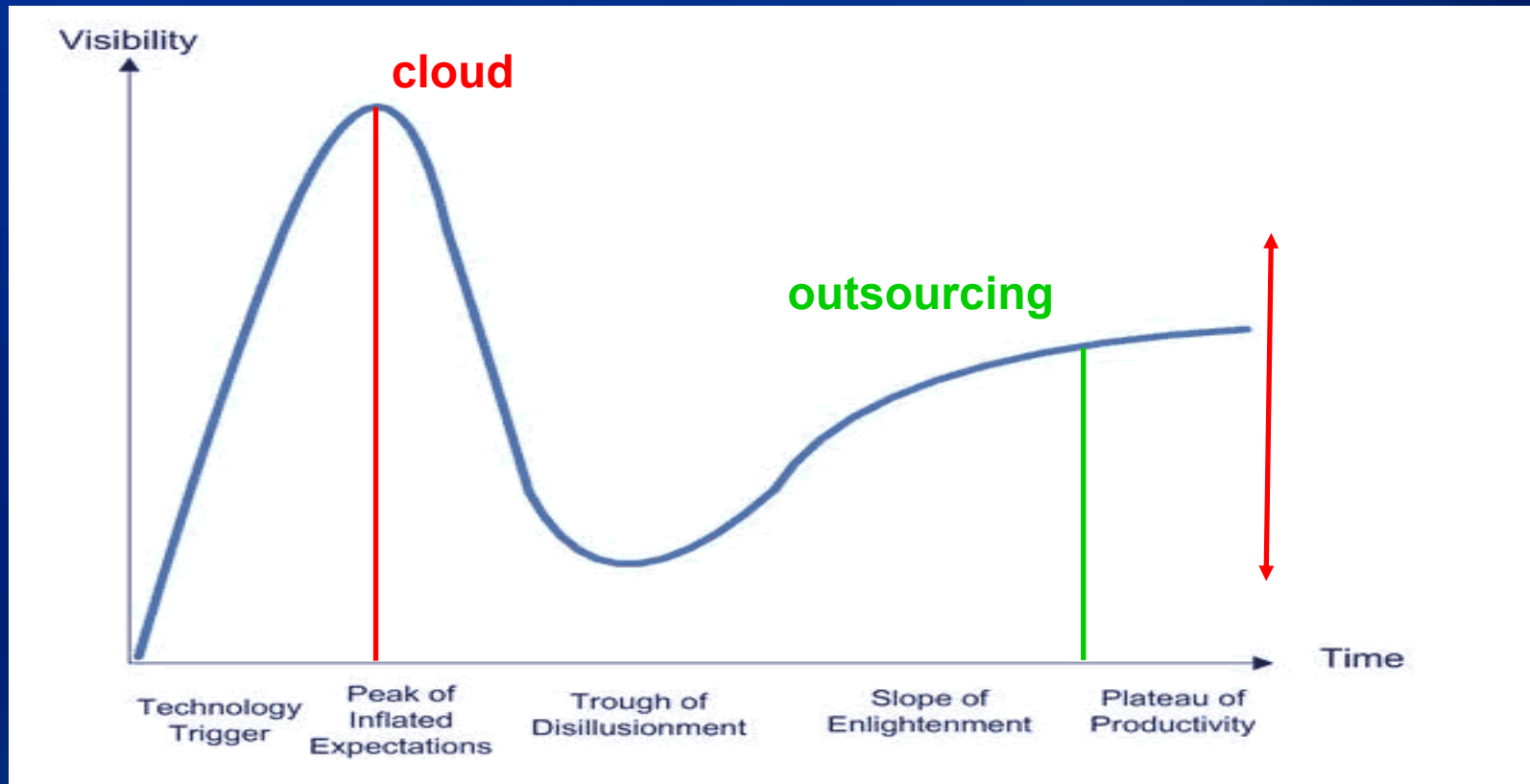
"Cloud computing is one of the most hyped terms in the industry right now," Cearley said. "In many ways it's overhyped. In the next 12-18 months, it's going to crash into the trough of disillusionment. But we do think cloud

Done

SIGN ME UP >

FAQ | Terms & Conditions | Privacy Policy

Hype



Forrás: Gartner

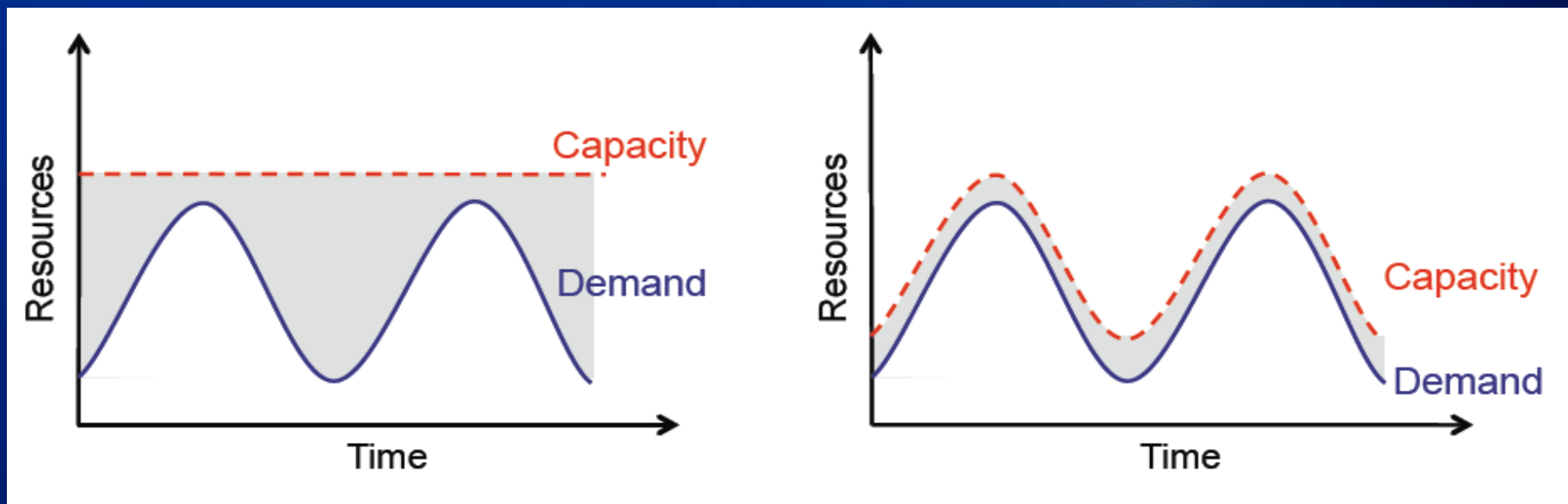
Mit is akarunk megoldani?

- Reagálási képesség növelése
- Költségek csökkentése
- Hatékonyság növelése
- Mutatók optimalizálása

Cloud

- IT kapacitás bérlünk szükség szerint (on demand)
- Kizárólag hálózati hozzáféréssel
- Helyfüggetlenül
- Használattal arányos költséggel (pay per use)
- Megosztott erőforrásokat használunk (hálózat, szerverek, tárolók, alkalmazások, szolgáltatások)
- Gyors és rugalmas kapacitásmenedzsment
- Szabványos konstrukciók
- Minimális interakció a szolgáltatóval

A lényeg



Adatközpont

Cloud

CFO szemmel

Szempont	Házon belül	Outsourcing	Cloud
Ráfordítás	CAPEX	OPEX	OPEX
Cash Flow	Előre fizetés	Éves díj	Használattal arányos havidíj
Pénzügyi kockázat	Előre bevállalt	Éves terített	Havi terített
P&L	Költség, Értékcsökkenés	Költség	Költség
Mérleg	Eszközök	-	-

CEO szemmel

Részvényesi érték

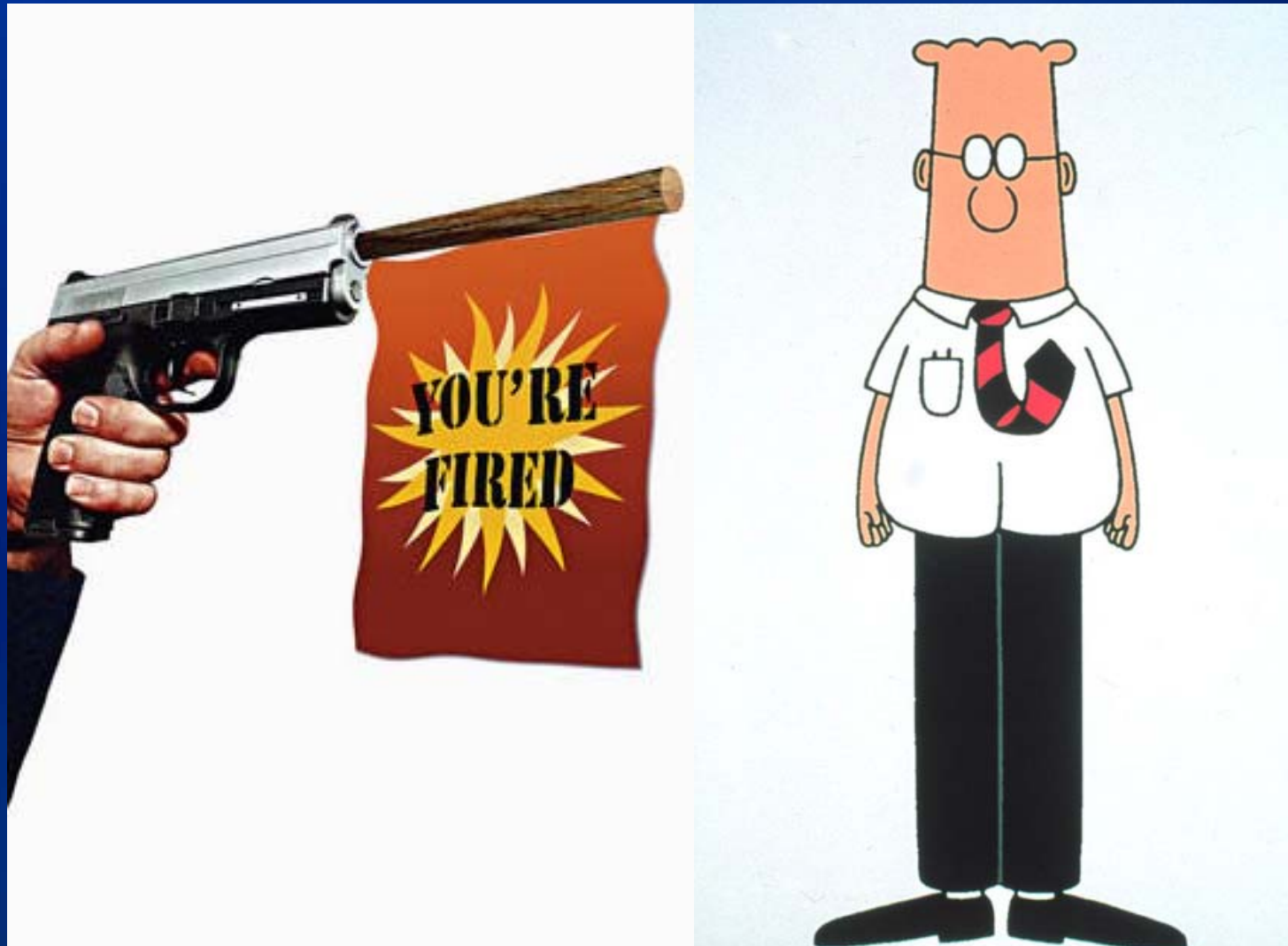
Gyorsaság

Hatékonyaság

Piacnyerés



IT-s szemmel



IT biztonsági szakértő szemmel



Adatközpont és cloud

Adatközpont

Ismert helyszínek

kb. 1000 processzor

Hardver redundancia

Fizikai és virtuális erőforrások

Cluster vagy grid architektúra

Statikus

Komplexitás



Cloud

Ismeretlen helyszínek

>10 000 standard processzor

Szoftver redundancia

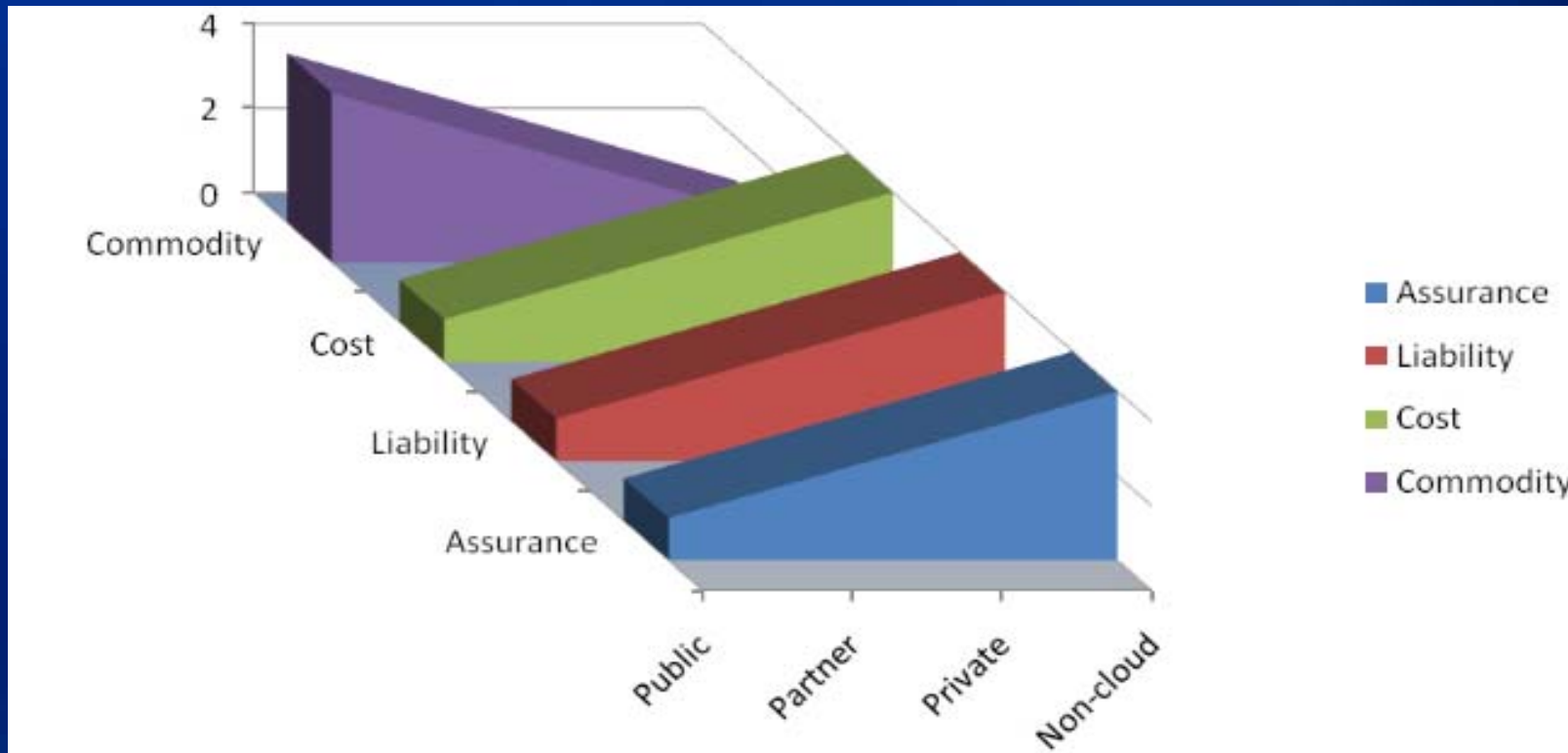
Virtuális erőforrások

Cloud architektúra

Rugalmas

Szabványosság

Cloud típusok és jellemzőik



Forrás: ENISA

Biztonsági előnyök és kockázatok

Előnyök

Méretgazdaságosság

Szabványos interfészek

Gyors és hatékony patchelés

Fajlagosan olcsóbb fizikai biztonság

Egyszerűbb és olcsóbb biztonságmenedzsment

Hatékonyabb forensic támogatás (elvileg)



Kockázatok

Bizalmas adatok védelme

Virtualizáció

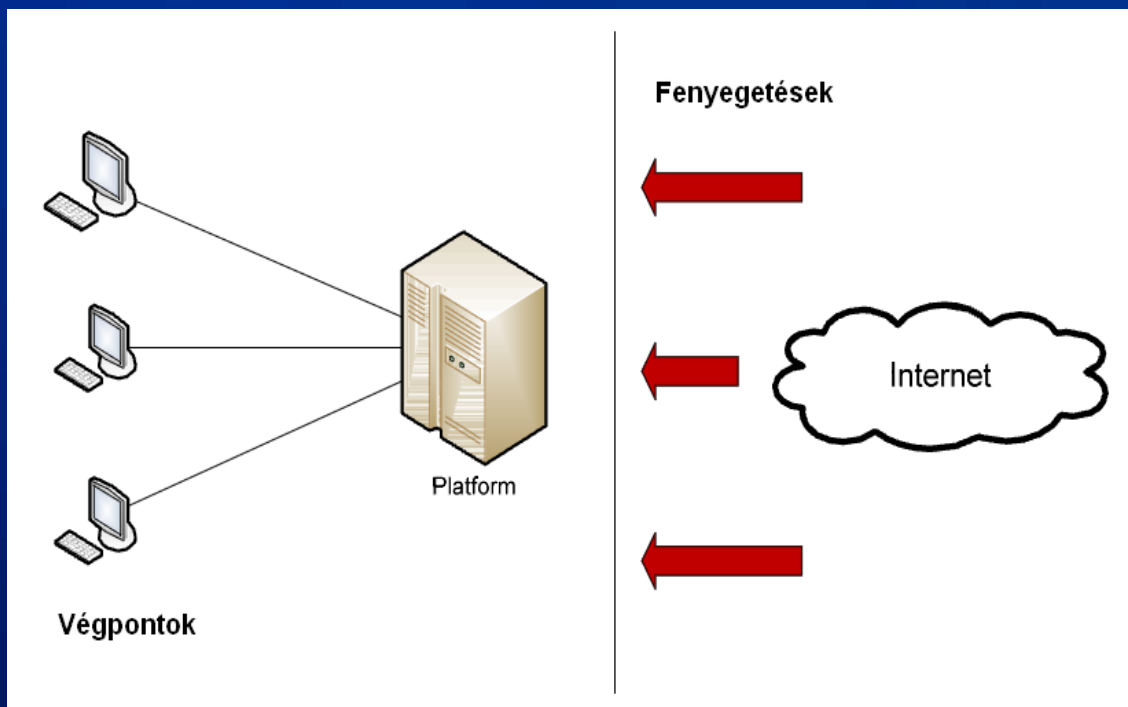
Hálózati védelem

Szegregáció

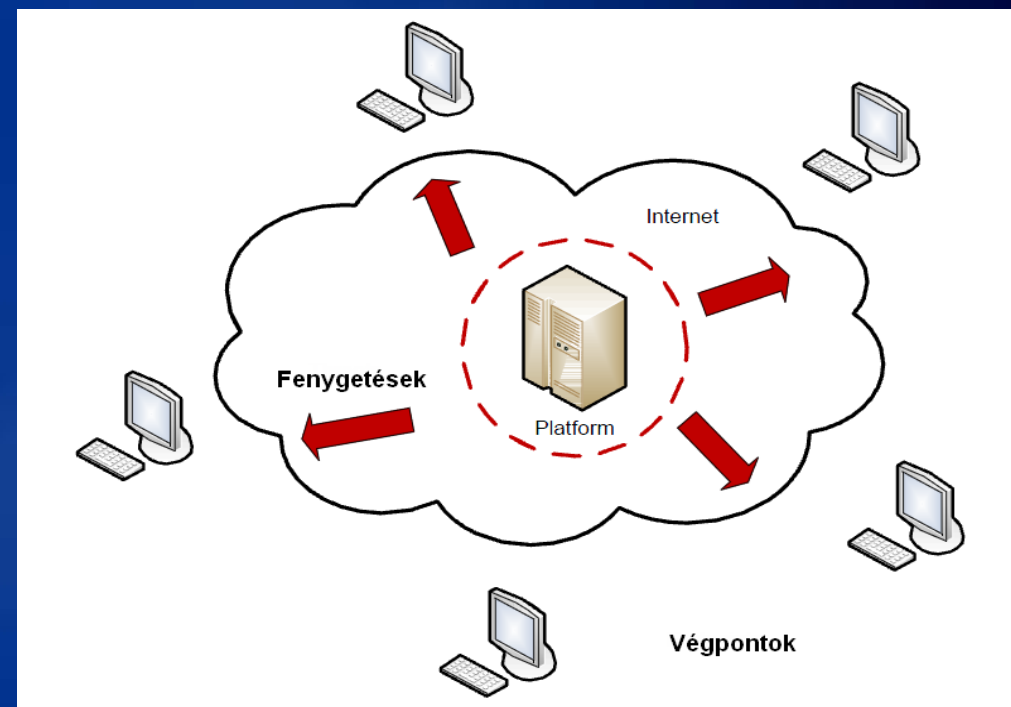
Auditálhatóság / törvényi megfelelés

Lock-in

Változó fenyegetettség



Adatközpont



Cloud

Kockázatok: bizalmas adatok

- Hol van a felhő?
- Mi van még a felhőben?
- Milyen előírások vonatkoznak
 - a felhőre?
 - az adataimra?
 - a kötelező adatszolgáltatásra?
- Hogyan ellenőrzöm a cloud szolgáltatót?

Kockázatok: bizalmas adatok

ftc031709.pdf (application/pdf Object) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf

Most Visited Getting Started Latest Headlines

Privacy group to FTC: Google's clou... x ftc031709.pdf (application/pdf O... x

1 / 15 83,7% Find

**Before the
Federal Trade Commission
Washington, DC 20580**

**In the Matter of)
)
Google, Inc. and)
Cloud Computing Services)
_____)**

**Complaint and Request for Injunction, Request
for Investigation and for Other Relief**

SUMMARY OF COMPLAINT

1. This complaint concerns privacy and security risks associated with the provision of "Cloud Computing Services" by Google, Inc. to American consumers, businesses, and federal agencies of the United States government. Recent reports indicate that Google does not adequately safeguard the confidential information that it obtains. Given the previous opinions of the Federal Trade Commission regarding the obligation of service providers to ensure security, EPIC hereby petitions the Federal Trade Commission to open an investigation into Google's Cloud Computing Services, to determine the adequacy of the privacy and security safeguards, to assess the representations made by the firm regarding these services, to determine whether the firm has engaged in unfair and/or deceptive trade practices, and to take any such measures as are necessary, including to enjoin Google from offering such services until safeguards are verifiably established. Such action by the Commission is necessary to ensure the safety and security of information submitted to Google by American consumers. American

Done

Kockázatok: virtualizáció

- Hipervizor sérülékenységek
- Middleware
- Rendszermenedzsment eszközök
- Monokultúra
- Erősen disztributált feldolgozási módok
 - race
 - check / use

Kockázatok: hálózati védelem

- A felhő védelme
 - komplexitás
- A hozzáférés (csatorna) védelme
 - gyakorlatilag SSL
- DDoS?
- Tűzfalak?
- IDS / IPS?

Kockázatok: hálózati védelem

Internet Storm Center
Today's Internet Threat Level: GREEN
Handler on Duty: Jim Clausing

Handler's Diary: The ISC and DShield websites will be unavailable on Wednesday Nov 25th from ...

Diary

previous next

TLS Man-in-the-middle on renegotiation vulnerability made public

Published: 2009-11-05,
Last Updated: 2009-11-05 19:03:13 UTC
by Swa Frantzen (Version: 2)

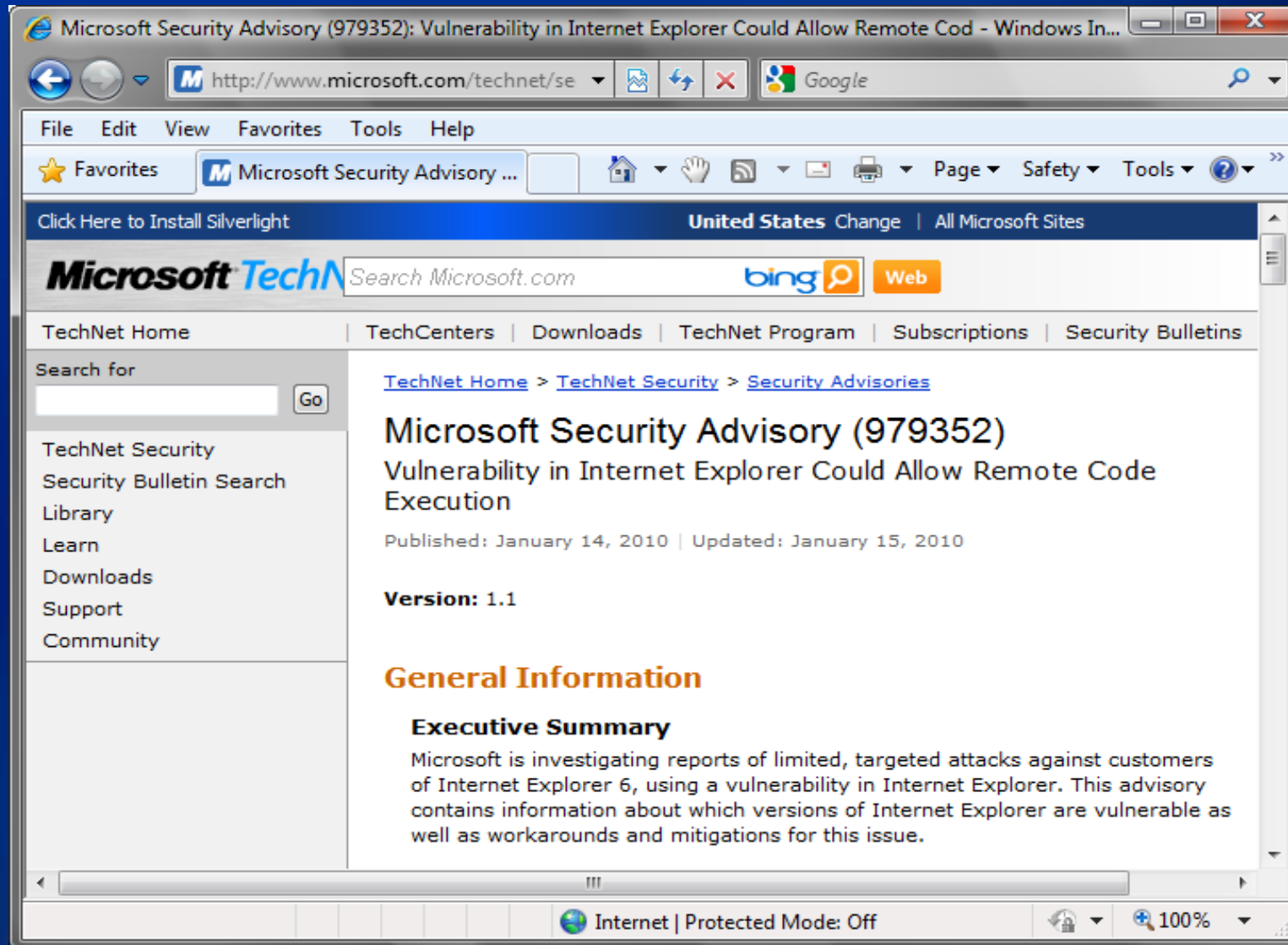
3 comment(s) Digg submit facebook twitter

TLS 1.0+ and SSL 3.0+ (known from among others "https") is vulnerable to a protocol weakness where a man in the middle attack could be worked in during the renegotiation phase in modern versions of the protocol.

While the details had been offered in a meeting with the IETF, vendors and the open source implementers of SSL privately, it appears an IETF mailing list came to finding it again. That seems to have prompted the original finders (Marsh Ray and Steve Dispensa) to offer up their finding publicly.

http://isc.sans.org/howto.html

Kockázatok: hálózati védelem



The screenshot shows a web browser window displaying a Microsoft Security Advisory. The browser's address bar shows the URL: <http://www.microsoft.com/technet/se>. The page title is "Microsoft Security Advisory (979352): Vulnerability in Internet Explorer Could Allow Remote Code Execution". The page content includes a search bar, navigation links, and the main advisory text.

Microsoft Security Advisory (979352)
Vulnerability in Internet Explorer Could Allow Remote Code Execution

Published: January 14, 2010 | Updated: January 15, 2010

Version: 1.1

General Information

Executive Summary

Microsoft is investigating reports of limited, targeted attacks against customers of Internet Explorer 6, using a vulnerability in Internet Explorer. This advisory contains information about which versions of Internet Explorer are vulnerable as well as workarounds and mitigations for this issue.

Kockázatok: szegregáció

- Ki van még a felhőben, és mit csinál?
- Virtuális erőforrások elszigetelése
- Rendszermenedzsment
- Biztonságos adatmegsemmisítés

Kockázatok: auditálhatóság / törv. megfelelés

- Dinamikus környezet
- Változásmenedzsment
- Kevés befolyás a kontrollkörnyezetre
- PCI, SOX, Hpt, ...

Összefoglaló

Cloud a hype ciklus tetején

Eltérő szolgáltatási modell eltérő biztonsági kockázatokat eredményez

A cloud biztonsági kockázatai kevésbé ismertek

Erősen szabályozott / nagyvállalati környezetben érdemes kivárni a cloud hype végét



Az előadó elérhetősége

Gaidosch Tamás

KPMG Tanácsadó Kft.

tamas.gaidosch@kpmg.hu

887-7139

www.kpmg.hu

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.