

IT saugumo auditas

Marius Celskis

UAB „Informacijos saugos sprendimai“

www.isec.lt

2009 m. gruodžio 9 d.



Turinys

- IT saugumo auditas
- Įsibrovimo testas
- Pagrindiniai etapai
- Rezultatai

IT saugumo auditas

- Informacinių technologijų saugumo auditas
- Svarbus tiek, kiek svarbus IT saugumas.
- Saugumo reikalavimai ir priemonės be kontrolės “neveikia”
- Kiek kainuoja ir kada atsiperka saugumo investicijos?

IT saugumo auditas

- Saugumo reikalavimų (politikos) auditas
- Control Objectives for Information and related Technology (COBIT)
- ISO 17799 - Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas.
- Įsibrovimo testas
- Kiti

Įsibrovimo testas

- Ang. - penetration test, pentest.
- Saugumo įvertinimas simuliuojant įsilaužimą.
- Tikslas – rasti saugumo spragas.

Įsibrovimo testas

- Pagrindiniai etapai:
 - Informacijos surinkimas
 - Įsibrovimas iš išorės
 - Socialinė inžinerija
 - Vidinės informacijos surinkimas
 - Įsibrovimas iš vidaus

Įsibrovimo testas

- Informacijos surinkimas:
 - Interneto resursai
 - Informacija apie darbuotojus
 - Informacija apie sistemas
 - Tiekėjų informacija
 - Pažeidžiamumų/spragų informacija

Įsibrovimo testas

- Įsibrovimas iš išorės:
 - Parenkamas greičiausias/lengviausias įsibrovimo kelias
 - Parenkamos metodikos
 - Parenkamos priemonės

Įsibrovimo testas

- Socialinė inžinerija:
 - Parenkamas metodas
 - Parenkamos scenarijus
 - Parenkamos priemonės
 - Pretexting, phishing, dumpster diving, road apple.

Įsibrovimo testas

- Vidinės informacijos surinkimas:
 - Vidiniai informaciniai resursai
 - Sistemos, tarnybinės stotys
 - Duomenų bazės

Įsibrovimo testas

- Įsibrovimas iš vidaus:
 - Parenkamas greičiausias/lengviausias įsibrovimo kelias
 - Parenkamos metodikos
 - Parenkamos priemonės

Rezultatai

- Didžiausi pažeidžiamumai ir spragos.
- Pažeidžiamumų šalinimo rekomendacijos.
- 80/20 taisyklė.

“Amateurs hack systems, professionals hack people”

Bruce Schneier

UAB „Informacijos saugos sprendimai“

www.isec.lt

2009 m. gruodžio 9 d.

Marius Celskis
marius@isec.lt

