VIAVIS střežíme podstatné

Bezpečnostní testování

Kybernetická a informační bezpečnost II

Vladimír Lazecký

vladimir.lazecky@viavis.cz

Proč bezpečnostní testování

- **Způsob prověření funkčnosti a účinnosti bezpečnostních opatření**
  - Někdy jde o jediný způsob
  - Nedílná součást systematického řešení KB
  - Testy technických opatření
  - Testy organizačních opatření
  - Testy jako motivace k dodržování pravidel

Limity bezpečnostních testů

- **Testy nikdy neodhalí všechny slabiny**
- Testy by měly být opakovatelné:
  - Nemusí platit vždy – měnící se podmínky
  - Vliv anomálií
- Testovací slepota:
  - Testující upadá do stejných vzorců

Kdy testovat

- Před implementací opatření:
  - Zjištění výchozího stavu
  - Motivace odpovědných
- Před nasazením do provozu:
  - Ověření stanovené míry bezpečnosti
  - Součást akceptačních testů

Kdy testovat

- Po implementaci a v rutinním provozu bezp. opatření:
  - Zda jsou splněny cíle
  - Zda je udržena stanovená míra bezpečnosti v čase
- Provozní rutina:
  - Dlouho se nic nedělo…
  - Provozní slepota

Typy bezpečnostních testů

- **„Check list testy“ = testy shody s definovanými požadavky**
  - **Trusted Information Security Assessment Exchange** (TISAX) – testy shody s požadavky, automotice
  - **The Digital Operational Resilience Act (DORA)** – finanční sektor
  - **BASEL III** – systém řízení operačního rizika bank
  - **Validace** – **GAMP 5** např. farmaceutických provozů, validace integrity dat

Penetrační testy – používané metodiky

- Open Source Security Testing Methodology Manual (OSSTMM)
- Open Web Application Security Project (OWASP)
- Web Application Security Consortium Threat Classification (WASC-TC)
- Penetration Testing Execution Standard (PTES)
- Information Systems Security Assessment Framework (ISSAF)

Typy penetračních testů

- **Systematické třídění neexistuje, přesto se o ně pokusíme ☺**

- **Vulnerability scan** – detekce zranitelností
  - Zjištění, zda testované systémy nemají známé zranitelnosti:
    - Databáze zranitelností
    - Konfigurační chyby
  - Obvykle jde o automatizované testy

  - Výhody/nevýhody?

Penetrační testy

- Testy s cílem průniku:
  - Ověření funkčnosti bezpečnostních mechanismů
  - Testuje se nejen vlastní průnik, ale za bude zachycen a jak bude reagováno
- Součástí jsou obvykle vulnerability scany

Typy penetračních testů

- **Testy bez znalosti:**
  - Blind test, double blind test
  - Testující nemá žádné vstupní informace
  - Součástí testů je OSINT
  - Testující postupuje jako útočník
- **Výhody/nevýhody?**

Typy penetračních testů

- **Testy se znalostí:**
  - Testující zná některé reálie, může mít oprávnění přístupu
  - Testy útoku ze strany zaměstnance, partnera…
- **Výhody/nevýhody?**

Typy penetračních testů

- **Externí testy**
  - Testy vedené z vnějšku perimetru
- **Interní testy**
  - Testy vedené za perimetrem

Typy penetrační testů

- **Nekooperativní testy**
  - Testy bez součinnosti se zadavatelem
  - Testuje se i zda je test zachycen
- **Kooperativní testy**
  - Testy za přímé účasti zadavatele
  - Obvykle se rovnou odstraňují nedostatky
  - Hardening

Sociotechnické testy

- **Sociotechnické testy**
  - Předmětem testování je uživatel a jeho chování
  - Etický kodex testování
- Cílem:
  - Testy uživatelských návyků, dodržování pravidel, jejich znalost, schopnost test odhalit
- Metody:
  - Manipulace, zneužití důvěry, podvrhy

- Výhody:
  - Motivace zaměstnanců k dodržování pravidel
- Nevýhody:
  - Ohrožení důvěry a firemní kultury

Kombinace testů

Testy lze vhodně kombinovat

- Technické testy x sociotesty
- Phishing, vishing – test průniku do systému

- Testy se znalostí x bez znalosti = tzv. GREY test

Kreativní testy

- Testovací scénář na míru

Fáze bezpečnostních testů

- **Přípravná etapa:**
  - Cíl testu
  - Získávání informací – OSINT, konzultace
- **Plánování testu:**
  - Volba technik testování
  - Tvorba testovacích scénářů
  - Validace scénářů

- **Detekce zranitelností:**
  - Výstupy OSINT:
  - Smlouvy, systémy..

Fáze bezpečnostních testů

- **Testování**
  - Realizace testovacích scénářů
  - Zvyšování brutality testů

  - Detekce zranitelností, hodnocení, částečné posouzení rizik
  - Návrhy protiopatření

Fáze bezpečnostních testů

- **Zpracování výsledků a předání zprávy**
  - Obsah zprávy:
    - Metodika
    - Popis realizace
    - Zjištěné zranitelnosti s hodnocením
    - Návrh jejich odstranění - protiopatření

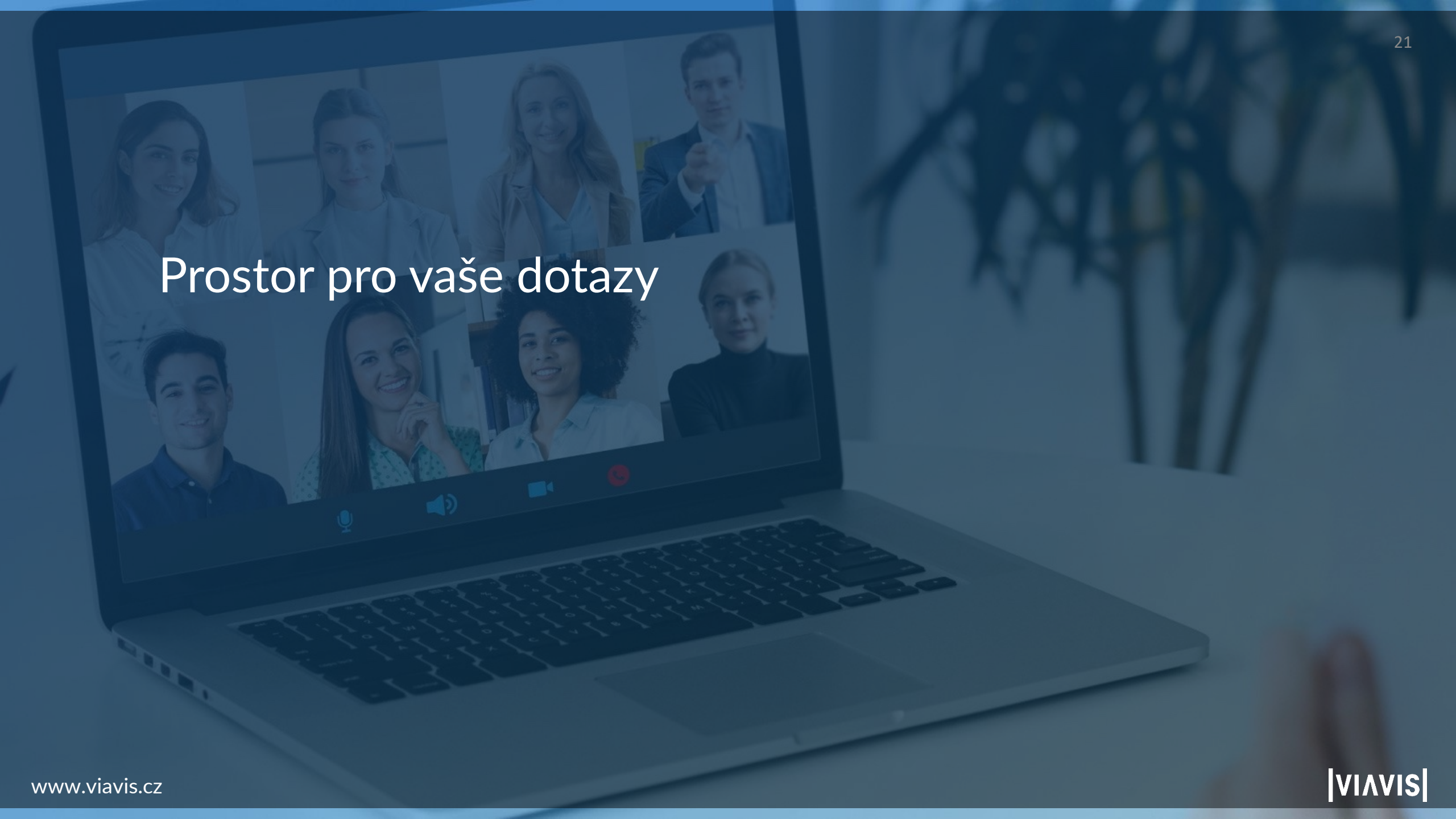
Pojďme si hrát

- **Jste firma nabízející penetrační testy**
  - Zákazník – cpzp.cz objednává blind test
  - Cílem testu je získat přístup do databáze pojišťenců
  - Připravte 3 testovací scénáře
  - Omezení:
    - Nedestruktivní test
    - Etický kodex
    - Cena testu 160.000 CZK

Pojďme si hrát

- **Jste firma nabízející penetrační testy**
  - Zákazník – slu.cz objednává test
  - Cílem testu je získat přístup do databáze studentů – zjištění odolnosti
  - Připravte 3 testovací scénáře
  - Omezení:
    - Nedestruktivní test
    - Etický kodex
    - Cena testu 160.000 CZK

Prostor pro vaše dotazy



Prostor pro vaše dotazy…

Děkuji za pozornost

Za tým VIAVIS a.s.

- Vladimír Lazecký