Phishingator

aneb cvičný phishing „nejen“ na ZČU

Martin Šebela

WIRT CIV ZČU, FLAB CESNET

EurOpen 2022 – 31. 5. 2022

Phishingator

= Systém pro rozesílání cvičných phishingových zpráv

- Prvotní myšlenka „o phishingu“ po semestrální práci, navázala bakalářská práce
- Příklad **cvičného phishingu** pro **studenty ZČU**:

Od Stravovací viceprezident SKM <vice@zcu.cz>

Předmět **Obědové stipendium pro studenti**

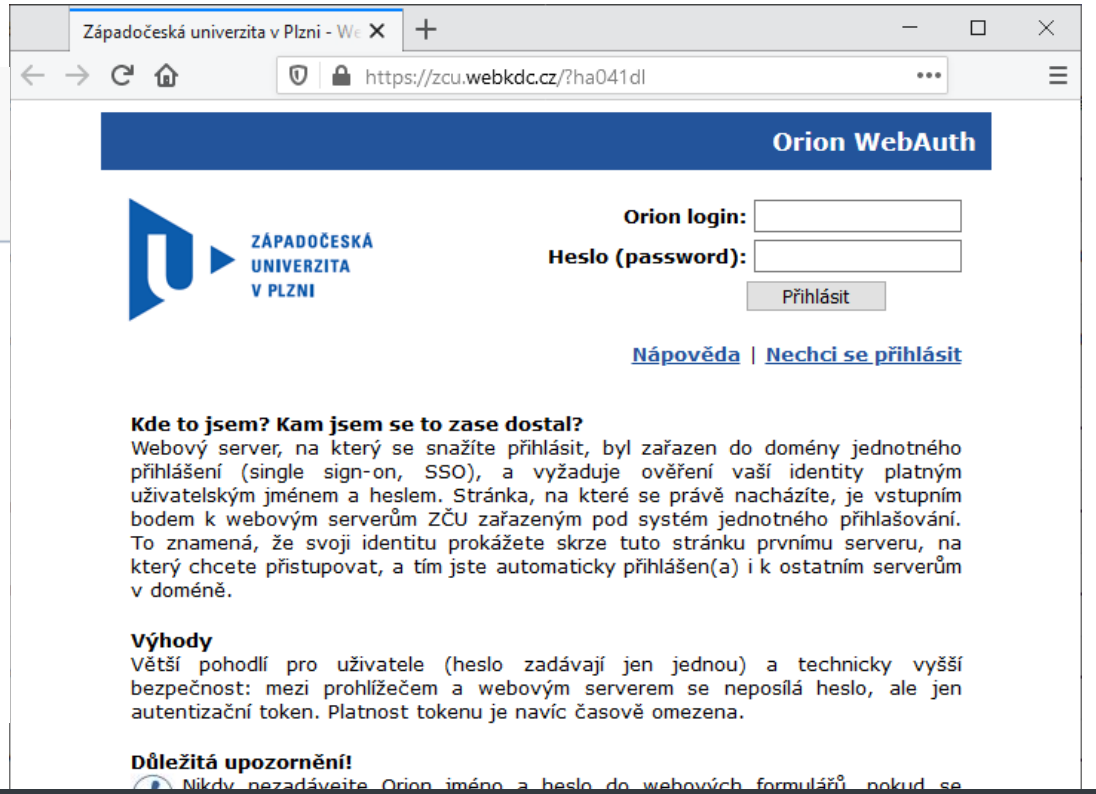
Komu já <msebela@students.zcu.cz>

Vážený strávníku msebela,
díky grantu EU 167/7669077-6429CZ je možné se přihlásit k bezplatným objedům.

Přihlásit se zde: https://zcu.webkdc.cz/?ha041dl

Časový limit pro přihlášání je 16. 4. 2019

Bc. et Bc. Jan Hladový
Stravovací viceprezident
vice@skam.zcu.cz
+555 123 646 888
SKM, ZČU ve v Plzni



Cvičný phishing na ZČU

- Phishingator = **automatizovaný nástroj** pro rozesílání cvičných phishingů

- Praktický **doplněk** ke **školení** „kdykoliv a kdekoliv“
- **Cílené školení**
- Založeno na **dobrovolné registraci** k odběru **cvičného phishingu**
- **Zpětná vazba pro uživatele** o absolvování cvičného phishingu

- Vytváření vlastních **phishingových kampaní** = podvodný e-mail + podvodná stránka

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 2021 je nyní k dispozici (důležitý)

Středa, Březen 10, 2021 11:30 CET

Komu

Západočeská univerzita caitrin.engle@webzcu.cz

msebela@civ.zcu.cz

Kalendář plánu mezd 2021 je nyní k dispozici:

- http://login.webzcu.cz/?ha0291dl

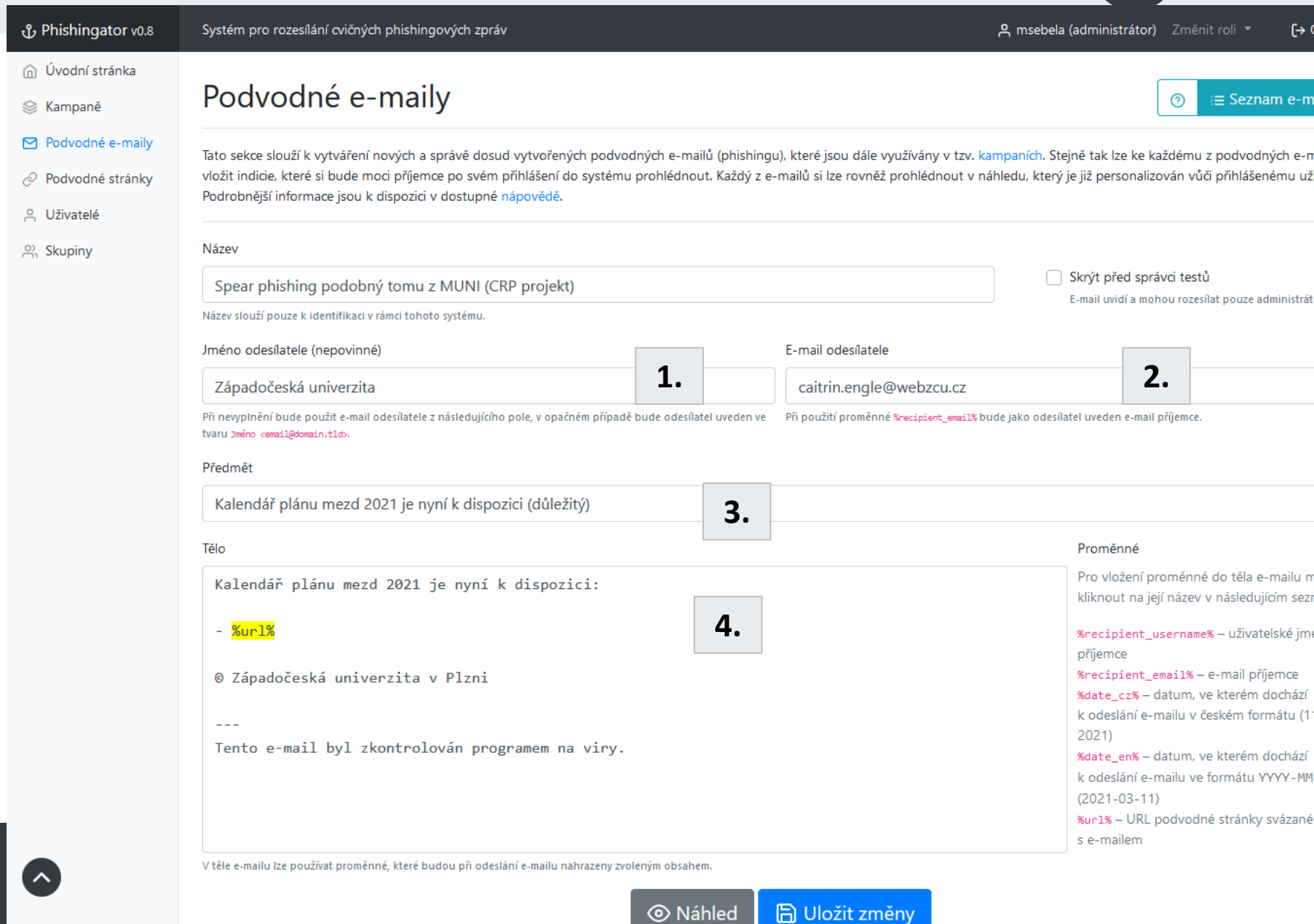
© Západočeská univerzita v Plzni

Tento e-mail byl zkontrolován programem na viry.

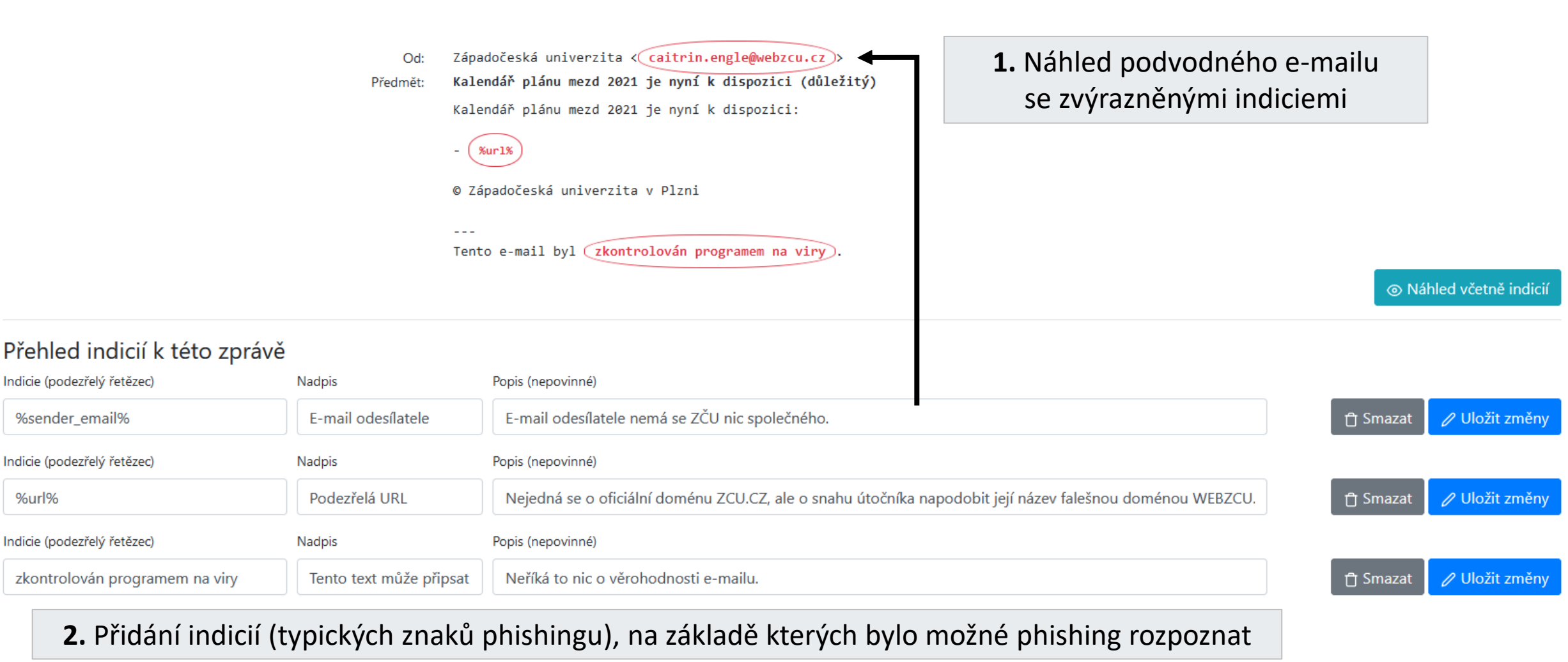
Z pohledu administrátora

- Vytvoření **cvičného phishingu**

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



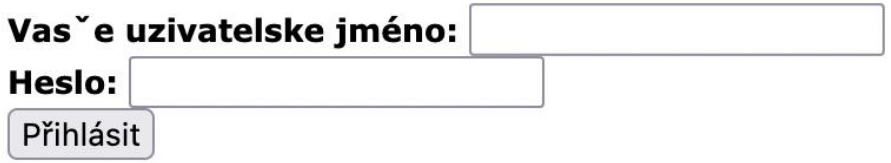
Indicie k rozpoznání phishingu



Vytvoření podvodné stránky

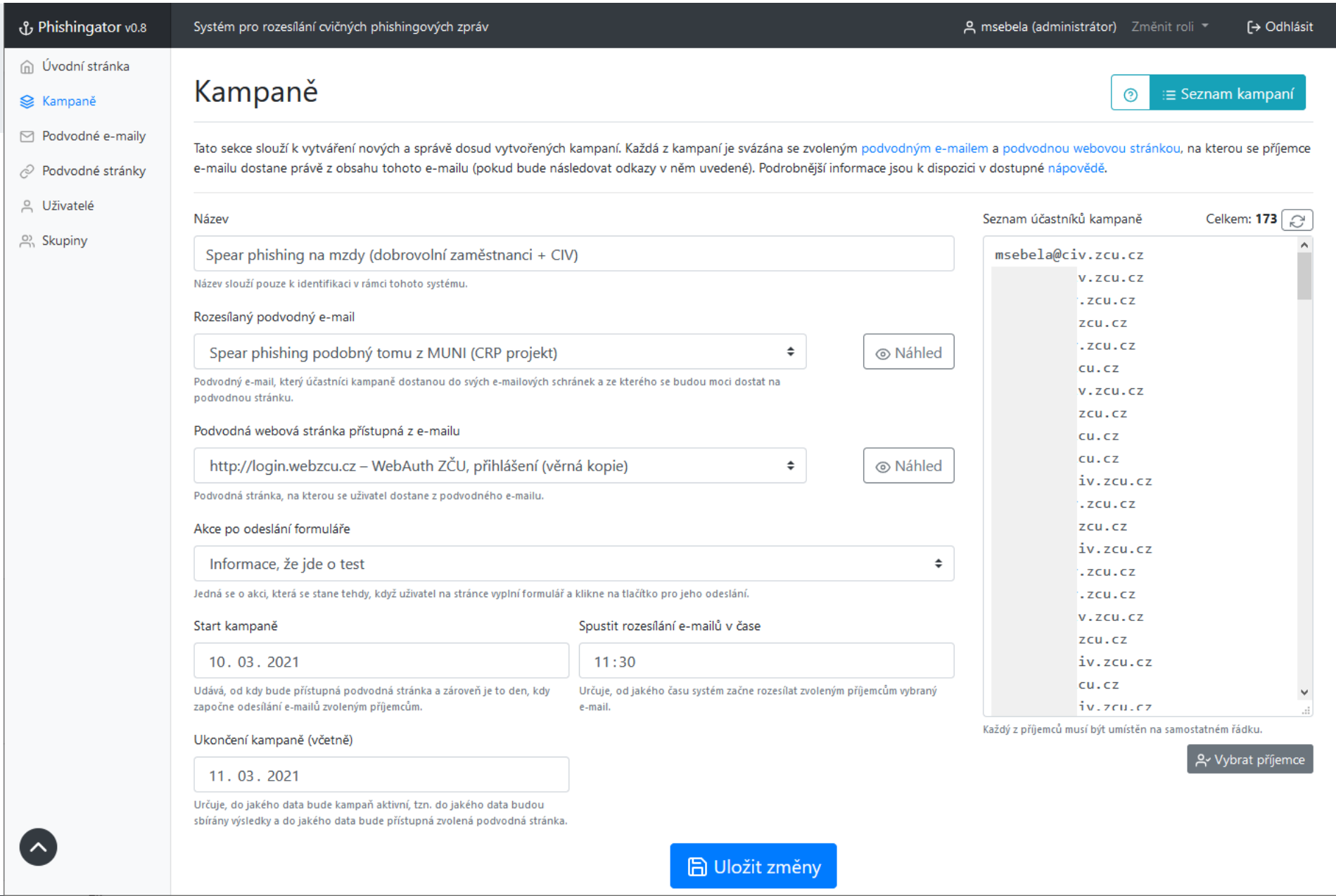
- Nákup vhodné, cvičné, phishingové **domény**
  - zcu.cz vs. zzu.cz, webzcu.cz, …
- Nasměrování DNS domény na aplikaci Phishingator
- Vytvoření a vložení **HTML šablony** s podvodnou stránkou do aplikace Phishingator
- Případně vydání **certifikátu**
- Phishingator na stránku **umístí logo** na základě domovské organizace uživatele

MUNI



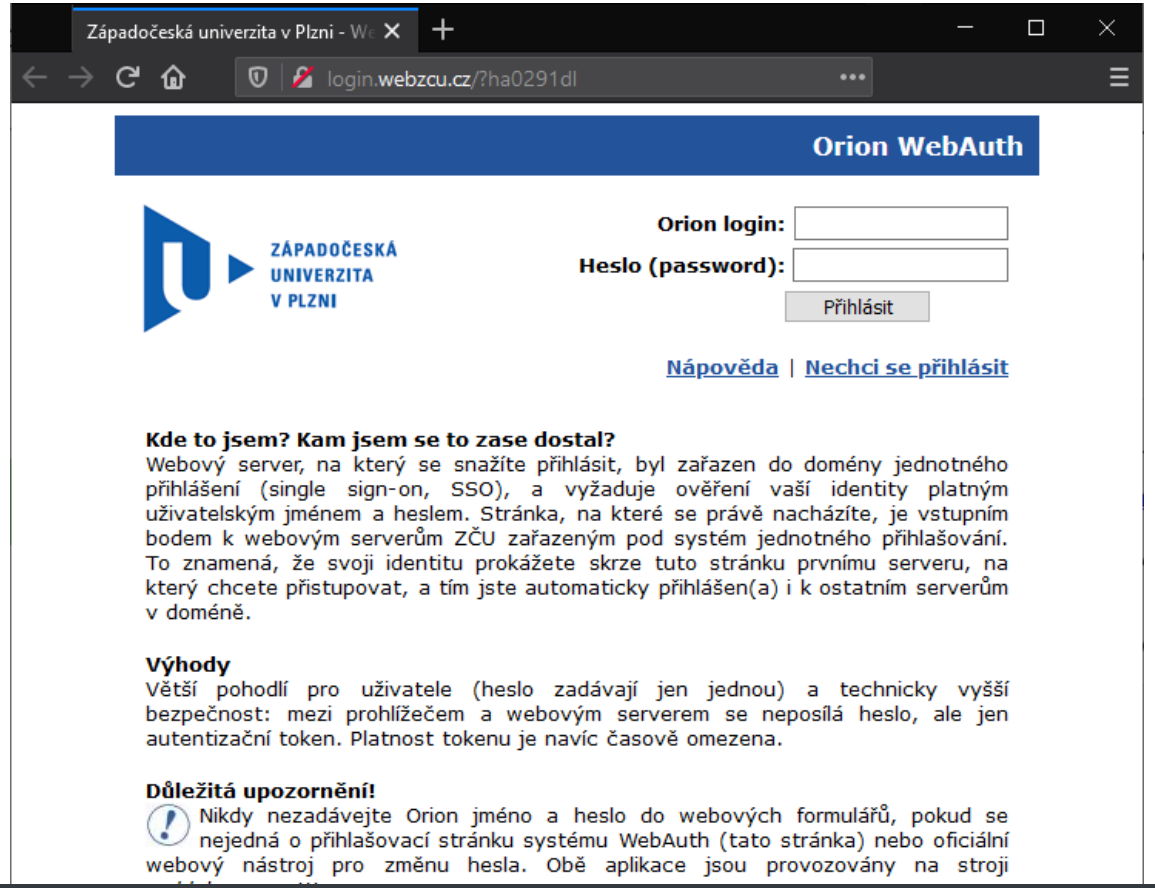
Kampaň

- **Phishingová kampaň** se skládá z:
  - **phishingový e-mail**
  - **podvodná stránka**
  - **co se stane** na podvodné stránce po odeslání formuláře
  - **od kdy, do kdy**
  - **čas** rozesílání
  - **příjemci**



Z pohledu uživatele

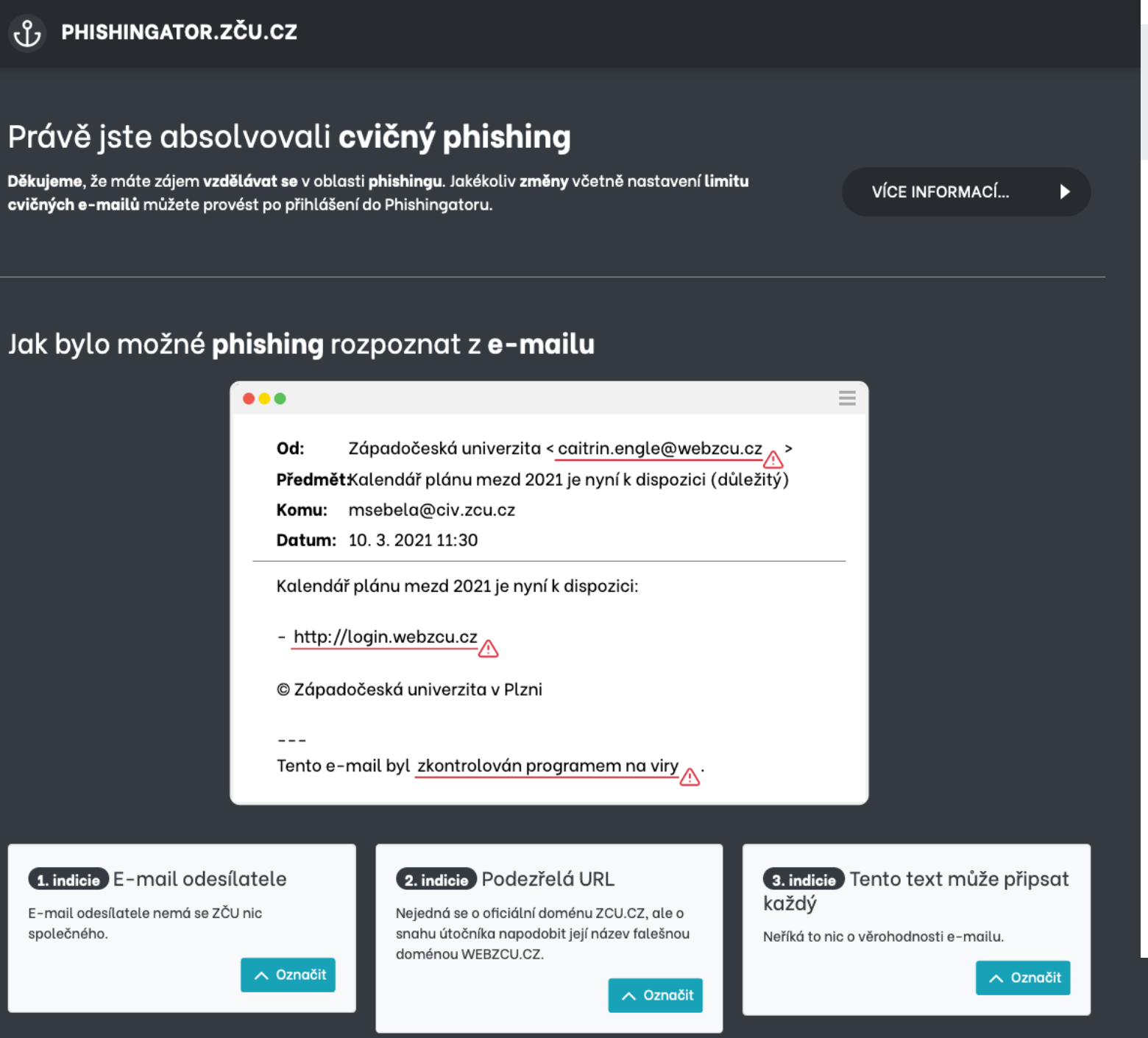
- **Podvodný e-mail** odeslaný z Phishingatoru s odkazem na **podvodnou stránku**



Po zadání údajů…

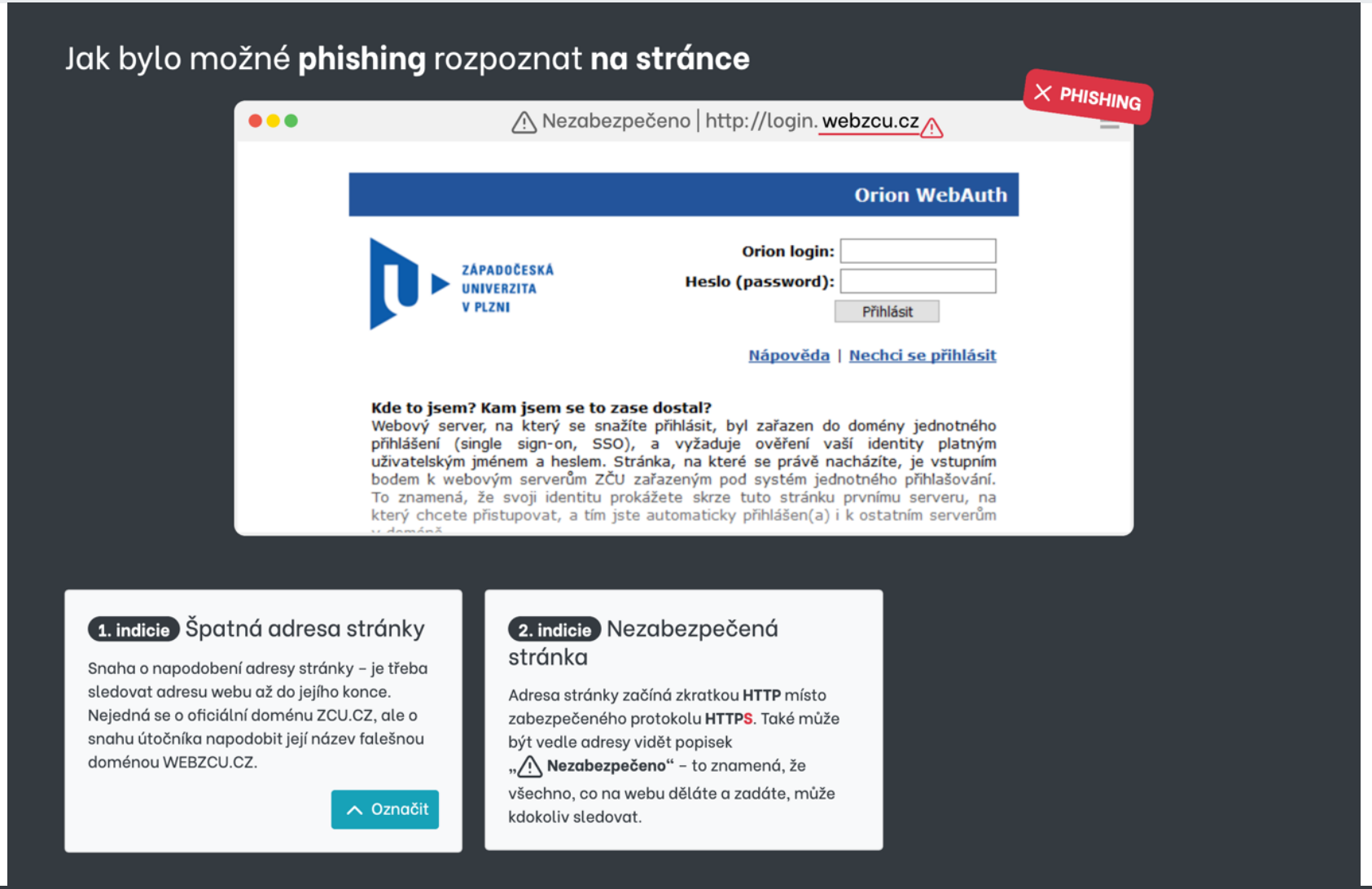
- Po vyplnění údajů na podvodné stránce:
  - Zobrazí se **podvodný e-mail**
  - **Včetně indicií** pro jeho rozpoznání

- **Okamžitá zpětná vazba** pro uživatele, kteří do formuláře cokoliv vyplnili



Po zadání údajů…

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



Po ukončení phishingové kampaně

- **Notifikace** (zpětná vazba) **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 10. 3. 2021

Čtvrtek, Březen 11, 2021 09:00 CET

Komu

Phishingator noreply@phishingator.zcu.cz

msebela@civ.zcu.cz

Automatická notifikace systému Phishingator

Dne 10. 3. 2021 (15:30) Vám byl odeslán e-mail "Kalendář plánu mezd 2021 je nyní k dispozici (důležitý)".
Jednalo se o cvičný phishing (podvodnou zprávu) s typickými znaky, které
útočníci používají při snaze získat Vaše heslo, číslo platební karty apod.

Gratulujeme, v testu jste obstáli :)

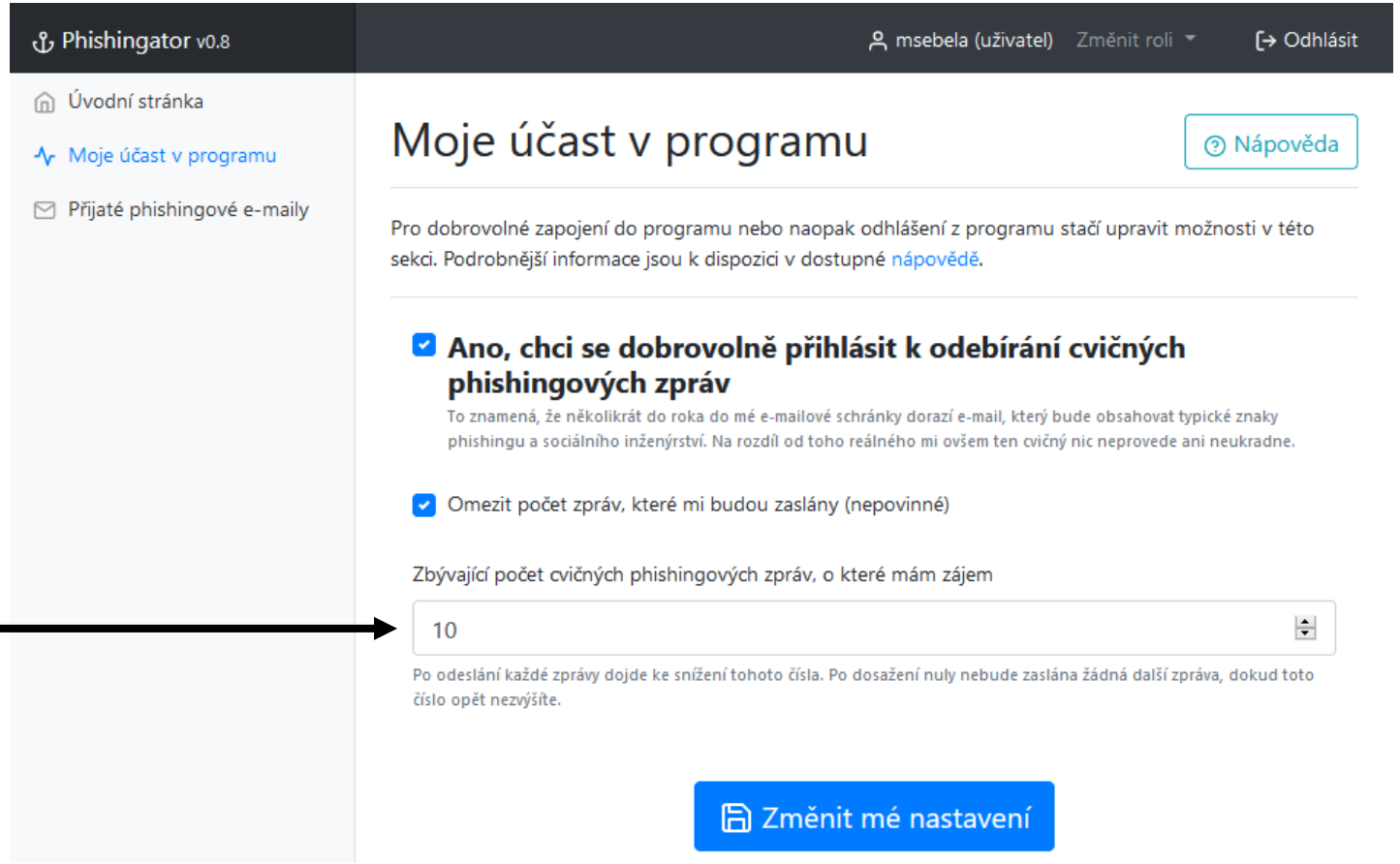
E-mail včetně indicií pro jeho rozpoznání si můžete prohlédnout zde:
https://phishingator.zcu.cz/phishing/ha0301dl

Děkujeme, že máte zájem vzdělávat se v oblasti phishingu.

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

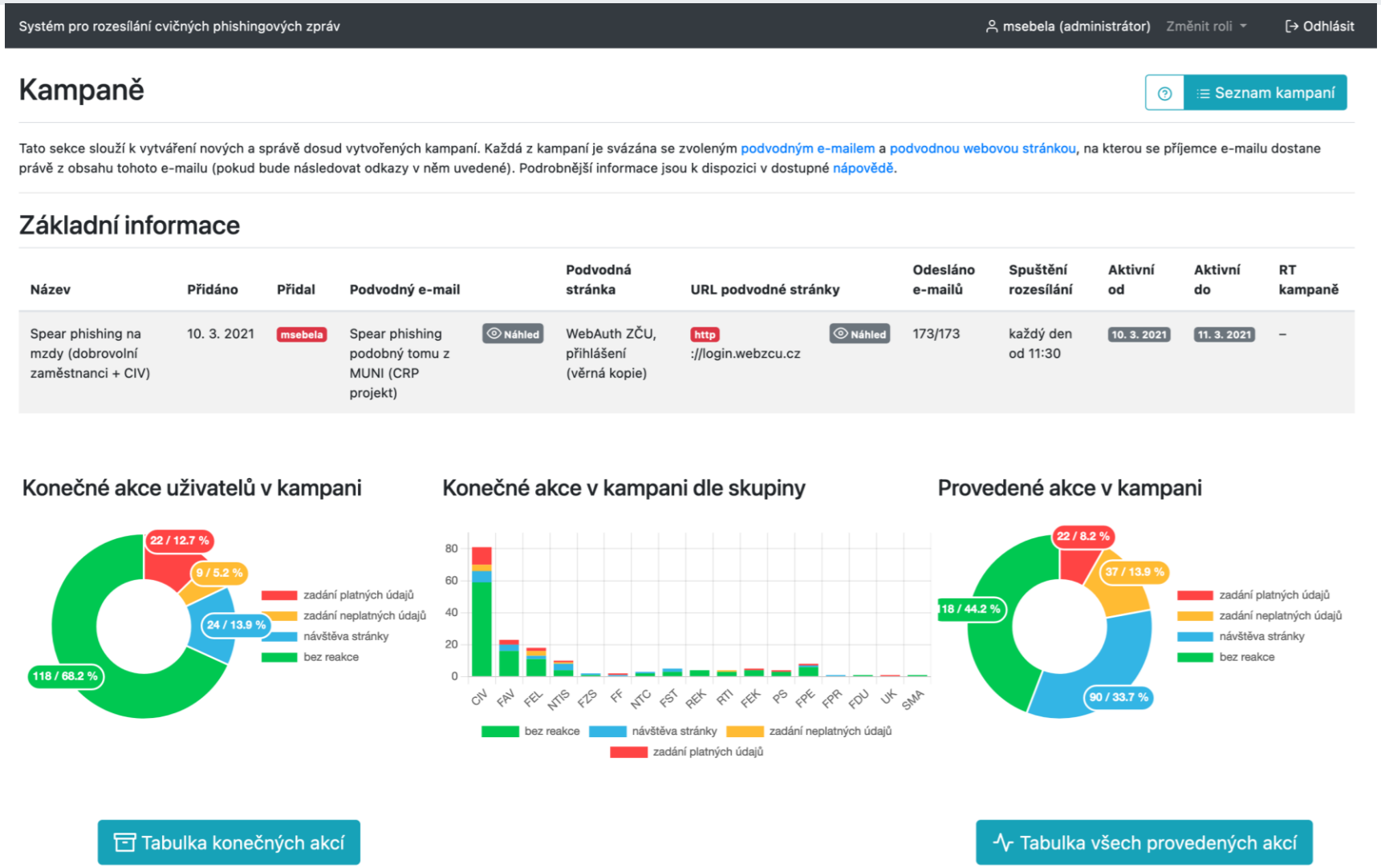
Z pohledu uživatele

- **Přístupné všem** ze ZČU
- Možnost se **dobrovolně přihlásit k odebírání**
  - Limit zasílaných cvičných e-mailů
- **Historie** přijatých e-mailů
- **Reakce uživatele** na e-mail
- **Indicie k rozpoznání phishingu**



Z pohledu administrátora – výsledky kampaně

- **Všechny reakce** příjemců:
  - **bez reakce**
  - **návštěva podvodné stránky**
  - vyplnění **neplatných** přihlašovacích údajů
  - vyplnění **platných** přihlašovacích údajů
- **Možnost sledovat průběžné výsledky**
- **Data zadaná** na **podvodné stránce** (anonymizováno)



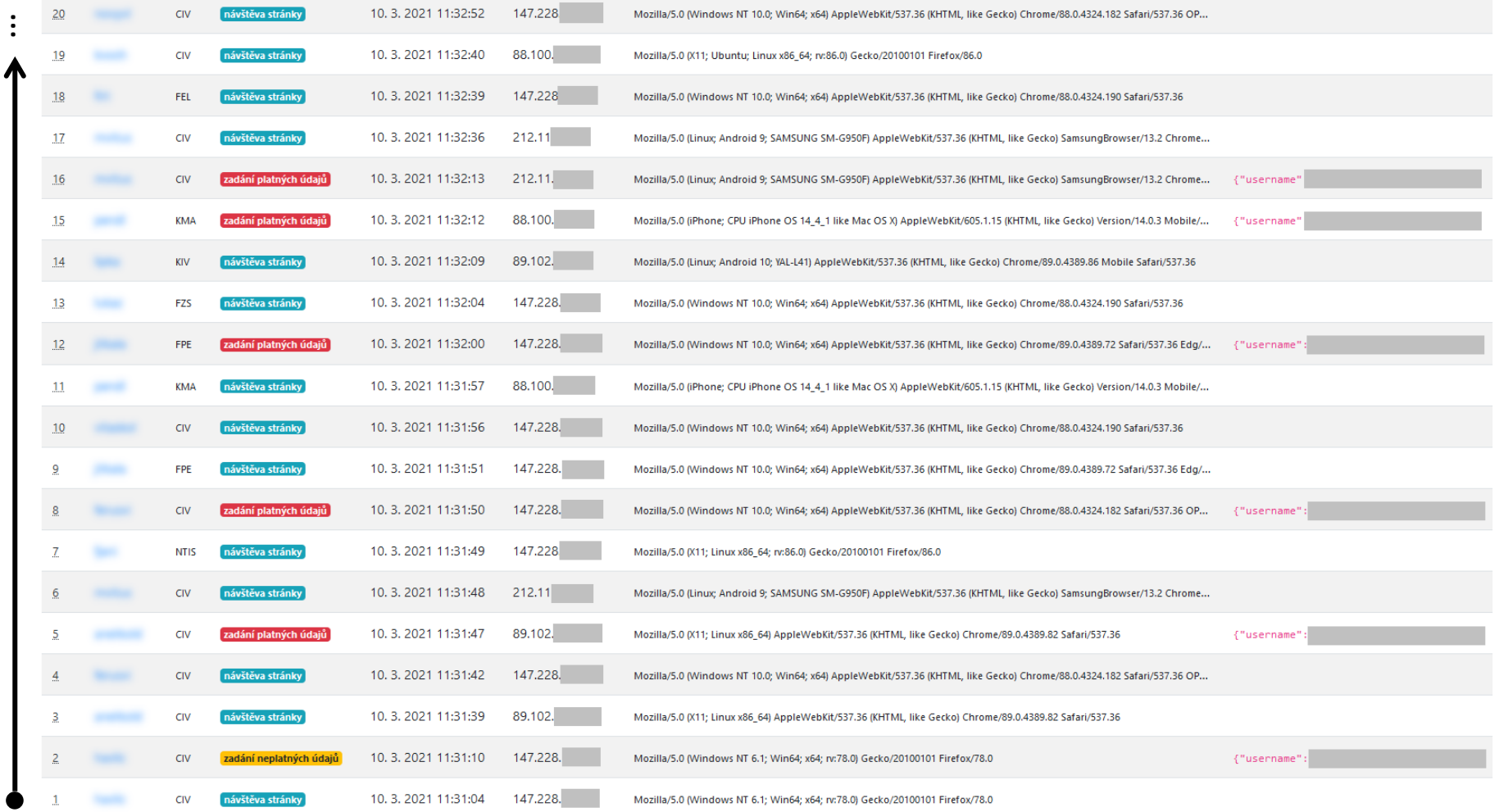
Cvičný phishing na mzdy

- **Rozesláno 173** vybraným **zaměstnancům**
  - napříč fakultami a dalšími součástmi ZČU
  - 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)**
- Stejná kampaň pro dalších **70** zaměstnanců

Časová osa cvičné 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	[redacted]	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	[redacted]	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	[redacted]	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	[redacted]	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	[redacted]	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" [redacted]
15	[redacted]	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" [redacted]
14	[redacted]	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	[redacted]	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	[redacted]	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": [redacted]
11	[redacted]	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	[redacted]	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	[redacted]	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	[redacted]	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": [redacted]
7	[redacted]	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	[redacted]	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	[redacted]	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": [redacted]
4	[redacted]	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	[redacted]	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	[redacted]	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": [redacted]
1	[redacted]	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

Cvičný phishing na doložení bezinfekčnosti

- **Podvodný e-mail** odeslaný z Phishingatoru s odkazem na **podvodnou stránku**
- Odesílatel `covid-19@webkdc.cz`
- Odkaz na stránku `https://kdc.webzcu.cz`

Doložení bezinfekčnosti - očkování/test/prodělaná nemoc

Pátek, Červen 22, 2021 16:30 CET

covid-19@webkdc.cz covid-19@webkdc.cz

Komu

msebela@civ.zcu.cz

Dobrý den,

žádáme Vás o doložení bezinfekčnosti Covid-19. Bezinfekčnost doložit nahráním dokumentu zde: https://kdc.webzcu.cz/?59937828 do 25.Jun.2021.

Bezinfekčnost je možné doložit:
* platný negativní test (AG/PCR)
* platný očkovací certifikát
* potvrzení o prodělané nemoci

S pozdravem
Matěj Poláček

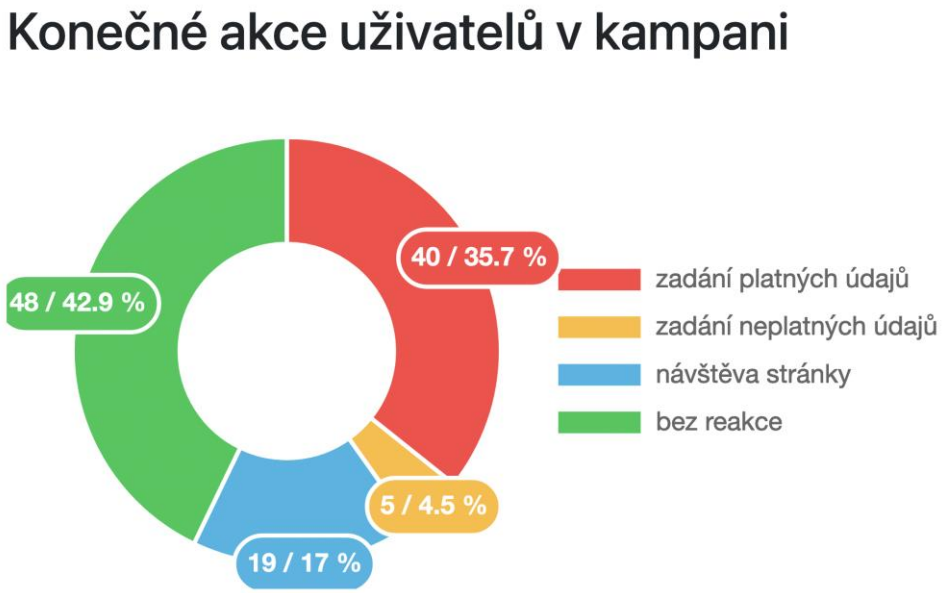
Anticovid tým ZČU

Cvičný phishing na doložení bezinfekčnosti

- **Rozesláno 112** vybraným **zaměstnancům**
  - získáno 40 platných identit
  - platné heslo zadáno 176×

- **Všechny reakce** příjemců:
  - **bez reakce (48)**
  - **návštěva podvodné stránky (19)**
  - vyplnění **neplatných** přihlašovacích údajů **(5)**
  - vyplnění **platných** přihlašovacích údajů **(40)**

- Podobný výsledek u **cvičného phishingu** na **elektronický výplatní lístek**



Cvičný phishing na doložení bezinfekčnosti

- Nezobrazována stránka s indiciemi
- Odesílateli cvičného phishingu dorazilo **12 odpovědí**

Dobrý den, certifikát Vám zasílám v příloze, protože na Vámi uvedený odkaz se nelze přihlásit přes můj orion přístup. Máte tam zřejmě nějaké jiné přihlašování, které jste mi zatím nezaslali.

POZN: Ani můj kolega se tam nedokázal přihlásit, takže to asi bude problém pro všechny. …

Dobrý den
Odkaz nejde otevřít, zůstává stále na přihlašovací obrazovce Certifikát Vám posílám proto zde v příloze.
S pozdravem …

Dobrý večer, Od pátka se tam nemůžu přihlásit. Posílám to v emailu. …

POTVRZENÍ O ABSOLVOVÁNÍ TESTU NA PRŮKAZ PŘÍTOMNOSTI AG SARS-COV-2

POTVRZUJI, ŽE

Cvičný phishing na doložení bezinfekčnosti

- Nezobrazována stránka s indiciemi
- Odesílateli cvičného phishingu dorazilo **12 odpovědí**

Dobrý den,

nerad bych poskytoval osobní údaje, když mám podezření, že se může jednat o "podvodný email". Vaší osobu zču telefonní seznam nezná, proto bych Vás chtěl požádat o prokázání, že se jedná o oficiální požadavek mého zaměstnavatele. …

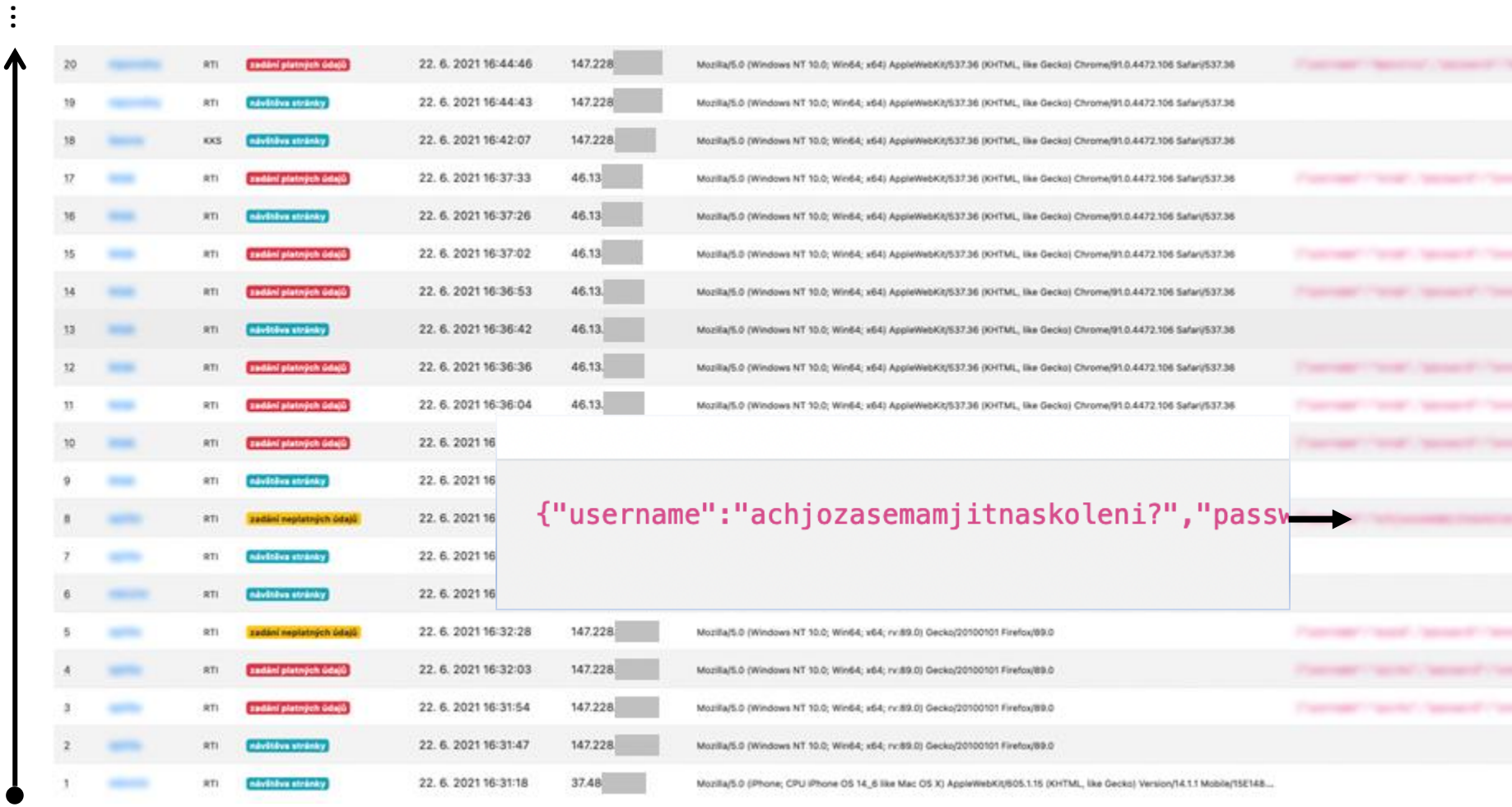
POTVRZENÍ O ABSOLVOVÁNÍ TESTU NA PRŮKAZ PŘÍTOMNOSTI AG SARS-COV-2

POTVRZUJI, ŽE

Časová osa cvičné phishingové kampaně

- **112 odeslaných e-mailů**

1. **16:30** – odeslání cvičného phishingu
2. **16:31** – první návštěva podvodné stránky
3. **16:31** – první získaná identita
4. **22:23** – získáno 12 platných identit



„Nejen“ na ZČU?

- Od **konce září** 2022 **bude možné nasadit** Phishingator i v jiných institucích
- Nabízeno v rámci **služeb bezpečnosti CESNET** – `sluzby@cesnet.cz`

- Režimy:

  1) instituce si vše řeší sama (nasazení, provoz, phishingové kampaně)

  2) CESNET řeší nasazení a provoz, kampaně vytváří instituce

  3) CESNET řeší vše – nasazení, provoz i vytváření kampaní

Závěr

- **Cílem** je uživatele **vzdělat** a ukázat na **nebezpečí phishingu**
- Nenásilné **poučení** pro uživatele

- **ZČU** má vlastní instanci pro **všechny své uživatele**
  - dobrovolné zapojení uživatelů ZČU
  - limit přijatých cvičných phishingů

- **CESNET** umožní a pomůže s nasazením a provozem Phishingatoru i jinde
  - **konec září 2022** – zájem pište na `sluzby@cesnet.cz`

Dotazy

Martin Šebela
msebela@civ.zcu.cz

WIRT CIV ZČU, FLAB CESNET