Hacking – Jak reálná je tato hrozba? Jak se jí bránit?

Mgr. Karel Miko, CISA (miko@dcit.cz)

DCIT, s.r.o (www.dcit.cz)

Úvod

- *Hacking – reálná hrozba současnosti, co si pod ní ale v praxi představit?*

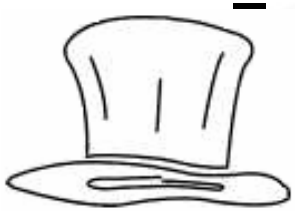
- Obsah přednášky:
  - Taxonomie hackingu (druhy útoků, typy hackingu aj.)
  - Hacking & reálná praxe (praktické hrozby a dopady)
  - Protiopatření v běžném provozu organizace
  - Penetrační test jako účinný kontrolní nástroj

Hacking je když …

- v kontextu této přednášky – *napadení a průniky do systémů a aplikací s cílem ovládnout cíl útoku nebo zneužít či alespoň negativně ovlivnit jeho funkčnost*
- historie sahá k počátkům prvních počítačů („internetový“ hacking - 1987 Internet Worm)
- hacking/cracking – nejednotná terminologie
- motivace bývá různá:
  - osobní prospěch (útočníka či třetí osoby)
  - prezentace osobních postojů hackera „hacktivism“
  - zviditelnění se v rámci komunity
  - „zábava“ (na různé etické úrovni)

Podle klobouku poznáš Hackera

- existují hackeři a ti co to o sobě jen tvrdí (script kiddies apod.) – obě skupiny mohou být stejně nebezpečné
- „politické“ rozdělení hackerské scény:
  - White Hats – někdy též etičtí hackeři, nezávislí experti a konzultanti, individuality, komerční security laboratoře aj. (jimi odhalené slabiny jsou zveřejňovány, často business)



  - Black Hats – uzavřená společnost hackerů, jejichž cílem je nalezení bezpečnostních slabin a jejich vyžití pro „vlastní potřebu“ (řadu bezpečnostních slabin odhalí dříve než WH, téměř nikdy je nezveřejňují)

- svět není černobílý (Gray Hats)
- vztahy WH-BH jsou často napjaté

Co potřebuje správný Hacker

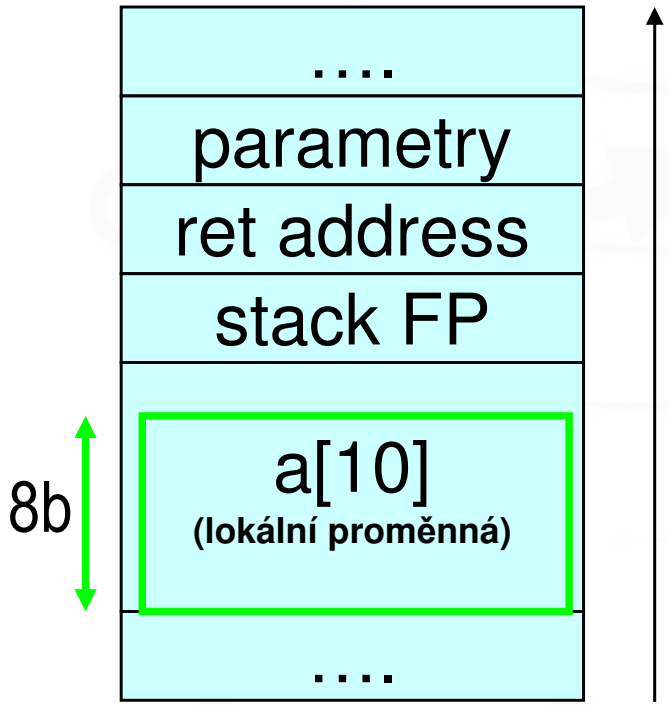
- Nástroje
  - škála používaných nástrojů je obrovská, řada z nich je volně dostupná na Internetu
  - řada nástrojů je vlastní výroby – hacker ≈ programátor
- Znalosti
  - hacker (s výjimkou script kiddies) obvykle disponuje poměrně detailní technikou znalostí, kterou si musí průběžně udržovat – tj. potřebuje i dostatek času
- Informace
  - hacker potřebuje přístup k informací (některé jsou veřejně dostupné jiné jen v uzavřené komunitě)

Nejčastější techniky

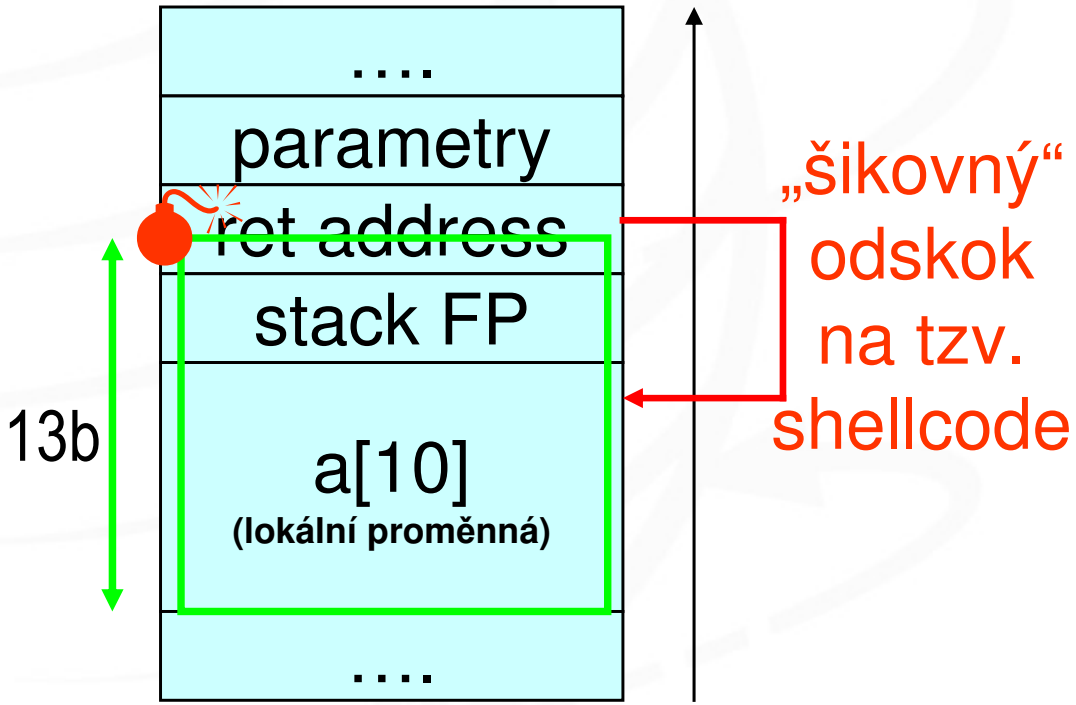
- Zneužití Buffer Overflow (BOF) – poměrně velký okruh slabin, jejichž příčinou je programátorská chyba … →
- Zneužití chyb ve WWW aplikacích – nejčastěji SQL injection či podobné variace
- Síťové techniky
  - Sniffing – odposlech síťové komunikace
  - IP Spoofing – předstírání cizí IP adresy
- Denial of Service (DoS) útoky
  - flooding (zahlcení linky, zahlcení systému požadavky, …)
  - distribuované DDoS (při současných technologiích prakticky není obrany)
- Červi, trojské koně („social hacking“ – sociální inženýrství) … →
- Útoky na heslo – hádání hesel, lámání hashů … →

Buffer overflow – princip

Stav zásobníku za normální situace



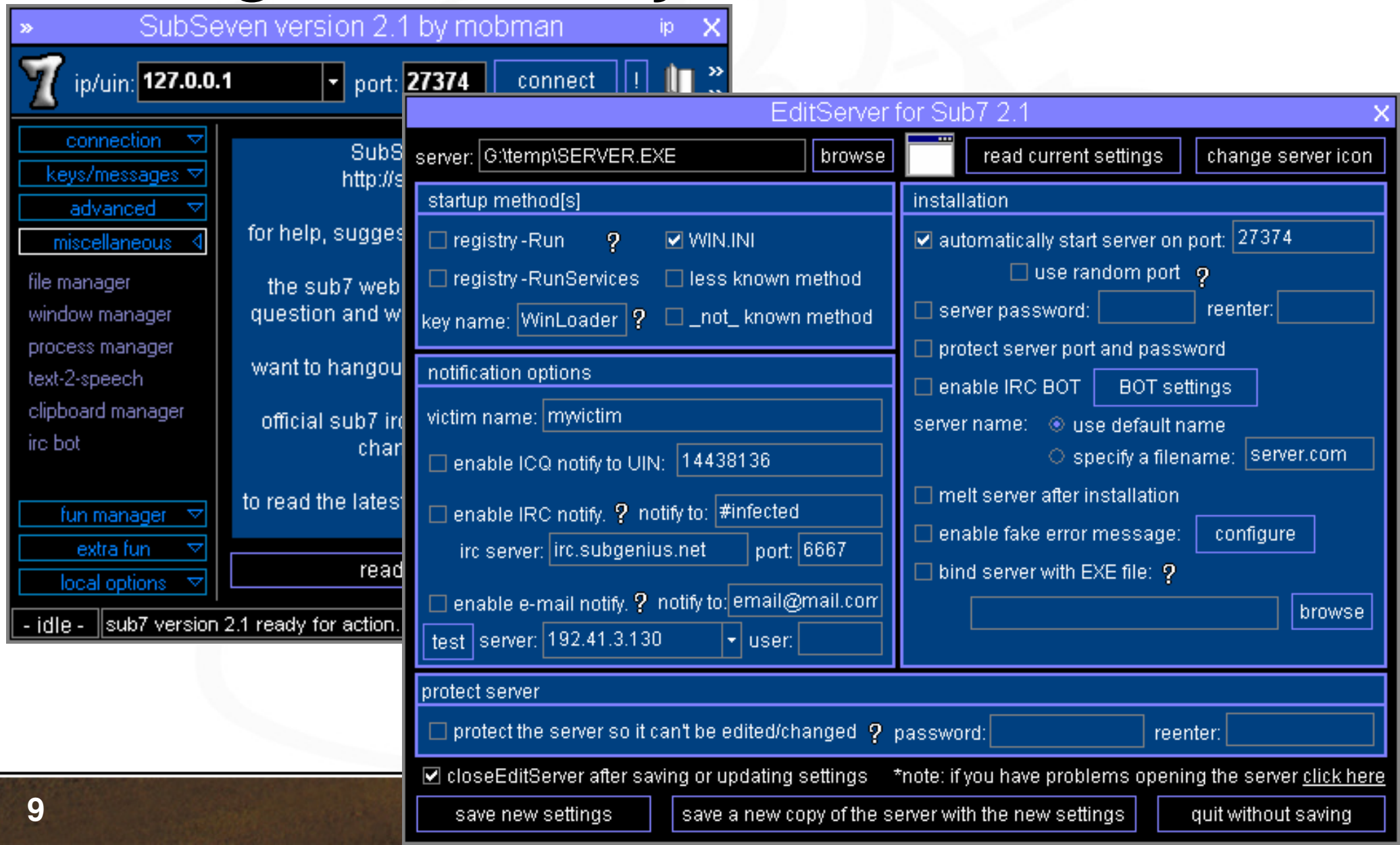
Stav zásobníku při neče-kaně dlouhém parametru



Útoky na hesla

- Hádání/lámání hesel
  - Základ: slovníkové útoky vs. hrubá síla
  - Dnes již i sofistikovanější heuristické metody
  - Výkonnost běžně dostupné výpočetní síly roste (kvalita hesel přirozeně stagnuje)
  - U některých slabších hashovacích funkcí není problém v historicky krátké době projít celý prostor hesel (o délce cca 15)
  - Přestože kvalita hesel je tradiční bezpečnostní problém, realita bývá i dnes velmi smutná

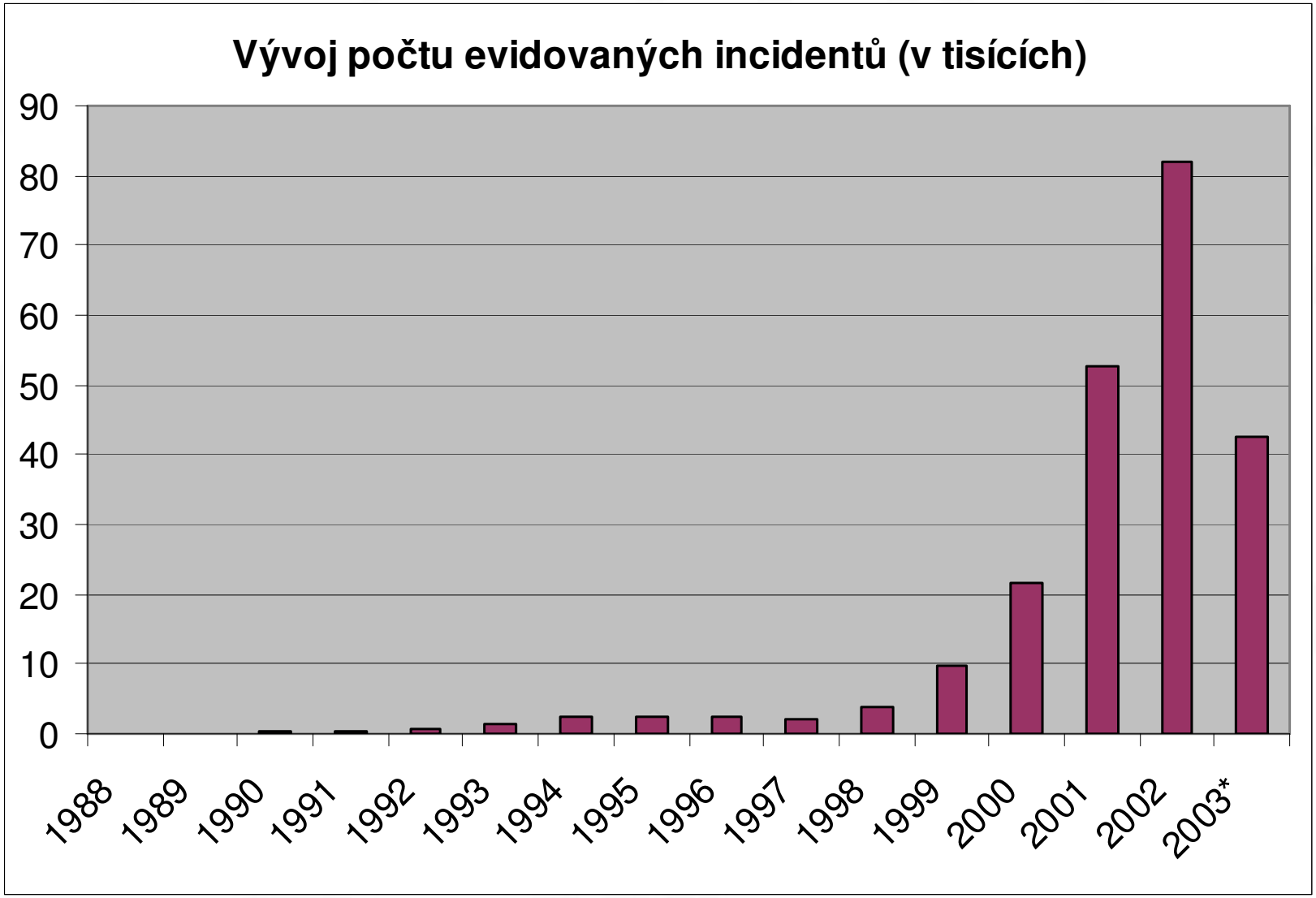
„konfigurace“ trojského koně Sub7



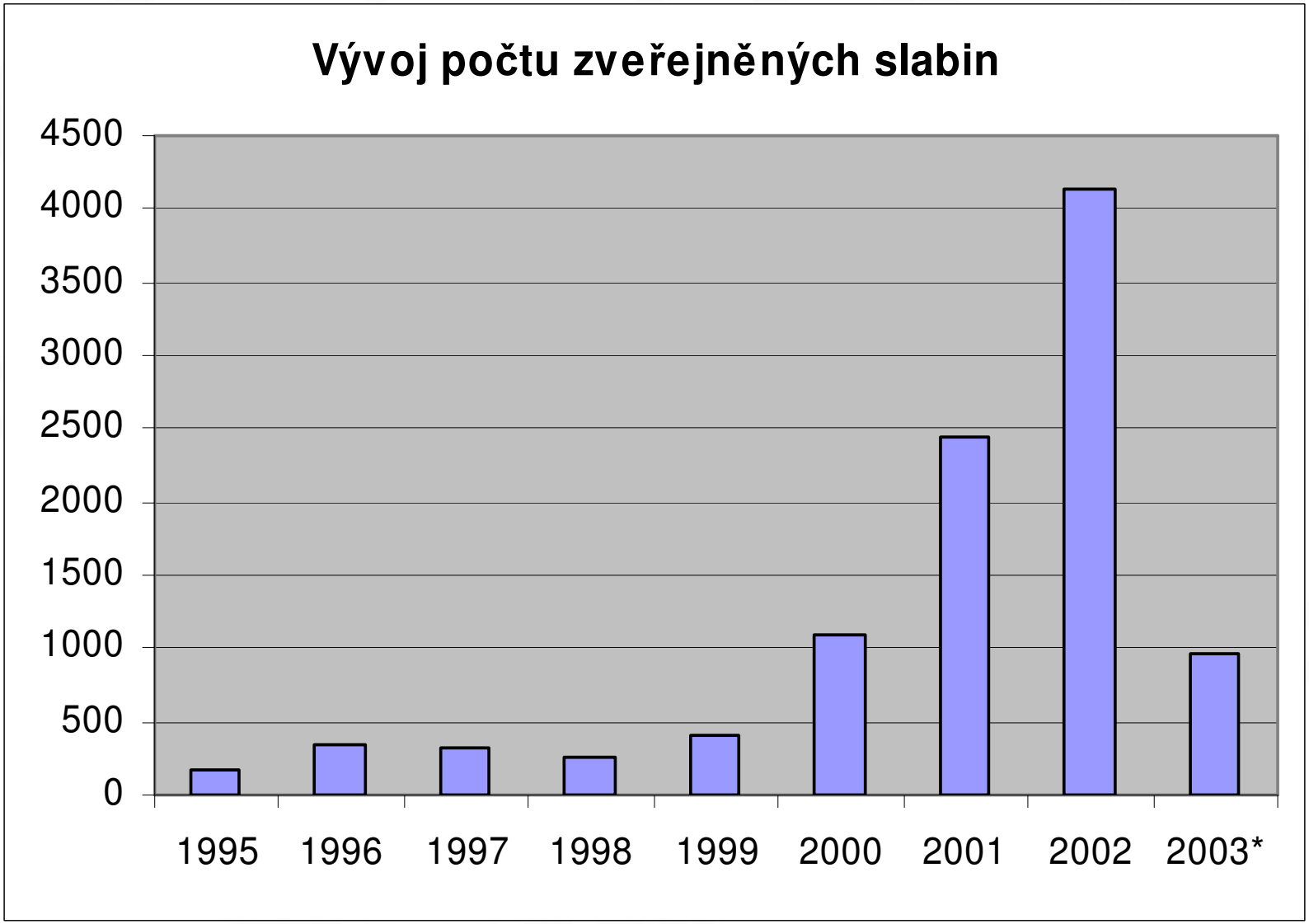
Hacking v reálné praxi

- bezpečnostní slabiny nevznikají, existují již léta jen se o nich neví - v horším případě je znají jen někteří (blackhats)
- zranitelný systém neochrání IDS ani správce u konzole
- zabezpečení dodávaných systémů není ani u renomovaných dodavatelů samozřejmostí (ti navíc často garantují funkčnost jen na „své“ konfiguraci)
- dobrá rada: systémy přístupné z Internetu by měly apriori počítat s tím, že budou (resp. mohou být) napadeny

Statistika – CERT (16.4.03)



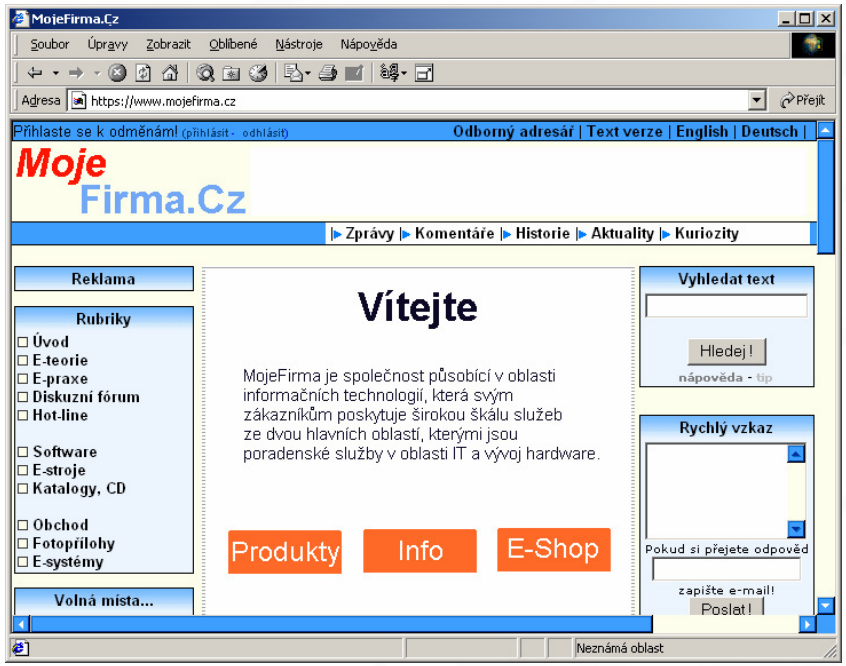
Statistika – CERT (16.4.03)



Jaký může být výsledek útoku

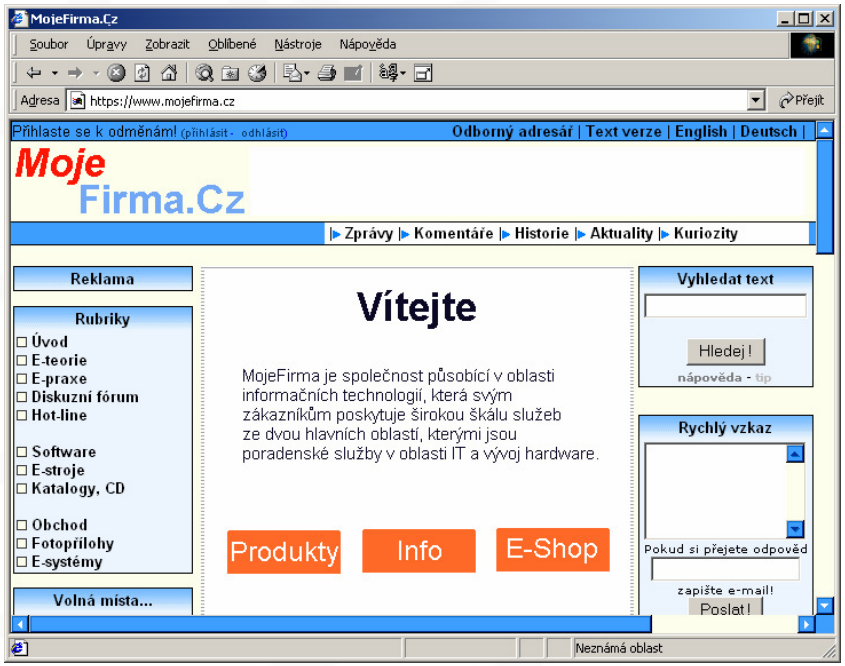
Příklad … →

před útokem



- firewall – instalován, funguje
- jediný přístupný port (443/tcp)
- WWW aplikace funguje

po útoku



- firewall – stále funguje
- stále jediný přístupný port (443/tcp)
- WWW aplikace stále funguje

(vizuální rozdíly nehledejte !!!)

Skutečné hrozby hackingu

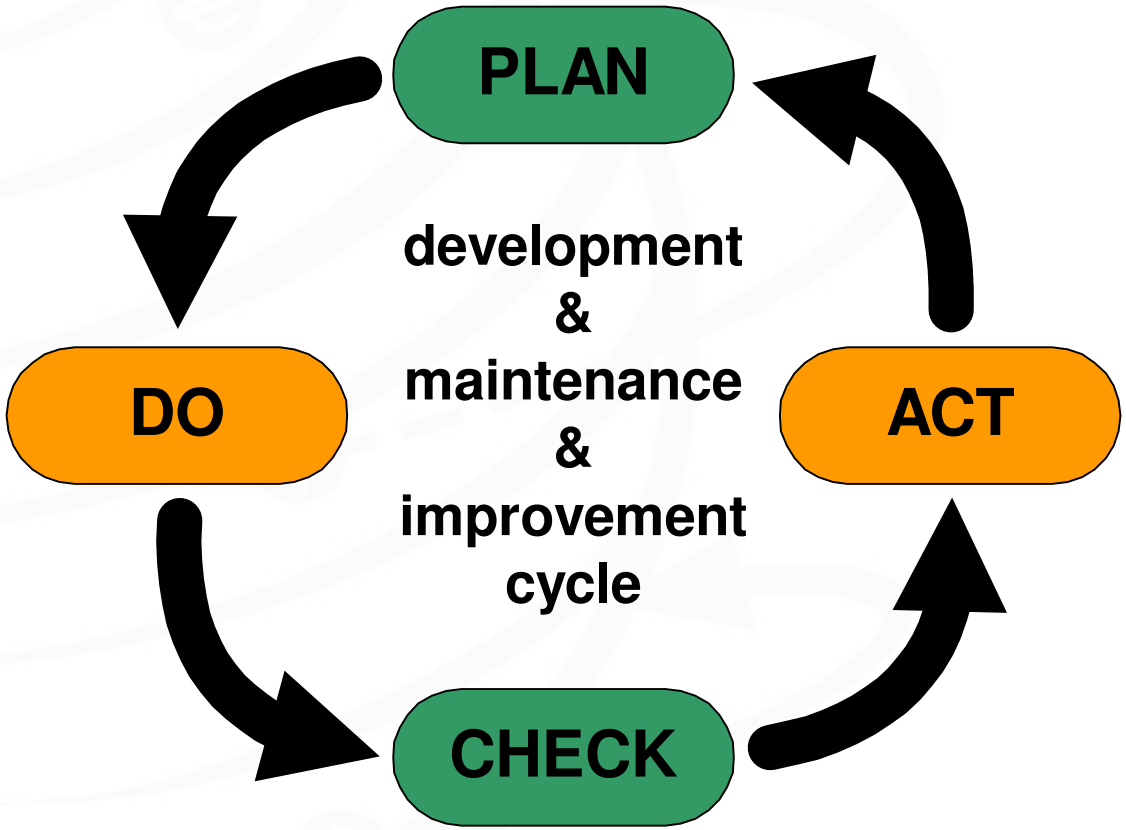
- napadení nemusí být na první pohled „viditelné“ (útočníci, kteří se nezviditelňují – skutečná hrozba)
- největší hrozbou je lidský faktor
  - zejména vlastní uživatelé (vědomě či nevědomě)
  - neodborné zásahy příp. „backdoory“ administrátorů
- z hlediska odhalení jsou nejproblematičtější zcela specifické chyby v aplikacích „na míru“
- červi (přijdou noví, horší), DDoS (stále není obrany)

Protiopatření (technická)

- Firewall
  - v současnosti prakticky nutnost, technologicky „usazená“ oblast
- IDS
  - hlavně monitorovací nástroj, možnosti předcházení útokům omezené (a často přeceňované) – efektivní provoz vyžaduje nastavení patřičných interních procesů
  - dynamický vývoj technologie – v budoucnu stoupne její význam
  - „stroj“ může efektivně bojovat pouze proti „stroji“
- Content security (ochrana před „zlovolným“ SW)
- I špičkovou technologii lze provozovat nebezpečně !

Bezpečnost – permanentní proces

- bezpečnost nelze vyřešit jednou pro vždy – cyklus kontinuálního zdokonalování
- musí existovat a fungovat patřičné interní procesy
- všechny hrozby nelze pokrýt technickými opatřeními
- v technologicky složitém prostředí nutno udržovat intelektuální infrastrukturu



Penetrační test – kontrolní nástroj

- Penetrační test je zhodnocení bezpečnosti hodnoceného systému (sítě) pokusem o průnik
  - metodami i použitými nástroji blízký reálnému útoku (zvláště varianta „bez znalosti“) - Ethical Hacking
  - je prováděn vzdáleně - po síti (z internetu - „externí“, z vnitřní sítě - „interní“)
  - ve „skryté“ variantě prověří také monitorovací a reakční mechanizmy (dohled nad systémem)
  - předmětem jednotlivá zařízení případně část sítě
  - jedním z hlavních přínosů je využití kombinačních schopností odborníků - v tzv. „aktivní variantě“

Průběh penetračního testu

- Varianty testů
  - externí (simulace hackera z Internetu)
  - interní (simulace útočníka uvnitř - př. nespokojený zaměstnanec)
  - speciální varianty (testy WWW aplikací, Wi-Fi sítí apod.)
- Základní kroky penetračního testu
  - rekognoskace - sběr informací o testovaném prostředí (registrované IP adresy, DNS domény, ...)
  - automatizované testy bezpečnostních slabin
  - detailní manuální testy na základě výsledků aut. testů
  - praktická demonstrace zneužití slabin (provedení útoku)

Výsledek penetračního testu

- Výsledek penetračního testu Vám poskytne obrázek o tom, čeho by při současné úrovni znalostí mohl dosáhnout útočník při reálném útoku
  - výstupem je nejen nález, ale i doporučení
  - ani negativní výsledek testu nedává „jistotu“ (ta se těžko hledá)
  - reálný útočník disponuje „neomezeným“ časem
  - nástroje a metody jsou stále agresivnější
  - znalost bezpečnostních slabin se neustále vyvíjí, řada existujících slabin nebyla doposud odhalena / zveřejněna (význam opakování)

Zkušenosti z praxe (1)

- Obejití filtrovacího mechanizmu
  - Testován WWW server, na kterém portscanem zjištěny pouze porty 21 a 80, žádná z těchto služeb netrpěla zneužitelnou bezpečnostní slabinou
  - Fragmentovaný portscan odhalil nedostatečný filtrovací mechanizmus (jako firewall použit „pouze“ filtrující router)
  - Připojením pomocí RPCklienta a fragrouteru na port 139 byl získán anonymní přístup (NULL session)
  - Z veřejně dostupné části registry přečteno „zahashované“ heslo k běžícímu VNC serveru
  - Po rozluštění (vypočtení) hesla získán plný přístup

Zkušenosti z praxe (3)

- SQL Injection
  - prověření dostupnými scannery nezjistilo žádné slabiny
  - WWW aplikace s dynamickými stránkami typu *https://app.firma.cz/pages/list.swx?p=1564*
  - Pomocí následujícího URL (výroba trvala několik dní) …

https://app.firma.cz/pages/list.swx?p=OV'+UNION+SELECT+'1','2',K_PRIJMENI||';'||K_RC||';'||K_ADR0||';'||K_ADR1||';'||K_ADR2||';'||K_NUM||';'||K_PSC||';'||K_EMAIL||';'||K_MOBIL||';'||K_NUM_UCTU+FROM+KLIENT+WHERE+AND+K_PRIJMENI+LIKE+'%25'+AND+1<2||,

  - … byla získána osobní data klientů z repliky provozní DB

Zkušenosti z praxe (4)

- Časté způsoby napadení
  - Slabá hesla (mnohdy stačí k uhodnutí <5000 pokusů)
  - Default hesla – SYSTEM-SYSTEM apod.
  - Trestuhodné chyby v návrhu WWW aplikací
  - Veřejně zapisovatelné skripty, jenž jsou pravidelně spouštěny pod privilegovaným uživatelem
  - Ukázkové příklady v adresářích WWW serverů (často obsahují řadu chyb a je možno je zneužít)
  - Hodně informací lze vytěžit z odposlechnuté komunikace (zejména odposlech na napadeném serveru)
  - Provozování „testovacích“ serverů

Zkušenosti z praxe (5)

- Test bezpečnosti Wireless sítě
  - V dohodnutém prostoru identifikována IEEE 802.11b síť na kanálu číslo 10 (2,457 GHz) s BSSID xx:yy:…
  - ESSID sítě je řetězec „COMPANY“, síť byla zabezpečena šifrováním (WEP – Wired Equivalent Privacy)
  - Odposlechem bylo v průběhu cca 4 hodin odchyceno asi 3 mil. šifrovaných datových rámců z nichž asi 3000 vyhovovalo použití pro následující kryptoanalytický útok, který odhalil použitý šifrovací klíč
  - Zpětně byla zjištěným klíčem dešifrována předchozí odchycená komunikace (identifikována „běžná“ komunikace vnitřní sítě)

Zkušenosti z praxe (6)

- Penetrační testy trochu jinak:

Na parkovišti dvoru budovy bylo zjištěno, že někteří zaměstnanci prověřované firmy chodí v pracovní době na tento dvůr, kde se objímají a líbají, a to ve dvou případech v rozmezí asi 30 min.

(úryvek ze zprávy z objektového penetračního testu)

Závěr
Otázky?

kontakt:

Karel Miko – miko@dcit.cz, tel. 220561353

DCIT, s.r.o. – http://www.dcit.cz