Efektivní řízení rizik webových a portálových aplikací

CLEVERLANCE Enterprise Solutions a.s.

Ing. Jan Guzanič, CISA, Senior IT Security Consultant

Mob.: +420 602 566 693

Email: jan.guzanic@cleverlance.com

18.2.2009

Naše kompetence z oblasti IT security

Podporujeme strategický růst svých klientů pomocí inovací a netradičních přístupů k řešení problémů v oblastech *bankovnictví, pojišťovnictví, telekomunikací a státní správy*.

Analýzy rizik IS, zavedení procesu řízení inform. rizik

Vlastní antivirové a antispamové řešení

Návrhy systémů v oblasti IT security (FW, DLP, IPS, PKI)

Bezpečnost při vývoji aplikací

Penetrační testy, prověrky frontendových aplikací

Školení a kurzy (hacking, bezpečnost ICT)

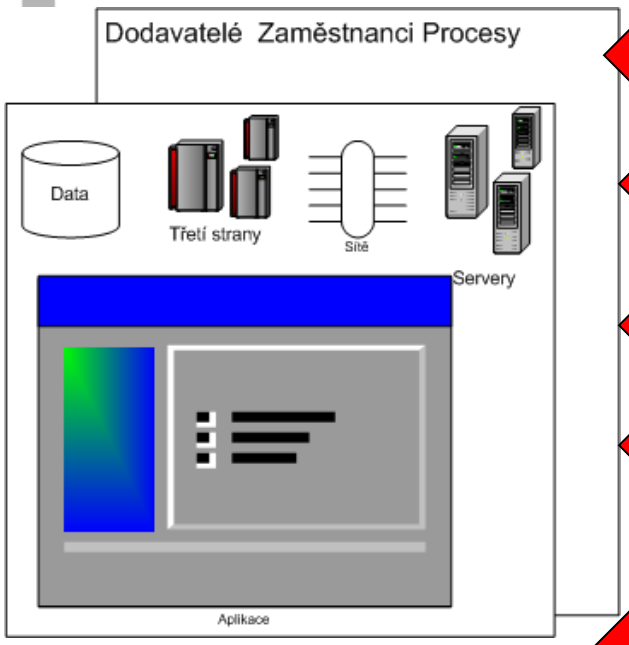
Návrh a implementace Fraud Detection Systémů

AEC
DATA SECURITY COMPANY

AEC, spol. s r.o. – security divize Cleverlance

Cleverlance
The Clever Enterprise Solutions

Hrozby elektronickému podnikání



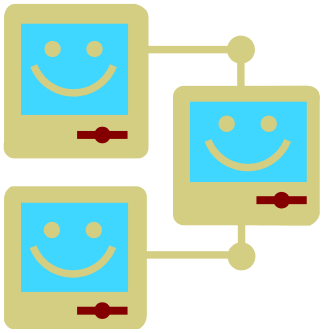
Porušení Důvěrnosti, Dostupnosti či Integrity Informací

Zcizení zákaznických dat, osobních údajů

Zcizení zboží, peněz, služeb, transakcí

Odepření služeb

Následné související škody, náklady



Zisk

Cleverlance
The Clever Enterprise Solutions

Ekonomika útočníků

Služby a zboží	Cena	Nástroje	Cena
Detaily o bankovních účtech	10 - 1000 USD	Botnet	150 - 300 USD
Kreditní karty s CVV2	0.5 - 12 USD	Autorooter	40 - 100 USD
Kreditní karty	0.10 - 25 USD	SQL Injection	15 - 150 USD
Plné identity	0.90 - 25 USD	Shopadmin	20 - 45 USD
Služby výběru peněz	8% - 50%	RFI, LFI,XSS scanner	5 - 100 USD

Zdroj: Symantec ISTR, 24.11.2008

Nikoliv „Mafie“, ale ekonomické zákonitosti jsou driverem útoků na nichž se podílí:

- Spammer , autor malware, majitel Botnetu
- Překupníci , **Cashieři – de facto určují poptávku**
- Hackeří
- Senioři vedou business
- Black hat komunita dodává know-how

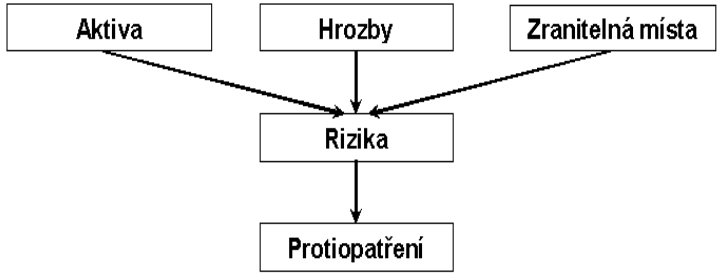
Cleverlance
The Clever Enterprise Solutions

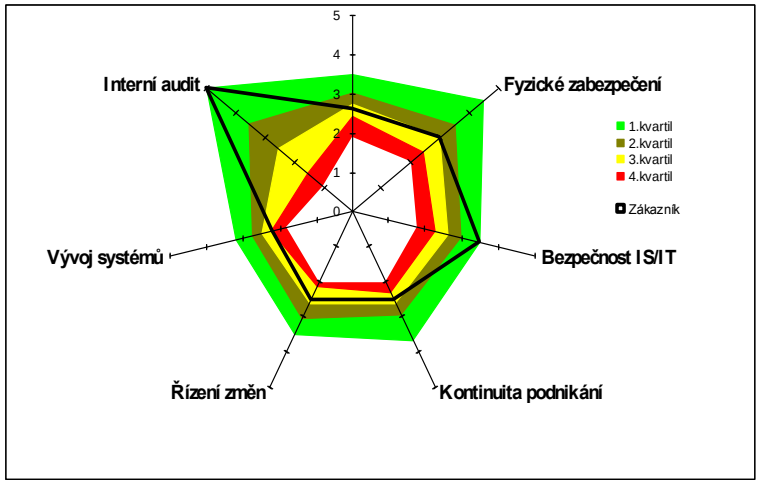
Životní cyklus aplikace a bezpečnost

"Bezpečnost budovaná od počátku je levnější"

Cleverlance
The Clever Enterprise Solutions

Kontinuální zlepšování bezpečnosti a význam přístupu analýzy rizik





Hlavní cíl analýzy rizik :

- Určit priority co a jak chránit.
- Jde o to netrávit čas chráněním něčeho, co nemá pro organizaci cenu.

Cleverlance
The Clever Enterprise Solutions

Bezpečnost vývoje aplikací - Metodiky

Důraz

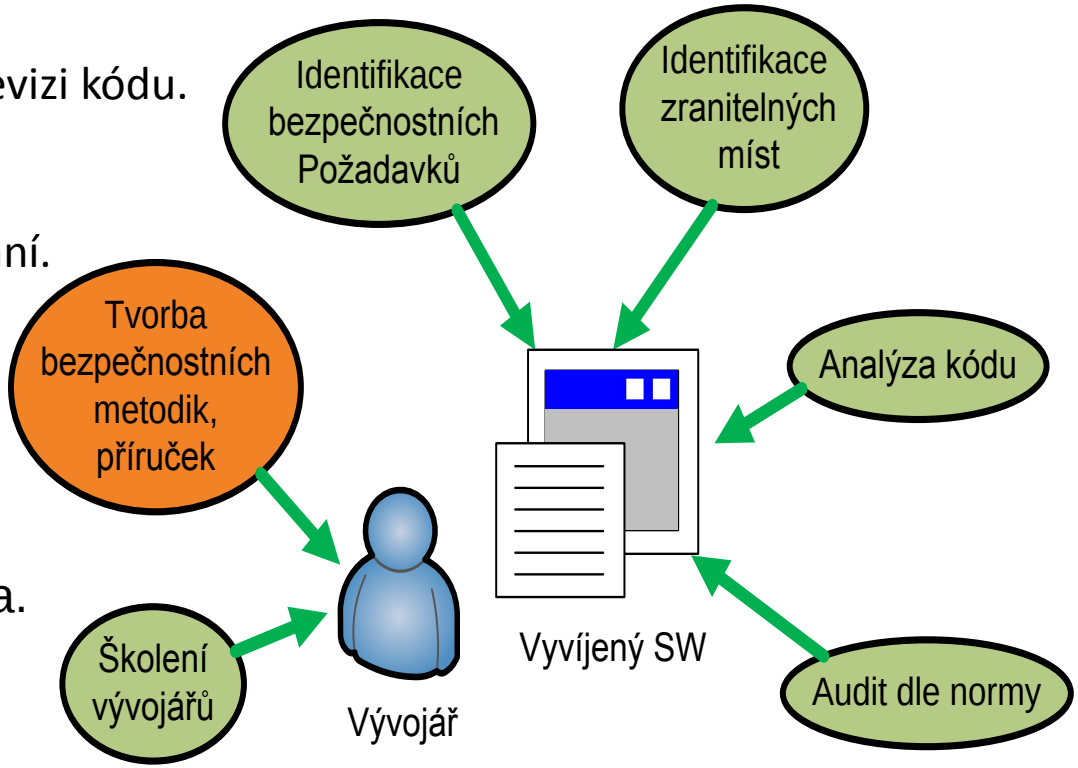
- Vypracování metodik, nástroje pro revizi kódu.
- Školení vývojářů.
- Výběr vhodných nástrojů pro testování.
- Odstranění bezpečnostních chyb

dříve než je SW uveden do provozu.

Metodiky

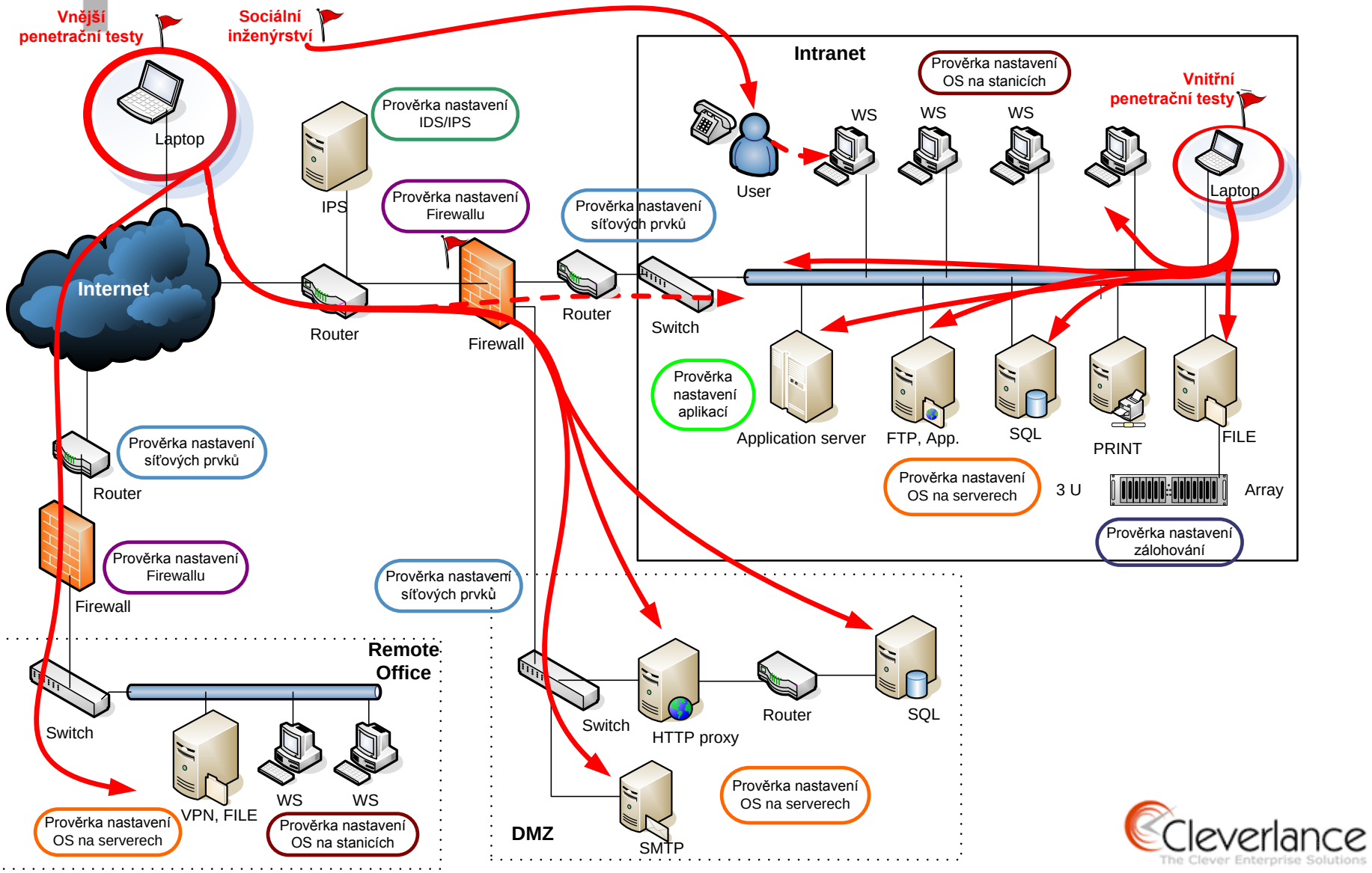
- ISO/IEC 15408 - Common Criteria.
- OWASP, WASC, IATF
- Metodiky založené na vlastních

praktických zkušenostech vývoje SW.



Cleverlance
The Clever Enterprise Solutions

Způsoby testování bezpečnosti



Cleverlance
The Clever Enterprise Solutions

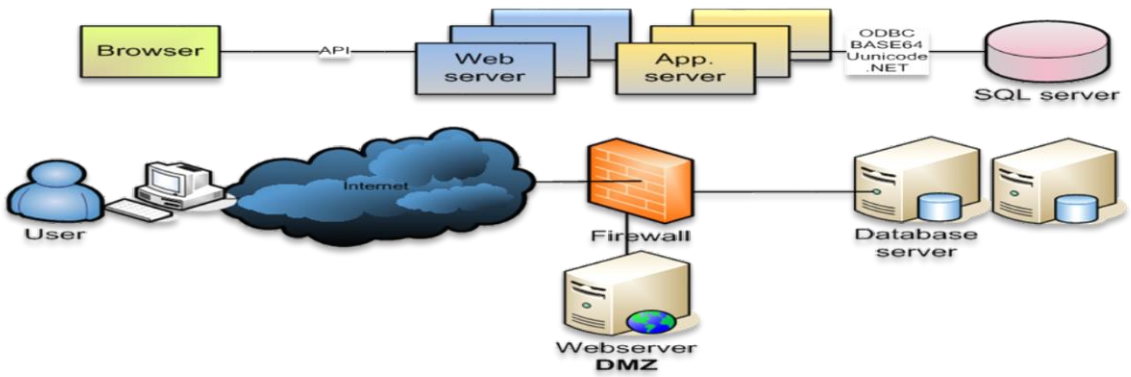
Prověrky bezpečnosti frontendových (webových) aplikací

U prověřování sofistikovaných IS na vícevrstvé architektuře selhávají klasické metody.

Proto jsme vyvinuli novou metodiku testování.

Těžiště zranitelnosti se posunulo k aplikačním zranitelnostem:

Cross Site Scripting
Injection Flaws
Malicious File Execution
Insecure Direct Object Reference
Cross Site Request Forgery
Zdroj: OWASP Top Ten 2007



Aplikace na různém framework (.NET, PHP, …)	Implementace SSL a protokol HTTPS	Pochopení logiky aplikace	Složitost systémů

Cleverlance
The Clever Enterprise Solutions

Hlavní bolesti při útoku

Symptomy:

Málo informací v prvotních fázích útoku	Nárůst počtu incidentů v čase	Prodleva při organizaci ad-hoc reakce	Prodleva při hledání, vývoji a nasazení ad-hoc protiopatření	Absence interních a externích zdrojů	Schopnost reagovat na rozsáhlá epidemie a případně DoS

Příčina: „Přetížení role bezpečnostního správce“

- Znalosti potřebné pro řešení útoku jsou vždy jiné
- Každý typ útoku vyžaduje odlišné kompetence,informační zdroje, procesy, scénáře a zdroje

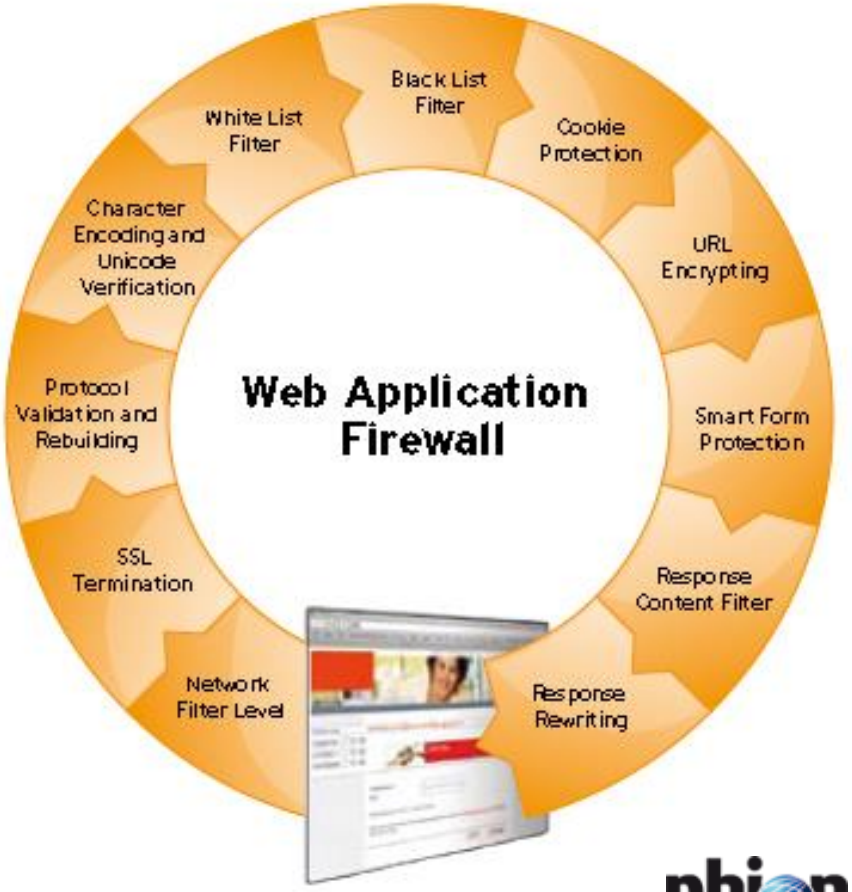
Cleverlance
The Clever Enterprise Solutions

Aplikační firewall – nový trend

Chrání datový a nikoliv jen síťový provoz!

Velmi vhodné pro aplikace:

- Jejichž bezpečnost je obtížné či nemožné řešit klasicky
- Zabezpečení obzvláště citlivých aplikací
- Efektivní zajištění provozní bezpečnosti více aplikací



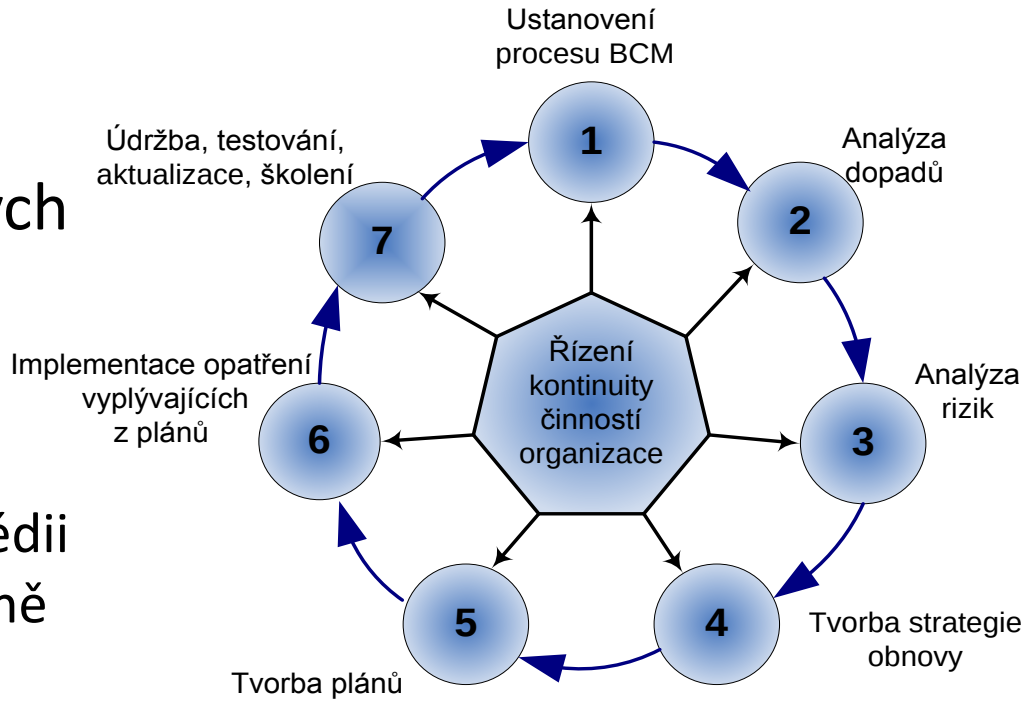
phion

Cleverlance
The Clever Enterprise Solutions

Účinná reakce

Být připraven – havarovat bezpečně !

- Havarijní plánování
  - Využití scénářů
  - Využití předem zajištěných zdrojů a partnerství
  - Plány obnovy
  - Plány komunikace
    - Interní, se zákazníky a médii
    - Informovat včas a korektně
    - Dát praktické informace
  - Vyhodnotit útok/událost
    - Následné kroky a poučení se



Cleverlance
The Clever Enterprise Solutions

Cleverlance
The Clever Enterprise Solutions

V krátkém období se zaměřujte na boj s aktuálními riziky
V dlouhém období se zaměřte na budování komplexního řešení

Efektivní řízení rizik webových a portálových aplikací

Děkuji za pozornost a přeji příjemný zbytek dne

Ing. Jan Guzanič, CISA, Senior IT Security Consultant
Cleverlance Enterprise Solutions a. s.
Mob.: +420 602 566 693
Email: jan.guzanic@cleverlance.com

18.2.2009