

# Modulární platforma pro podporu penetračního testování

**Willi Lazarov**

Penterep, VUT v Brně

[lazarov@vut.cz](mailto:lazarov@vut.cz)



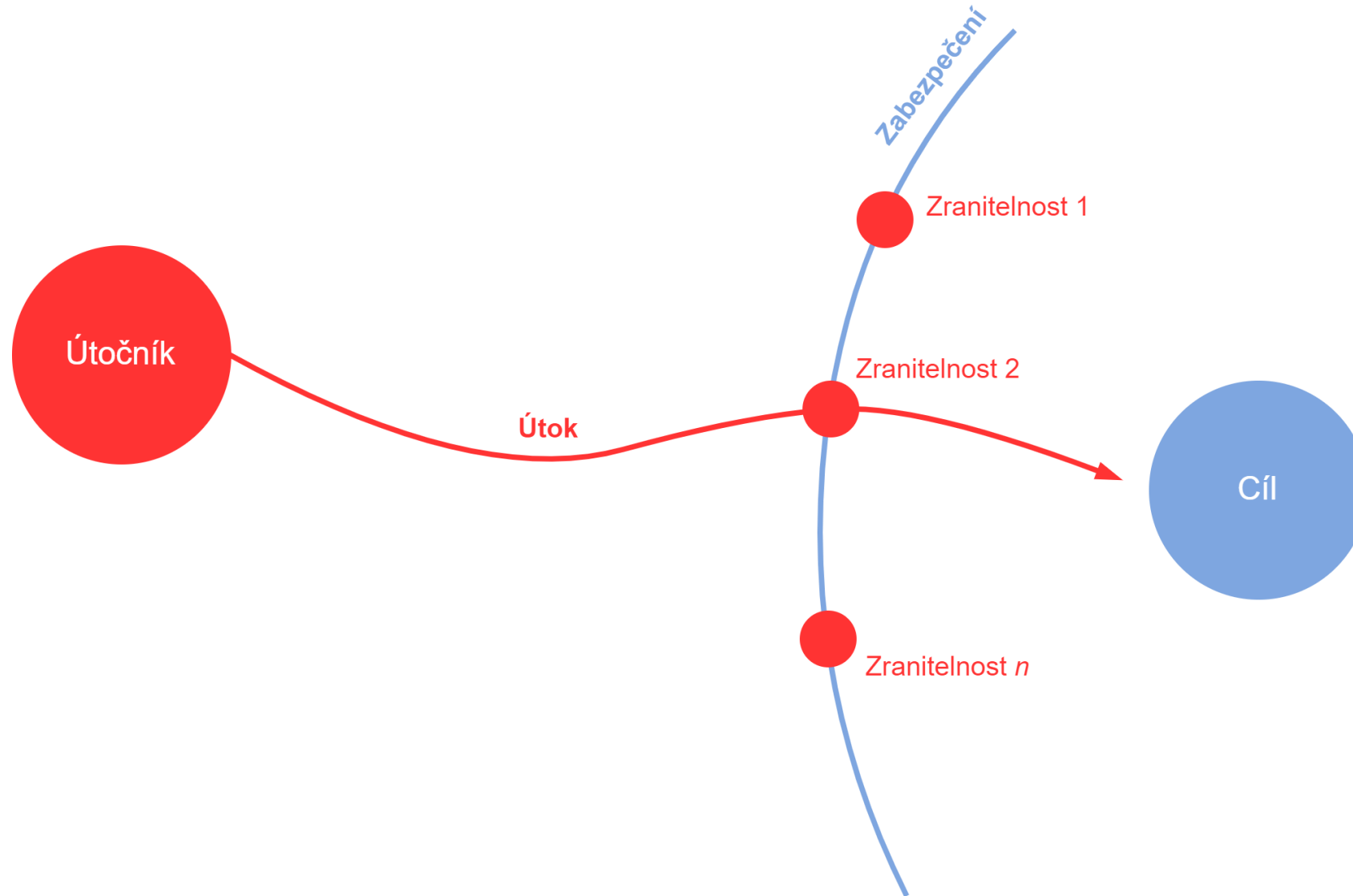
**penterep**



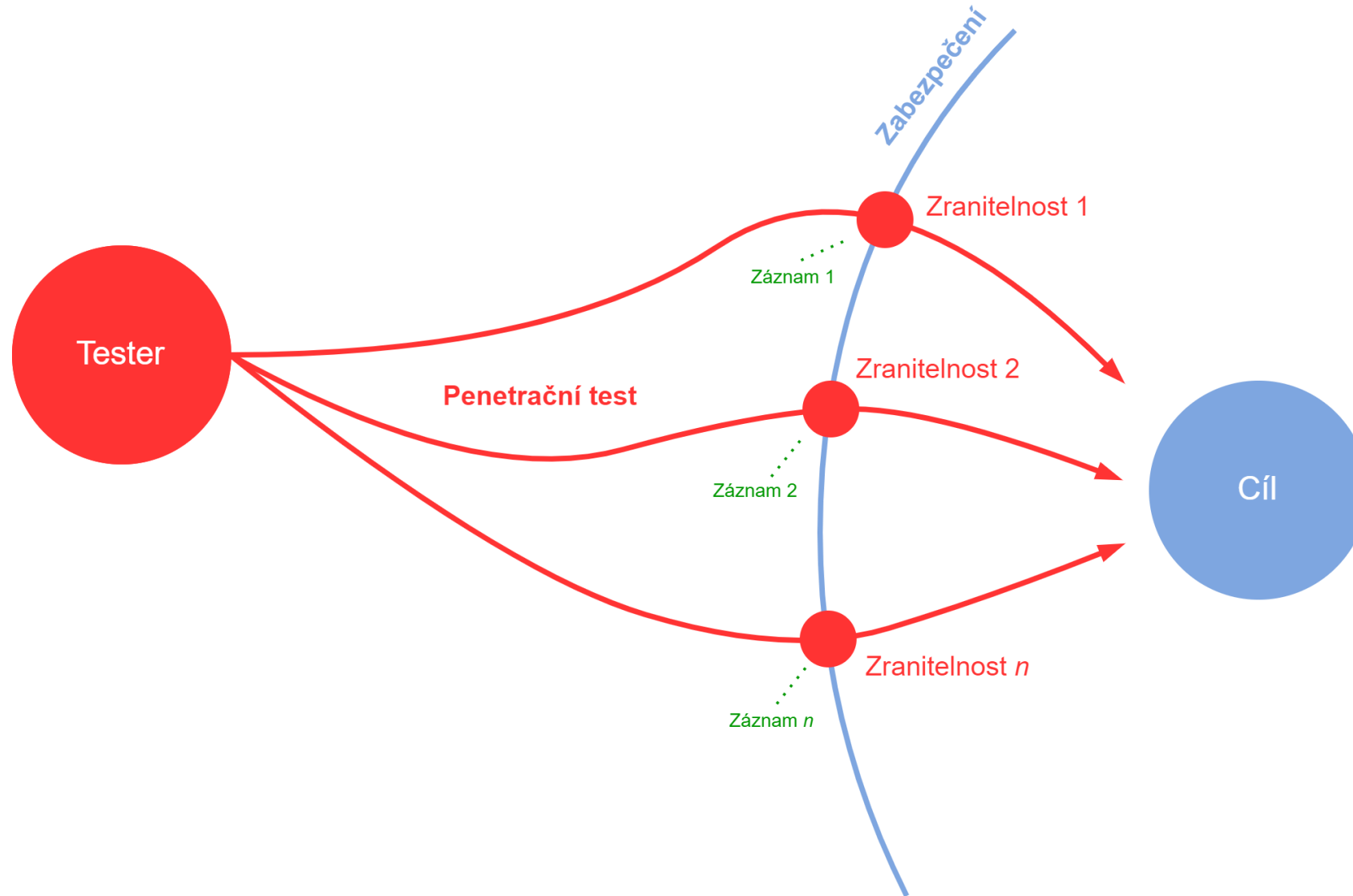
# Penetrační testování

- 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



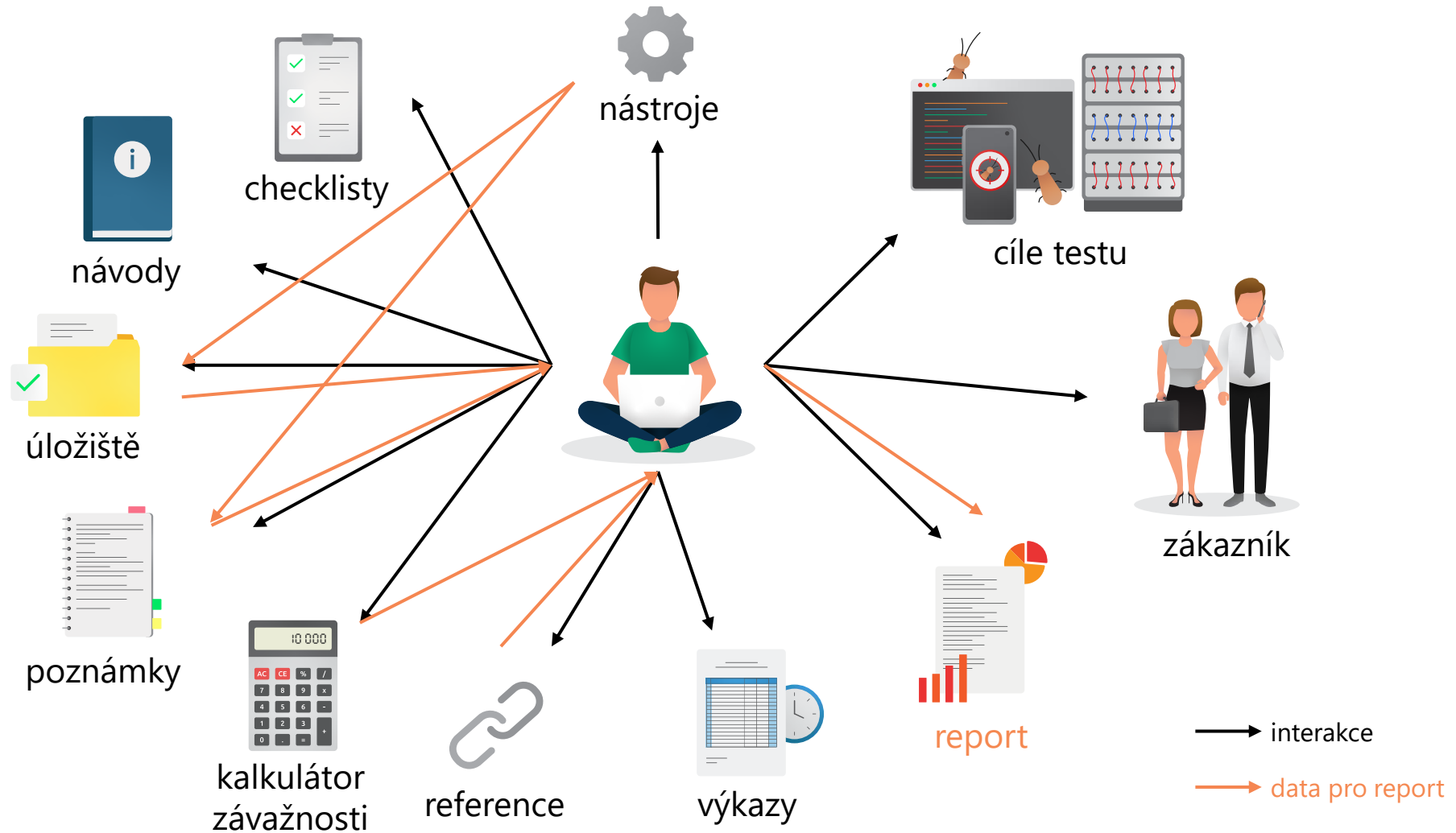
# Penetrační testování vs. běžný útok



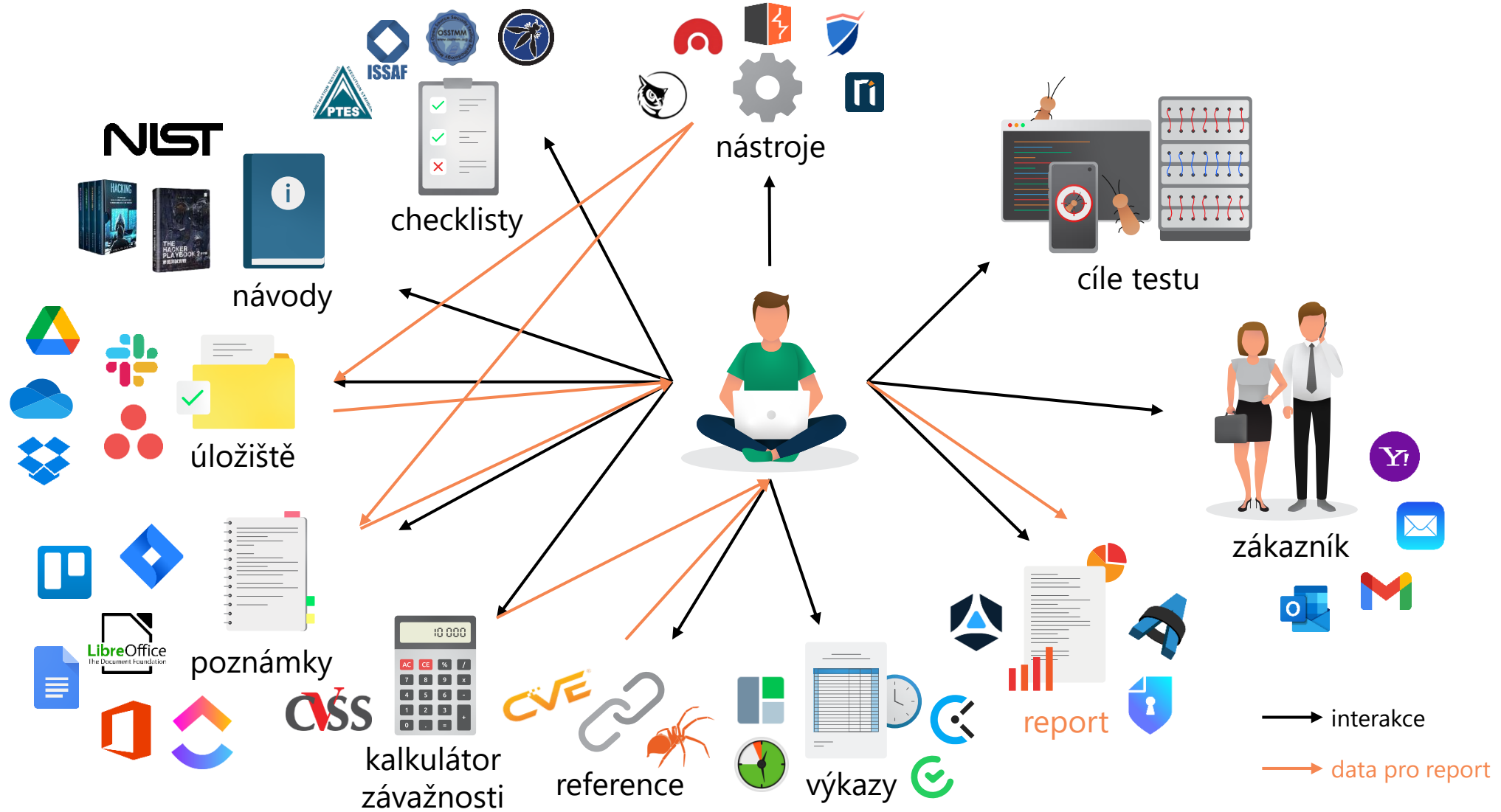
# Současný stav penetračního testování

- **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

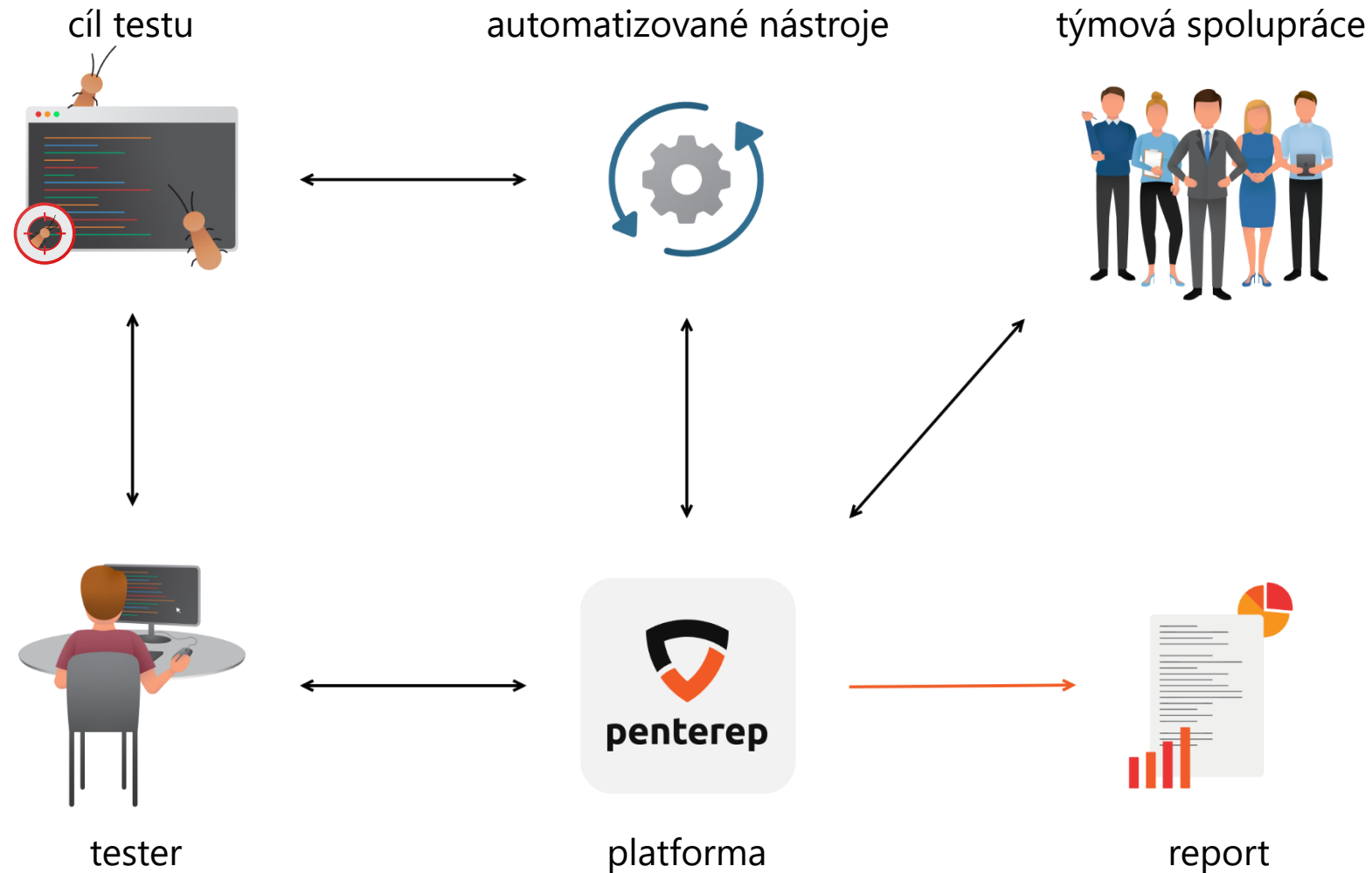


# Penterep

- 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

The screenshot displays the Penterep web security platform interface. The top navigation bar includes the Penterep logo, the user name "Vysoké učení technické v Brně", and icons for home, mail, and profile. The breadcrumb trail shows the path: "Brno University of Technology > cyberarena.utko.feec.vutbr.cz > Autentizace > Jménem a heslem".

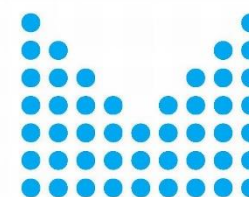
The main content area is titled "Jménem a heslem" and features an "Informace" button and a toolbar with icons for checkmark, bug, attachment, edit, and refresh. Below this is a "Testy" section with a table of test results.

Označení↑↓	Úkol↑↓	Obt...↑↓	Stav↑↓	Nález↑↓
PTL-WEB-AUTH-PWSPA	Není zakázáno použít znak mezery v hesle?	Snadné	✓	✗
PTL-WEB-AUTH-PWREM	Nejsou z hesla vypouštěny mezery?	Snadné	—	□
PTL-WEB-AUTH-PWSPL	Nedochází ke slučování více po sobě jdoucích mezer do jednoho znaku?	Snadné	—	□
PTL-WEB-AUTH-PWTRI	Nedochází k ořezávání bílých znaků na začátku, nebo konci hesla?	Snadné	✓	✗
PTL-WEB-AUTH-PWCOD	Jsou mezery v hesle při přenosu správně kódovány a následně dekód...	Snadné	✓	□
PTL-WEB-AUTH-PWUNI	Je povoleno použít v hesle UNICODE znaky?	Snadné	✓	□
PTL-WEB-AUTH-PWINT	Jsou UNICODE znaky v hesle interpretovány správně jako jeden znak?	Snadné	✓	✗
PTL-WEB-AUTH-PWFAU	Neznemožní UNICODE znaky v hesle možnost ověření hesla?	Snadné	✓	✗
PTL-WEB-AUTH-PWCHG	Může si uživatel změnit své heslo?	Snadné	□	□
PTL-WEB-AUTH-PWINV	Je po změně hesla původní heslo zneplatněno?	Snadné	□	□

The interface also shows a sidebar with a tree view of the scanned application structure, including folders like "API rozhraní", "Autentizace", "Lokální úložiště", "Software", and "Zdroje".

# 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](http://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.



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY

# Otázky?

**Willi Lazarov**

Penterep, VUT v Brně

[lazarov@vut.cz](mailto:lazarov@vut.cz)



**penterep**

