DCIT

Bezpečnost otevřených a uzavřených řešení

Autor: Martin Mačok
(macok@dcit.cz)

DCIT, a.s., http://www.dcit.cz

Otevřená řešení

K dispozici jsou zdrojové kódy software a určitá míra svobody s nimi nakládat.

- Free/Open source software licence
  - GPL, BSD, Apache, MIT, public domain
- Obvykle je software volně šiřitelný.
- Neplést se softwarem „zadarmo“.

Příklady

- GNU/Linux, Apache, PHP
- Mozilla Firefox

Uzavřená řešení

Kód má pouze výrobce (dodavatel). Celý „potravní“ řetězec je víceméně závislý na jednom subjektu.

- Proprietární/„Komerční“ software
- Microsoft Windows, HP-UX, IBM AIX
- Adobe Reader / Flash
- AutoCAD
- Internet Explorer, Opera

Něco mezi

Kód máme, ale je „nepoužitelný“.

Kód je jen pro někoho.

Kód není celý (nebo je neaktuální).

- IBM Websphere
- Apple Mac OS X
- Microsoft Shared Source
- Nokia Symbian OS, Sun JDK
- Visual Basic
- Mozilla + Flash
- Google Chrome

Co je to bezpečnost?

Schopnost bránit se útokům

- únik informací
- modifikace dat
- nedostupnost

Není to jednorozměrná veličina.

Je to spíše trvalý proces než stav.

Nelze přesně definovat.

Kriteria srovnání

Kvalita software

Praxe v reálném světě

Cena

Reálná bezpečnost závisí na velkém množství faktorů a je velmi těžké stanovit univerzální smysluplná kriteria.

Kvalita software – přehled

Záleží především na

- celkovém přístupu
- způsobu vývoje (např. Microsoft SDL)
- množství zúčastněných
- jejich znalostech (např. OWASP) a schopnostech

Výsledek snahy

- množství chyb a jejich závažnost
- rychlost a kvalita reakcí na chyby

Kvalita software – chyby

Nikdo neumí psát software bez chyb.

Počítání chyb nebo patchů?

- OSVDB Advanced Search

Reakční doba?

Nezávislá analýza kódu

- Coverity Scan, crowdsourcing

Kerckhoffsův princip, Linusův zákon

Možnost backdooru? Důvěryhodnost?

Placení za chyby? Hacking soutěže?

Záruka? Přečtěte si EULA…

Praxe – skutečný svět

Ekosystém Internetu

- software nelze posuzovat v izolaci

Ekonomika kyberzločinu

- atraktivita cílů, výdělečnost
- Malware (in the wild)
- APT – Advanced Persistent Threats

Šedá ekonomika

- motivace komunity, reciprocita – altruismus
- obchodování s nalezenými slabinami

Penetrační testy

- ukazují především lajdáctví správců

Cena software – TCO

Pořizovací cena

Cena zabezpečení

Cena údržby, outsourcing

Možnost změny dodavatele

Riziko EOL

U otevřených řešení lze obvykle úroveň zabezpečení (výši investic) flexibilně přizpůsobovat potřebám. U proprietárních častěji situace „ber nebo neber“.