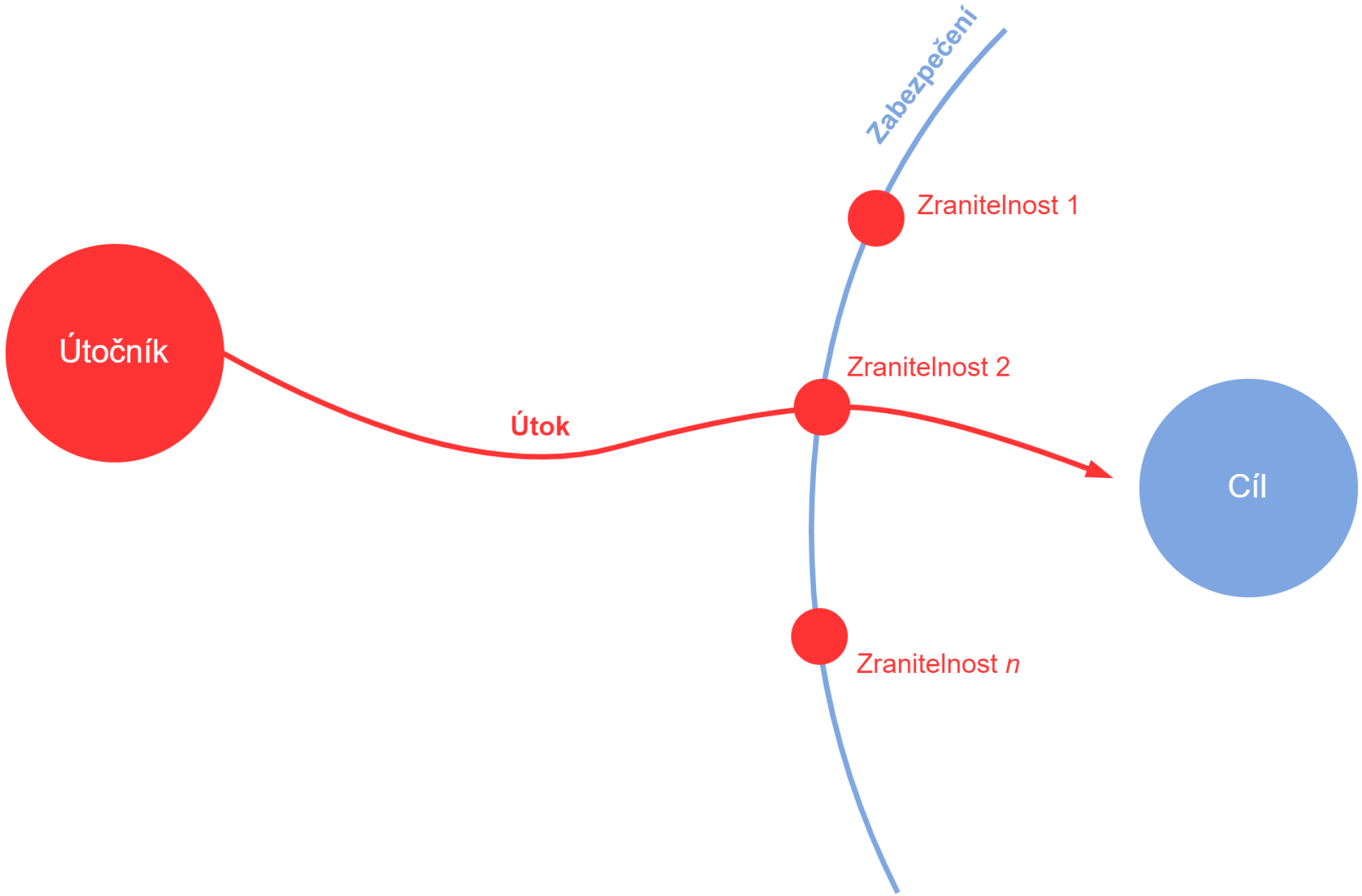
Modulární platforma pro podporu penetračního testování

Willi Lazarov
Penterep, VUT v Brně
lazarov@vut.cz

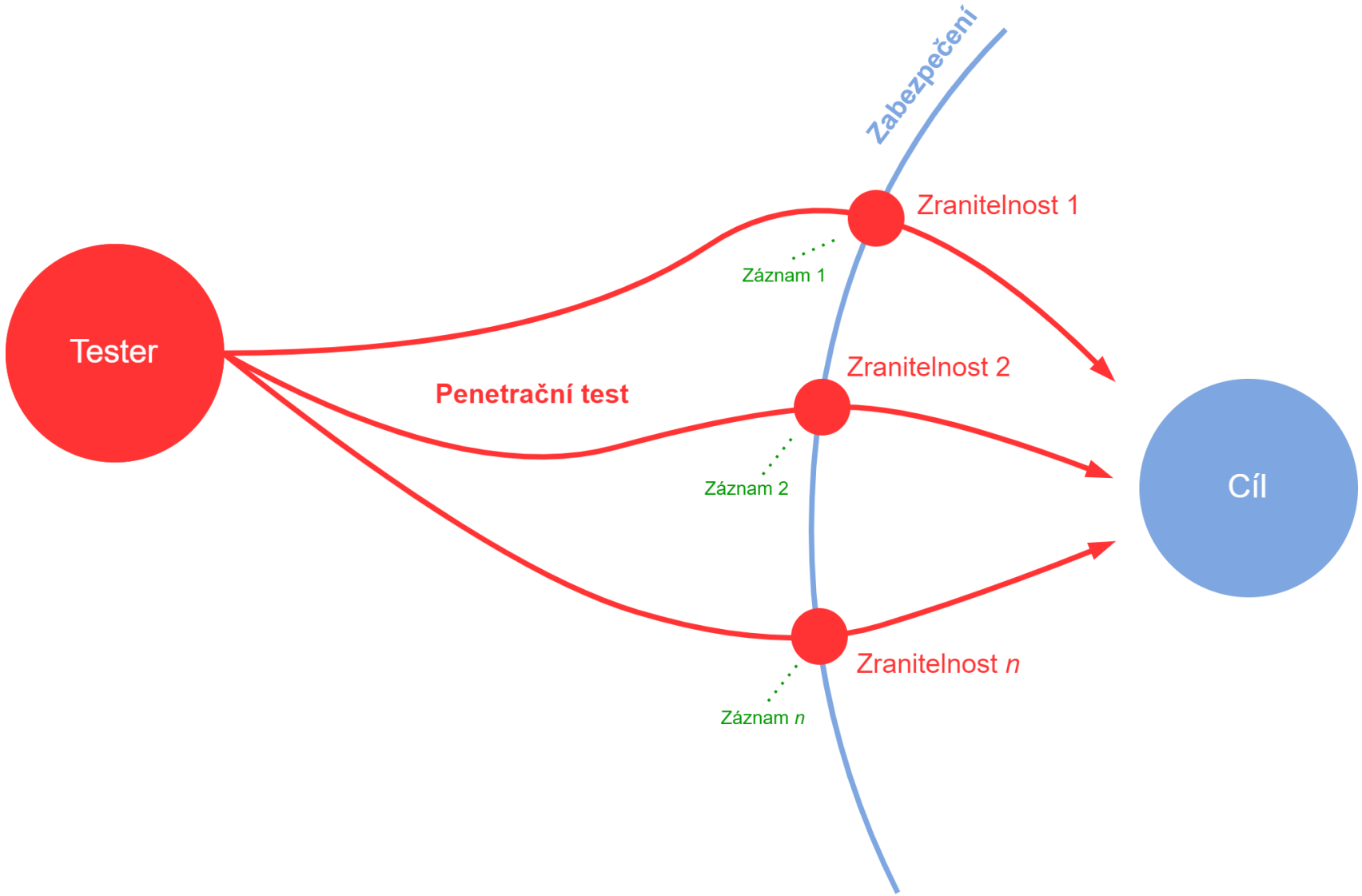
Penetrační testování

- Penetrační testování je rozsáhlá technika **hodnocení úrovně bezpečnosti** metodou pokusu o průnik do prvků spadajících do oblasti informačních a komunikačních technologií.
- Hlavním cílem penetračních testů je preventivně **odhalit**, **ověřit** a **popsat zranitelnosti** testovaného cíle, aby mohla být sjednána **náprava** v podobě jejich odstranění.
- Penetrační testování lze dále posuzovat:
  - podle **strany provedení** – externí a interní testování,
  - podle **úrovně znalosti** – black-box, white-box a gray-box testy,
  - podle **způsobu provedení** – manuální, automatické a poloautomatické testování.
- Obecně lze penetrační testování označit jako **komplexní** a **časově náročný proces**.

Penetrační testování vs. běžný útok



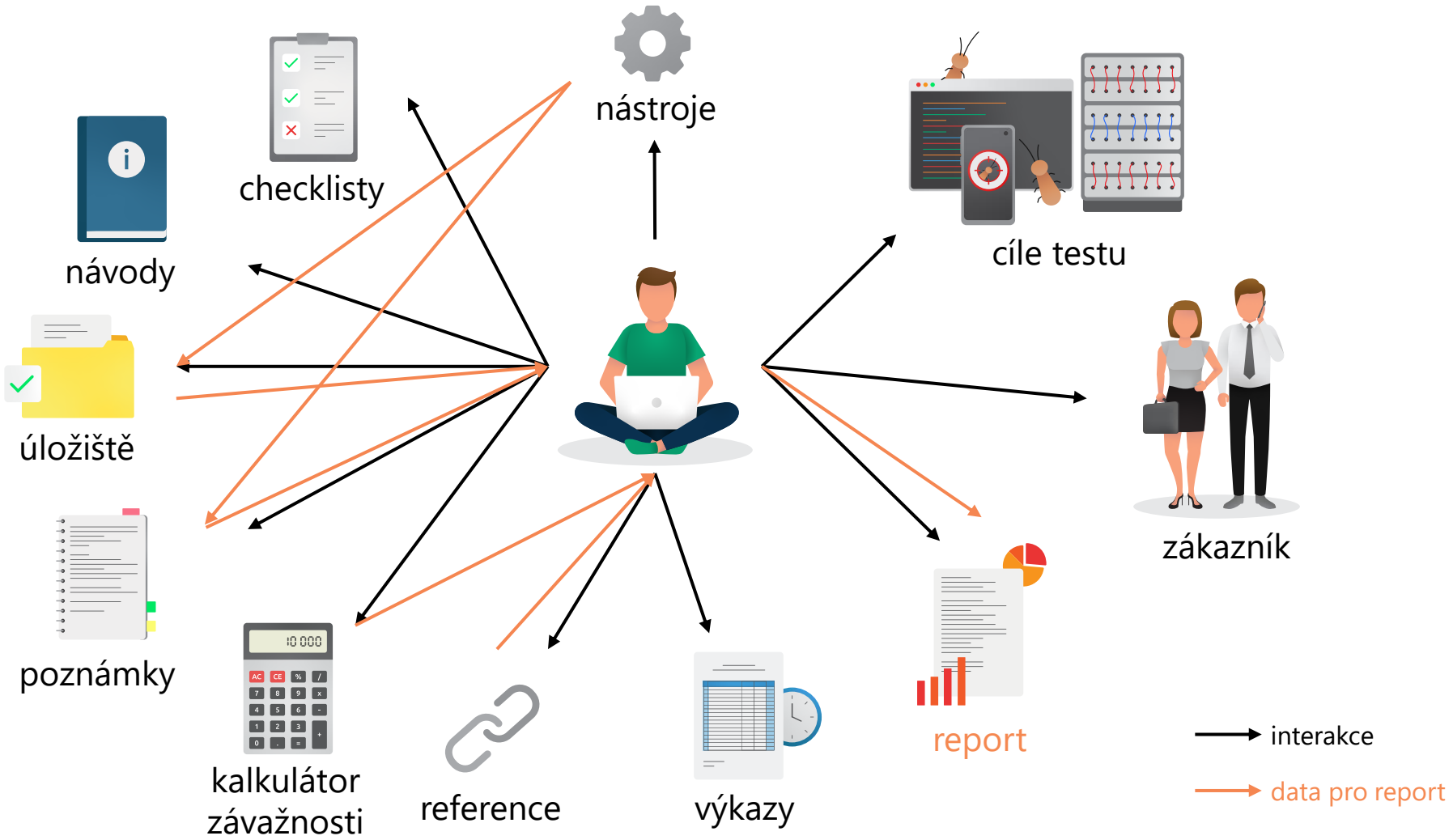
Penetrační testování vs. běžný útok



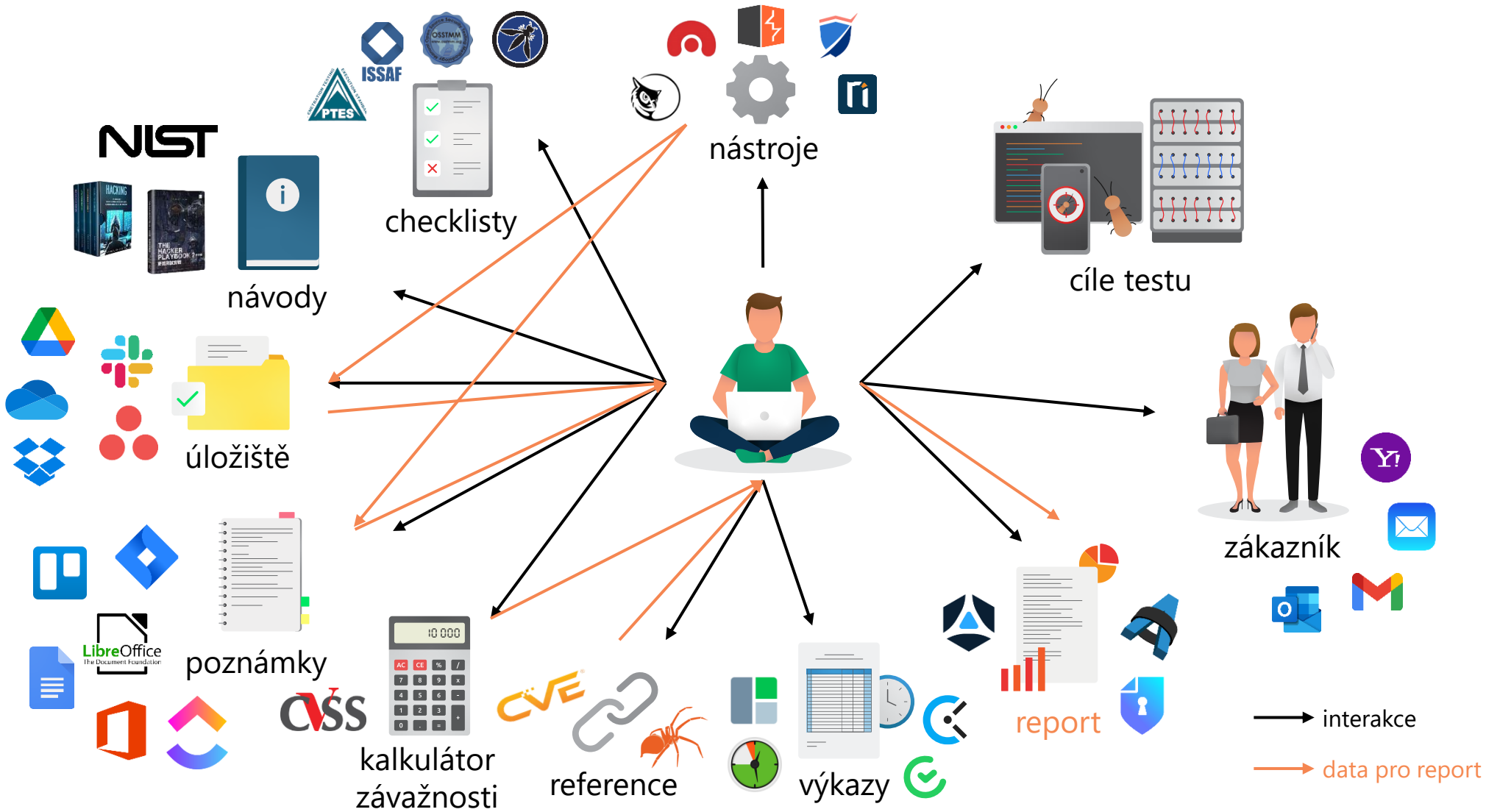
Současný stav penetračního testování

- **Problematika penetračního testování**:
  - velká závislost na zkušenostech testera,
  - specializace testera pouze na konkrétní oblast,
  - nedostatek kvalitních (zkušených) pracovníků,
  - automatizované testy neodhalí všechny zranitelnosti,
  - malé množství kontrolních seznamů pro realizaci testů,
  - během testování se používá velké množství různých nástrojů,
  - výsledky automatizovaných nástrojů se přepisují do poznámek,
  - report se píše v textovém editoru a jeho tvorba je časově náročná.
- Penetrační tester věnuje **velké množství času jiným věcem než samotnému testování**.
- Efektivním řešením problematiky může být **poloautomatické testování**.

Současný stav penetračního testování



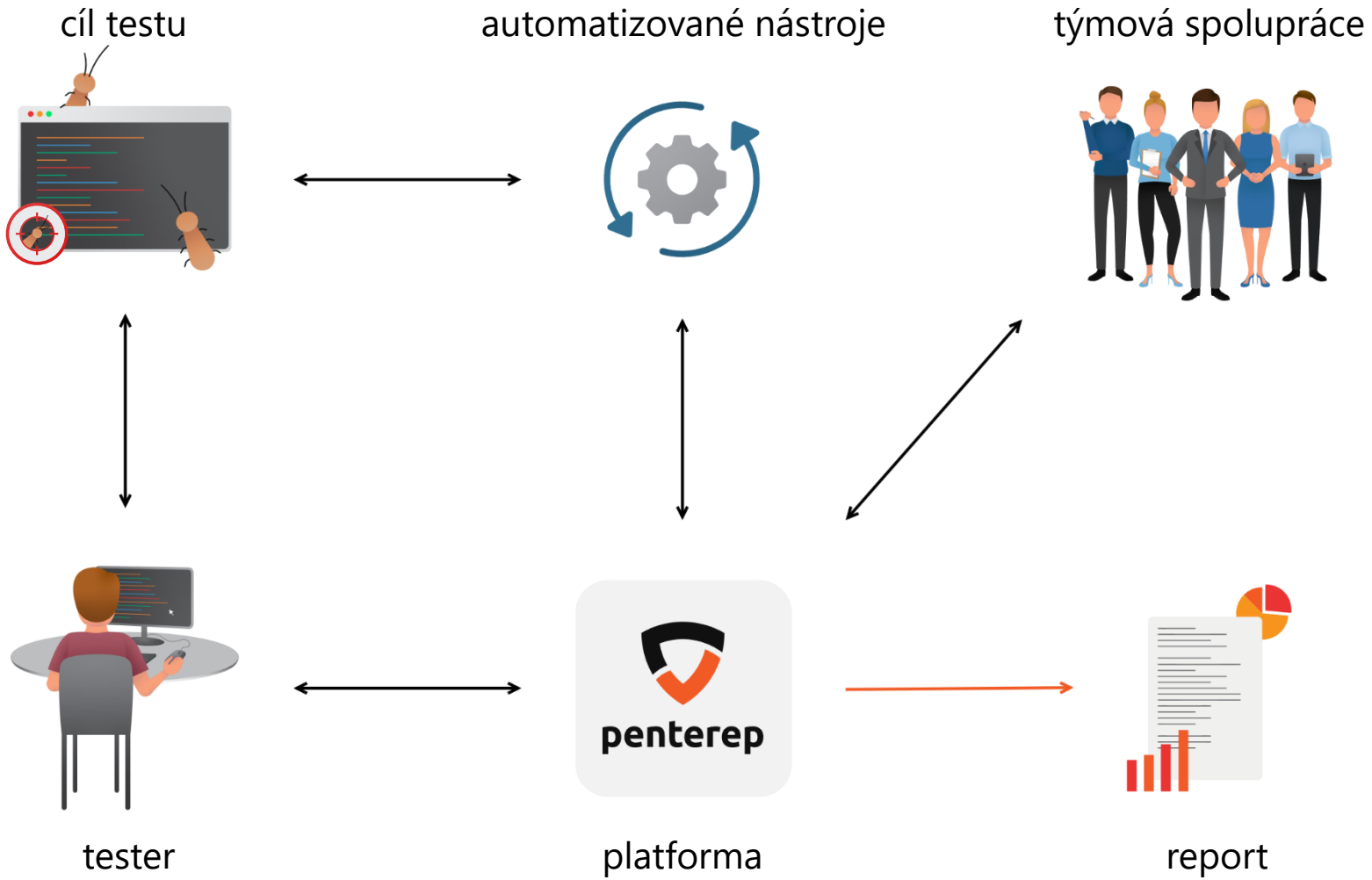
Současný stav penetračního testování



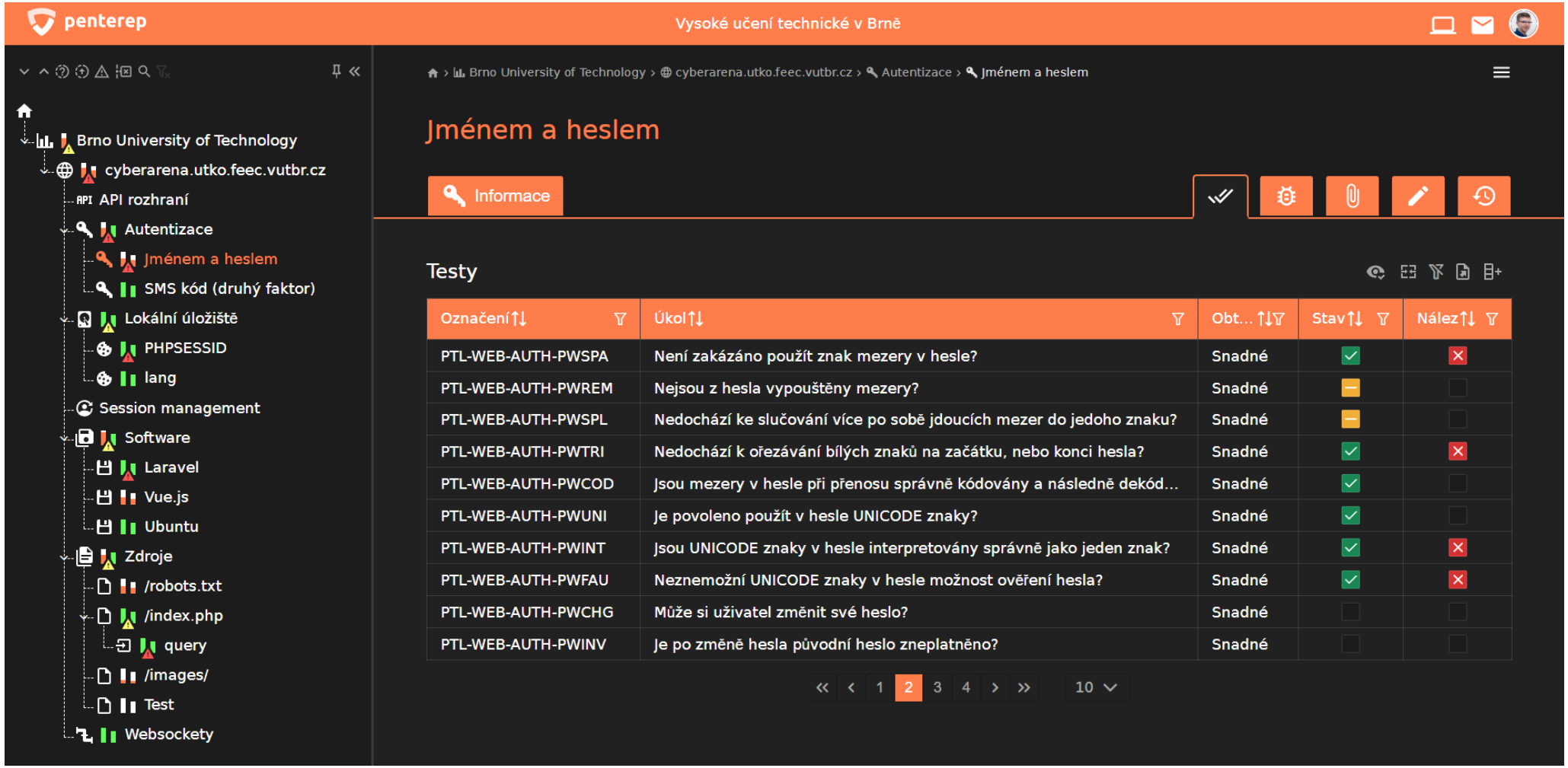
Penterep

- Výsledek projektu aplikovaného výzkumu **TA ČR** (Program ZÉTA, č. projektu TJ04000456).
- Hlavním cílem platformy Penterep je **usnadnit** a **zrychlit** práci penetračním testerům.
- Platforma představuje řešení, které:
  - poskytne „step-by-step“ návody,
  - propojí automatické a manuální testování,
  - umožní ukládat relevantní informace na jednom místě,
  - umožní týmovou spolupráci nejen mezi testery,
  - automaticky vytvoří pracovní výkazy,
  - vygeneruje report ze sesbíraných dat,
  - poskytne odhad pracnosti a manažerské přehledy.
- Penetrační tester může s pomocí platformy věnovat **více než 90 % času** samotnému testování.

Řešení s platformou Penterep



Ukázka platformy

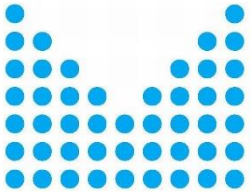


Shrnutí

- Platforma **Penterep**:
  - hlavní výsledek projektu TA ČR ZÉTA,
  - projekt řešen v období 1.5.2020–30.4.2022,
  - probíhající beta testování do konce roku 2023,
  - k dispozici v předběžném přístupu (early access),
  - více informací na www.penterep.com.
- Navazující projekt **OPSEC**:
  - projekt řešený v rámci Bezpečnostního výzkumu ČR,
  - doba aktivního řešení projektu 1.1.2023–31.12.2023,
  - síťová infrastruktura, aplikační server a bezpečnostní analýza,
  - poskytovatelem programu OPSEC je Ministerstvo vnitra ČR.

NÚKIB

penterep



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Otázky?

Willi Lazarov
Penterep, VUT v Brně
lazarov@vut.cz