

IT Outsourcing partnerek ellenőrzése

*Technológiai megoldás a jogi útvesztők
helyett...*

*Marosvári Gábor
Termékmarketing menedzser
BalaBit kft.*

Agenda

Kihívások

Piaci válaszok

Jó Megoldások



Kihívások: Külsősök okozta incidensek

Former Bank Contractor Charged in Fraud Scheme

Bank of New York reports that a sub-contractor computer technician has stolen over SIM by using identity theft of employee data.

As reported in **The New York Times**

Citigroup's customer data stolen

HONG KONG: Hackers stole account information of more than 360,000 of Citigroup Inc.'s United States credit card customers in a recent data breach, the bank said on Wednesday, almost double the number initially thought.

Citi said last week about one per cent of its credit card customers had account information hacked online but did not say exactly how many. The actual number of customers affected was thought to be about 200,000, based

on Citi's 2010 annual report, which said the company had roughly 21 million North American credit card customers. But the number was actually 360,083, the bank said in a statement posted on its website on Wednesday.

The bank said it discovered hackers used its Account Access service to access the data for nearly 1 million credit cards in

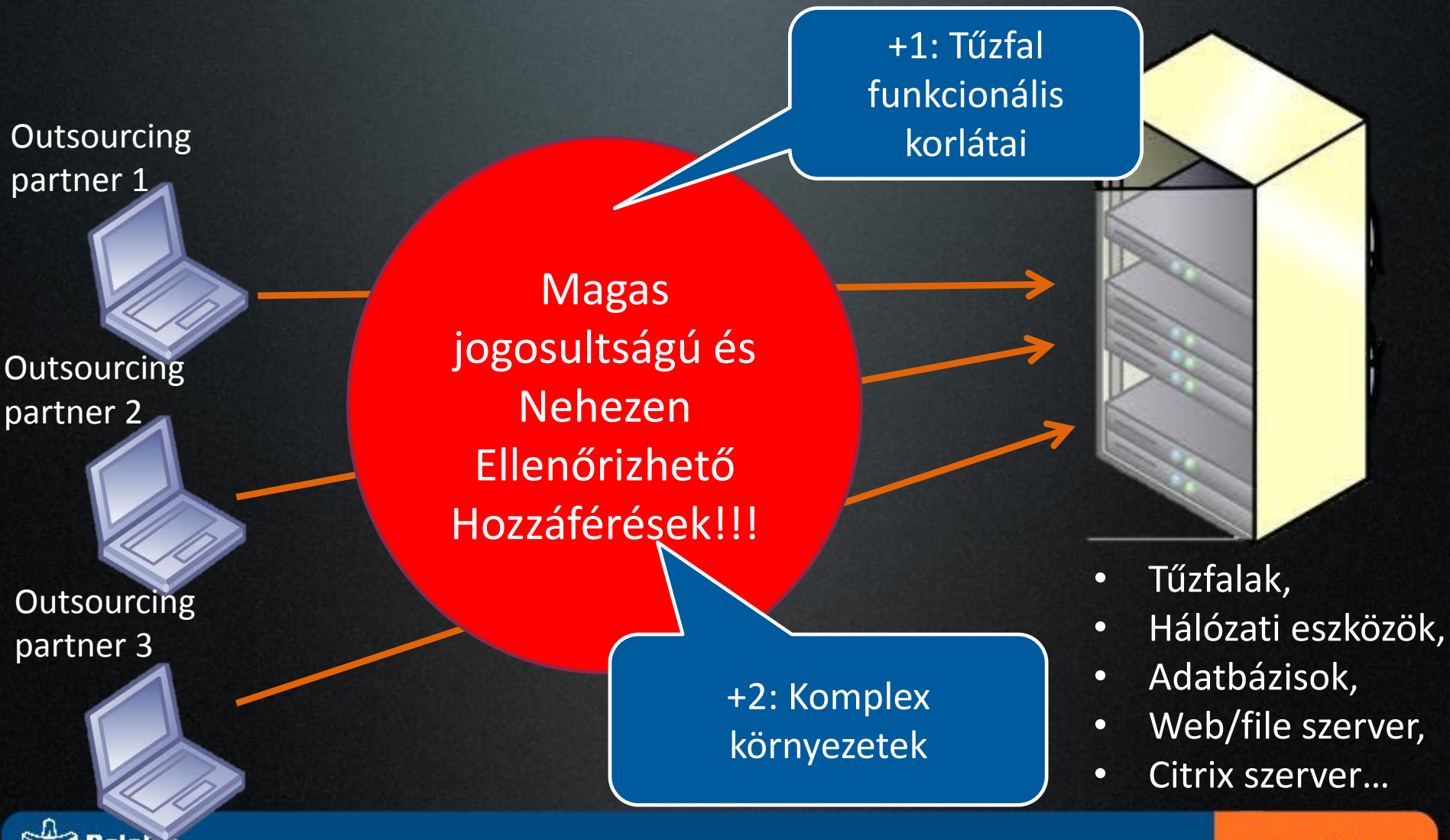
Was RBS brought to its knees by
ONE junior IT technician?
'Inexperienced operative' in India
blamed for meltdown that wiped
£1.7bn off bank shares

Source code stolen from U.S. software company via India branch

Software vendor Jolly Technologies reports that an insider at its overseas R&D center in Mumbai stole portions of the source code and confidential design documents, including one of its key products.

InfoWorld

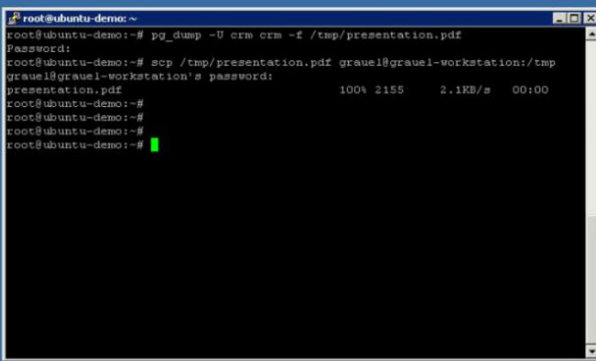
Kihívások: Külsős „Superuser”-ek



Kihívások: A naplózás NEM elég...

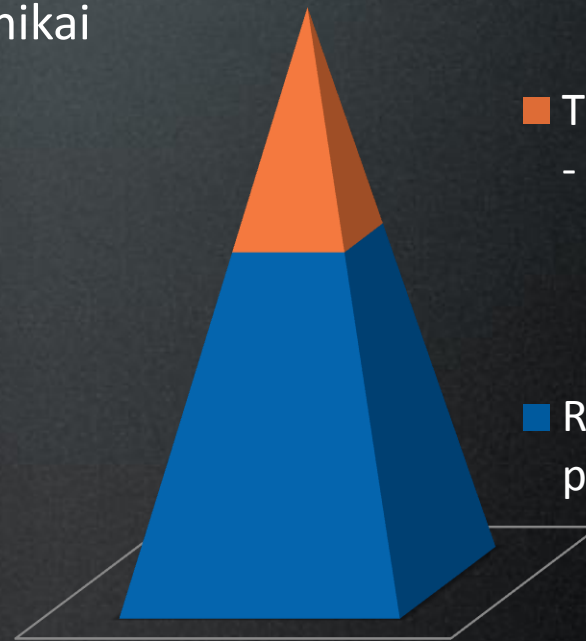
1. Sok biztonsági esemény nincs naplózva!
2. A log-ok jellemzően nem azt mutatják, hogy ki mit csinált.
3. A log-ok sokszor csak homályos technikai részleteket mutatnak.

```
1-0117:04:45+01:00 localhost sshd[5585]: pam_unix(sshd:session): session opened for user grauel by (uid=0)
1-0117:04:56+01:00 localhost sudo: grauel: sudo: /bin/bash : PWD=/home/grauel ; USER=root ; COMMAND=/bin/bash
1-0117:06:46+01:00 localhost postgres[5814]: [3-1] LOG: connection received: host=[local]
1-0117:06:50+01:00 localhost postgres[5814]: [3-1] LOG: connection received: host=[local]
1-0117:06:50+01:00 localhost postgres[5814]: [3-1] LOG: connection authorized: user=crm database=crm
1-0117:06:50+01:00 localhost postgres[5814]: [4-1] LOG: disconnection: session time: 0:00:00.094 user=crm
ss=crm host=[local]
```



NO LOGS!!!

Felhasználó-felügyeleti „Piramis”



■ Tevékenység rögzítés
- biztonsági kamera

■ Rendszernapló -
pillanatkép

Kihívások: Megfelelési Kényszer és Jogi Útvesztők

- Törvényi előírások
- Hatósági ajánlások (pl. PSZÁF)
- Iparági standardok (pl. ISO2700x, PCI-DSS)



Megfelelés
adminisztratív
eszközökkel nem
megoldható!

- Partneri szerződések
- SLA megállapodások
- KPI-k



Napi Tevékenység
Nehezen
Felügyelhető!

Technológiai válaszok

- Jump hostok
- Agent-alapú megoldások
- Network snifferek
- **Proxy gateway-ek**



Proxy gateway

- Forgalom-elemzés „alkalmazás” szinten
- Teljes protokoll-ellenőrzés
- Transzparens működés
- Független a klientsztől és a szervertől
- Visszahat a forgalomra (autentikáció, engedélyeztetés, megszakítás, stb.)
- Időpecsétes, aláírt, titkosított audit-trail-ek
- File-átvitel elemzés



Privilegizált Munkamenet-felügyelet

Outsourcing partner 1



Outsourcing partner 2



Outsourcing partner 3



HTTP, Telnet
RDP, VNC

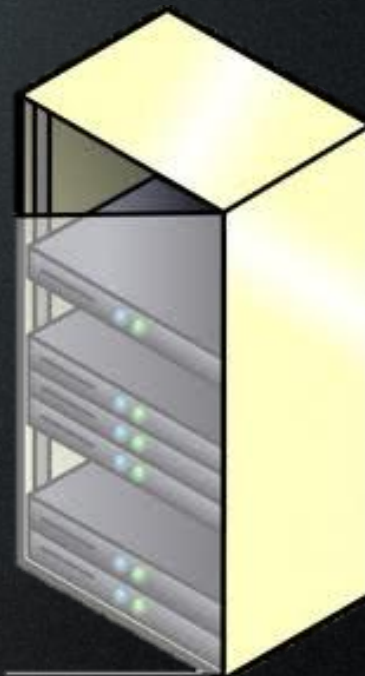
SSH, Citrix



HTTP, Telnet

RDP, VNC

SSH, Citrix



- Tűzfalak,
- Hálózati eszközök,
- Adatbázisok,
- Web/file szerver,
- Citrix szerver...

Konklúzió

Üzleti előnyök

Gyorsabb ROI

- Egyszerűbb és jobb minőségű auditok
- Alacsonyabb hibaelhárítási költségek
- Központi hitelesítés és hozzáférés-szabályozás
- Teljes körű partner-felügyeleti megoldás

Alacsonyabb kockázat

- Magasabb törvényi/iparági megfelelés
- Szigorúbb SLA-kontroll
- Partnerek felelősségérzete nő
- Erős bizonyíték felelősségi vitákban

KÖSZÖNÖM A FIGYELMET!



Jelentkezés auditor tréningre:

mgabor@balabit.hu

+36 20 366 7620