cesnet

Phishingator

Cvičný phishing nejen na českých univerzitách

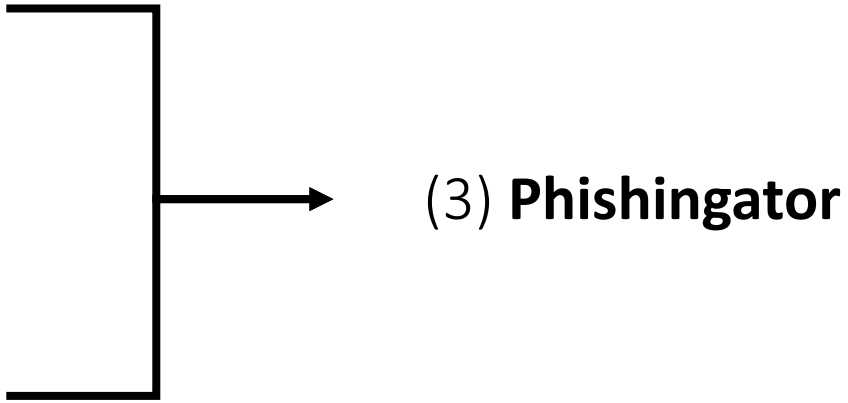
Martin Šebela – CESNET FLAB

31. května 2023

K čemu Phishingator?

- **Bezpečnostní riziko phishingu**
  - Prozrazení přístupových údajů
  - Potřeba vzdělaného uživatele
  - Propracovanější techniky útočníků

- (1) **Testy sociálního inženýrství** (FLAB CESNET)
  - Služba na klíč
  - Teoretické i praktické školení uživatelů
  - Závěrečná zpráva, prezentace výsledků
- (2) **Vlastní realizace** v organizaci
  - Teoretické školení – snadné
  - Praktický test – komplikovanější



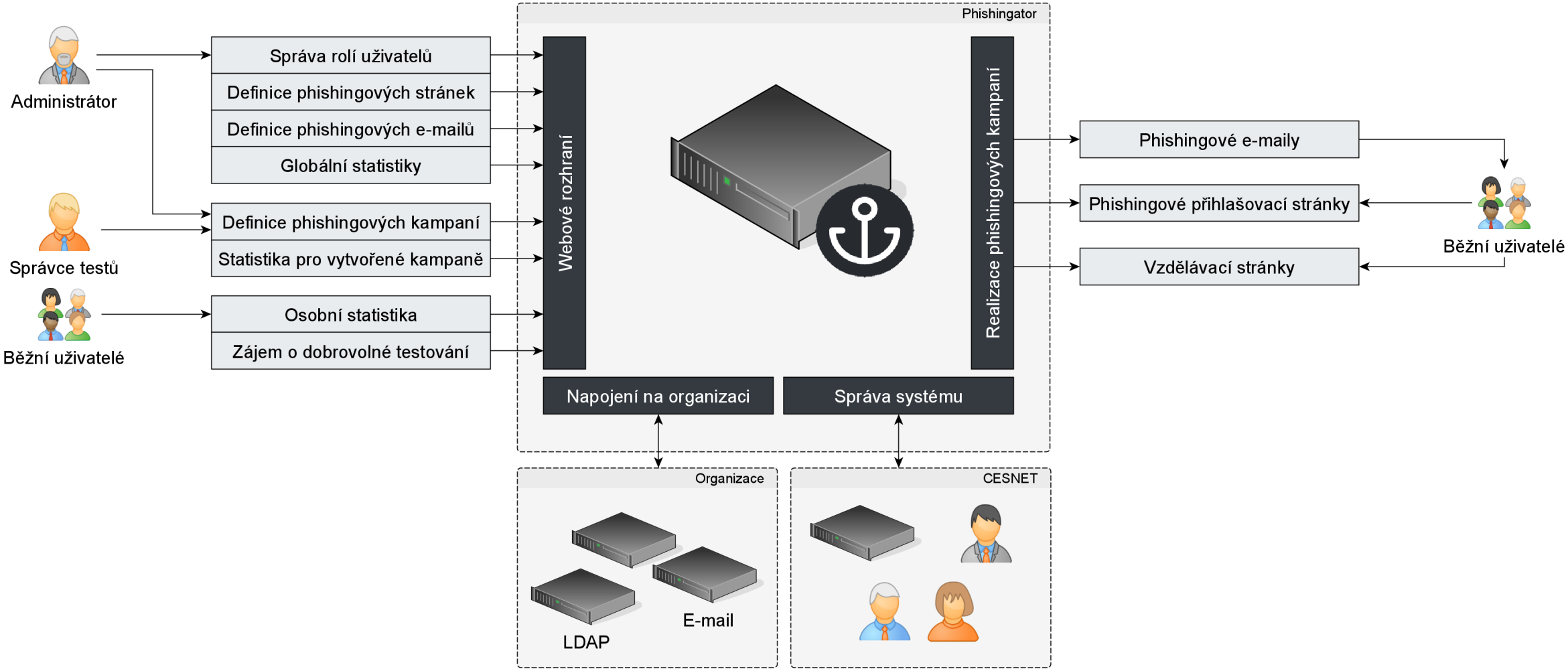
Phishingator

= Webová aplikace pro automatizované **rozesílání cvičných phishingových zpráv**

- Původně **bakalářská práce na ZČU** (2019), nyní OpenSource
- **CESNET poskytuje** formou **Software as a Service**
  - Technicky se nemusíte o nic starat
  - Phishingator napojíme na Vaši organizaci
  - Každá organizace = **vlastní instance Phishingatoru**

- Praktický doplněk ke školení „kdykoliv a kdekoliv“
  - Přímá **konfrontace** s phishingem
  - **Cílené školení** uživatelů
- **Zpětná vazba pro uživatele** o absolvování cvičného phishingu

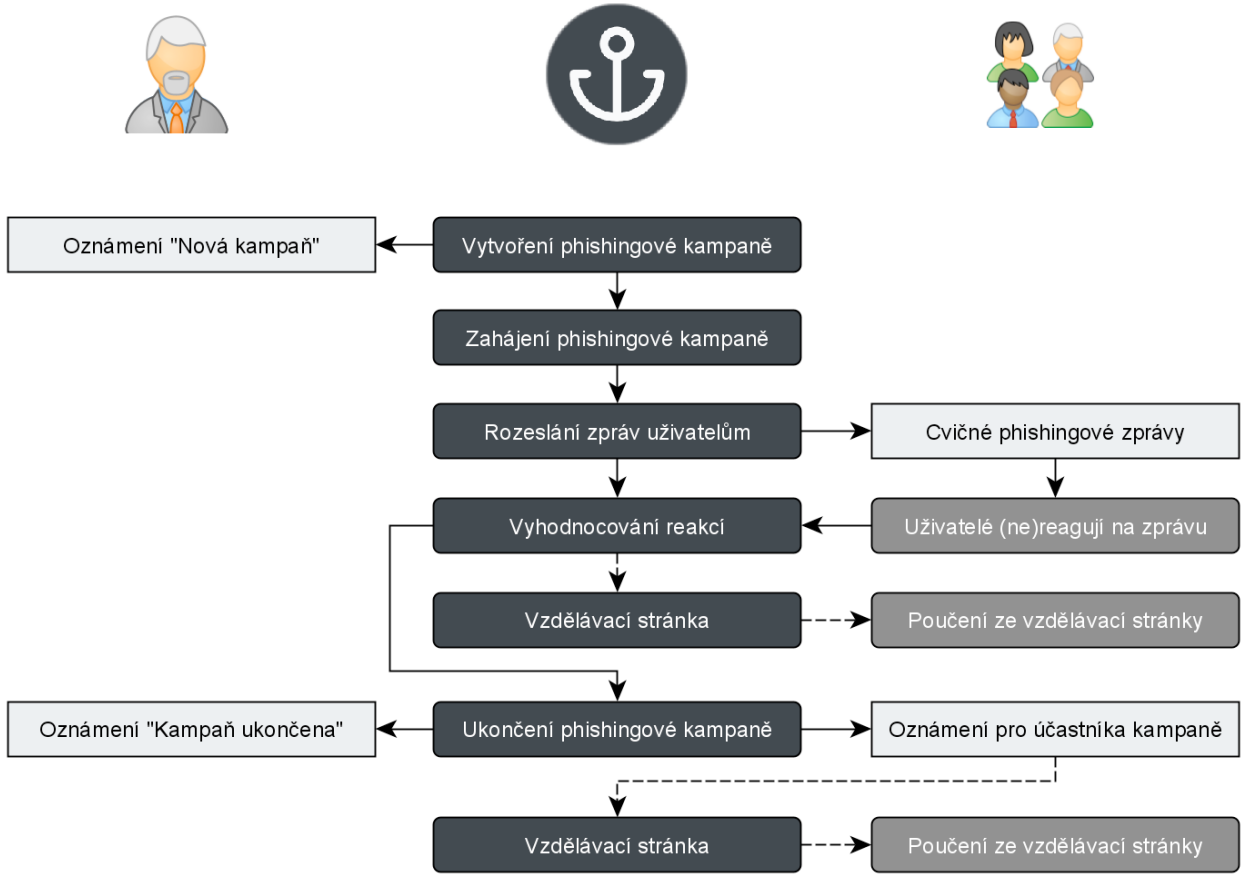
Phishingator



Průběh phishingové kampaně

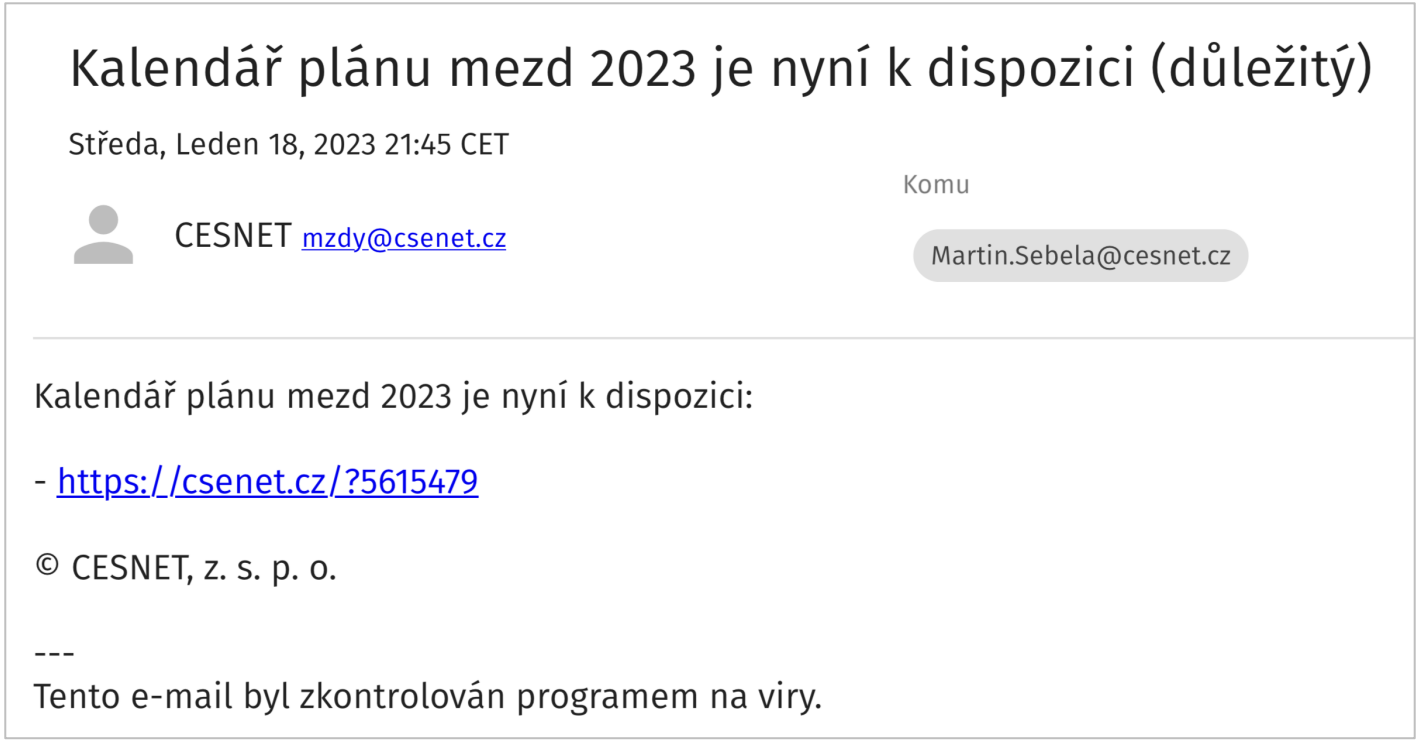
- **Phishingová kampaň** = podvodný e-mail + podvodná stránka

1. Vytvoření **e-mailu** a **indicií**
2. Nákup podvodné **domény**
3. Vytvoření **podvodné stránky** (šablona + URL)
4. Rozeslání e-mailů **konkrétním příjemcům**
5. Sledování **reakcí příjemců**
6. Automatická **zpětná vazba pro příjemce**



Příklad cvičného phishingu

- Na základě **skutečného phishingu na mzdy** registrovaného několika univerzitami v ČR
- **Podvodný e-mail** odeslaný z Phishingatoru s odkazem na **podvodnou stránku:**



Kalendář plánu mezd 2023 je nyní k dispozici (důležitý)

Středa, Leden 18, 2023 21:45 CET

CESNET mzdy@csenet.cz

Komu

Martin.Sebela@cesnet.cz

Kalendář plánu mezd 2023 je nyní k dispozici:

- https://csenet.cz/?5615479

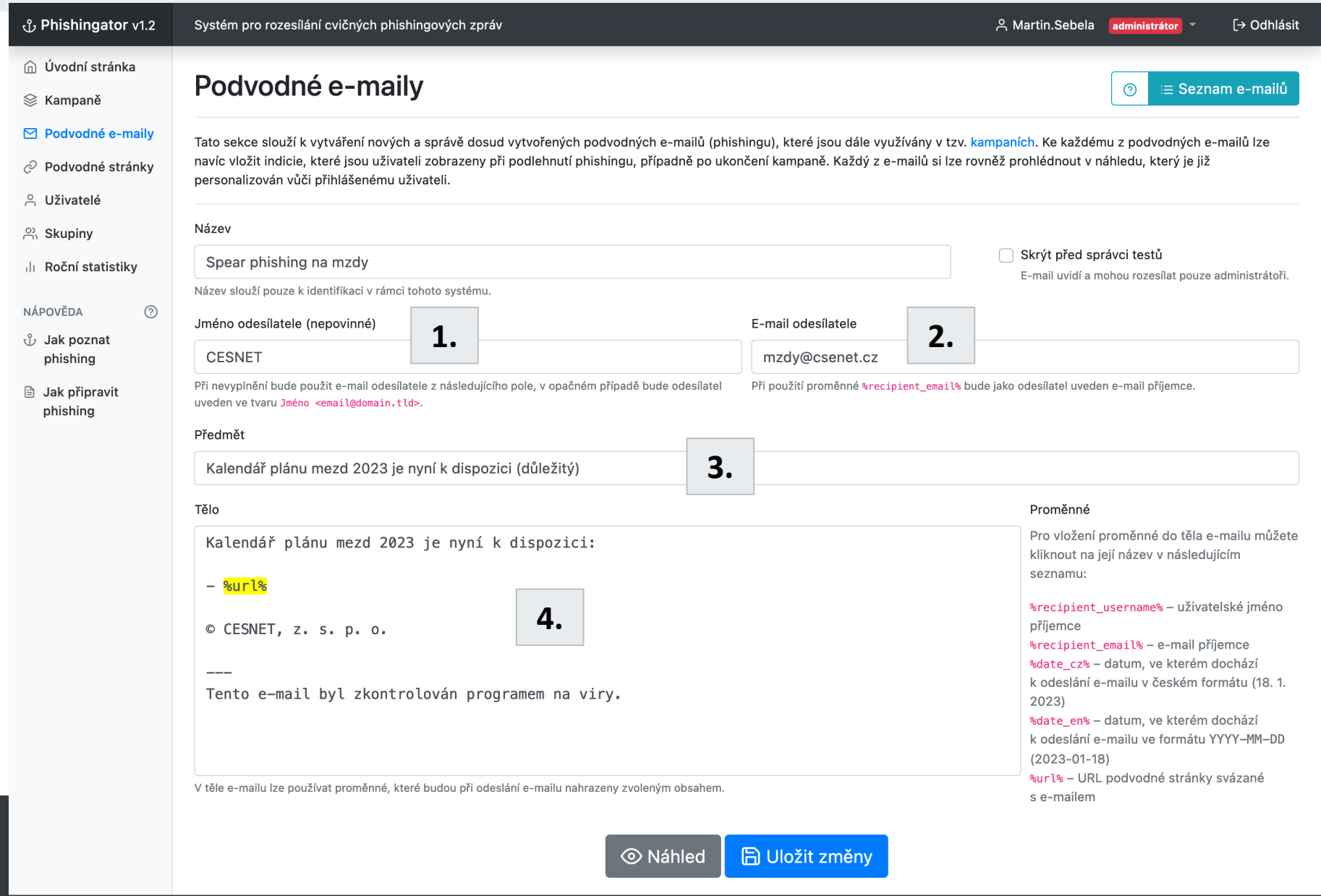
© CESNET, z. s. p. o.

Tento e-mail byl zkontrolován programem na viry.

Z pohledu administrátora – vytvoření phishingu

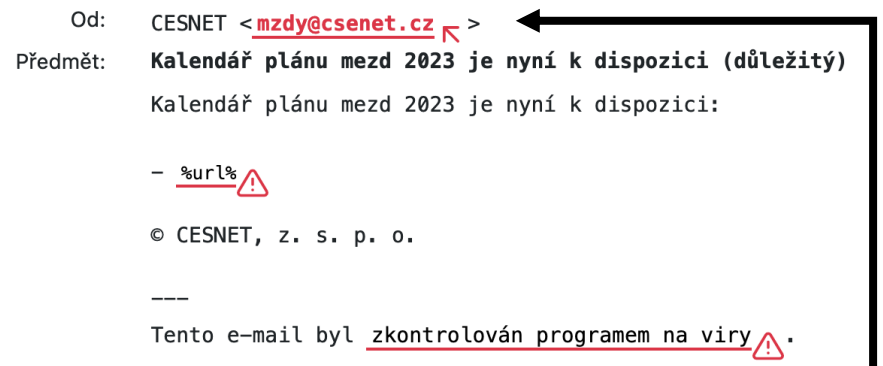
- Vytvoření **cvičného podvodného e-mailu**

1. **Jméno** odesílatele
2. **E-mail** odesílatele
3. **Předmět**
4. **Parametrizované tělo** e-mailu
   - Možnost personalizace



Vyplnění indicií k rozpoznání phishingu

1. Náhled podvodného e-mailu s červeně zvýrazněnými indiciemi



Náhled včetně indicií

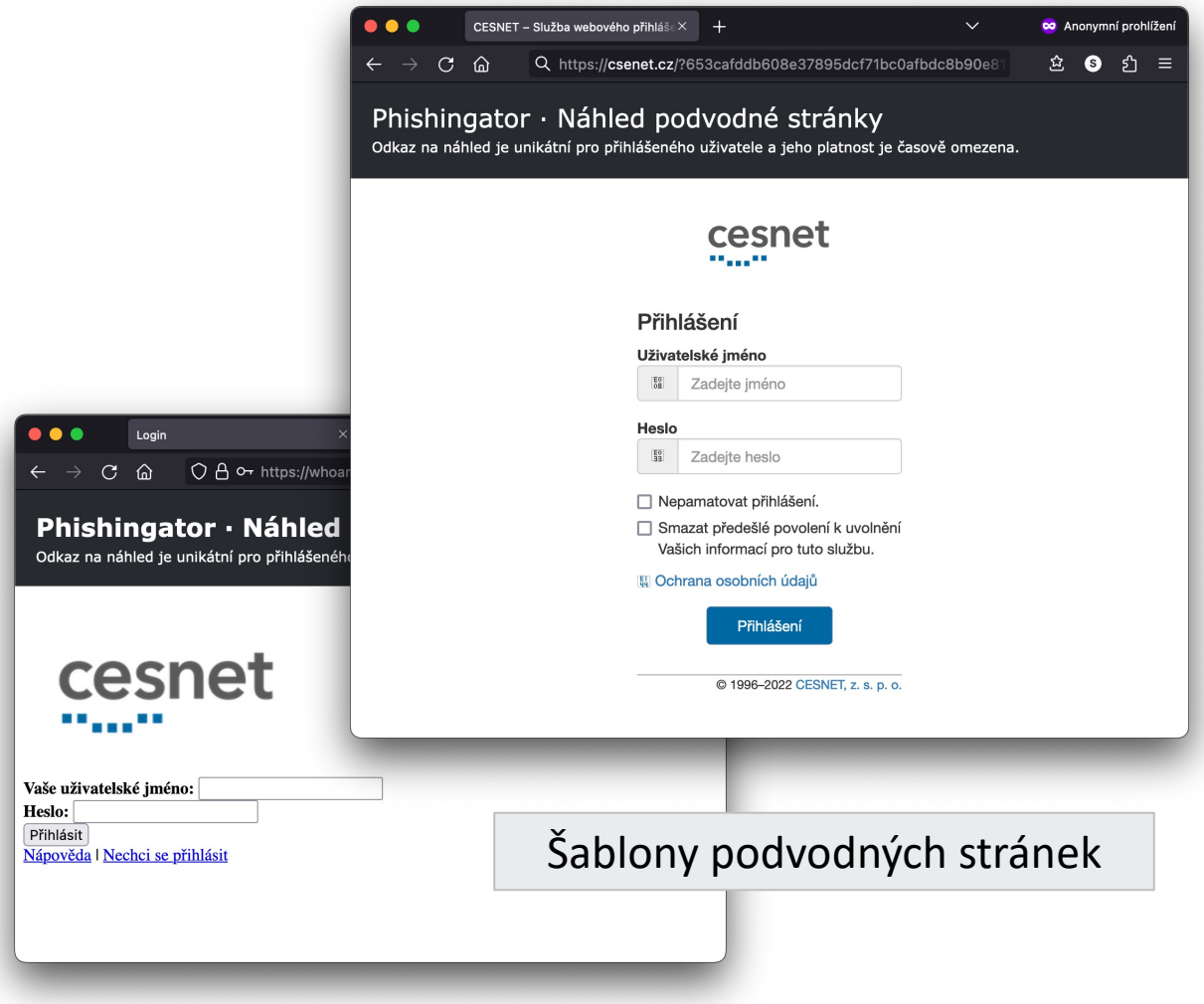
Indicie (3) k rozpoznání tohoto phishingu

Indicie (podezřelý řetězec)	Nadpis	Popis (nepovinné)	
%sender_email%	E-mail odesílatele	E-mail odesílatele nemá s organizací CESNET nic společného.	Smazat / Uložit změny
%url%	Podezřelá URL	Nejedná se o oficiální doménu CESNET.CZ, ale o snahu útočníka napodobit její	Smazat / Uložit změny
zkontrolován programem na vir	Tento text může připsat každý	Neříká to nic o věrohodnosti e-mailu.	Smazat / Uložit změny

2. Přidání indicií (typických znaků phishingu), na základě kterých bylo možné phishing rozpoznat

Vytvoření podvodné stránky

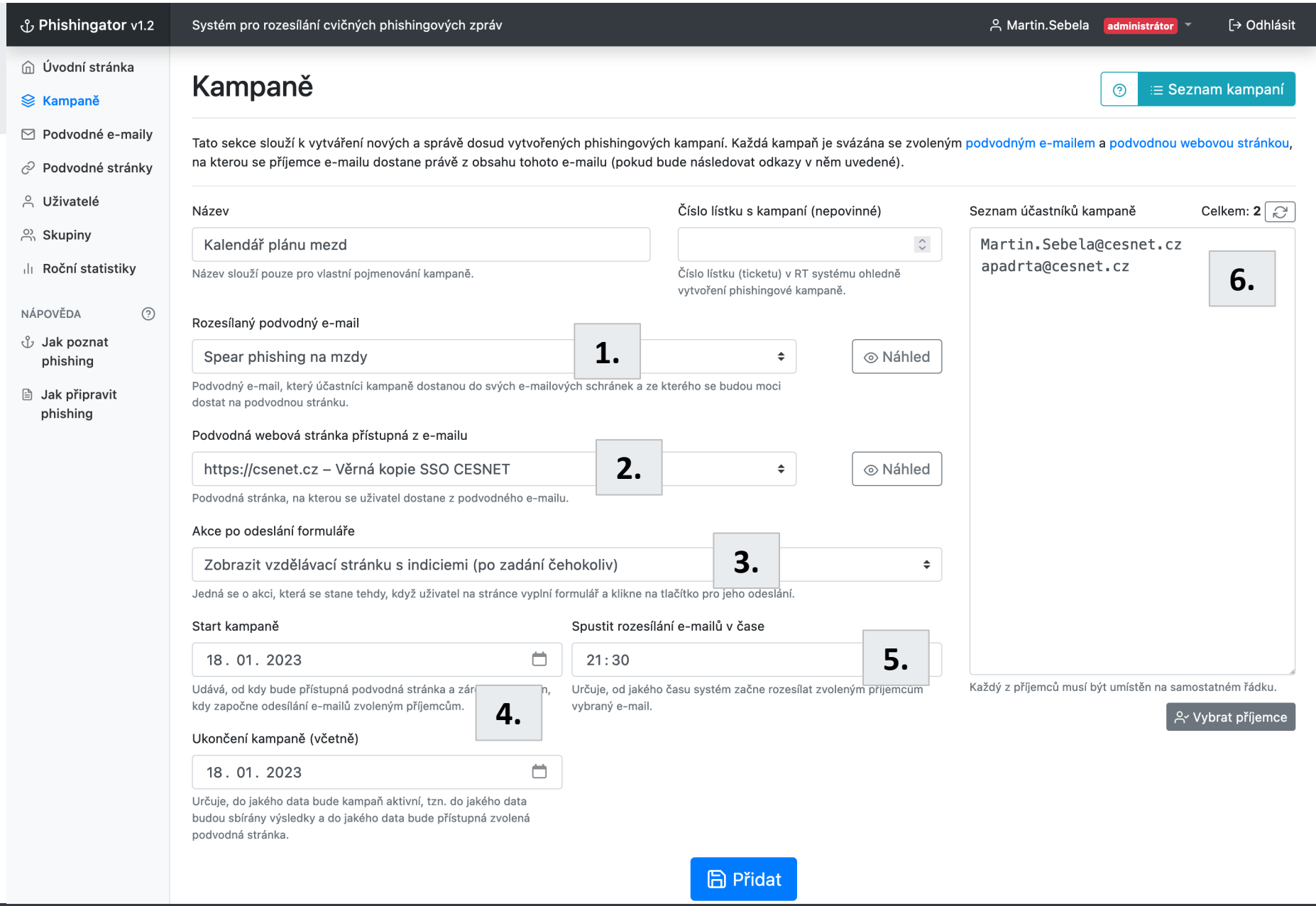
- Nákup cvičné, phishingové **domény**, kde bude hostována podvodná stránka
  - Překlepy, snaha napodobit název organizace
  - Např. pro CESNET: cesnet.cz vs. csenet.cz, oesnet.cz, …
- Nasměrování **DNS** na Phishingator
- Vytvoření **HTML šablony** pro podvodnou stránkou
- Případně vydání **HTTPS certifikátu**
- Volba **URL adresy** (různé adresáře a parametry v adrese)



Šablony podvodných stránek

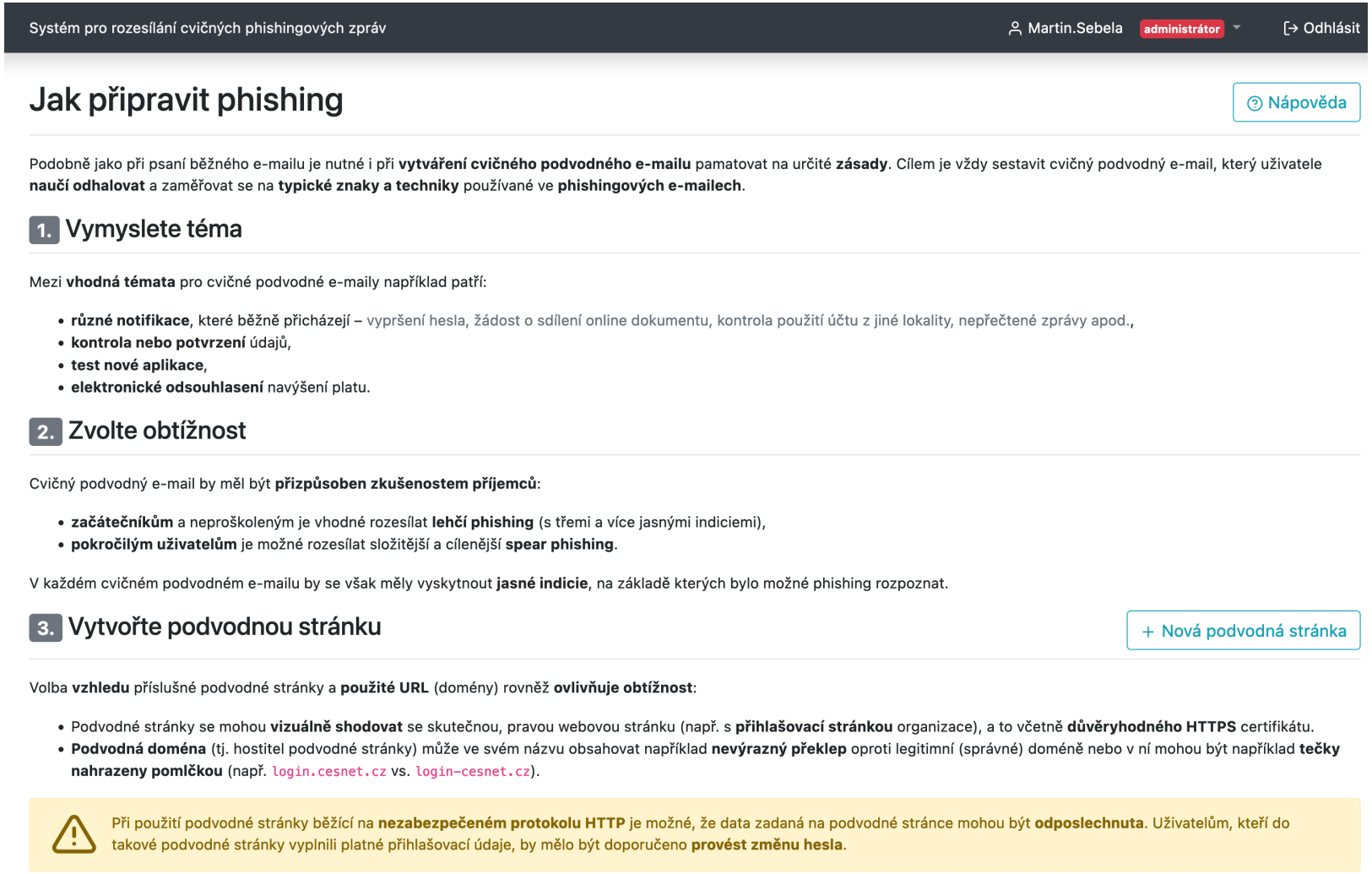
Kampaň

- **Phishingová kampaň** se skládá z:
  1. podvodný **e-mail**
  2. podvodná **stránka**
  3. co se stane po **vyplnění formuláře** na podvodné stránce
  4. od **kdy**, do kdy
  5. **čas** rozesílání
  6. **příjemci**



Nápověda

- Pro **administrátory**
  - Jak správně připravit cvičný phishing
- Pro **uživatele**
  - Jak rozpoznat phishing
  - Typické znaky



Z pohledu uživatele

- **Podvodný e-mail** odeslaný z Phishingatoru s odkazem na **podvodnou stránku**

Kalendář plánu mezd 2023 je nyní k dispozici (důležitý)

Středa, Leden 18, 2023 21:45 CET

CESNET mzdy@csenet.cz

Komu

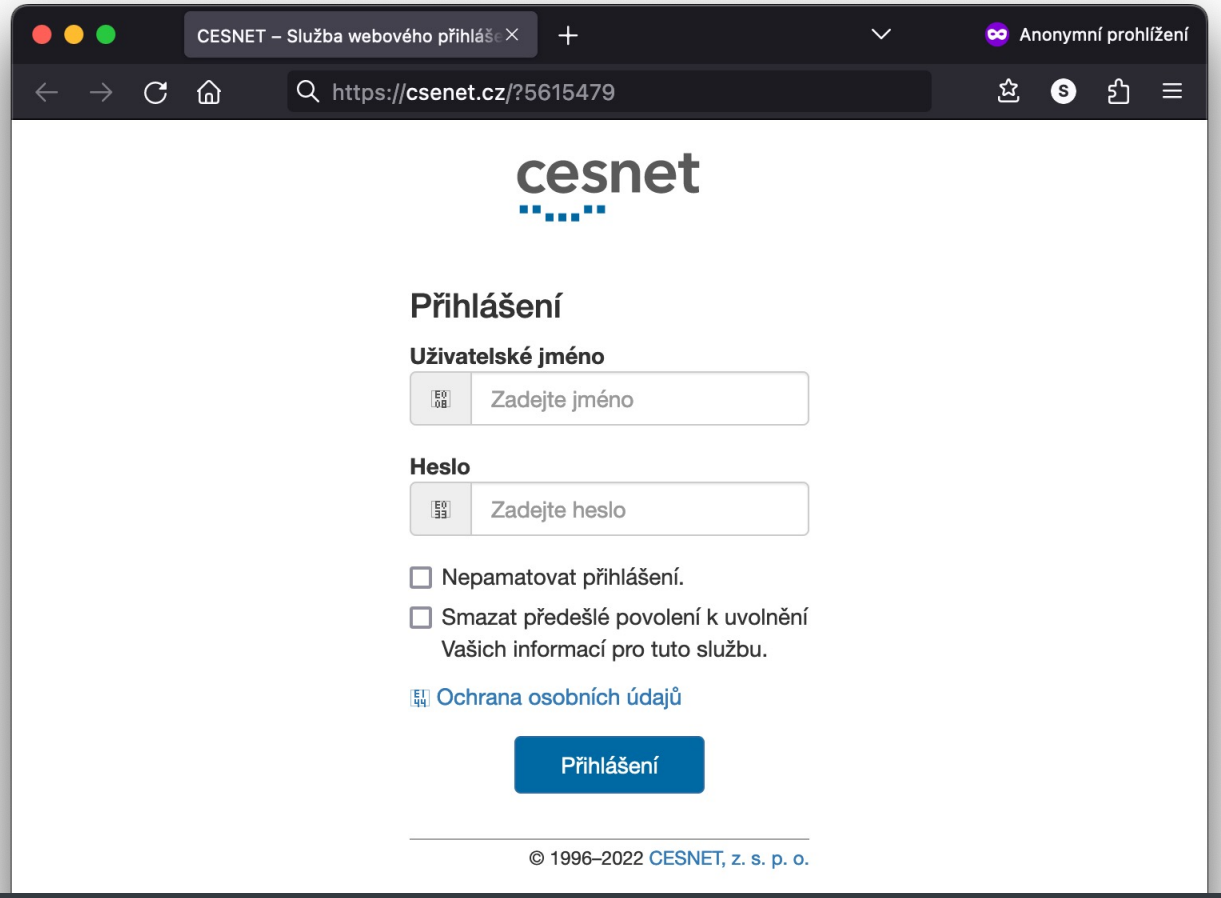
Martin.Sebela@cesnet.cz

Kalendář plánu mezd 2023 je nyní k dispozici:

- https://csenet.cz/?5615479

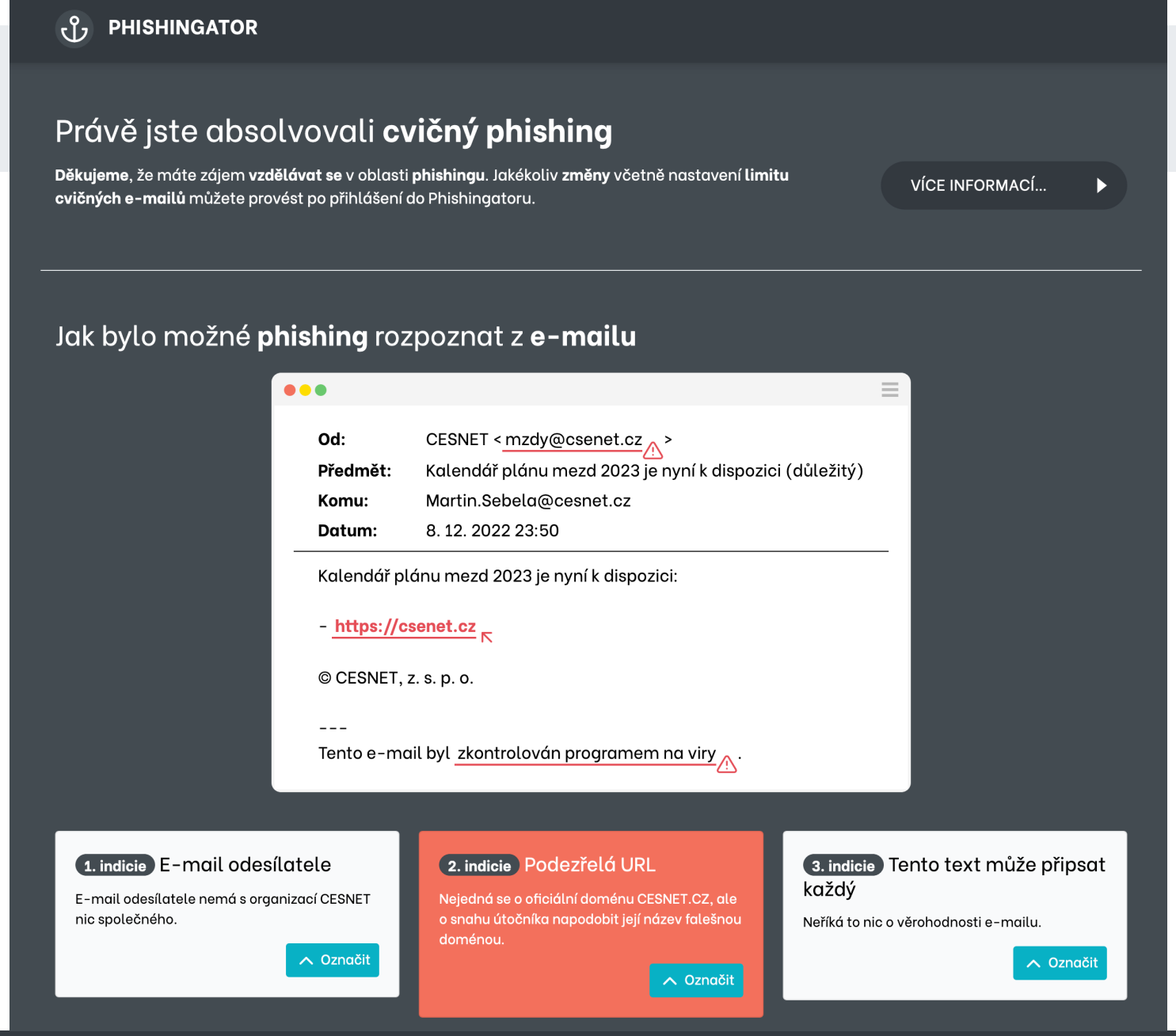
© CESNET, z. s. p. o.

Tento e-mail byl zkontrolován programem na viry.



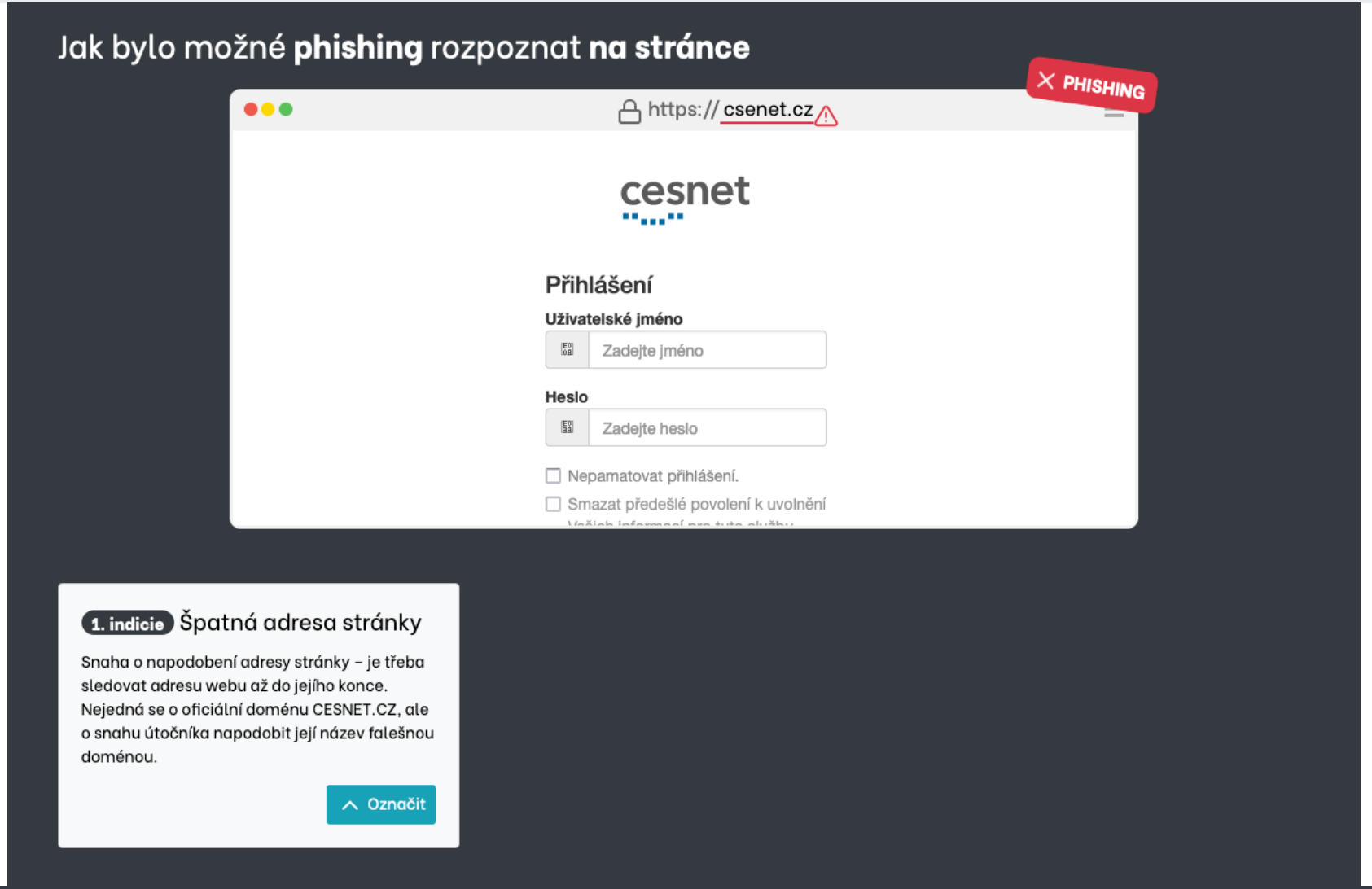
Po zadání údajů…

- Po **vyplnění formuláře** na podvodné stránce:
  - Zobrazí se **podvodný e-mail**
  - **Včetně indicií** pro jeho rozpoznání
- **Okamžitá zpětná vazba** pro uživatele, kteří do formuláře cokoliv vyplnili
  - *„Co jsem udělal špatně?“*



Po zadání údajů…

- Kromě indicií na podvodný e-mail jsou zobrazeny i **indicie** k **rozpoznání podvodné stránky**
- Upozornění na **nesprávnou URL**, případně chybějící **HTTPS**



Po ukončení phishingové kampaně

- **Zpětná vazba** (formou notifikace) pro všechny příjemce

- Především pro uživatele:
  - kteří se na stránku s indiciemi vůbec **nedostali** (cvičný phishing rozpoznali a obratem smazali)
  - kteří se do Phishingatoru registrovali, ale už na to **zapomněli**

Phishingator · Cvičný phishing z 18. 1. 2023

Čtvrtek, Leden 19, 2023 00:00 CET

Komu

Phishingator noreply@phishingator.cesnet.cz

Martin.Sebela@cesnet.cz

Automatická notifikace systému Phishingator

Dne 18. 1. 2023 (21:45) Vám byl odeslán e-mail "Kalendář plánu mezd 2023 je nyní k dispozici (důležitý)". Jednalo se o cvičný phishing (podvodnou zprávu) s typickými znaky, které útočníci používají při snaze získat Vaše heslo, osobní údaje nebo číslo platební karty.

Gratulujeme, v testu jste obstáli :)

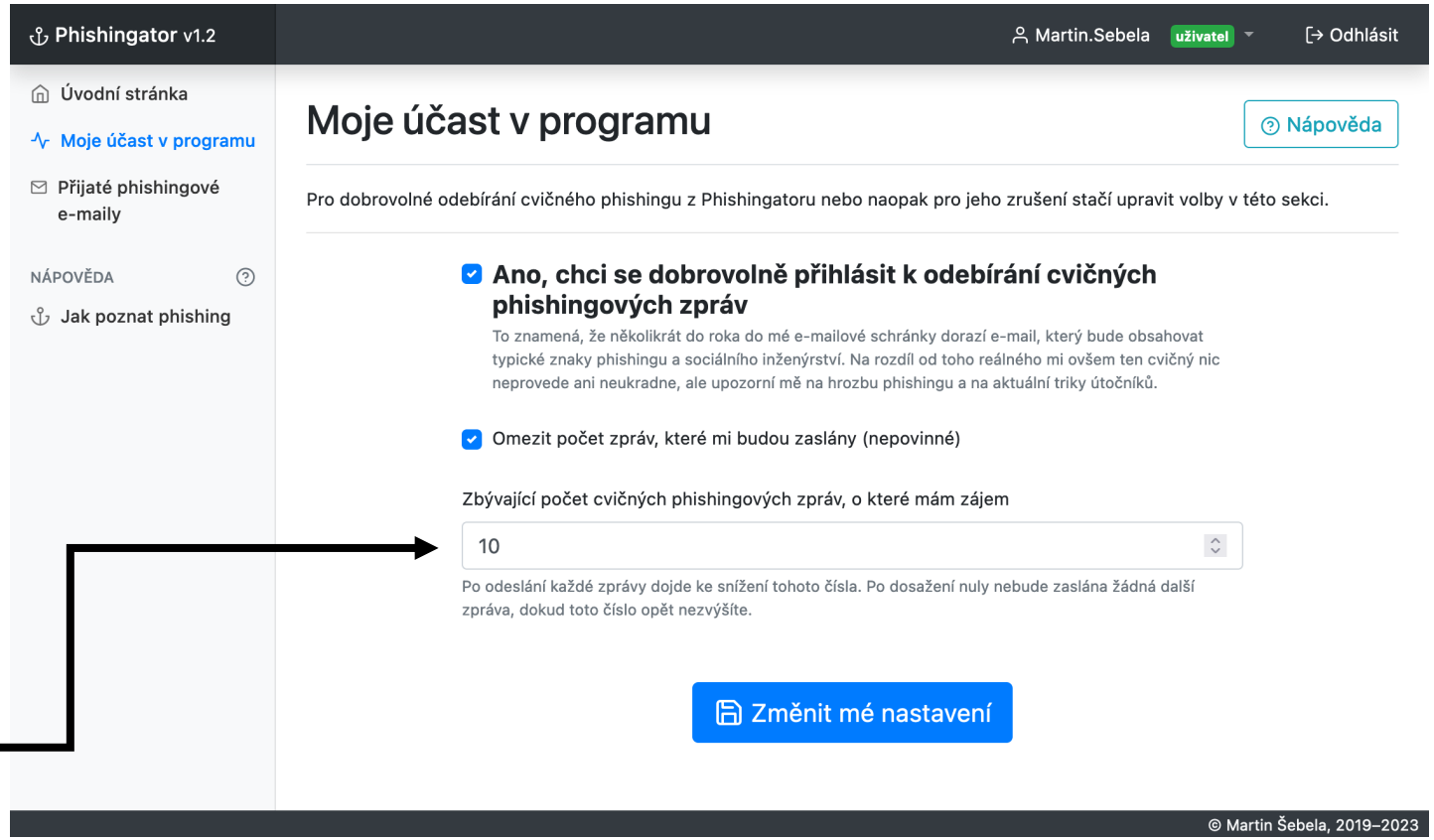
E-mail včetně indicií pro jeho rozpoznání si můžete prohlédnout zde:
https://phishingator.cesnet.cz/phishing/5615479

Děkujeme, že máte zájem vzdělávat se v oblasti phishingu.

Váš zbývající počet cvičných phishingových zpráv: 9
Změnu můžete provést po přihlášení na:
https://phishingator.cesnet.cz

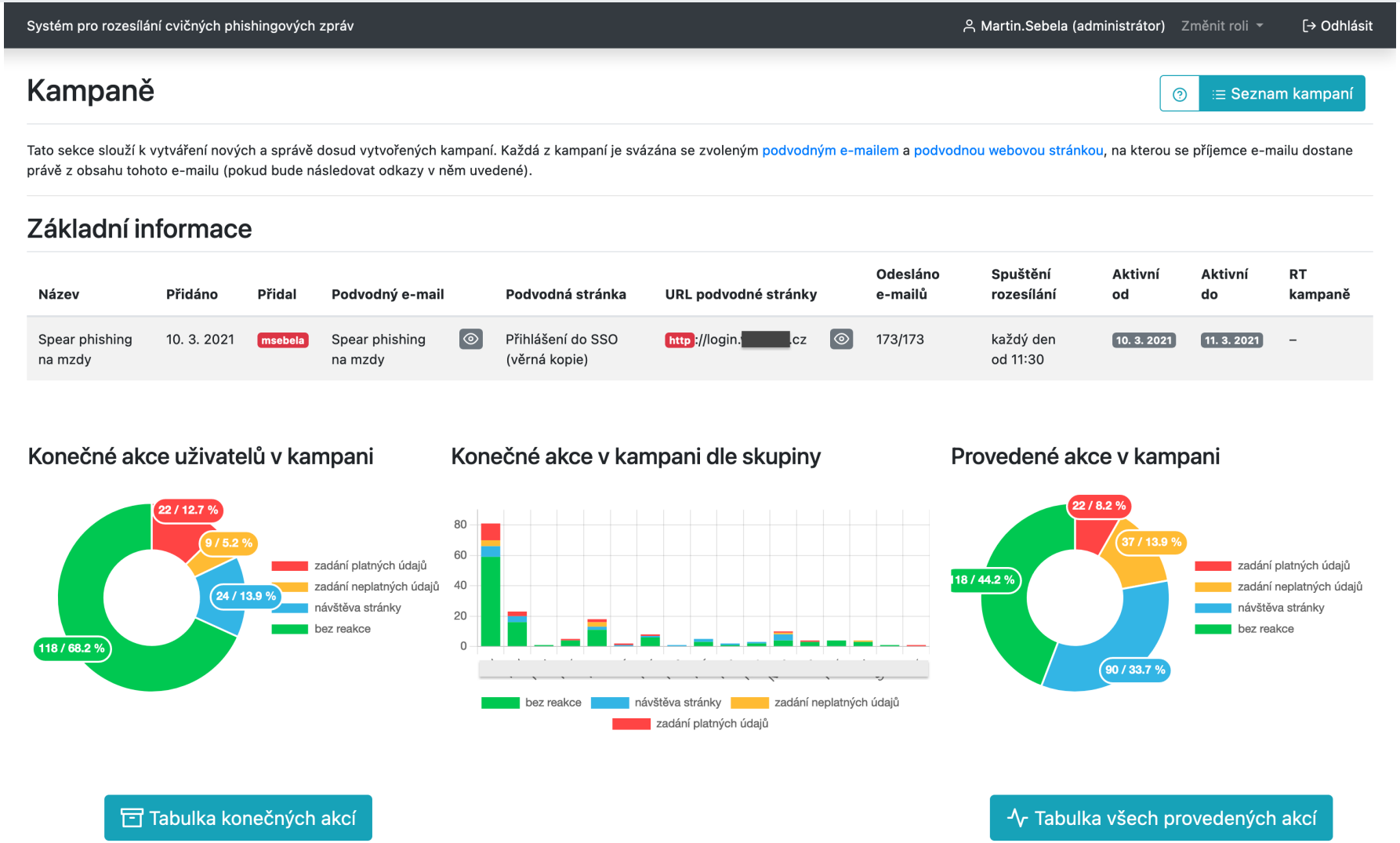
Z pohledu uživatele

- **Přístupné všem** uživatelům organizace
- **Historie** přijatých e-mailů
  - **Reakce uživatele** na e-maily
  - **Indicie** k rozpoznání phishingu
- Možnost se dobrovolně přihlásit k **odebírání cvičného phishingu**
  - Nastavení limitu



Z pohledu administrátora – výsledky kampaně

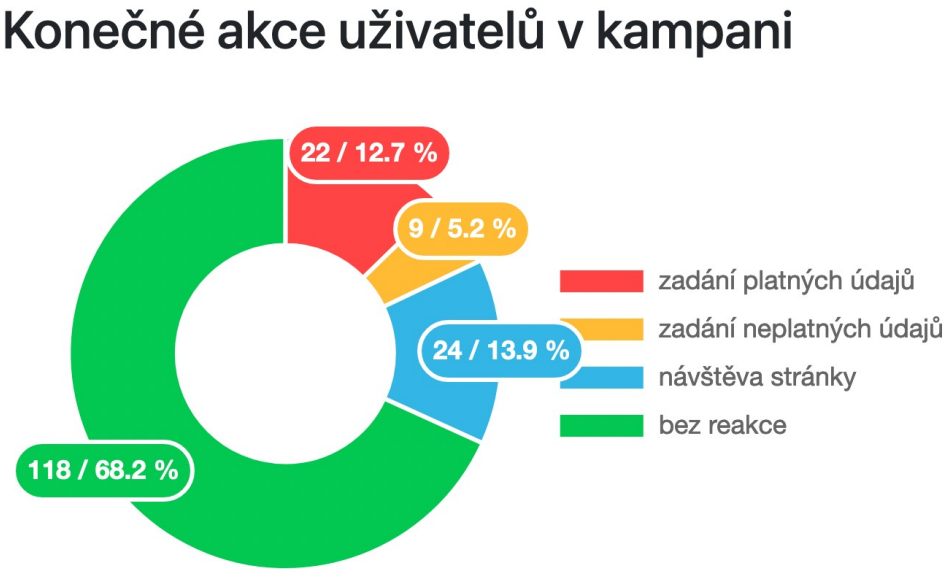
- Zaznamenány **reakce** příjemců:
  - **Bez reakce**
  - **Návštěva podvodné stránky**
  - Vyplnění **neplatných** přihlašovacích údajů
  - Vyplnění **platných** přihlašovacích údajů
- Sledování **průběžných výsledků**
- **Data zadaná** na **podvodné stránce** (anonymizováno)



Příklad: Cvičný phishing na mzdy

- **Rozesláno 173** vybraným **zaměstnancům**
  - Napříč fakultami a dalšími odděleními
  - Získáno 22 platných identit během 2 hodin

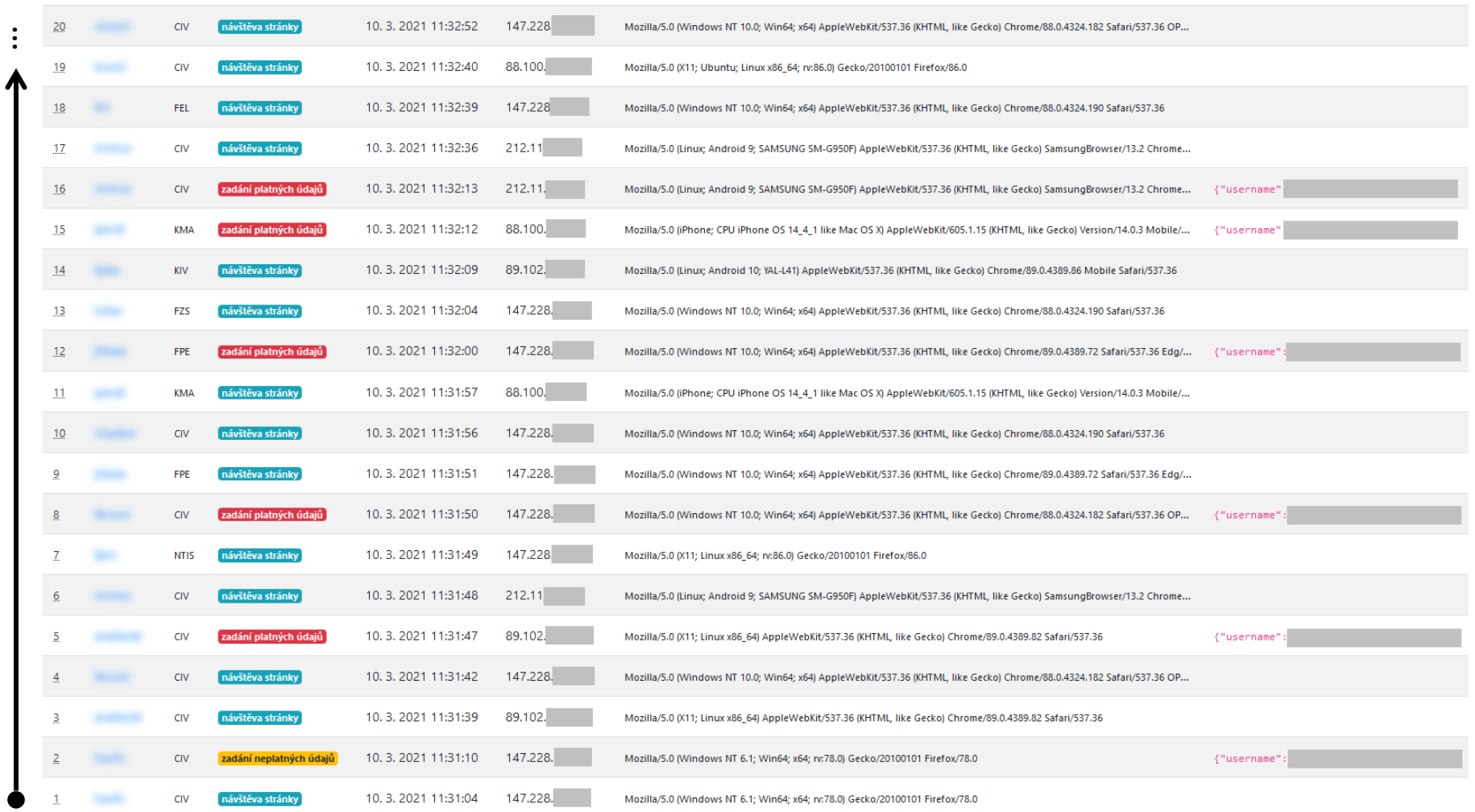
- **Všechny reakce** příjemců:
  - **Bez reakce (118)**
  - **Návštěva podvodné stránky (24)**
  - Vyplnění **neplatných** přihlašovacích údajů **(9)**
  - Vyplnění **platných** přihlašovacích údajů **(22)**



Příklad: Časová osa phishingové kampaně

- **173** odeslaných **e-mailů**

1. **11:30** – odeslání cvičného phishingu
2. **11:31** – první návštěva podvodné stránky
3. **11:31** – první získaná identita
4. **11:35** – získáno 8 platných identit
5. **do 12:00** – získáno 15 platných identit



20	CIV	návštěva stránky	10. 3. 2021 11:32:52	147.228	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36 OP...	
19	CIV	návštěva stránky	10. 3. 2021 11:32:40	88.100.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0	
18	FEL	návštěva stránky	10. 3. 2021 11:32:39	147.228	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36	
17	CIV	návštěva stránky	10. 3. 2021 11:32:36	212.11	Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-G950F) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/13.2 Chrome...	
16	CIV	zadání platných údajů	10. 3. 2021 11:32:13	212.11.	Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-G950F) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/13.2 Chrome...	{"username"
15	KMA	zadání platných údajů	10. 3. 2021 11:32:12	88.100.	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.3 Mobile/...	{"username"
14	KIV	návštěva stránky	10. 3. 2021 11:32:09	89.102.	Mozilla/5.0 (Linux; Android 10; YAL-L41) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.86 Mobile Safari/537.36	
13	FZS	návštěva stránky	10. 3. 2021 11:32:04	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36	
12	FPE	zadání platných údajů	10. 3. 2021 11:32:00	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.72 Safari/537.36 Edg/...	{"username":
11	KMA	návštěva stránky	10. 3. 2021 11:31:57	88.100.	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.3 Mobile/...	
10	CIV	návštěva stránky	10. 3. 2021 11:31:56	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36	
9	FPE	návštěva stránky	10. 3. 2021 11:31:51	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.72 Safari/537.36 Edg/...	
8	CIV	zadání platných údajů	10. 3. 2021 11:31:50	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36 OP...	{"username":
7	NTIS	návštěva stránky	10. 3. 2021 11:31:49	147.228	Mozilla/5.0 (X11; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0	
6	CIV	návštěva stránky	10. 3. 2021 11:31:48	212.11	Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-G950F) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/13.2 Chrome...	
5	CIV	zadání platných údajů	10. 3. 2021 11:31:47	89.102.	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36	{"username":
4	CIV	návštěva stránky	10. 3. 2021 11:31:42	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36 OP...	
3	CIV	návštěva stránky	10. 3. 2021 11:31:39	89.102.	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36	
2	CIV	zadání neplatných údajů	10. 3. 2021 11:31:10	147.228.	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0	{"username":
1	CIV	návštěva stránky	10. 3. 2021 11:31:04	147.228.	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0	

Reakce příjemců

- Vyplnění **platných** přihlašovacích údajů

{"username":"nic ti nedam! a zdravim bezpecaky","…

- Vyplnění **neplatných** přihlašovacích údajů
  - Překlepy
  - **Vzkazy** od příjemců cvičného phishingu

{"username":"Sebela","password":"m…

101	[redacted]	návštěva stránky	10. 3. 2021 13:01:11	188.94.[redacted]	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
100	[redacted]	návštěva stránky	10. 3. 2021 12:59:09	147.228.[redacted]	Mozilla/5.0 (Linux; Android 8.0.0; SM-G935F) AppleWebKit/537.36 (KHTML, like Geck…
99	[redacted]	zadání neplatných údajů	10. 3. 2021 12:58:32	147.228.[redacted]	Mozilla/5.0 (Linux; Android 8.0.0; SM-G935F) AppleWebKit/537.36 (KHTML, like Geck… {"username":"Děkuji za nabídku, al…
98	[redacted]	návštěva stránky	10. 3. 2021 12:57:49	147.228.[redacted]	Mozilla/5.0 (Linux; Android 8.0.0; SM-G935F) AppleWebKit/537.36 (KHTML, like Geck…

{"username":"Děkuji za nabídku, ale můj plat je více než adekvátní..."

- **Hlášení** cvičného phishingu na helpdesk, IT oddělení
- **Debaty** o phishingu v kuloárech, u oběda, …

Shrnutí

- **Phishingator = nová služba** CESNETu v oblasti **bezpečnosti**
  - Nenásilná forma **vzdělávání uživatelů**
  - Cílem zvýšit povědomí o phishingu
  - Živý **vývoj**

- Poskytováno formou **Software as a Service**
  - Servery CESNETu, oddělená data i instance
  - Připravíme 3 podvodné stránky, 3 vzorové podvodné zprávy
  - Zaškolení administrátorů, L2 support

- **Zájem o Phishingator** – *Oddělení péče o uživatele*
  - Cenová nabídka, obchodní podmínky
  - *phishingator@cesnet.cz*

cesnet

Dotazy

Martin Šebela
martin.sebela@cesnet.cz

CESNET FLAB