DCIT

Bezpečnostný audit a penetračné testy

Autor: Martin Zajíček
(zajicek @ dcit-consulting.sk)

DCIT Consulting, http://www.dcit-consulting.sk

IT Security SR 2008

CONSULTING
DCIT

Stručný prehľad prezentácie

- Motivácia realizácie bezpečnostných auditov
- Penetračný test
- Technický bezpečnostný audit
- Penetračný test vs. technický bezpečnostný audit
- Podoba výstupov

Motivácia realizácie bezpečnostných auditov

Kedy realizovať bezp. audit?

DCIT

- snaha začať riešiť technickú bezpečnosť a definovať jej východiskový stav/úroveň

- pravidelný audit preverujúci aktuálny stav/úroveň bezpečnosti

- audit naviazaný na implementáciu/ aktualizáciu/migráciu vybranej časti infraštruktúry či pri personálnych/ organizačných zmenách

CONSULTING DCIT

Penetračný test

Penetračný test - všeobecne

- preverenie sieťovej infraštruktúry automatizovanými nástrojmi i „manuálne“
- kvalita závislá od podielu manuálneho testovania na celkovom testovaní (spravidla relevantnejšie nálezy)
- rôzne variácie a možnosti:
  - otvorená i skrytá (utajená) podoba
  - bez / s poskytnutím informácií (blackbox)

Penetračný test – všeobecne 2

DCIT

- rôzne variácie a možnosti (pokrač.):
  - interný / externý variant
  - zamerania na celú infraštruktúru alebo len na špecifickú časť (DMZ, WWW aplikácia, atď.)
  - prierezové alebo plnohodnotné
  - možnosť doplniť rôzne doplnkové testy (DoS, test AV ochrany, testy trójskym koňom)

- ide často krát o simuláciu útoku bez spolupráce so systémovou podporou

CONSULTING DCIT

Penetračný test – na čo myslieť

- **špecifikovať dôležité služby, ktorých výpadok môže spôsobiť vážne problémy**
  - vyňatie z testovania alebo presun testovania mimo špičky
- **zmluvné podchytenie testovania (NDA!)**
- **jasne definované komunikačné kanály v prípade vážnych nálezov**
- **podchytiť aj následné odstránenie prípadných nedostatkov**

DCIT

Technický bezpečnostný audit

CONSULTING
D C I T

Technický audit – všeobecne

DCIT

- zameranie na špecifickú časť infraštruktúry:
  - sieťové prvky
  - operačné systémy serverov / pracovných staníc
  - databázové systémy a i.

- je jasne definovaný rozsah auditu z pohľadu definovania vzorky ale aj obsahu

- nevyhnutná spolupráca so systémovou podporou auditovaných zariadení (!)

CONSULTING DCIT

Technický audit – na čo myslieť

- v čase auditu čiastočné obmedzenie auditovanej infraštruktúry
- možnosť náhľadu na zozbierané dáta
- pripraviť „pôdu“ pre realizáciu auditu
- zmluvné podchytenie testovania (NDA!)
- podchytiť aj následné odstránenie prípadných nedostatkov

Penetračný test vs. technický bezpečnostný audit

Pen. test vs technický audit

- penetračný test je zameraný len na sieťovú oblasť
- technický bezpečnostný audit je komplexnejší
- vzájomný prienik pri sieťových službách
- simulácia útoku vs spolupráca

Podoba výstupov

Výstupy

- spravidla ide o technicky detailnú správu

- management summary, stručné zhodnotenie úrovne testovaného/auditovaného prostredia

- summary všetkých odporúčaní (checklist)

- prezentácia výsledkov s možnosťou diskutovať nálezy a odporúčania

Výstupy

- ukážky konkrétnych výstupov

Hlavné odkazy prezentácie

- penetračný test <> technický bezpečnostný audit

- dostatočnú pozornosť venovať oblasti mlčanlivosti a odkomunikovaní projektu smerom dovnútra

- dostatočnú pozornosť venovať aj odstráneniu prípadných nedostatkov

Záver

DCIT

Ďakujem za pozornosť

CONSULTING
D C I T