# Aplikační bezpečnost

Ing. Vladimír Lazecký
vladimir.lazecky@viavis.cz

VIAVIS střežíme podstatné

## Pojďme si hrát

- Představte si, že:
  - Jste management renomované banky
  - Otevíráte nové business příležitosti – krypto měny
  - Potřebujete vyvinout SW pro trading kryptoměn
  - Víte, že jako banka potřebujete záruku vysoké bezpečnosti
- Úkol:
  - Připravte zadání pro externí SW firmu – specifikace bezpečnostních požadavků
  - Definujte, jak ověříte splnění zadání SW firmou u hotového SW
  - Zadání prezentujte

## Pojďme si hrát

- Představte si, že:
  - Jste management SW firmy, 30 zaměstnanců
  - Získali jste zakázku banky na vývoj systému tradingu krypto měn
  - Banka specifikuje extrémní bezpečnostní požadavky – máme je
  - Navrhněte, jak budete postupovat a jak požadavky naplníte
    - Jaké máte limity?
    - Co vše musíte ošetřit?
  - Svůj návrh odprezentujte

## Smysl hry

- Aplikační bezpečnost je průšvih
- Neexistují vše řešící metodiky a postupy
- Často se aplikační bezpečnost zužuje na testování
- Víra
  - *Nejsem expert, nabízím zkušenosti*
  - *Vývoj šifrovací komunikační platformy*
  - *Mnoho chyb…*

## Malé opakování

- Co je  a co není bezpečnost?
- Informační a kybernetická bezpečnost?
- Co je důvodem pro bezpečnost

# Základní pojmy – bezpečnost

- **Bezpečnost není stav** – častý omyl (nic není absolutně bezpečné)
- **Je vlastnost aktiva určená svou mírou – schopností odolávat hrozbám**

- Neexistuje „oddělená bezpečnost“
  - BOZP
  - Informační
  - Kybernetická
  - Fyzická
  - Personální
  - Krizová
  - Administrativní
  - Procesní
  - …

# Základní pojmy – bezpečnost informace

- **Bezpečnost = zajištění důvěrnosti, dostupnosti a integrity informace**

  *ISO/IEC 27001*

  - **Důvěrnost** – zajištění přístupu k informacím pouze oprávněným osobám
  - **Dostupnost** – zajištění přístupu k informacím v požadovaném čase
  - **Integrita** – zajištění celistvosti a neměnnosti informace:
    - Zobrazená data jsou totožná se zdrojovými
    - Data jsou kompletní, nic nechybí
    - Neexistují osiřelá data (SPZ bez auta…)
    - Zachování dat v jejich definované struktuře
    - Zabezpečení dat u prováděných změn:
      - Odolnost proti neoprávněným změnám
      - Identifikace pokusů o neoprávněnou změnu

# Základní pojmy – bezpečnost informace

- **Bezpečnost - ochrana informací:**
  - Během jejich **vzniku, zpracování, ukládání, přenosu a likvidace**
  - Využitím **logických, technických, fyzických a organizačních opatření**
  - Všechny aspekty musí být v souladu:
    - Technická bezpečnost x chování uživatele
    - Bezpečnost x komfort užívání
    - Nesoulad generuje hrozby

# Základní pojmy – bezpečnost systému

- Bezpečnost není jen funkcí systémů zpracovávajících informace
- Bezpečnost systému není pouze funkcí bezpečnosti jednotlivých komponent
- Bezpečný celek není pouhé sestavení z bezpečných prvků

- **Požadavky na bezpečnost systému:**
  - Systém jehož činnost nezpůsobuje nebezpečné stavy
  - Každá porucha vede bezpečným směrem
  - Míra bezpečnosti x míra spolehlivosti
  - Bezpečnostní incidenty lze identifikovat
  - Je definována míra bezpečnosti

# Kybernetický prostor – bezpečnost

- **Komplexní zajištění bezpečnosti:**
  - Informací
  - Systémů
  - Uživatelů
  - Poskytovaných služeb
  - Na výše uvedeném závislých aktiv:
    - Businessu
    - Ekonomiky
    - Organizací
    - Státu
    - Jednotlivců
    - …..

# Aplikační bezpečnost – bezpečnost aplikací

- Zajištění **stanovené** míry bezpečnosti:
  - Důvěrnosti
  - Dostupnosti
  - Integrity

- Během životního cyklu SW:
  - Vývoj
  - Provozování
  - Release cykly
  - Ukončení užívání

## Trochu motivačního úvodu

- Unikátnost informačních systémů
  - Neexistují dva identické systémy
    - Kombinace HW, OS, SW
    - Data
    - Procesy a kultura užívání
    - Uživatelé
  - Problém testování…

§ 25

**Aplikační bezpečnost**

(1) Povinná osoba provádí penetrační testy informačního a komunikačního systému se zaměřením na důležitá aktiva, a to

a) před jejich uvedením do provozu a

b) v souvislosti s významnou změnou podle § 11 odst. 3.

# Aplikační bezpečnost – těžké téma

- Zjednodušené zúžení:
  - Testování aplikací
    - Funkční testy
    - Validační testy
    - Integrační testy
    - Výkonové testy
    - Penetrační testy

## Standardy pro aplikační bezpečnost

- **TCSEC – Trusted Computer System Evaluation Criteria**
  - US standard od roku 1983
  - Definice úrovně bezpečnosti:
    - D – Minimální ochrana (Minimal Protection)
    - C1 – Oddělovaná bezpečnostní ochrana (Discretionary Security Protection)
    - C2 – Kontrolovaná ochrana přístupu (Controlled Access Protection)
    - B1 – Označovaná bezpečnostní ochrana (Labeled Security Protection
    - B2 – Strukturovaná ochrana (Structured Protection)
    - B3 – Bezpečnostní domény (Security Domains)
    - A1 – Ověřený design (Verified Design).

## ITSEC – Information Technology Security Evaluation Criteria

- Od roku 1990
- Opět nejde o standard pro bezpečný vývoj
- 7 úrovní bezpečnostních hodnocení aplikací E0 – E6

- Ověřování se provádí pomocí testování

# ISO 15 408 – Common Criteria for Information Technology Security Evaluation

- Od roku 1999 jako ISO standard
- Opět validace a testování
  - Posuzování a hodnocení funkcionality
  - Hodnocení implementace – významný posun
    - ***CC budou v samostatné přednášce***

## Black box x crystal box

- Black box?
- Crystal box?
  - Problém kombinace pro SW vývojáře…

# Vývoj SW

- Mnoho metodik

- Zjednodušeně:
  - Specifikace požadavků
  - Návrh
  - Kódování
  - Testování
  - Dokumentace

## Problémy SW vývoje

- Jak stanovit míru bezpečnosti
- Jak ji ověřit
- Jak ji udržet
- Destabilizující prvek – zpětná kompatibilita

# Vývoj SW

- Do vývoje vstupuje:
  - Požadavky na SW
  - Technika:
    - Vývojové nástroje, HW
  - Lidský faktor
    - Klient
    - Vývojáři
    - Testeři
    - Uživatelé
    - Správci
  - Business model
  - Plánovaný životní cyklus

## Netechnické téma – lidský faktor

- Klíčová otázka:
  - ***Jak zkontrolujete vývojáře? Analytika…***
  - ***Jak postavíte vývojový tým?***
  - ***Jaké role lze/nelze slučovat?***
    - ***(Architekt, analytik, vývojář, tester, tvorba dokumentace, implementátor, podpora…)***

## Skladba týmu

- Několik zásad:
  - Překryv a zálohování rolí
  - Nastavení procesů osobní odpovědnosti
  - Motivační a kontrolní systém
  - Dokonalé právní zajištění

## Právní zajištění – znáte autorský zákon? Zákon č. 121/2000 Sb.

- Pro bezpečnost aplikací je zásadní
- SW je autorské dílo
  - *Kdo je autorem?*
  - *Jaká má práva autor?*

## Právní zajištění –autorský zákon č. 121/2000 Sb.

- Počítačový program – software je autorské dílo
- Autorem je vždy fyzická osoba
- Může jít o kolektivní autorské dílo – spoluautoři
- Autorská práva – osobnostní práva, nelze se jich vzdát

# Právní zajištění – znáte autorský zákon? Zákon č. 121/2000 Sb.

- Autor má právo – osobnostní práva:

**Osobnostní práva**

**§ 11**

**(1)** Autor má právo rozhodnout o zveřejnění svého díla.

**(2)** Autor má právo osobovat si autorství, včetně práva rozhodnout, zda a jakým způsobem má být jeho autorství uvedeno při zveřejnění a dalším užití jeho díla, je-li uvedení autorství při takovém užití obvyklé.

**(3)** Autor má právo na nedotknutelnost svého díla, zejména právo udělit svolení k jakékoli změně nebo jinému zásahu do svého díla, nestanoví-li tento zákon jinak. Je-li dílo užíváno jinou osobou, nesmí se tak dít způsobem snižujícím hodnotu díla. Autor má právo na dohled nad plněním této povinnosti jinou osobou (autorský dohled), nevyplývá-li z povahy díla nebo jeho užití jinak, anebo nelze-li po uživateli spravedlivě požadovat, aby autorovi výkon práva na autorský dohled umožnil.

**(4)** Osobnostních práv se autor nemůže vzdát; tato práva jsou nepřevoditelná a smrtí autora zanikají. Ustanovení odstavce 5 tím není dotčeno.

**(5)** Po smrti autora si nikdo nesmí osobovat jeho autorství k dílu. Dílo smí být užito jen způsobem nesnižujícím hodnotu díla. Je-li to obvyklé a nejde-li o dílo anonymní, musí být při jeho užití uveden autor. Ochrany se může domáhat i po zániku majetkových práv osoba autorovi blízká, právnická osoba sdružující autory nebo příslušný kolektivní správce.

https://www.zakonyprolidi.cz/cs/2000-121#cast1

**Právo na nedotknutelnost**

## Právní zajištění –autorský zákon č. 121/2000 Sb.

- Majetková práva
  - Právo dílo šířit
  - Právo dílo užít
  - …
- Vykonavatel majetkových práv autorů
  - Může být právnická osoba
  - Může být zaměstnavatel
  - **ALE…**

## Právní zajištění – autorský zákon č. 121/2000 Sb.

- ALE:
  - Zaměstnavatel prokazuje, že dílo je plnění prac. úkolu
  - Vytvoření díla externisty na objednávku
  - POZOR na právo nedotknutelnosti
- Extrémní situace:
  - SW vytvořený v pracovní době bez úkolu
  - Významná bezpečnostní rizika

## Právní zajištění – autorský zákon č. 121/2000 Sb.

- Vady SW
  - Pokud není sjednáno, vada neexistuje
  - Vada = rozpor mezi dokumentací a reálným stavem
    - (Pokud dokumentace existuje…)
  - POZOR na právní vady
    - Užití „stažených“ knihoven, ověření licencí
    - Omezení způsobu užití
    - Záruka a odpovědnost za vady

# Máte nějaké dotazy?

Děkuji za pozornost

Ing. Vladimír Lazecký