MI-SP-SP-1 (MI-BPR.16) (přednáška 1)

Základní bezpečnostní principy. Modelování bezpečnostních rizik, metodiky STRIDE a DREAD.

hrozba - (potenciální) příčina nežádoucího incidentu (prolomení autentizace hrubou silou)

zranitelnost - slabé místo, které může být využité hrozbou / hrozbami

Kvalitní software - bezpečný & spolehlivý ← dělá jen to co má
↑ chrání důvěrnost, integritu a dostupnost dat

- bezpečnost softwaru se musí řešit už v návrhové části
  - chyby opravuje vždy autor!

SD^3 : Secure by Design — vyhodit starý kód; penetrační testy; vzdejme se všech nepotřebných práv
Secure by Default — výchozí instalace maximálně bezpečná
Secure in Deployment — neinstalovat rozšíření, které většina nepoužije

další pravidla: myslet jako útočník, minimalizace ploch pro útok, víceúrovňová bezpečnost
externí systémy jsou nebezpečné, bezpečné selhání!
no security through obscurity

STRIDE: (model pro identifikaci bezp. rizik) — možná řešení:

Spoofing of Identity	podvržení identity	○ lepší autentizace, nukládat hesla, ...
Tampering with data	neautorizovaná změna dat	○ autorizace, hashing, MAC, ...
Repudiation	popření transakce uživatelem	○ digitální podpis, časové otisky, ...
Information disclosure	únik informací	○ autorizace, šifrování, ...
Denial of service		○ filtrování, throttling, QoS, ...
Elevation of privilege	neautorizované vyšší oprávnění	○ oprávnění snížit

modelování hrozeb

 ◦ proces - jednotka zpracování dat [S,T,I,D,E]

 ◦ úložiště [T,R,I,D]

 ◦ hranice - počítač, adresní prostor, hranice důvěry

 ◦ interaktor - vstup do systému [S,R]

 ◦ tok dat [T,R,I,D]

- hodnocení rizik : DREAD
  - průměr hodnot ze pěti kategorií, každá [0,10]
    - ◦ Damage potential
    - ◦ Reproducibility - jak snadné je zopakovat
    - ◦ Exploitability - jaké úsilí je třeba
    - ◦ Affected users - množství potenciálních útočníků
    - ◦ Discoverability

- vylepšení : CVSS - více metrik, méně hodnot (škála)
  CWSS - novější a komplikovanější