SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Jak zorganizovat penetrační testy a nespálit se

Jiří Vábek

Komerční banka, a.s.

Obsah

- Úvodem (o čem to bude)
- Co, proč a jak chceme
- Výběr dodavatele
- Organizační zajištění
- Výsledky a jejich zpracování
- Co dál? Příběh nekončí…
- Závěr

Úvodem

„I don’t get what all these pentesting companies are doing. Just how much testing does a pen need?”

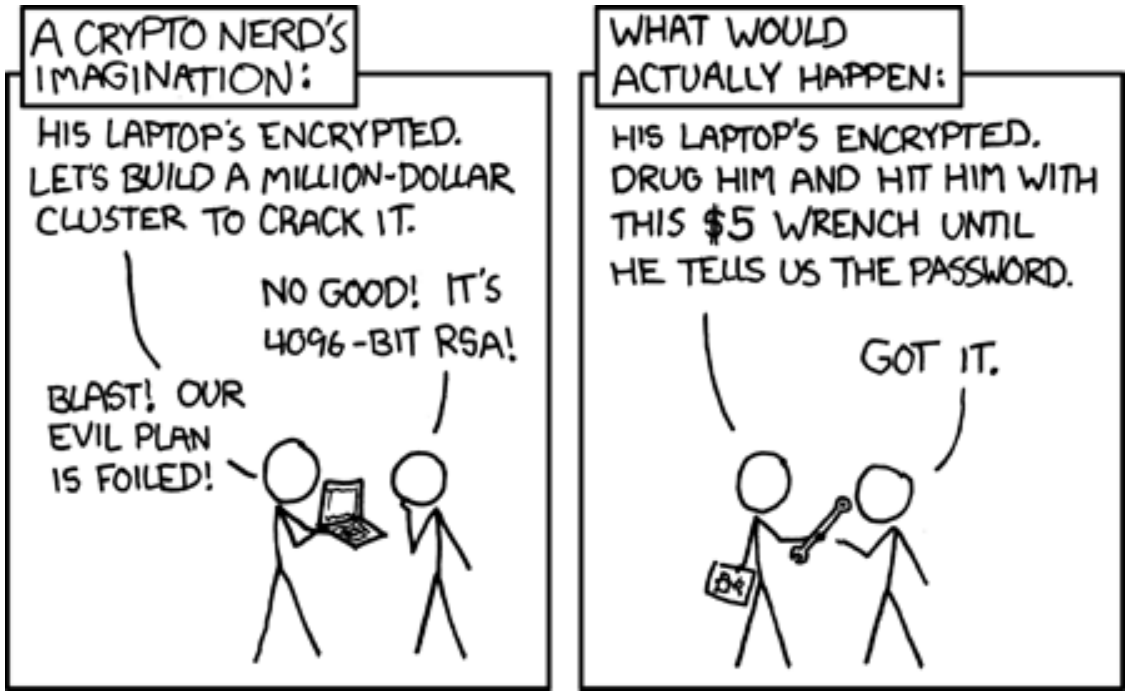
O čem bude prezentace

- Pohled z role bezpečnostního architekta
  - …který má v zodpovědnosti (0-100%):
    - Diskuze s klientem o požadavcích
    - Tvorba zadání penetračních testů
    - Výběr dodavatele
    - Interní organizace
    - Vyhodnocení výsledků, řízení nálezů
- Jak snížit rizika plynoucí z právních aspektů souvisejících činností

O čem nebude prezentace

- Obecná moudra o penetračních testech
  - …které jistě lépe znáte sami
- Jak sepsat smlouvu
  - …protože se často používají „šablony“
  - …protože je to spíše práce právníků
- Jak se soudit
  - …protože cílem architekta je, aby nikdy k žádnému soudu nedošlo

Co, proč a jak chceme testovat



Proč testovat

- Různá motivace pro penetrační testy:
  - Klient chce „bezpečný“ IS nebo prostředí
    - …ale neví co to znamená. Je na architektovi rozhodnout o jejich potřebnosti.
  - Klient chce provést penetrační testy
    - …ale nedefinuje akceptační kriteria. S jakými chybami je ještě možné nasazení do produkce? Je na architektovi je posoudit závažnost.
  - Penetrační testy z důvodu compliance
    - …potřebujeme výsledek penetračních testů podle standardu pro audit.

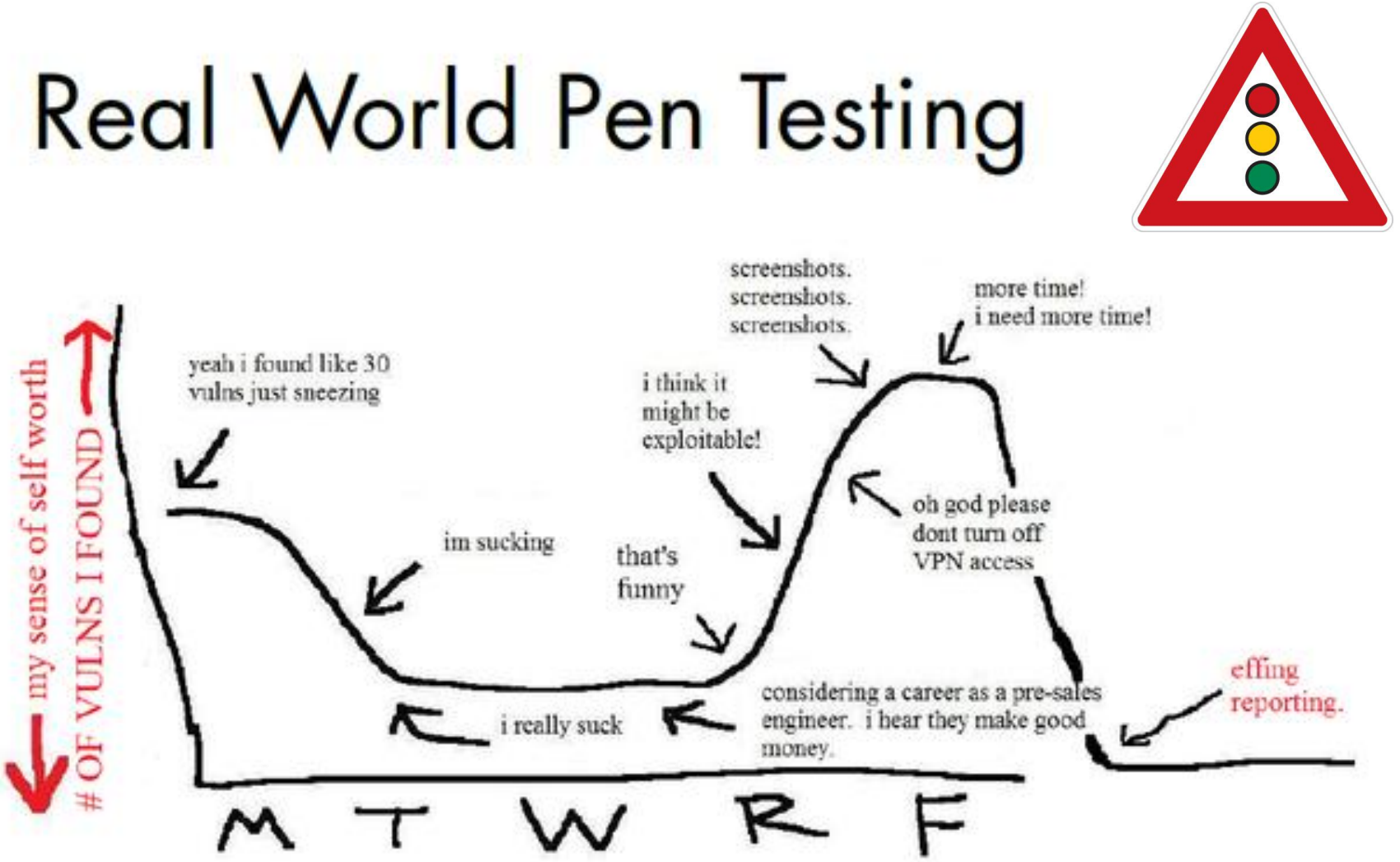
Jak testovat

- Penetrační testy:
  - Metoda pro ohodnocení IS simulováním útoku
- „Širší vnímání“ penetračních testů:
  - Revize designu
  - Revize kódu
  - Audit konfigurace
  - Audit procesů
  - Sken zranitelnosti
  - Sociální inženýrství
  - …

Co testovat

- Vymezení rozsahu testů
  - Víme už jak, od toho se odvíjí i typ testu:
    - Black-box v. white-box
    - Automatizované testy v. ruční testy
  - Správné ohraničení je důležité pro správnou nabídku a pro rozsah interního organizačního zajištění
    - (nejen) IP adresy (ale i)
    - typ testované aplikace, bezpečnostní architektura, infrastruktura pod aplikací, integrace, procesy, správa uživatelů, rozsah kódu,…

Výběr dodavatele



Zadání penetračních testů

- Jak sepsat zadání penetračních testů
  - Jaký zvolit detail?
    - Přiměřený nákladům na testy.
    - Nelze specifikovat přesně, co aplikace nemá umět
  - Někteří dodavatelé zadání občas ani nečtou
  - Zadání si píšete hlavně pro sebe, abyste věděli, co chcete
  - Diskuzí s dodavateli si ujasníte rozsah a srovnáte je na stejnou startovací čáru

Výběrové řízení

- Jak zorganizovat výběr
  - Je nutné respektovat interní procesy a předpisy
  - Ideální je variabilita výběrového procesu na základě rozsahu testů
  - Je dobré předkládat k rozhodnutí pouze jasně porovnatelné nabídky s porovnatelným rozsahem
  - Stálí dodavatelé v. noví hráči (nutnost nové smlouvy)

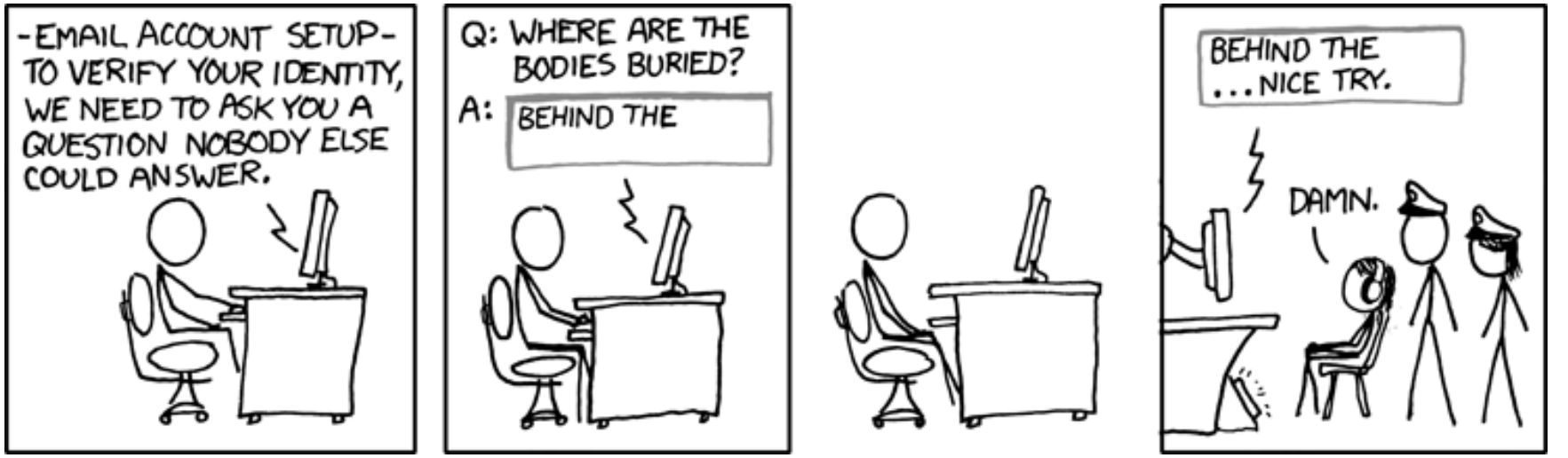
Smlouva s dodavatelem

- Obsah standardní smlouvy určují většinou právníci (šablona)
  - Smlouva typicky obsahuje klauzule o mlčenlivosti a odpovědnosti za škodu
  - Často již existuje rámcová smlouva
  - Podstatné je zadání (co, jak, do kdy), které se odráží v nabídce (smlouvě)

Proč je to všechno důležité?

- Bez ohledu na smlouvu chcete, aby:
  - Neunikla citlivá data (need-to-know)
  - Nebyla způsobena škoda (rozsah, metody)
  - Nezůstala v systému díra (kvalitní dodavatel)
  - …
- Soudit se o některou z předešlých odrážek by byla katastrofa z pohledu reputačního rizika
  - Dodavatel musí především vědět, že příště může testy dělat klidně někdo jiný…

Organizační zajištění



Součinnost

- Je potřeba mít co nejlépe vydefinované požadavky na součinnost od dodavatele
  - Účty a přístupy
  - Informace, zdrojové kódy, předpisy
  - Časové možnosti
- Je potřeba znát interní prostředí, co jak dlouho trvá a kdo co schvaluje
  - Co je reálné poskytnout a co není
  - Princip need-to-know

Interní komunikace

- Koho seznámit s konáním a předmětem penetračních testů?
  - Sociální inženýrství je v tomto specifické
  - U ostatních typů testů nejlépe „všechny“, protože
    - Provozní nebo bezpečnostní incident může být často závažnější než nalezená zranitelnost
    - Dotčení lidé málokdy začnou narychlo „opravovat“ svůj IS (a když začnou, je to jen dobře – cílem je mít bezpečný IS, ne najít co nejvíc chyb)
    - Můžete se dostat do problémů s předpisy

Výsledky, jejich zpracování

„Security is always excessive
until it's not enough.”

„In God we trust. All others,
we virus scan. ”

Zpráva a její prezentace

- O kvalitě dodavatele často vypovídá kvalita zpracování výsledné zprávy
- Je třeba brát na zřetel, kdo je konzument (architekt v. auditor v. manager)
  - Fakta a reálné scénáře v. kompletní informace v. barvy a semafory
- Závažnosti nálezů určené dodavatelem nemusí být relevantní v kontextu jiných opatření, které dodavatel nezná

Řízení nálezů

- Nálezy z penetračních testů jsou citlivé údaje, neměly by být volně k dispozici
  - K nálezům je třeba se chovat jako k jiným chybám v testech, avšak detaily poskytovat pouze relevantním osobám
  - Je potřeba evidovat a řídit (abychom mohli dokladovat) řešení nálezů
  - Je potřeba poměřit závažnost nálezů oproti závažnosti jiných chyb z testů

A co dál?

„Amateurs hack systems, professionals hack people.„— Bruce Schneier

(… a co řekne B.S., to se počítá, protože např:

When God needs a new secure certificate, he uses Bruce Schneier as the signing authority.)

Po-implementační revize

- Projekt může skončit, ale oprava všech nálezů se již nestíhá, je potřeba:
  - Nadále nálezy řídit, plánovat jejich opravu
  - Počítat s budoucími retesty dodavatele
  - Počítat s tím, že se může objevit nový problém
- Opravy je potřeba přetestovat na produkci (i poměrně dlouho) po skončení projektu, je potřeba:
  - Opět počítat s budoucími retesty dodavatele

Závěr

To důležité

- Důkladně si rozmyslete, co chcete
- Pečlivě a opatrně vybírejte dodavatele
- Vždy testy oznamte (alespoň někomu)

SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Jiří Vábek
Komerční banka, a.s.
jiri_vabek@kb.cz