

Buzzword Dictionary Vol. II Security Buzzwords

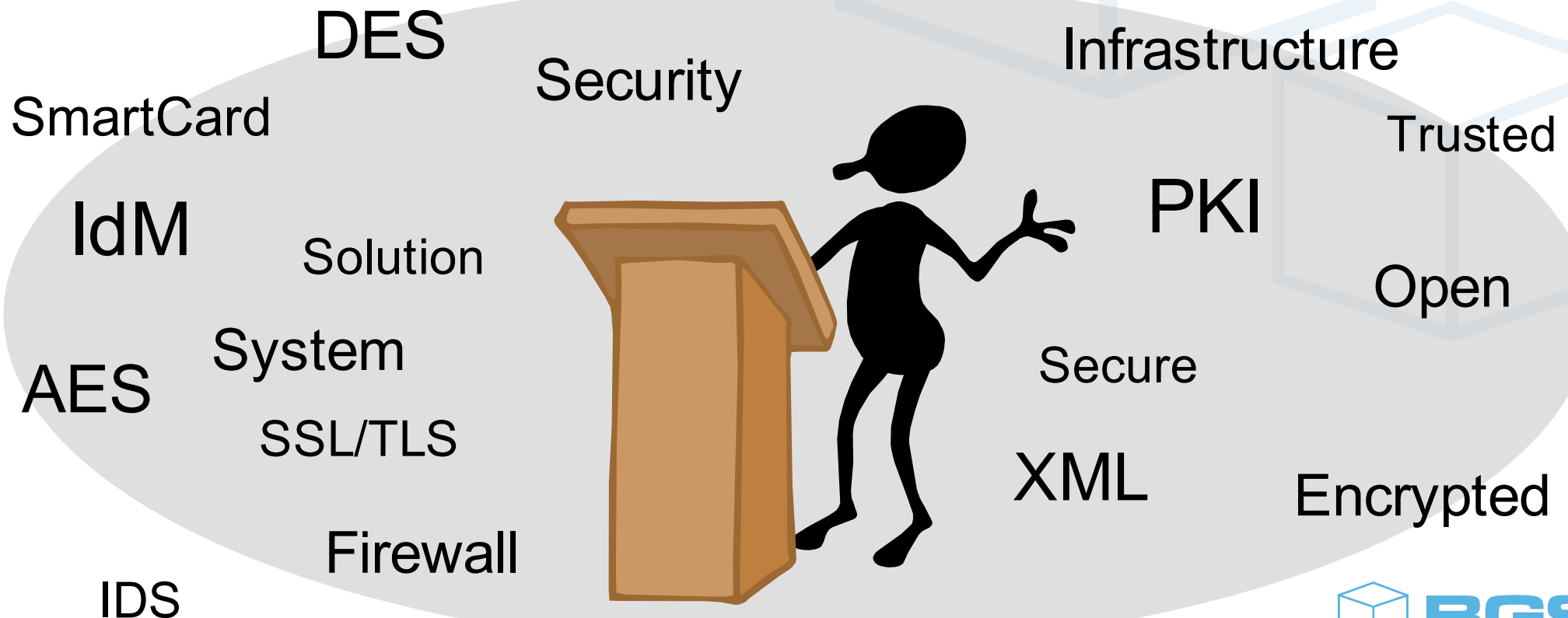
Radovan Semančík

“Buzzword”

buzzword

n : stock phrases that have become nonsense through endless repetition *syn: cant*

WordNet



Bezpečnostné povery a mýty

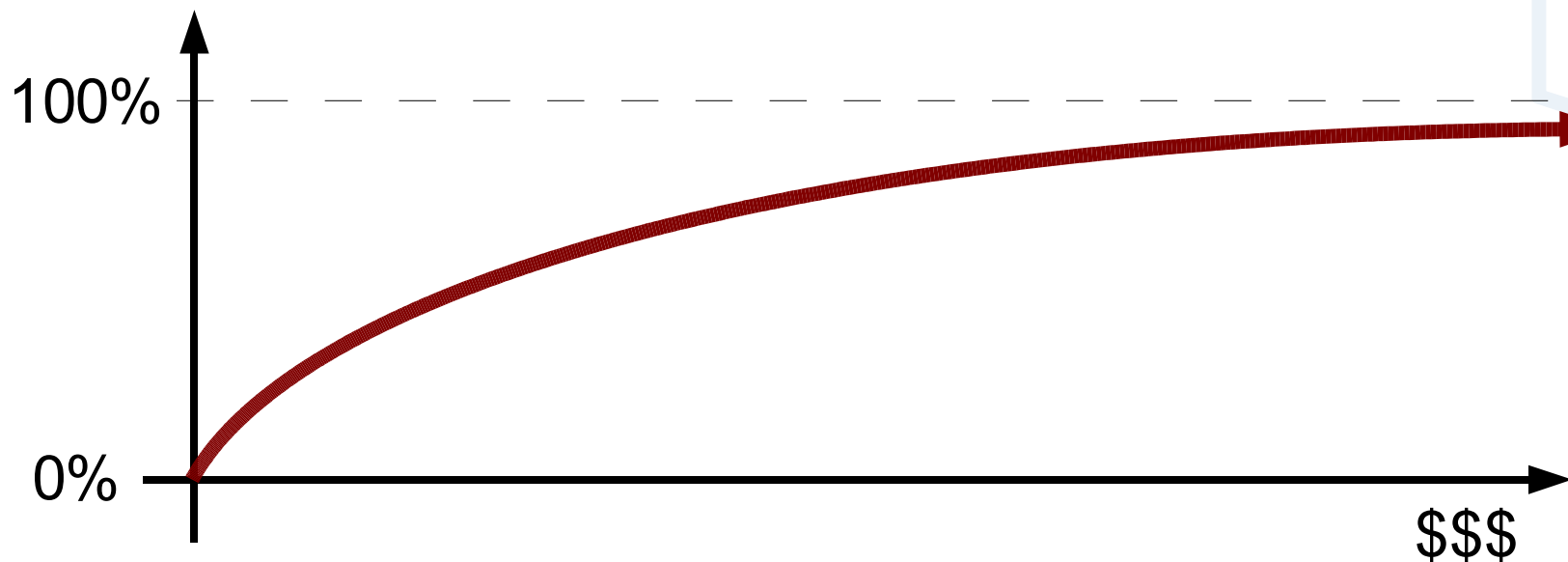
- 100% bezpečnosť
- Bezpečnostný projekt
- Firewall
- Šifrovanie
- Certifikácia “EAL4”



“Zaručená” bezpečnosť

- “Bezpečnosť nášho produktu je zaručená”
- Nič nie je dokonalé, ani bezpečnosť
 - “Delo a pancier”
 - Koľko bude stáť útok?
 - Akú hodnotu majú moje údaje?
 - Čo môže útočník získať?

Riziková analýza
(reziduálne riziko)



Lineárny bezpečnostný projekt

- “Máme predsa bezpečnostný projekt!”

Príprava projektu

Riziková analýza

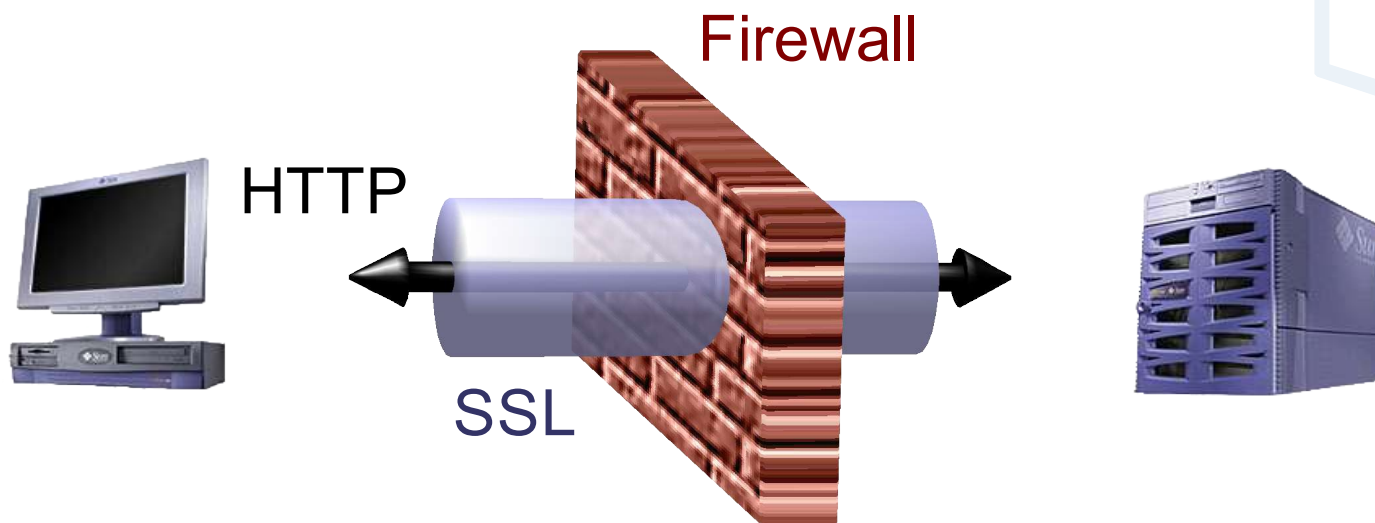
Návrh opatrení

Implementácia

Zmena
Incident

Firewall

- “Je to za firewallom, je to bezpečné”
- RFC 3093: Firewall Enhancement Protocol (1 April 2001)
- httunnel, corkscrew, firepass, htsneak, ...
- Vidí firewall do aplikačnej vrstvy?



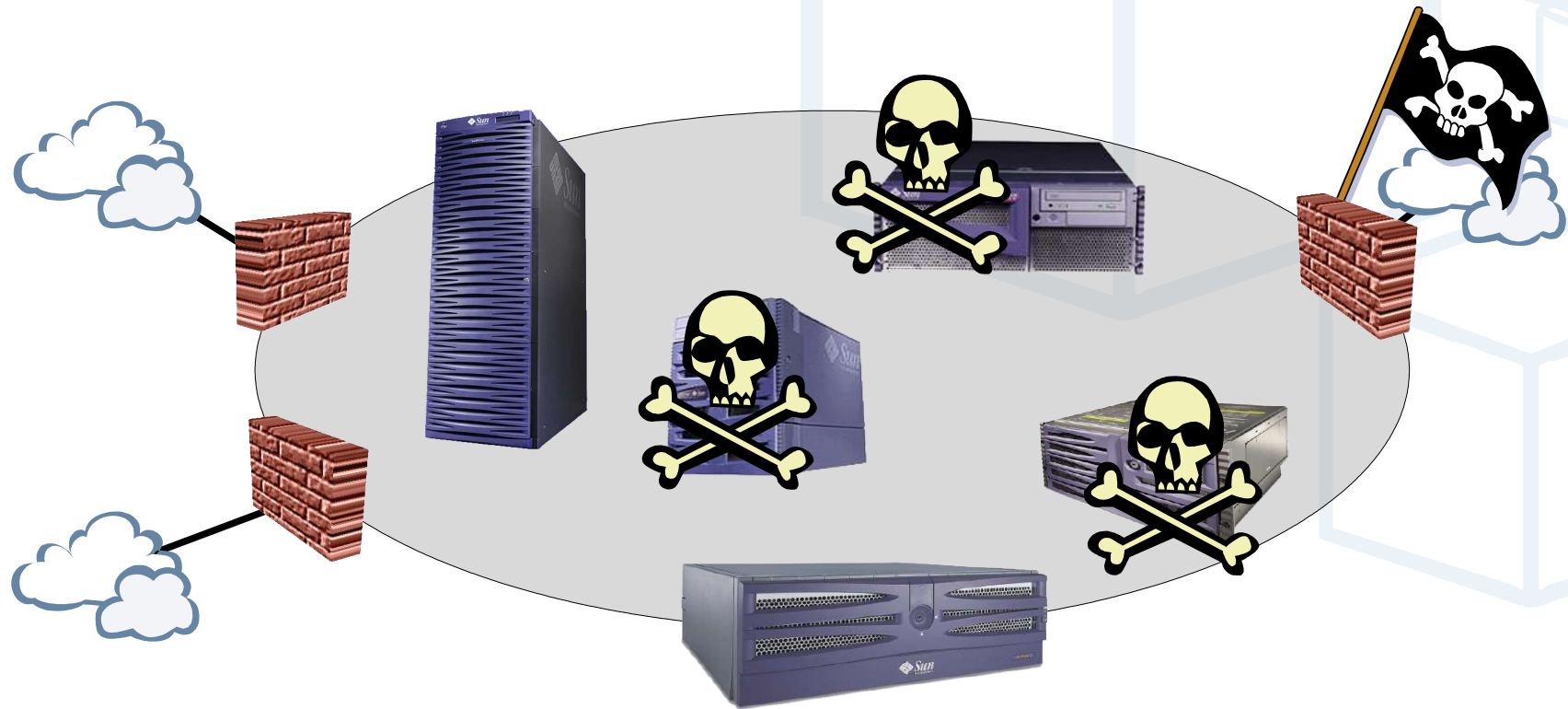
Jediný úplně bezpečný firewall

“The Air Gap”



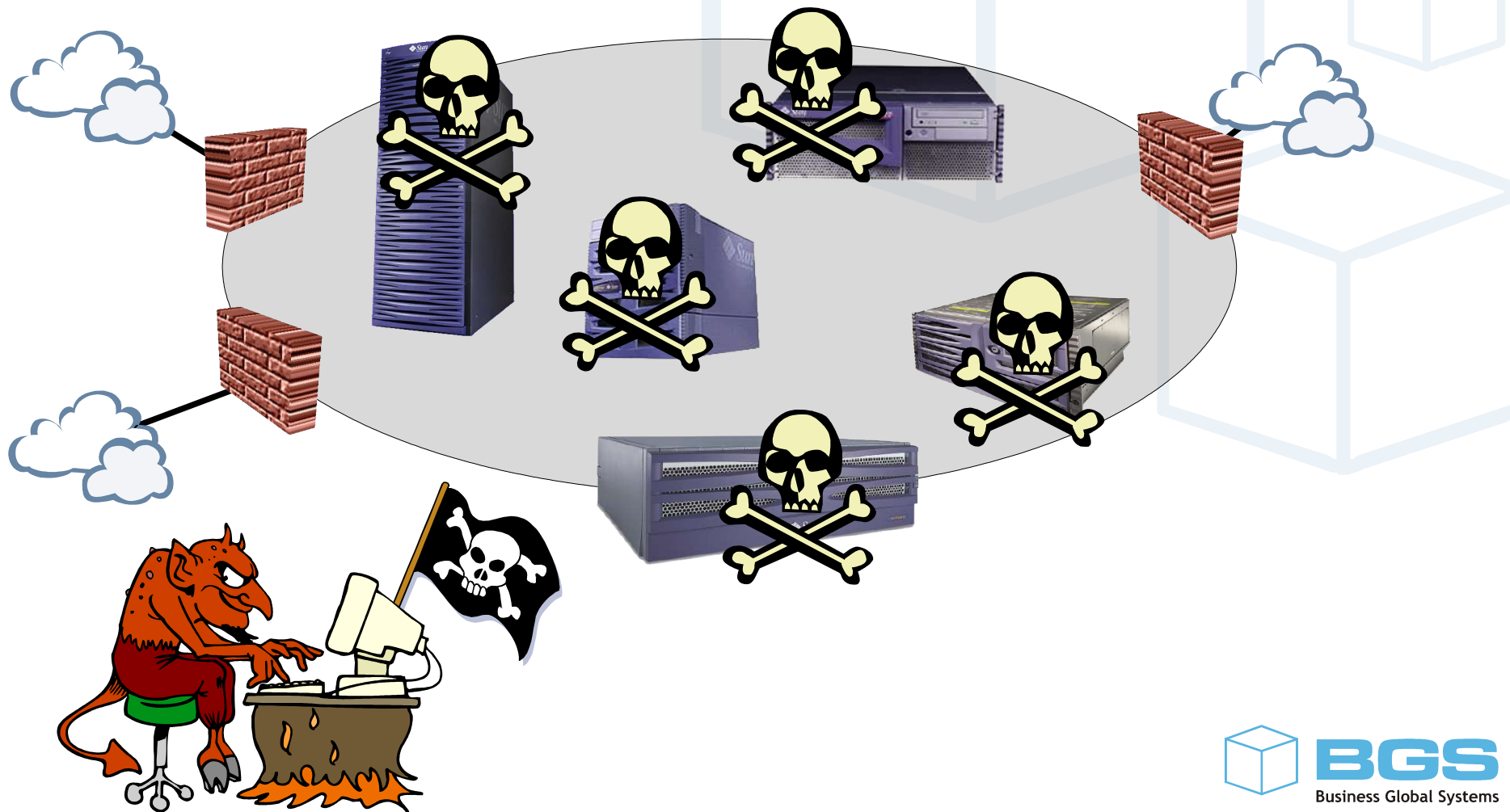
Perimeter Security is Dead!

- Perimeter Security



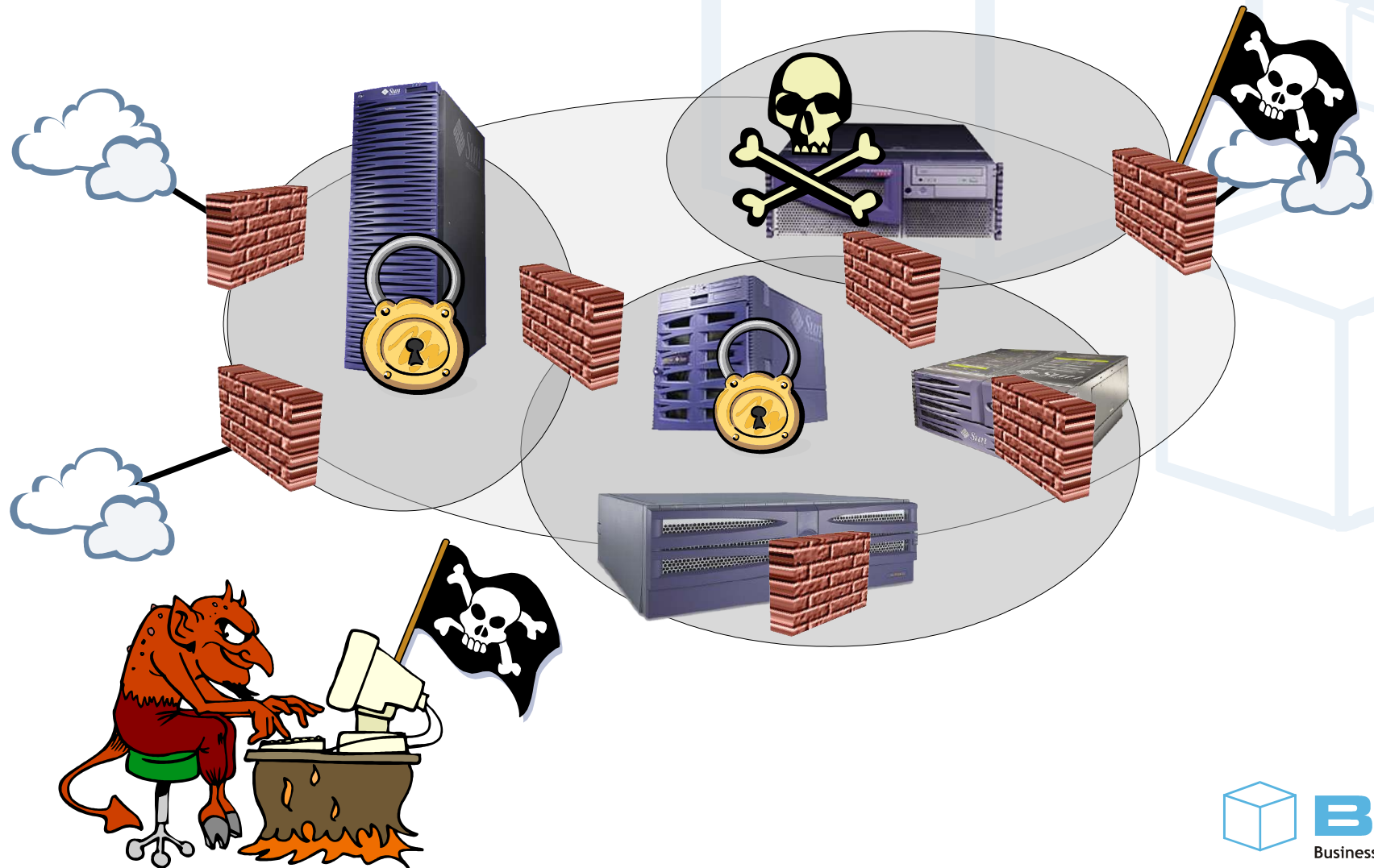
Perimeter Security is Dead!

- Perimeter Security



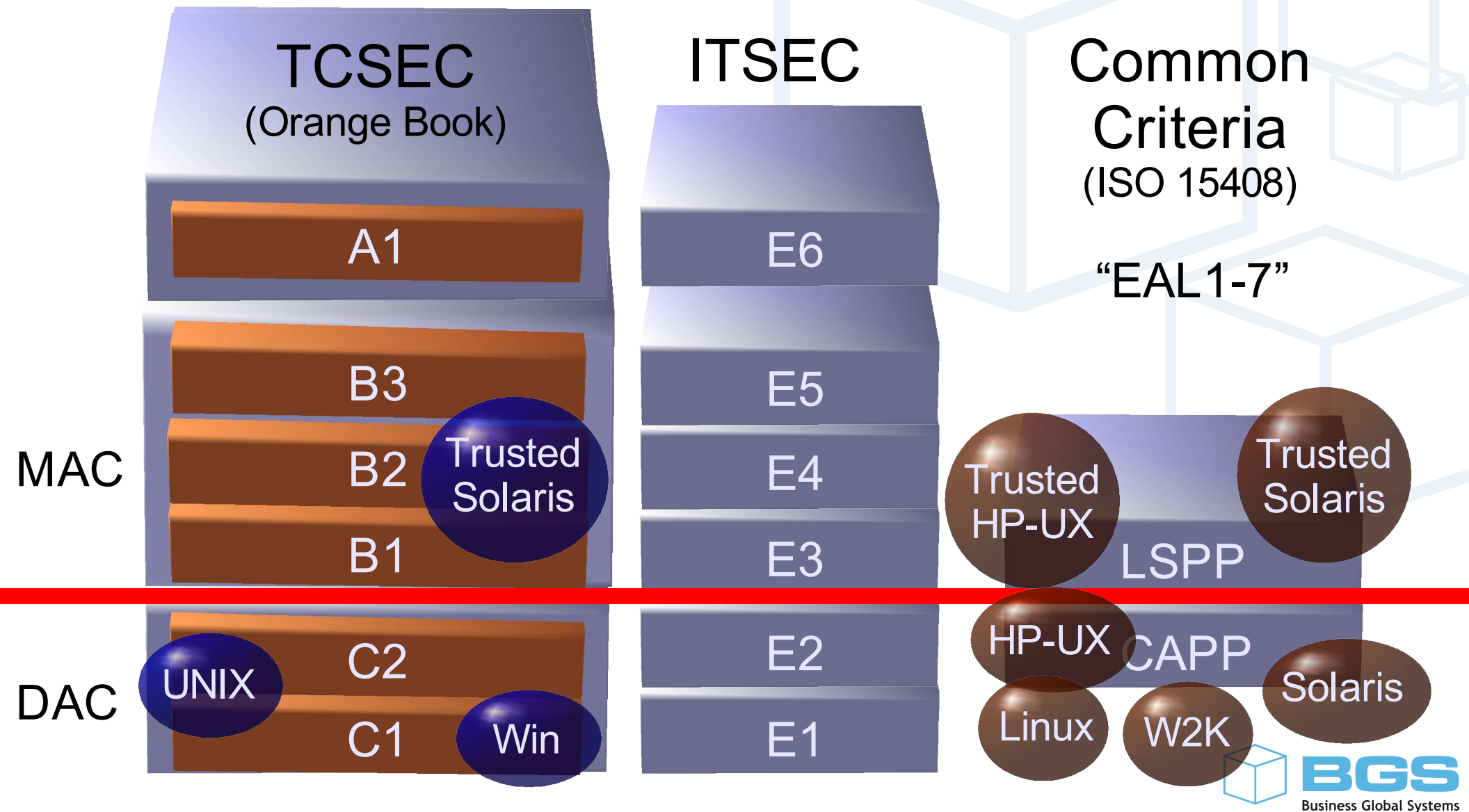
Perimeter Security is Dead!

- Defense in Depth



Common Criteria EAL4

- “Náš produkt bol certifikovaný na EAL4“



Šifrovanie

- **“chránené šifrovaním s použitím 128bit kľúča”**
- Aká šifra?
 - Cézarova? NULL?
- Aký to je kľúč?
 - Nie je to náhodou heslo s entropiou 20bit?
- Aký je kľúčový manažment?
 - Ako sa kľúče generujú? Akú majú životnosť? kde sú uložené?
- Variácia: “Chránené pomocou SSL”

Heslá

- Slabé heslá (“rum”)

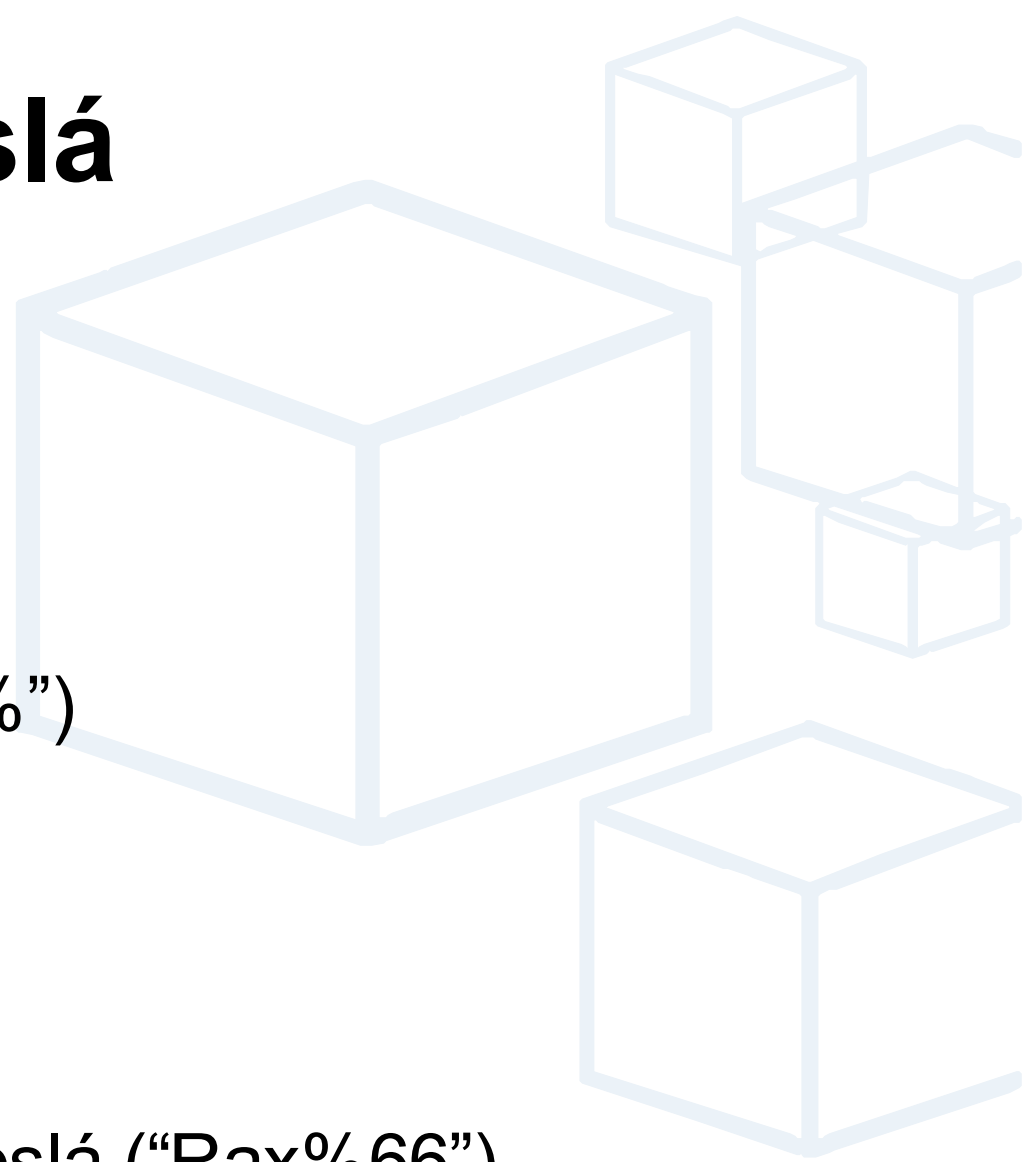
Dížka (Znaky)	Entropia (bit)
4	10
8	18
16	30

- Kombinované heslá (“Rum40%”)

Dížka (Znaky)	Entropia (bit)
4	15
8	24
16	36

- Neslovníkové kombinované heslá (“Rax%66”)

Dížka (Znaky)	Entropia (bit)
4	16
8	30
16	38



Elektronický podpis

- **“chránené pomocou elektronického podpisu”**
- Samotný podpis nič neznamená
- Porebujeme vedieť:
 - Kto podpisuje? (Identita zdroja)
 - Čím podpisuje? (Key management)
 - Čo podpisuje? (formát/jednoznačnosť správy)
 - Ako podpisuje? (algoritmy, zariadenia)
 - Ako často podpisuje? (Je možný brute force útok?)

Zaručený elektronický podpis

Akreditovaná certifikačná autorita

- “elektronický podpis v budúcnosti umožní ...”
- Zákon NR SR č. 215/2002 o elektronickom podpise
- Vyhlášky NBÚ č.537-542/2002
 - Právna účinnosť <= Zaručený el. podpis <= Akreditovaná CA + Bezpečné zariadenie
- Akreditovaná CA:
 - Akreditácia NBÚ Stav k 13.11.2003: 0
- Bezpečné zariadenie
 - Certifikácia NBÚ Stav k 13.11.2003: 2 (pre CA)

Zaručený elektronický podpis

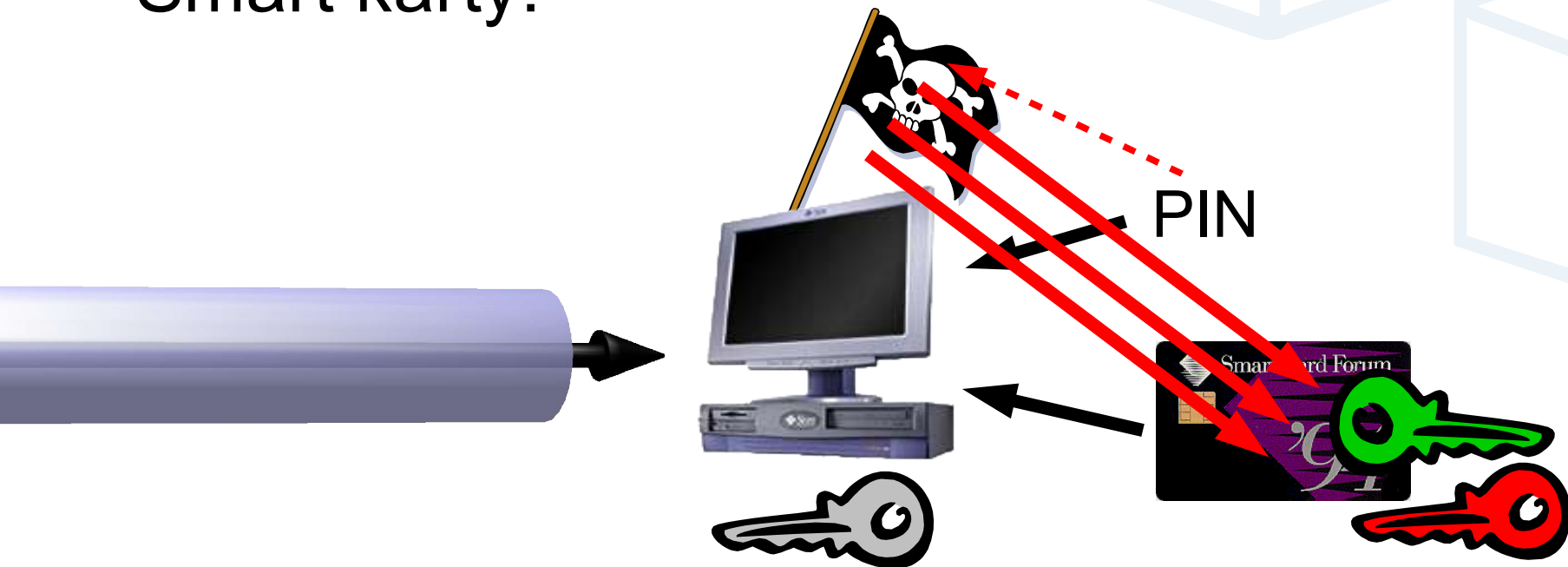
- **“elektronické daňové priznanie”**
- Q: Čo podpisujem?
 - A: ASCII, RTF, PDF, HTML, XML, XHTML, OpenOffice.org XML, HTTPS, S/MIME
(vyhláška NBÚ č.542/02)
 - Problémy:
 - ASCII: znaková sada?
 - HTML: “zobrazovací formát” (#f0f0f0 text na #ffffff podklade)
 - RTF, PDF, XHTML, OOo: to isté ... a neštrukturované
 - HTTPS, S/MIME: protokoly, nie formáty
- Q: Čím podpisujem
 - “Bezpečné zariadenie ...” (zákon č. 215/01)

Public Key Infrastructure

- **“Vytvorenú štruktúru PKI je možné použiť na”**
- **Je náročné vytvoriť všeobecne použiteľnú PKI**
 - Pravdu povediac, takmer nemožné (\$\$\$)
- **Praktické PKI “certifikujú” väčšinou neživé objekty**
 - Servery (HTTPS), Sieťové zariadenia (IPsec), ...
- **Verejná PKI: Problém súkromia**
 - uid=0311136667,cn=Radovan Semančík, ...
 - uid=0311136667
 - cn=Radovan Semančík,mail=semancik@bgs.sk

SmartCard

- “... je bezpečne uložený na Smart Karte”
- Magentické karty, Pamäťové karty, ...
- Wireless prístupové karty – pamäťové
- Smart karty:



Záver

- Pozor na “Snake Oil”
- Pýtajte sa, pýtajte sa, pýtajte sa ...
- Konzultujte

Questions?



Thank you ...

Ing. Radovan Semančík

Business Global Systems, a.s.
Pluhová 2
83248 Bratislava

semancik@bgs.sk

