Metodiky v oblasti počítačové bezpečnosti

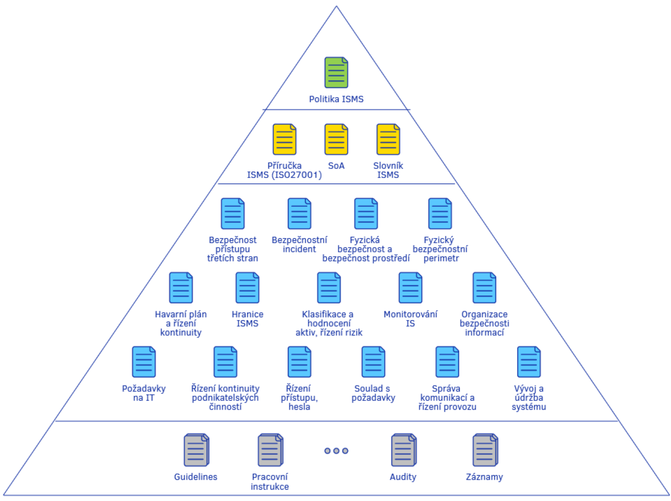
Oblast počítačové bezpečnosti (cybersecurity) nabyla - nejen, ale především - v posledních letech zásadního významu. Bezpečnost je proces - nejde o to provést bezpečnostní testy software, odhalit chyby a ty záplatovat (i když o to jde také), ale software je třeba od začátku navrhovat a vyvíjet s ohledem na bezpečnost a také jej tak provozovat.

ISO 27000

Rodina standardů ISO 27000 (a z ní nejčastěji zmiňovaný standard ISO 27001) pokrývá téma zabezpečení informací ve firmě - tedy téma celkově procesní a organizační, nikoliv pouze technologické. Popisuje, jak by měl vypadat tzv. Systém řízení bezpečnosti informací (Information Security management System, ISMS).

ISMS v organizaci musí pokrývat oblasti jako je

- bezpečnostní politika,
- vymezení aktiv, podléhajících ochraně; analýza rizik, stanovení úrovní bezpečnosti a citlivosti dat; role odpovědnosti a pravomoci,
- procesy k identifikaci a poučení z bezpečnostních incidentů,
- řízení přístupu,
- fyzický bezpečnostní perimetr,
- řízení kontinuity podnikatelských činností
- atp.



Obrázek 38 – ISMS pyramida

Norma ISO 27001 definuje oblasti kontrol, které musí být v organizaci přítomny, aby byly spolehlivě pokryty oblasti zájmu naznačené výše. Norma ISO 27002 pak dává konkrétní doporučení (dobrou oborovou praxi - best practice).

Secure Software Development Lifecycle (SSDLC)

Jak jsme uvedli výše, bezpečnost je třeba mít na paměti od samotného začátku. O životním cykly vývoje software (Software Development Lifecycle - SDLC) se budeme v detailu bavit později, ale věřte že v zásadě zahrnuje různé fáze od stanovení požadavků, přes návrh, kódování, testování až po akceptaci a nasazení i provoz. Metodiky a doporučení v oblasti Secure SDLC pak říkají, jak v té které fázi je třeba zohlednit bezpečnost - tak, abychom na konci dostali bezpečný software.

Obrázek 39 – nazev

Mezi aktuální metodiky SSDLC patří

- Microsoft SDL
- NIST 800-160 (SDLC)
- Grip on Secure Software Development (CIP-SDD)
- OWASP CLASP.

OWASP

Open Web Application Security Project (OWASP) zastřešuje řadu projektů komunity v oblasti počítačové bezpečnosti, především pak webových aplikací. Mezi nejvýznamnější projekty patří:

- OWASP Top 10 - přehled deseti nejvážnějších hrozeb pro bezpečnost (možných cest útoku, typických selhání)
- OWASP Application Security Verification Standard - standard využívaný při hodnocení bezpečnosti aplikací
- OWASP Web Security Testing Guide - podklady k bezpečnostnímu testování webových aplikací
- OWASP Cheat Sheet Series - popisy dobrých praktik
- OWASP Mobile Security Testing Guide - zaměřeno na testování mobilních aplikací