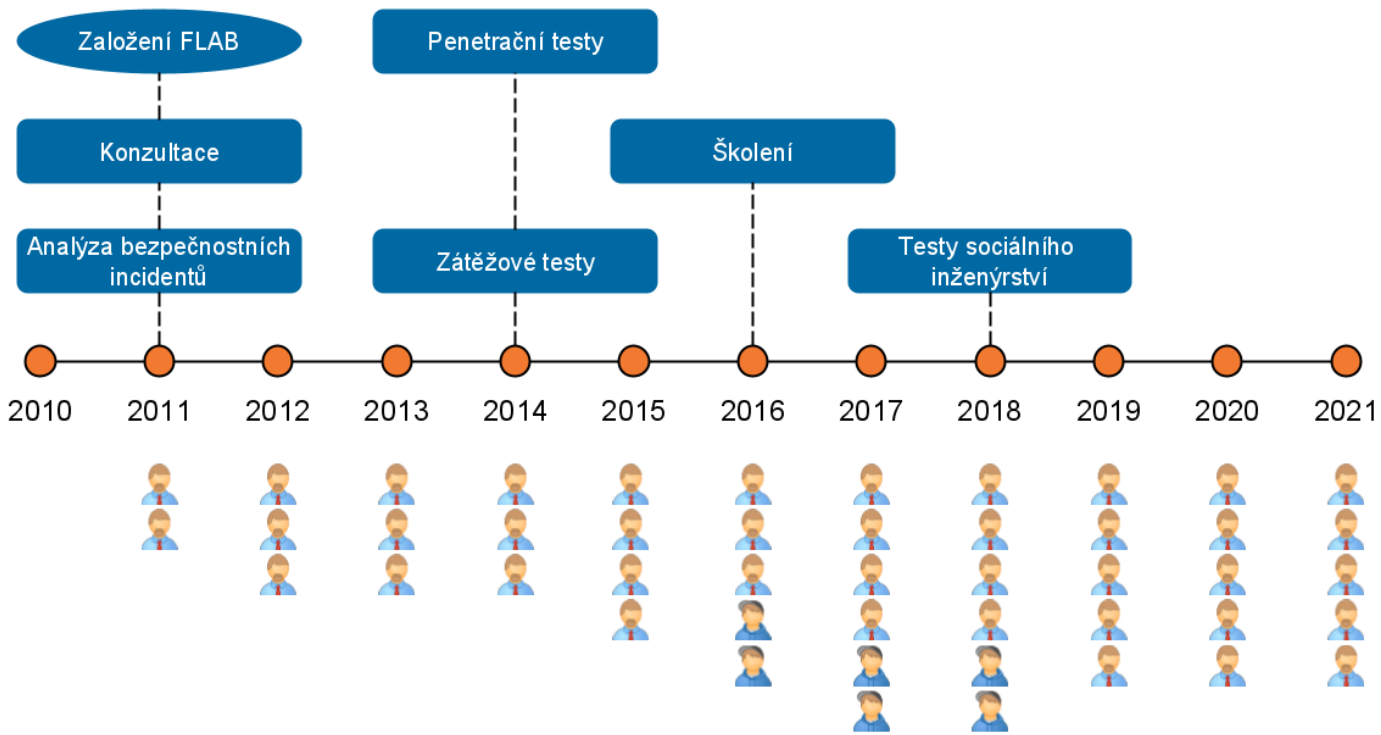
Forenzní laboratoř (FLAB)

Aleš Padrta, Michal Kostěnec

Klasifikace dokumentu: Veřejný

Úvodní seznámení

- FLAB – Forenzní LABoratoř
  - Podpůrné pracoviště CESNET-CERTS
  - Vývoj v čase



Analýza bezpečnostních incidentů

Analýza bezpečnostních incidentů

- Součást reakce na BI
  - Poskytuje informace
  - Běžný BI ⇒ CSIRT
- Závažný BI
  - Zásadní vliv na organizaci
  - Podložené závěry
  - Forenzní analýza ⇒ specializované pracoviště

Analýza bezpečnostních incidentů

- Průběh z pohledu zákazníka
  - Úvodní konzultace
  - Pomoc s formulováním otázek
  - Podpora při zajišťování dat
  - Administrativa (NDA, ...)
  - Průběžné informace
  - Celkový výsledek
- Výstupy
  - Dokumentace postupu
  - Závěrečná zpráva
  - Prezentace výsledků

Penetrační testy

Penetrační testy

- Zranitelnost – základ BI
  - Chybný návrh
  - Chybná implementace
  - Chybné používání
- Nalezení chyby
  - Kyberkriminálník ⇒ zneužití
  - Slušný nálezce ⇒ nahlášení a oprava
- Penetrační testy = cílené hledání zranitelností

Penetrační testy

- Průběh z pohledu zákazníka
  - Úvodní konzultace
  - Pomoc s formulováním zadání
  - Administrativa (NDA, smlouva)
  - Kontakt pro mimořádné události
  - Průběžně – kritické zranitelnosti
  - Celkový výsledek
- Výstupy
  - Seznam nálezů
  - Seznam doporučení
  - Závěrečná zpráva
  - Prezentace výsledků

Zátěžové testy

Zátěžové testy

- Infrastruktura a služby – omezený výkon
  - Přenosové pásmo (uplink)
  - Síťová infrastruktura (routery, firewally ...)
  - Servery, aplikace
- Zátěžové testy
  - Zjištění stavu (vlastní, služby ISP)
  - Detekce slabých míst
  - Nápravná opatření (a jejich ověření)
  - Procvičení

Zátěžové testy

- Průběh z pohledu zákazníka
  - Úvodní konzultace
  - Pomoc s formulováním zadání
  - Administrativa (NDA, smlouva, informování ISP)
  - Výběr vhodné doby
  - Realizace – s telefonním spojením
  - Sada krátkodobých testů
  - Celkový výsledek
- Výstupy
  - Vyhodnocení jednotlivých testů
  - Seznam doporučení
  - Závěrečná zpráva, (prezentace výsledků)

Testy sociálního inženýrství

Testy sociálního inženýrství

- Lidé (uživatelé, administrátoři)
  - Psychologický nátlak
  - Poskytování informací (přístupové údaje)
  - Provádění činností (spuštění přílohy)
- Přínosy testů sociálního inženýrství
  - Vzdělání uživatelů
  - Zjištění odolnosti organizace
  - Prověření vnitřních postupů

Testy sociálního inženýrství

- Průběh z pohledu zákazníka
  - Úvodní konzultace
  - Výběr uživatelů a parametrů
  - Administrativa (NDA, smlouva)
  - Rozeslání zprávy
  - Vyhodnocení
  - Školení uživatelů
- Výstupy
  - Vyhodnocení průběhu + výsledné počty
  - Závěrečná zpráva
  - Prezentace výsledků

Ostatní služby

Ostatní služby

- Využití znalosti / vybavení
  - Obnova smazaných dat
  - Analýza technologií
  - Scanner zranitelnosti
- Konzultace
  - Zájem o službu
  - CESNET-CERTS
  - Členské sítě
  - ...
- Školení
  - Forenzní trénink
  - Forenzní trénink 2: Síť

Dotazy a diskuse