PragoData Consulting

Antiphishingový modul a jeho využití v LMS Moodle

Lucie Zavadilová

moodle Partner
CERTIFIED SERVICES PROVIDER

Phishing

- **Typ kybernetického útoku založeného na důvěřivosti lidí**
  - Tváří se jako komunikace ze sociálních sítí, platebních portálů či úřadů státní správy, od IT administrátorů a podobně
  - Mají za cíl vylákat z uživatelů osobní a citlivé údaje
- **Nezbytnost edukace**
  - Školení kybernetické bezpečnosti
- **Nutno ověřit v praxi!**

Modul Antiphishing

- **Lokální rozšíření pro LMS Moodle**
- **Umožňuje efektivně propojit teoretické vzdělávání v oblasti kybernetické bezpečnosti s praktickou ukázkou „skutečného“ útoku**

Cvičný útok

- **Útok přijde formou e-mailu**
- **Pokud uživatel klikne na odkaz v „podvodném“ e-mailu, je přesměrován na edukační stránku**
- **Správci a manažeři mají přístup k přehlednému reportingu**

Co potřebujeme

- **Instanci LMS Moodle s modulem Antiphishing**
  - Příslušná nastavení na úrovni systému a na úrovni kurzu
- **Náletovou stránku**
  - Na jiné IP adrese a doméně než LMS Moodle
- **Odesílací mailový engine**
  - Na jiné adrese než LMS Moodle
  - KDIM, SPF, reverzní IP, atd.

Náletová stránka

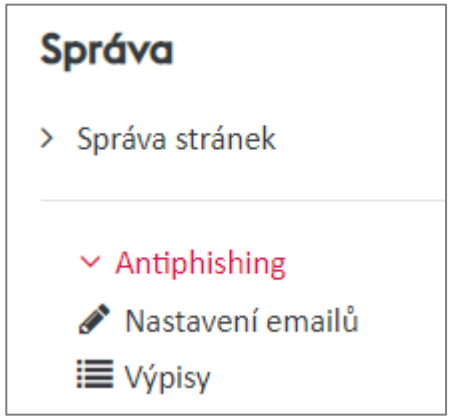
- **Stránka, na kterou se dostane uživatel v případě, že se stane obětí cvičného phishingového útoku**
  - Cílem je, aby obsahovala edukační část
- **Řešení podporuje automatické prolinky do kurzu KB, který uživatel absolvoval**
  - Hash

Odesílací mailový engine

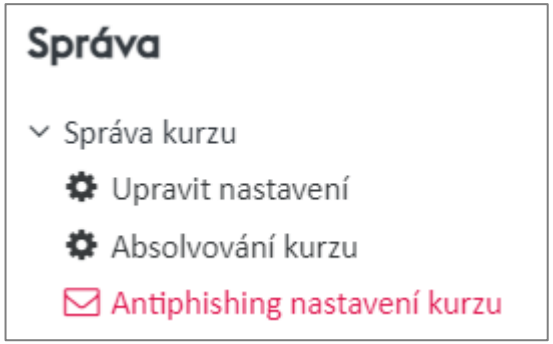
- **Odesílá cvičné phishingové e-maily na základě definovaných parametrů**
- **Konfigurace období rozesílky**
- **Odesílání v náhodném intervalu po absolvování kurzu v LMS Moodle**

Nastavení na straně LMS Moodle

- **Nastavení na úrovni systému**
  - Nastavení šablon phishingových emailů
  - Reporting

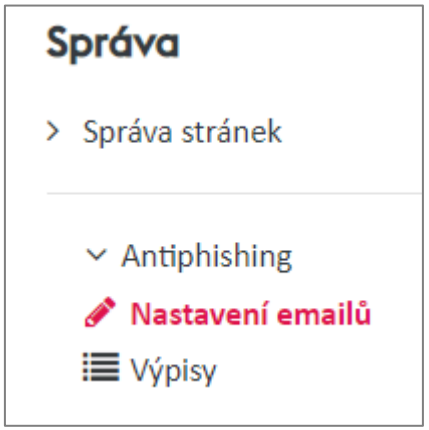


- **Nastavení na úrovni kurzu**
  - Kdy a komu se má poslat který email

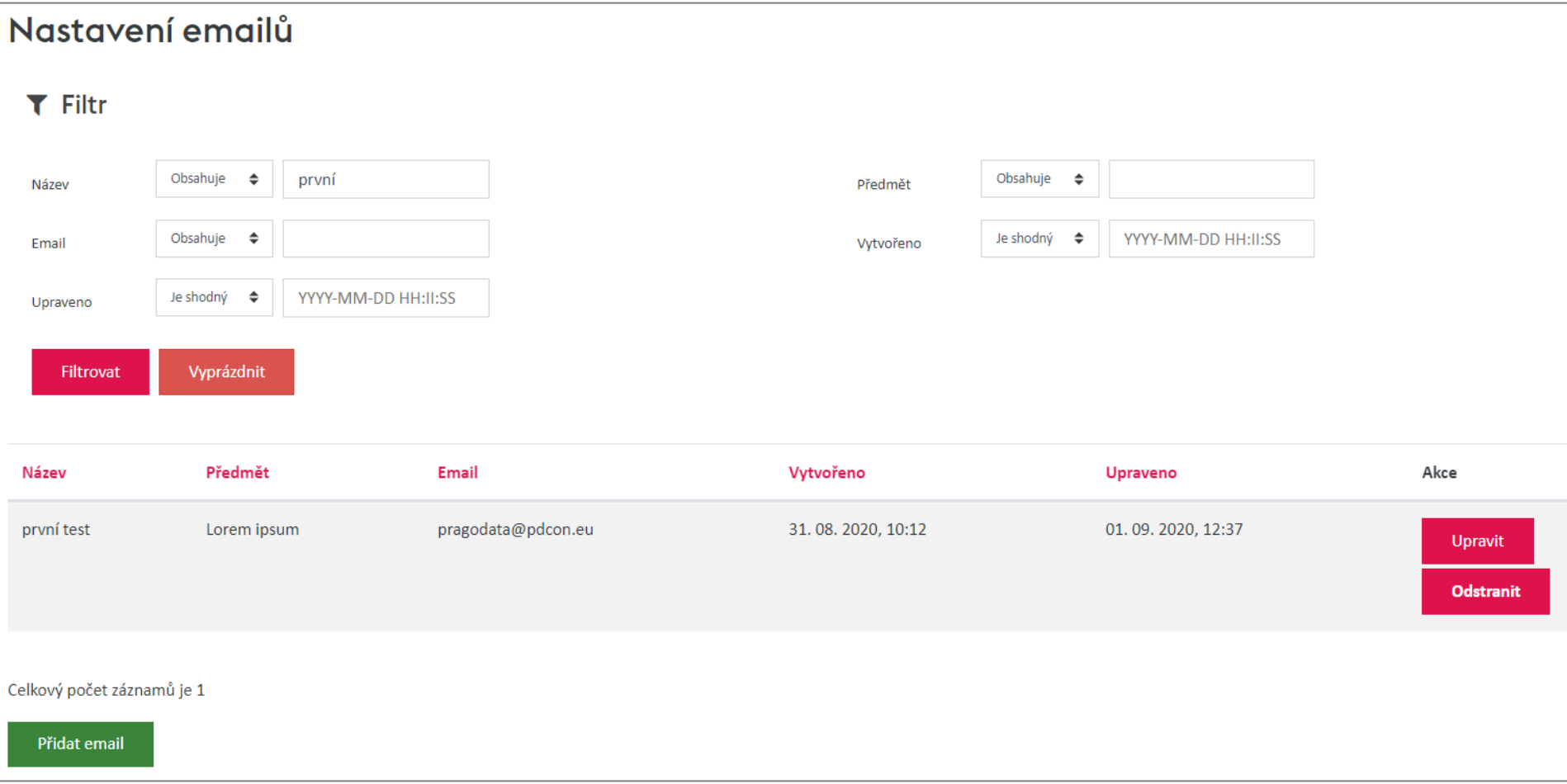


Nastavení e-mailů

- **Pod menu položkou „Nastavení emailů“ se nacházejí 2 obrazovky:**
  - Přehled již nastavených šablon emailů
  - Obrazovka pro nastavení nového emailu



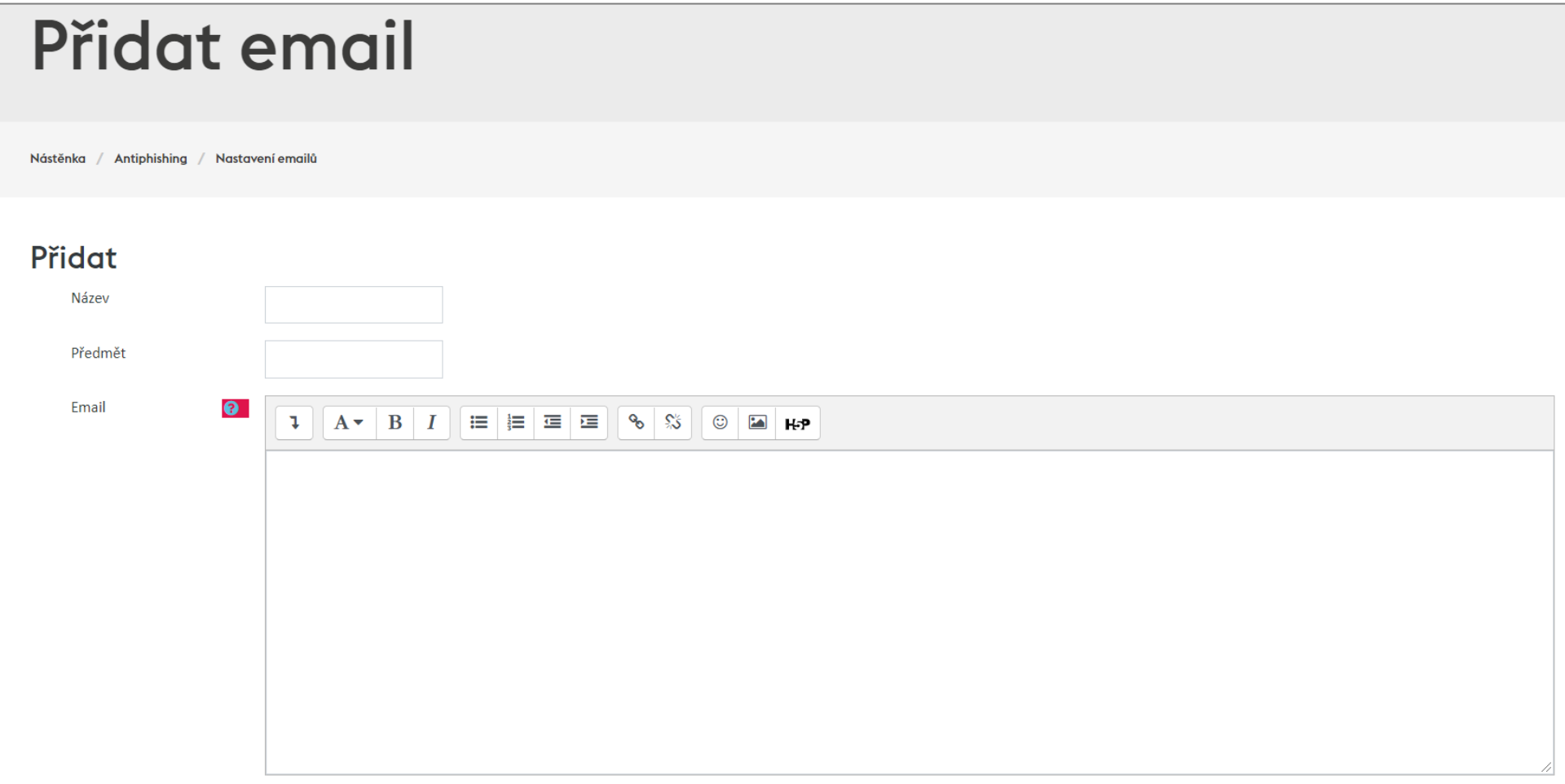
Přehled stávajících šablon emailů



Přehled stávajících šablon emailů

- **Filtr**
- **Přehledová tabulka stávajících emailů**
- **Upravit**
- **Odstranit**
- **Přidat email**

Nová šablona phishingového e-mailu

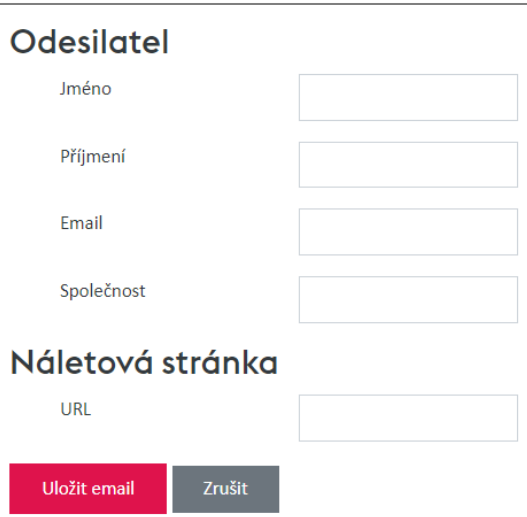


Nová šablona phishingového e-mailu

- **Název**
  - Uživatel nevidí, pro naši orientaci v systému
- **Předmět**
  - Předmět emailu, který dostane uživatel
- **Email**
  - Vlastní text emailu
  - WYSIWYG
  - Klíčová slova {jmeno}, {prijmeni}, {link}

Nová šablona phishingového e-mailu

- **Pokračování formuláře**



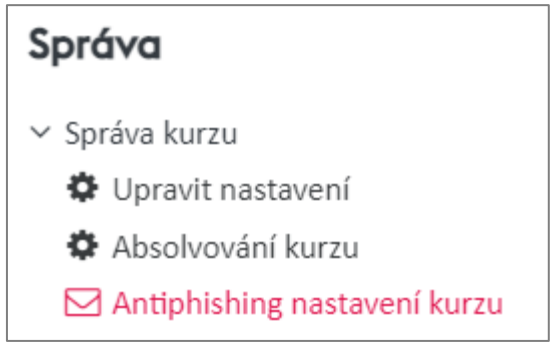
Nová šablona phishingového e-mailu

- **Odesílatel**
  - Uživatel uvidí v poli „Od“
  - Jméno, Příjmení, Email, Společnost
- **Náletová stránka**
  - Zadáváme URL „náletové stránky“, tj. stránky, na niž bude přesměrován uživatel, který podlehne cvičnému phishingovému útoku
  - V nastavení těla emailu na ni odkazujeme klíčovým slovem {link}
  - Obsahuje edukační obsah

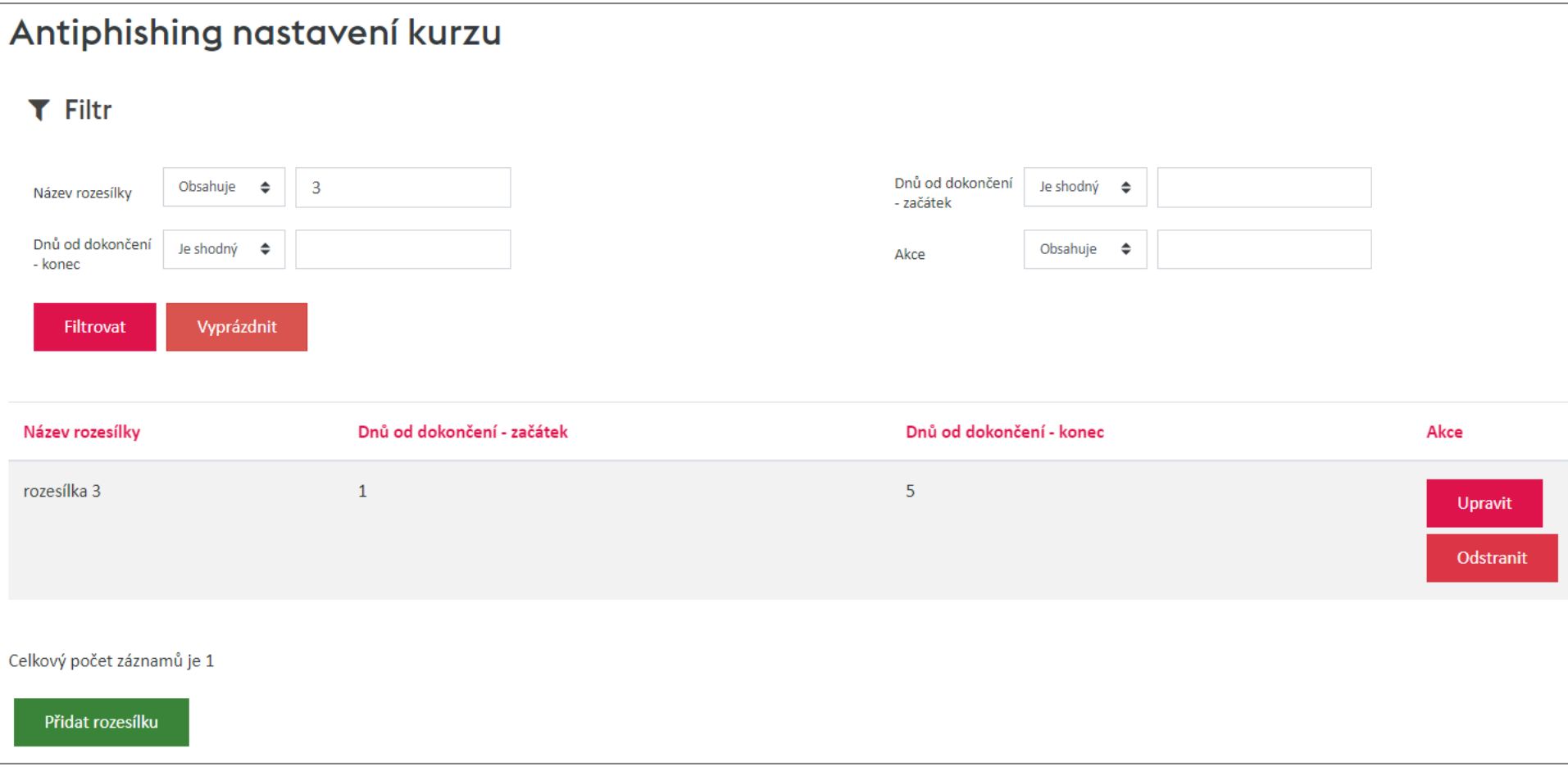
Nastavení rozesílek v kurzu

- **Ve správě kurzu se pod menu položkou Nastavení emailů nacházejí 2 obrazovky:**
  - Přehled již nastavených rozesílek

    (+ filtr, + tlačítko Přidat email)
  - Obrazovka pro nastavení nové rozesílky



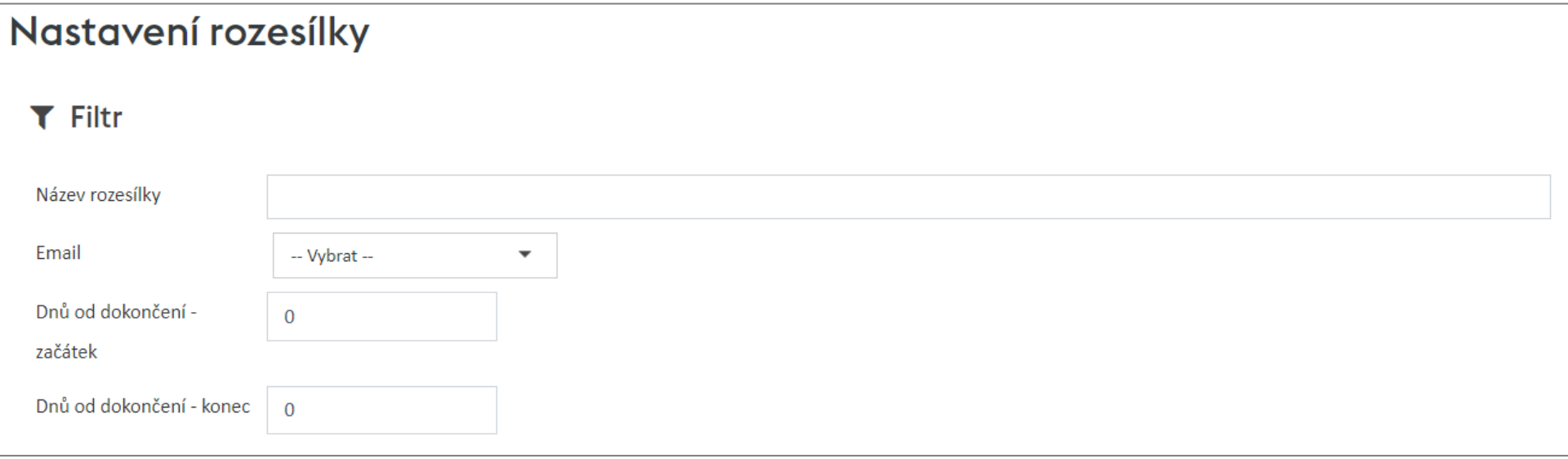
Přehled stávajících rozesílek



Přehled stávajících rozesílek

- **Filtr**
- **Přehledová tabulka stávajících rozesílek**
- **Upravit**
- **Odstranit**
- **Přidat rozesílku**

Vytvoření nové rozesílky



- **Název rozesílky**
  - Interní název pro naši orientaci v systému
- **Email**
  - Vybíráme šablonu emailu z rolovacího pole

Vytvoření nové rozesílky

- **Dnů od dokončení – začátek**
  - Kolik dnů od absolvování nejdříve přijde definovaným uživatelům email
  - Hodnota se zadává ve dnech
- **Dnů od dokončení - konec**
  - Kolik dnů od absolvování nejpozději přijde definovaným uživatelům email
  - Hodnota ve dnech musí být vyšší než u „Dnů od dokončení - konec“

Vytvoření nové rozesílky

- **Pokračování formuláře – výběr uživatelů**

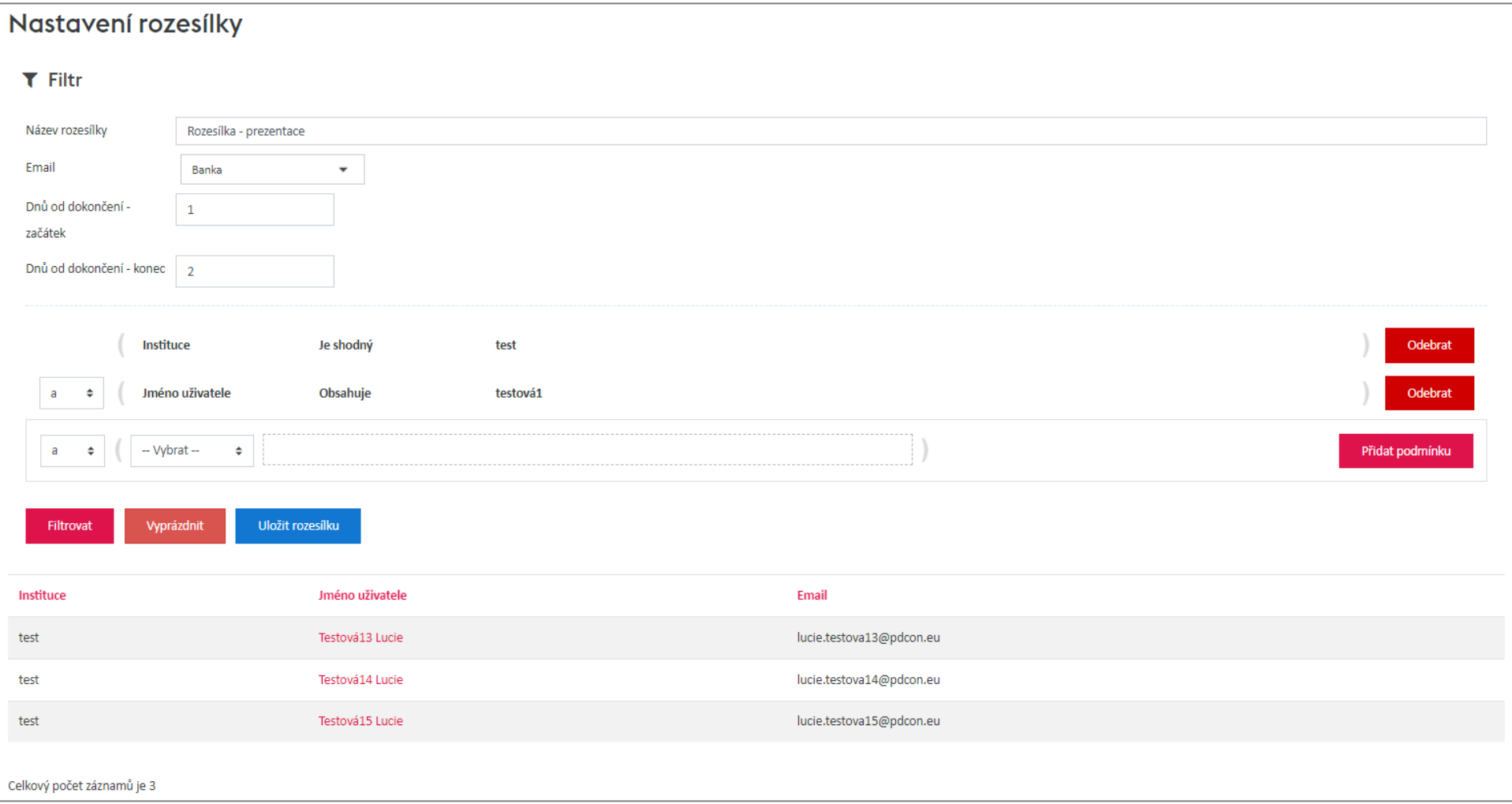
Instituce	Jméno uživatele	Email
test	Testová13 Lucie	lucie.testova13@pdcon.eu
test	Testová14 Lucie	lucie.testova14@pdcon.eu
test	Testová15 Lucie	lucie.testova15@pdcon.eu

Celkový počet záznamů je 3

Vytvoření nové rozesílky

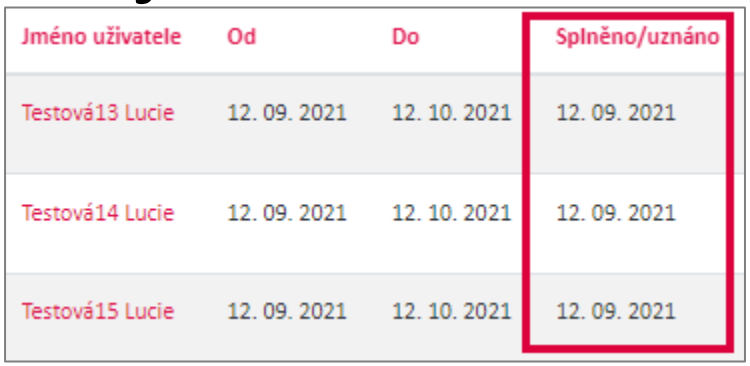
- **Definování příjemců emailů**
  - Pokročilé filtry
  - Kombinace podmínek (a, nebo)
  - Filtrování dle Instituce, Jména uživatele, Emailu
  - Výsledkem je množina uživatelů, jimž v zadaném rozmezí od absolvování kurzu ke kybernetické bezpečnosti přijde cvičný mailový útok

Vytvoření nové rozesílky – celý příklad



Podmínky odeslání emailu

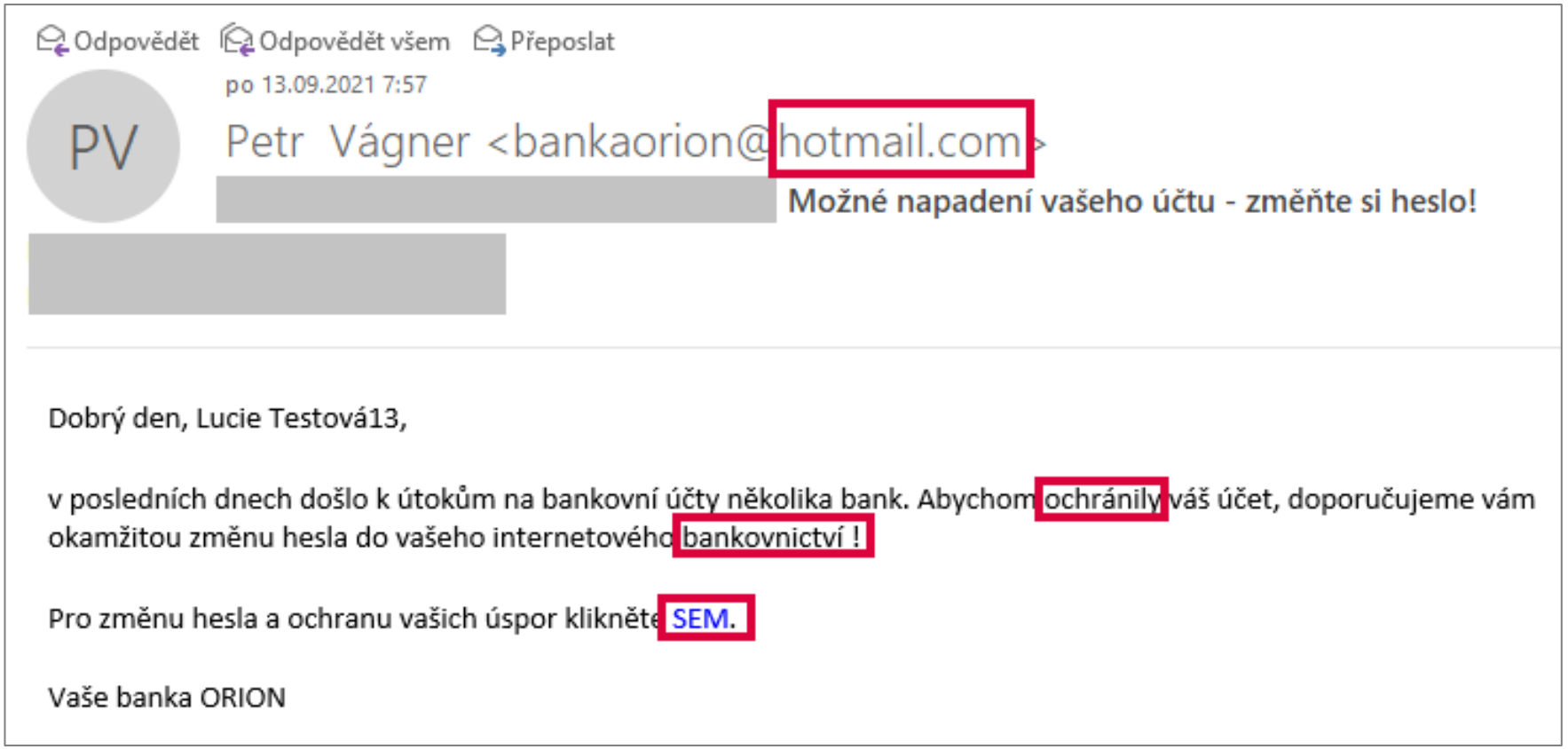
- **Uživatel je součástí rozesílky přiřazené ke kurzu**
- **Uživatel absolvuje kurz**



Jméno uživatele	Od	Do	Splněno/uznáno
Testová13 Lucie	12. 09. 2021	12. 10. 2021	12. 09. 2021
Testová14 Lucie	12. 09. 2021	12. 10. 2021	12. 09. 2021
Testová15 Lucie	12. 09. 2021	12. 10. 2021	12. 09. 2021

- **V časovém rozmezí definovaném v rozesílce proběhnou úlohy cronu**
  - Dávková příprava fronty antiphishingových emailů
  - Rozeslání antiphishingových emailů

Příklad podvodného emailu



Odpovědět Odpovědět všem Přeposlat

po 13.09.2021 7:57

PV

Petr Vágner <bankaorion@hotmail.com>

Možné napadení vašeho účtu - změňte si heslo!

Dobrý den, Lucie Testová13,

v posledních dnech došlo k útokům na bankovní účty několika bank. Abychom ochránily váš účet, doporučujeme vám okamžitou změnu hesla do vašeho internetového bankovnictví !

Pro změnu hesla a ochranu vašich úspor klikněte SEM.

Vaše banka ORION

Příklad podvodného emailu

- **Vykazuje známky podvodných emailů**
  - Podezřelá doména odesílatele
  - Gramatická chyba
  - Chyba v interpunkci
  - Podvodný odkaz nesměřuje do bankovnictví, ale na podvodnou stránku – vylákání přihlašovacích údajů uživatele

Náletová stránka

- **Stránka, na niž se dostane uživatel, který klikne na link v podvodném emailu**
- **URL z „Nastavení emailu“ + hash**
  - Identifikace konkrétního uživatele + kurzu, ze kterého přichází

Příklad náletové stránky

Dobrý den,

na tuto webovou stránku jste se dostal/a, protože jste klikl/a na odkaz v emailu, který měl simulovat tzv. phishingový útok.

Tento email vám byl zaslán na základě absolvování kurzu **Kybernetická bezpečnost 2021** a měl ověřit, zda jste si informace zapamatoval/a a dokážete se dle nich na internetu chovat.

Jelikož se vám na odkaz podařilo kliknout, doporučujeme vám věnovat pozornost následujícím informacím.

Co je to phishing

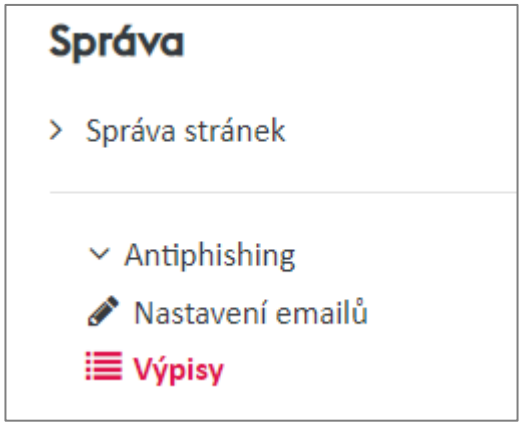
Phishing je podvodná technika používaná na internetu k získávání citlivých údajů v elektronické komunikaci. K nalákání důvěřivé veřejnosti komunikace předstírá, že pochází z populárních sociálních sítí, aukčních webů, on-line platebních portálů, úřadů státní správy nebo od IT administrátorů.

Jak se mohu bránit

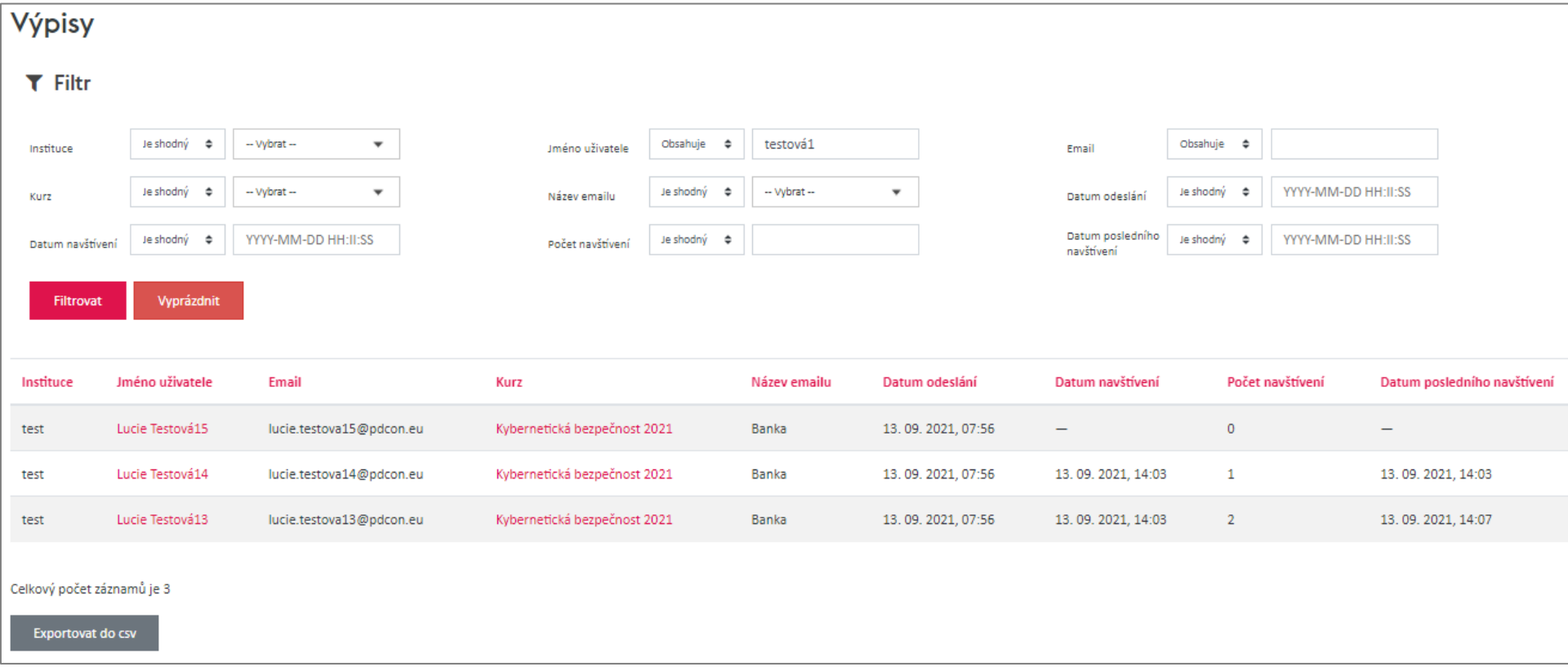
Nachystali jsme pro vás přehlednou **příručku ke stažení**. Také se můžete vrátit ke studiu kurzu **Kybernetická bezpečnost 2021** ve vašem **LMS systému**.

Výpisy a reporting

- **K vyhodnocování antiphishingových kampaní slouží obrazovka Výpisy**
- **Přehledná tabulková podoba**
- **Filtrování dle množství parametrů**



Výpisy a reporting



Výpisy – důležité funkce

- **Filtrování dle řady parametrů**
- **Seřazení informací kliknutím na záhlaví sloupce**
- **Export do CSV**

Jaké informace obsahují výpisy

- **Instituce**
- **Jméno uživatele**
- **Email**
- **Kurz**
  - Kurz, ve kterém byla nastavena konkrétní rozesílka, tzn. který kurz uživatel absolvoval
- **Název emailu**
  - Název šablony emailu z „Nastavení emailů“, tzn. který email uživatel obdržel

Jaké informace obsahují výpisy – pokr.

- **Datum odeslání**
  - Datum odeslání cvičného útoku z LMS
- **Datum navštívení**
  - Datum navštívení podvodného odkazu uživatelem
  - Pokud uživatel na odkaz neklikne, je zobrazena pomlčka
- **Počet navštívení**
- **Datum posledního navštívení**

Dotazy?

PragoData Consulting

Díky za pozornost

Lucie Zavadilová

moodlepartner.pragodata.cz

www.pragodata.cz

moodle Partner
CERTIFIED SERVICES PROVIDER