Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnostné povedomie a tréningy zamestnancov

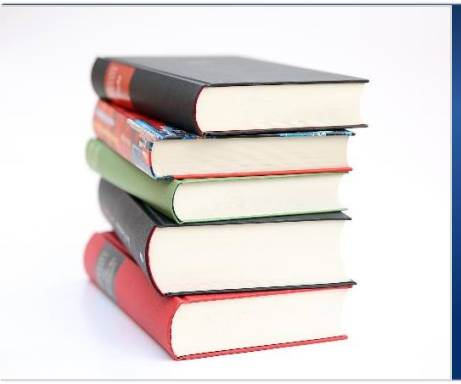
Zvyšovanie povedomia o KB a testovanie bezpečnosti (Blok VIII)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Jana.Uramova@fri.uniza.sk



Obsah

- Usmernenia na vytvorenie efektívneho programu bezpečnostného povedomia a školení v oblasti informačných technológií
- Druhy rámcov pre vzdelávanie so zameraním na NIST SP 800-50 r1
- Čo vieme využiť z rámca NIST SP 800-50 r1
- Vzdelávacie nástroje:
  - tvorba školení
  - bezpečnostné tréningy
- Organizácia bezpečnostných kampaní:
  - phishing simulácie
  - edukácia zamestnancov

Strengthening the Weakest Link

- Kybernetická bezpečnosť je taká silná, ako jej najslabší článok.
- Najslabším článkom kybernetickej bezpečnosti môže byť personál organizácie a sociálne inžinierstvo predstavuje jej veľkú bezpečnostnú hrozbu.
- Jedným z najúčinnejších bezpečnostných opatrení, ktoré môže organizácia prijať, je:

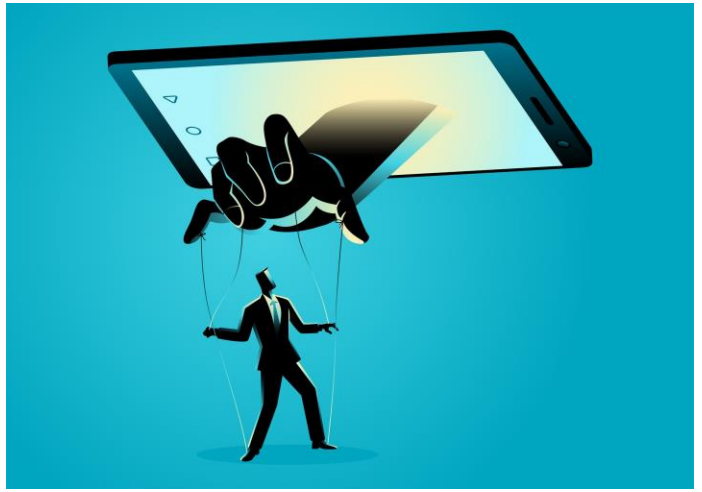
  školenie svojich zamestnancov
  a
  vytvorenie ‘kultúry povedomia
  o bezpečnosti’

Typy útokov mierené na používateľa

Typy útokov mierené na používateľa

Sociálne inžinierstvo

- Technika, ktorá využíva manipuláciu ľudí na vykonanie určitých akcií alebo prezradenie dôverných informácií
- **Útočník sa nesnaží prelomiť systémy, ale presvedčiť človeka, aby mu dvere otvoril sám**
- Používa sa v rôznych typoch útokov
- **Najčastejší typ útoku – Phishing**



Znaky

- Manipulácia a psychologický nátlak
- Zneužívanie dôvery a autority
- Použitie technológií (telefón, e-mail, sociálne siete)
- Vyvolávanie silných emócií (strach, zvedavosť, naliehavosť)
- Vydávanie sa za dôveryhodné osoby alebo inštitúcie
- Využívanie sociálnej dynamiky a zraniteľností ľudí

Príklad

- Útočník sa predstaví ako IT technik a pošle e-mail:
  „Vaše konto bude zablokované, ak si okamžite nezmeníte heslo. Kliknite sem.“
  Zamestnanec klikne na odkaz a zadá svoje prihlasovacie údaje na falošnej stránke

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Typy útokov mierené na používateľa

Fyzické útoky

- Tailgating (nasledovanie používateľa)
- Shoulder surfing (vizuálne odpočúvanie ,,ponad plece")
- Skimming a keylogger (zaznamenávanie pomocou fyzického zariadenia)
- Baiting (útok s návnadou)
- Dumpster diving (prehľadávanie odpadkov)
- Krádež zariadenia
- Coercion / extortion (priame donútenie, nátlak / vydieranie)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Sledovanie používateľa

Tailgating (nasledovanie používateľa)

- útočník vchádza za zamestnancom cez zabezpečený vstup bez vlastného oprávnenia (niekto bez prístupu „nasleduje“; niekoľko osôb pri vstupe do organizácie bez autorizácie)

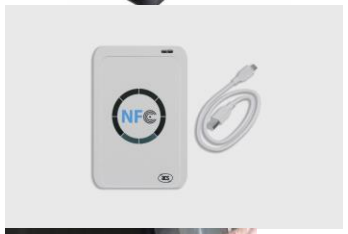
Shoulder surfing (vizuálne odpočúvanie „ponad plece")

- priame sledovanie zadávania PIN, hesla alebo citlivých údajov (niekto stojí príliš blízko pri zadávaní údajov, smartfónov smerom k obrazovke...)

Zaznamenávanie pomocou fyzického zariadenia

Skimming a keylogger

- **„malé zariadenie implantované do zariadenia“** znamená **skrytý hardvérový komponent**, ktorý útočník fyzicky umiestni do cudzieho zariadenia, aby tajne zaznamenával citlivé údaje.
- Môže to byť miniatúrne:
  - **skimmer** – zachytáva údaje z magnetického pásika platobnej karty,
  - **keylogger modul** – napojený medzi klávesnicu a počítač, zachytáva stlačené klávesy,
  - **BLE/NFC zachytávač** – odčítava ID z bezkontaktnej karty,
  - **PIN pad overlay** – tenká vrstva nasadená na klávesnici bankomatu alebo POS terminálu.



- Kde sa to nachádza?
  - Útočník ho môže:
  - vložiť **dovnútra notebooku alebo PC**,
  - pripojiť **medzi klávesnicu a počítač** (vyzerá ako adaptér),
  - prilepiť **na klávesnicu bankomatu**,
  - vložiť **do POS terminálu**,
  - ukryť **pod kryt dverovej čítačky**.
- Čo robí?
  - tajne **zachytáva heslá, PIN kódy alebo čísla kariet**,
  - ukladá ich do pamäte alebo posiela bezdrôtovo útočníkovi,
  - je bežne tak malé, že si ho používateľ nevšimne.

Návnady (Baiting)

- Technika sociálneho inžinierstva, pri ktorej útočník láka obeť na nejakú **„návnadu“** – niečo, čo vyzerá atraktívne, užitočné alebo zadarmo – aby ju prinútil vykonať akciu, ktorá ohrozí jej bezpečnosť.

Najčastejší príklad

- USB kľúč „náhodne“ položený na verejnom mieste
- Po vložení do počítača sa spustí malware

Ďalšieyzické útoky

Dumpster diving (prehľadávanie odpadkov)

- hľadanie dokumentov/zariadení vo firme alebo okolo kontajnerov s cieľom získať informácie

Krádež zariadenia

- odcudzenie notebooku, telefónu alebo tokenu priamo z ruky alebo stola

Coercion / extortion (priame donútenie, nátlak / vydieranie)

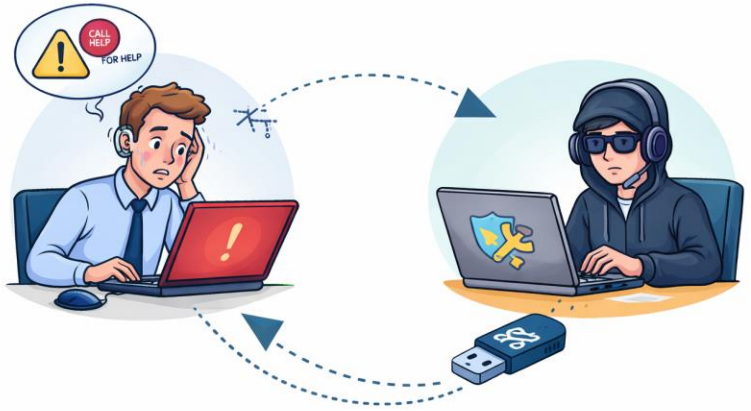
- fyzické/psychologické nátlaky (hrozba, vydieranie) vedúce používateľa k odhaleniu informácií a vykonaniu akcie.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy útokov mierené na používateľa

Reverzné sociálne inžinierstvo

- Útočník najskôr spôsobí problém alebo simulovanú poruchu a potom sa vydáva za „pomoc“ alebo odborníka
- **Obete samy oslovujú útočníka** a požiadali o podporu, čím mu poskytnú prístup, prihlasovacie údaje alebo vykonajú požadované kroky
- Častá podmienka „dočasného“ prístupu, inštalácie nástroja



Znaky

- Najprv sa objaví „problém“ (výpadok služby, falošné chybové hlásenie, nefunkčná aplikácia)
- Následne sa objaví „odborná pomoc“ (e-mail, telefonát...) s inštrukciami, ako problém odstrániť
- Požiadavka, aby používateľ zavolal/klikol na odkaz a poskytol údaje/udelil vzdialený prístup
- Využitie dôvery v „support“, externého dodávateľa alebo interného technika

Príklad

- Zamestnanec narazí na chybové hlásenie. O chvíľu príde e-mail od „IT supportu“ s inštrukciami: „*Pre rýchle vyriešenie nám zavolajte na toto číslo alebo nainštalujte tento nástroj na vzdialenú pomoc.*“ Zamestnanec kontaktuje číslo alebo inštaluje nástroj → útočník získa vzdialený prístup alebo prihlasovacie údaje

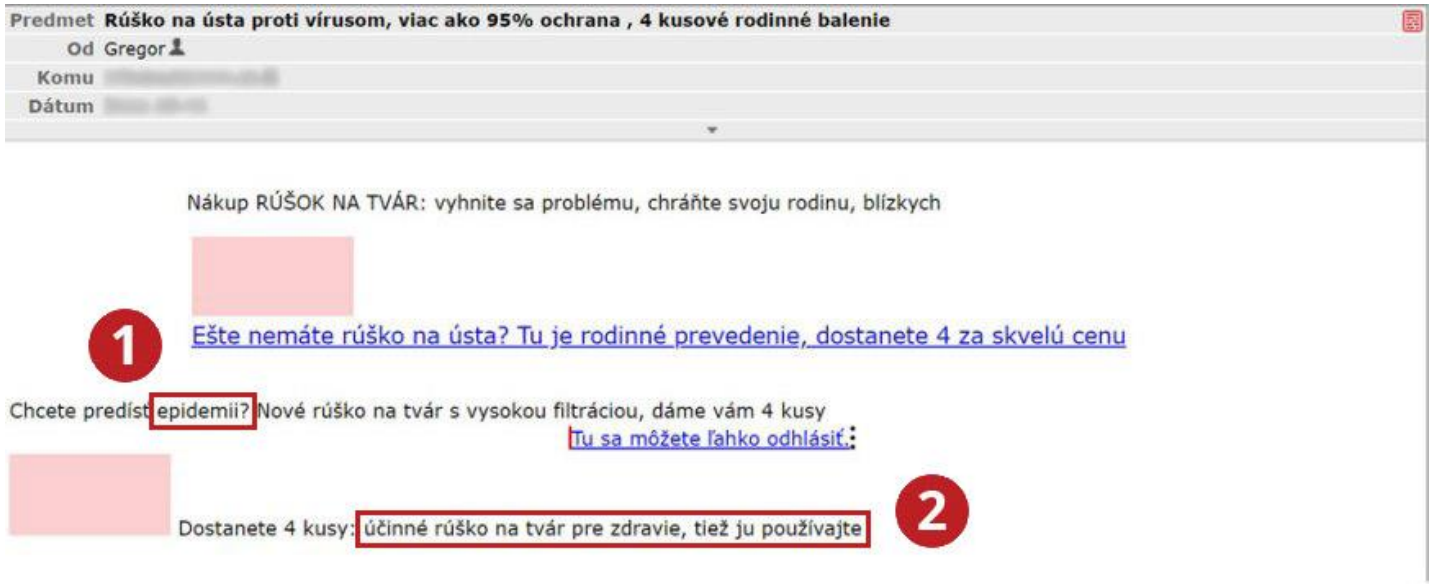
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy útokov mierené na používateľa

E-mailové útoky

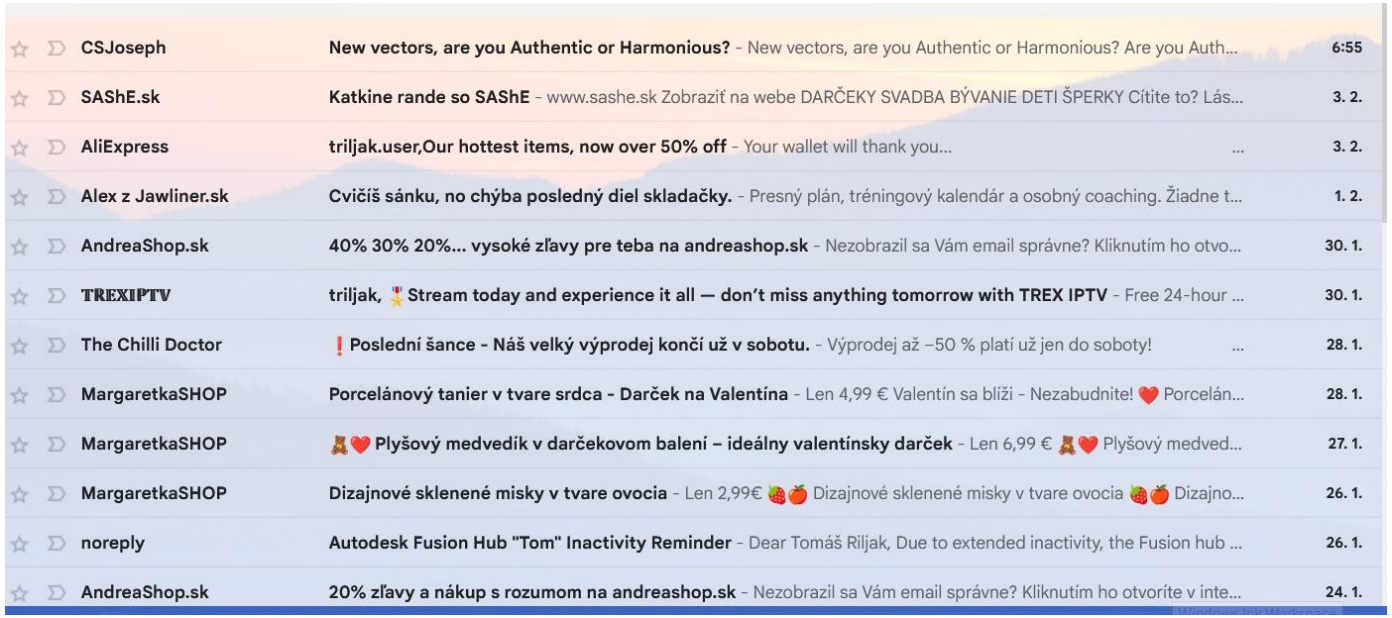
Phishing

- masová alebo polomasová falošná komunikácia s výzvou na akciu (klik, príloha, zadanie údajov)



Spam (nevyžiadané hromadné správy)

- hromadné reklamné alebo podvodné správy; nie vždy s cieľom priamo kompromitovať (často šum, ale môže viesť k phishingu)



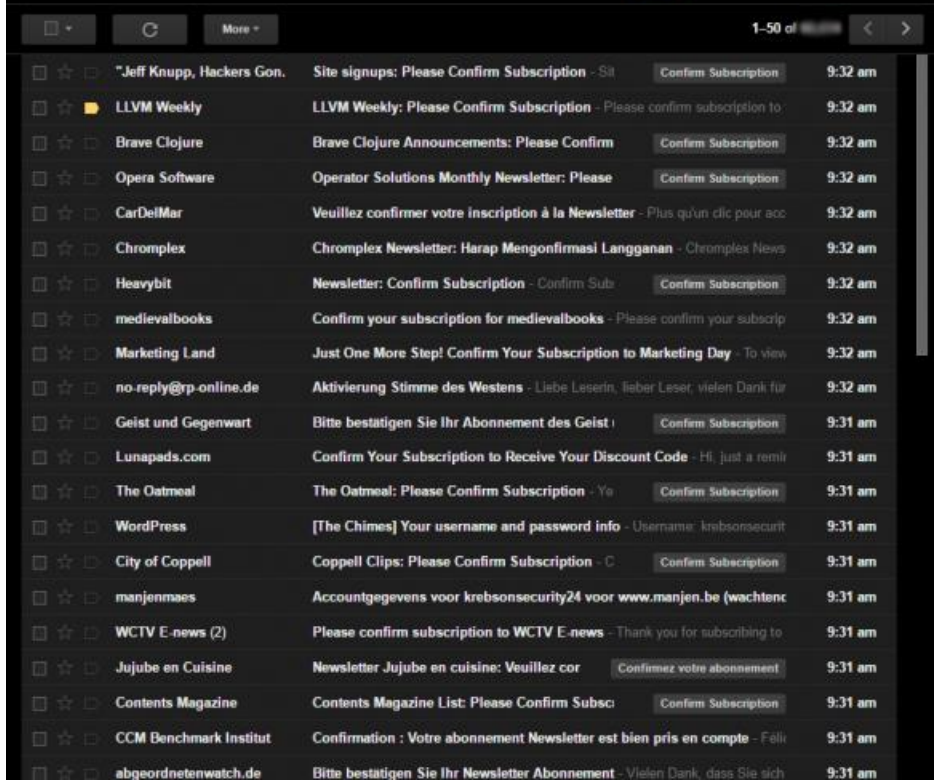
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy útokov mierené na používateľa

E-mailové útoky

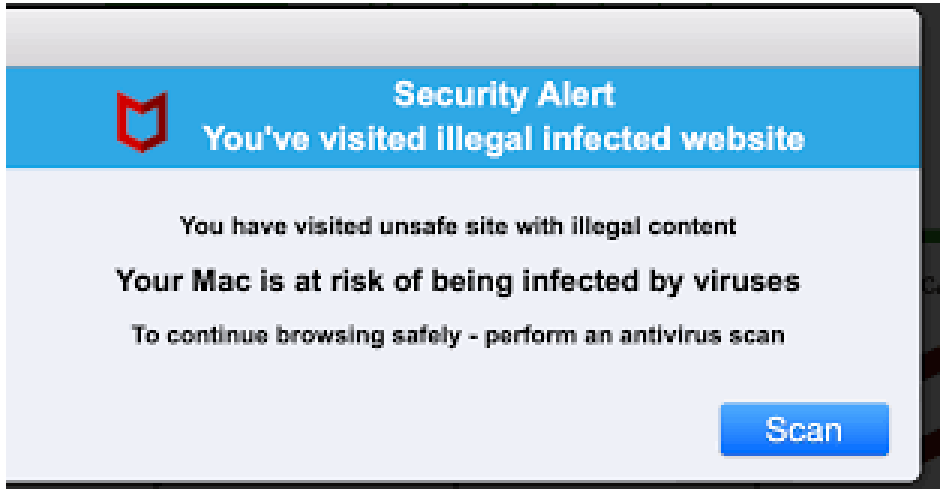
Email bombing (zaplavenie schránky)

- masívne odoslanie e-mailov cieľu s úmyslom zahltiť schránku alebo vyvolať DoS efekt pre používateľa.



Sociálne inžinierstvo cez automatickú odpoveď

- falošné notifikácie o nedoručení, vírusových nálezoch alebo falošné automatické odpovede, budiace dôveru.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Phishing

- útočník posiela falošnú komunikáciu (e-mail, SMS, telefón, správa na sociálnej sieti) s cieľom oklamať používateľa, aby spravil neželanú akciu alebo prezradil dôverné informácie
- najbežnejšia forma sociálneho inžinierstva
- množstvo variant (spear-phishing, whaling, smishing, vishing, clone phishing atď.)

Znaky

- Falošná/napodobnená komunikácia (e-mail, SMS, telefón, DM)
- Naliehavé výzvy („Okamžitá akcia“, „Bezodkladné overenie“, „Zablokované konto“)
- Požiadavky na citlivé údaje (heslá, OTP, bank. údaje)
- Požiadavky nakliknutie na link/prílohu
- Neznáme alebo mierne pozmenené domény/odkazy (malé preklepy, náhradné znaky)
- Personalizácia pri cieľových útokoch (použitie mena, pozície, interných údajov)
- Požiadanie o obídenie bežných procesov (rovnako ako „schváľovanie mimo systému“)

Phishing

Čo útočník často chce dosiahnuť

- Získať prihlasovacie údaje alebo OTP (One-Time Password, Jednorázové overenie)
- Presmerovať platbu/falošné zmeny platobných údajov
- Donútiť obeť nainštalovať malvér cez prílohu alebo link
- Získať prístup k interným systémom prostredníctvom legitimných účtov

Príznaky podozrivého e-mailu / správy (čo hlásiť)

- Neočakávané prílohy alebo odkazy.
- Gramatické chyby alebo neštandardný štýl správy.
- Žiadosť o citlivé informácie cez nešifrované kanály.
- Naliehanie, hrozby alebo extrémne sľuby/odmeny.
- Odosielateľ mimo bežnej firemnej domény alebo s drobnými odchýlkami.

Príklad

E-mail od „security@bank-secure.com" „Vaše konto bude zablokované za 24 hodín – kliknite sem a obnovte overenie.“

Zamestnanec klikne, zadá prihlasovacie údaje na falošnej stránke → kompromitované konto

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Delenie podľa typu obete

Masový phishing

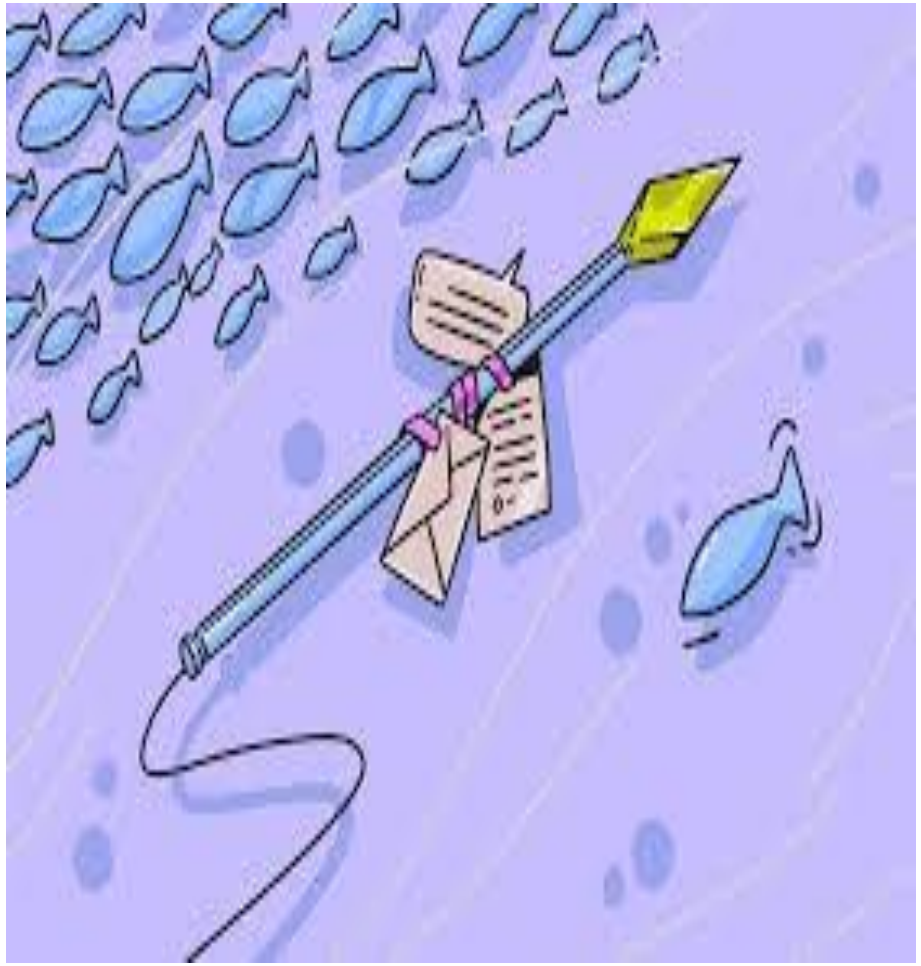
- Všeobecný, neselektívny phishing (napr. "Vaša zásielka bola zadržaná, kliknite sem")
- Rozposielaný hromadne bez výberu cieľa

Spear phishing (cielený phishing)

- Cielený útok na konkrétnu osobu alebo organizáciu.
- Personalizované e-maily s detailmi o obeti.
- Typické riziko: získanie prístupu, malware, krádež údajov

Whaling/Harpooning (Lov harpúnou)

- Spear phishing zameraný na vrcholový manažment (CEO - Chief Executive Officer, CFO - Chief Financial Officer, manažment, atď).
- Obsahuje presne cielené správy (napr. falošné požiadavky na prevod peňazí, alebo poskytnutie informácii).
- Typické riziko: finančné podvody, prevody peňazí, zneužitie dôverných dát



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy phishingových útokov

Delenie podľa použitého média

Email phishing

- Najčastejšia forma – falošné e-maily s odkazom na podvodnú stránku

Fyzický phishing

- Útočník nalepí podvrhnutý QR kód na plagát alebo zariadenie

Smishing (SMS + phishing)

- Útoky cez SMS správy (napr. „Vaša zásielka je pozastavená – kliknite sem.“)

Vishing (Voice phishing)

- Telefonický phishing – útočník sa vydáva napr. za banku, technickú podporu, políciu.
- Typické riziko: vymámiť heslá, PIN kódy alebo zrealizovať podvodný prevod

Pharming

- Presmerovanie na falošnú web stránku bez vedomia používateľa (napr. cez infikovaný DNS)
- Nevyžaduje kliknutie – stačí navštíviť legitímnu URL
- Útočníci „**zbierajú**“ (collect/harvest) veľké množstvo citlivých údajov od používateľov, ktorí sú **presmerovaní na falošné stránky**.
  - Tak ako poľnohospodár „zbiera úrodu“, útočník „zbiera prihlasovacie údaje“.
  - „ph“ evokuje podvod, manipuláciu, internetový útok

Angler phishing

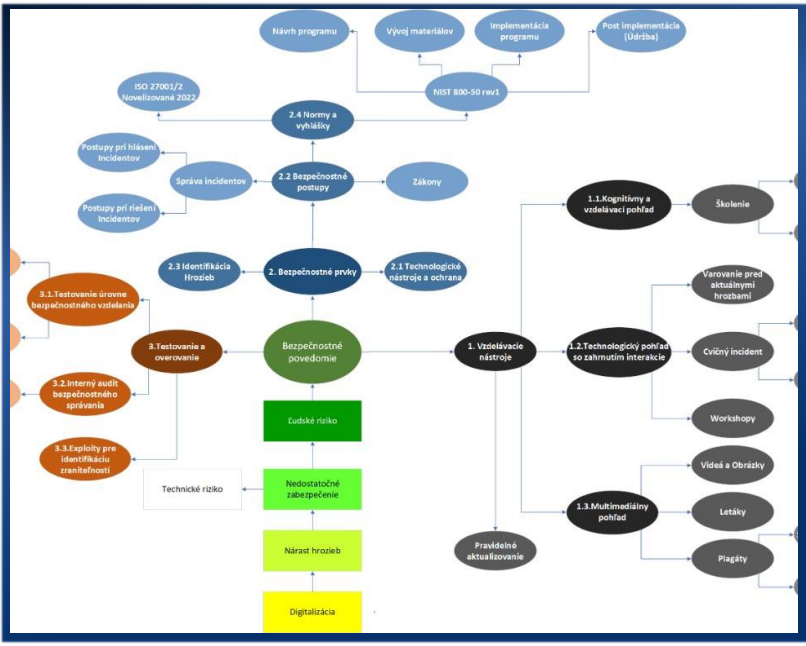
- Phishing cez **sociálne siete** (napr. falošný profil zákazníckej podpory Facebooku...)
- Typické riziko: získať údaje alebo presvedčiť obeť na kliknutie na škodlivý odkaz

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Postupy ochrany pred sociálnym inžinierstvom

The Social Engineer Toolkit (SET)

- **open-source nástroj**, ktorý umožňuje etickým hackerom (white-hat) a bezpečnostným špecialistom vytvárať realistické simulácie útokov, ako napr.:
  - phishingové kampane
  - spear phishing
  - klonovanie webstránok
  - odchyt hesiel (credential harvesting)
  - útoky cez USB, QR kódy, prehliadač
  - vytváranie škodlivých payloadov (na testovanie!)
- Je súčasťou distribúcií ako **Kali Linux** a používa sa vo firmách na **zvyšovanie bezpečnostného povedomia a testovanie:**
  - testovanie odolnosti zamestnancov voči manipulácii
  - simulácie phishingových útokov
  - overenie, či používateľ vie rozpoznať podvod
  - bezpečnostné audity
  - školenia a zvyšovanie bezpečnostného povedomia



Pohľad na bezpečnostné povedomie

Delenie podľa obsahu správy - rôzna motivácia útočníka

Získavanie prihlasovacích údajov

- Správy s odkazmi na falošné prihlasovacie stránky (Office 365, VPN, banka…)
  Cieľ: získať meno, heslo, kód MFA

Malware a škodlivé prílohy

- E-maily s infikovanými dokumentmi (DOC, XLS, ZIP) alebo odkazmi na škodlivé súbory
  Cieľ: infikovať zariadenie a získať prístup do siete

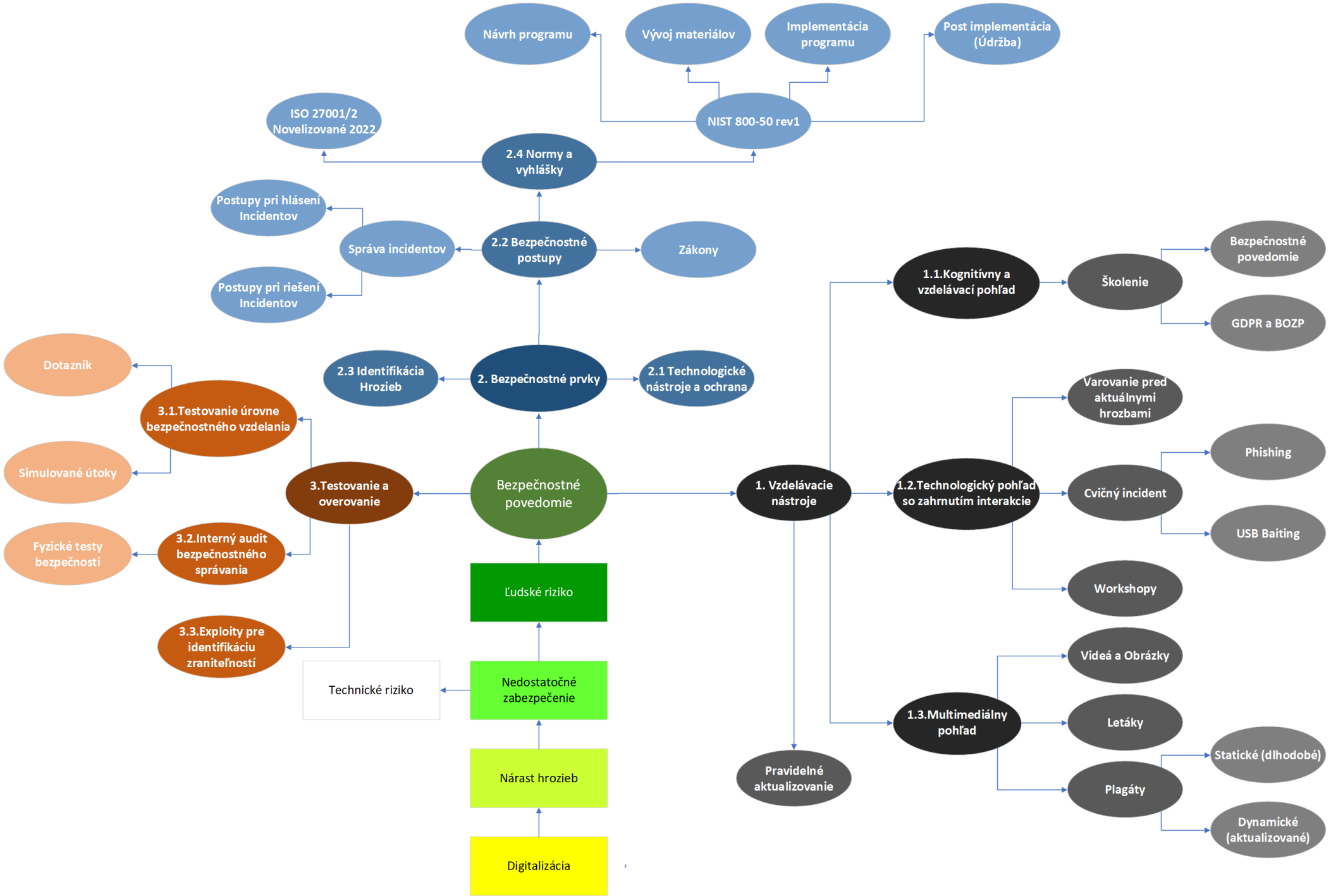
Finančné podvody / BEC (Business Email Compromise)

- Správy s falošnými faktúrami, zmenami účtov alebo žiadosťami o urgentné platby
  Cieľ: presmerovať platbu alebo vylákať finančné prostriedky.

Vydieranie / extortion

- E-maily tvrdia, že útočník má kompromitujúce materiály a žiada výkupné
  Cieľ: finančné vydieranie, vyvolanie strachu.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline


Návrh programu
Vývoj materiálov
Implementácia programu
Post implementácia (Údržba)
NIST 800-50 rev1
ISO 27001/2 Novelizované 2022
2.4 Normy a vyhlášky
Postupy pri hlásení Incidentov
Správa incidentov
2.2 Bezpečnostné postupy
Zákony
Postupy pri riešení Incidentov
Dotazník
2.3 Identifikácia Hrozieb
2. Bezpečnostné prvky
2.1 Technologické nástroje a ochrana
3.1.Testovanie úrovne bezpečnostného vzdelania
Simulované útoky
3.Testovanie a overovanie
Bezpečnostné povedomie
Fyzické testy bezpečnosti
3.2.Interný audit bezpečnostného správania
Ľudské riziko
3.3.Exploity pre identifikáciu zraniteľností
Technické riziko
Nedostatočné zabezpečenie
Nárast hrozieb
Digitalizácia
1. Vzdelávacie nástroje
1.1.Kognitívny a vzdelávací pohľad
Školenie
Bezpečnostné povedomie
GDPR a BOZP
1.2.Technologický pohľad so zahrnutím interakcie
Varovanie pred aktuálnymi hrozbami
Cvičný incident
Phishing
USB Baiting
Workshopy
1.3.Multimediálny pohľad
Videá a Obrázky
Letáky
Plagáty
Statické (dlhodobé)
Dynamické (aktualizované)
Pravidelné aktualizovanie

Pohľad na bezpečnostné povedomie

1. Vzdelávacie nástroje

- **1.1. Kognitívny pohľad**
  - Teoretické aspekty, prehľad hrozieb
- **1.2. Technologický pohľad so zahrnutím interakcie**
  - Spojenie teoretických a praktických poznatkov
- **1.3. Multimediálny pohľad**
  - Vizuálne materiály

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

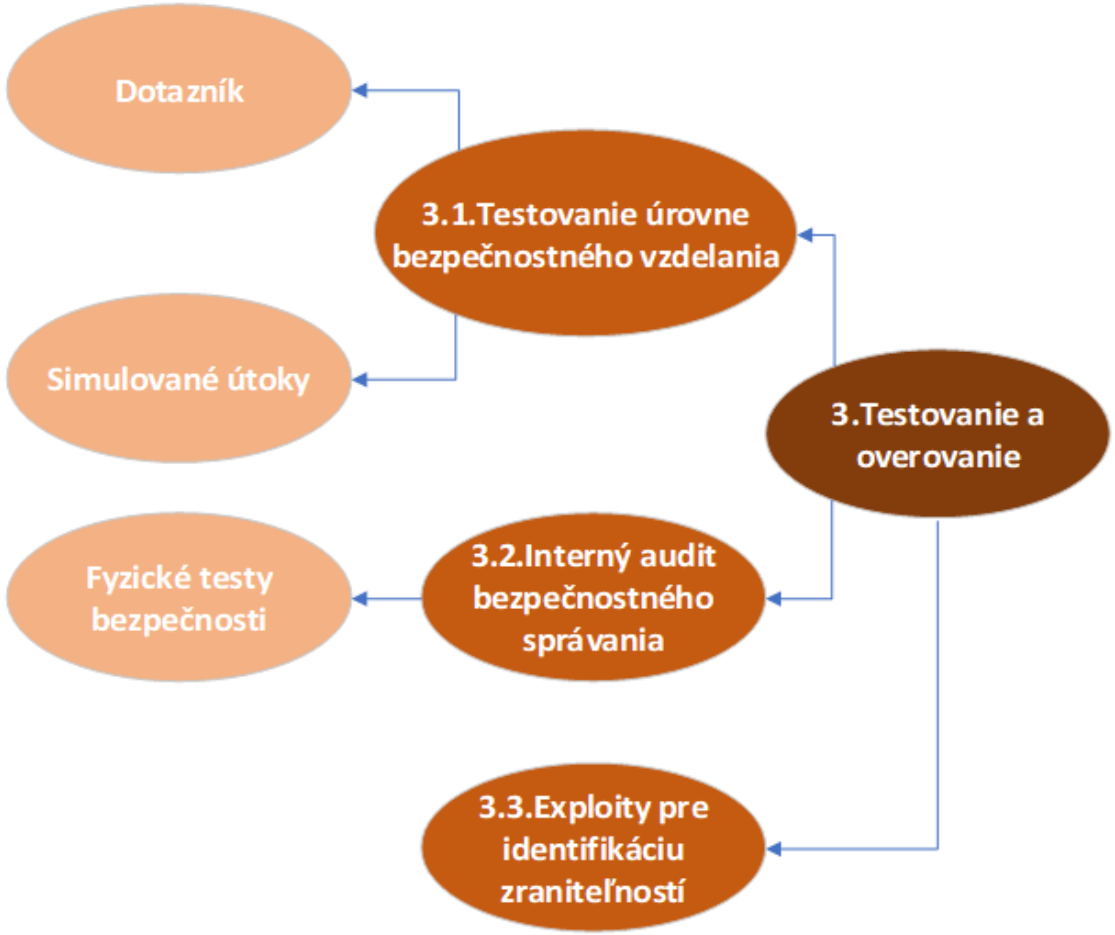
Pohľad na bezpečnostné povedomie

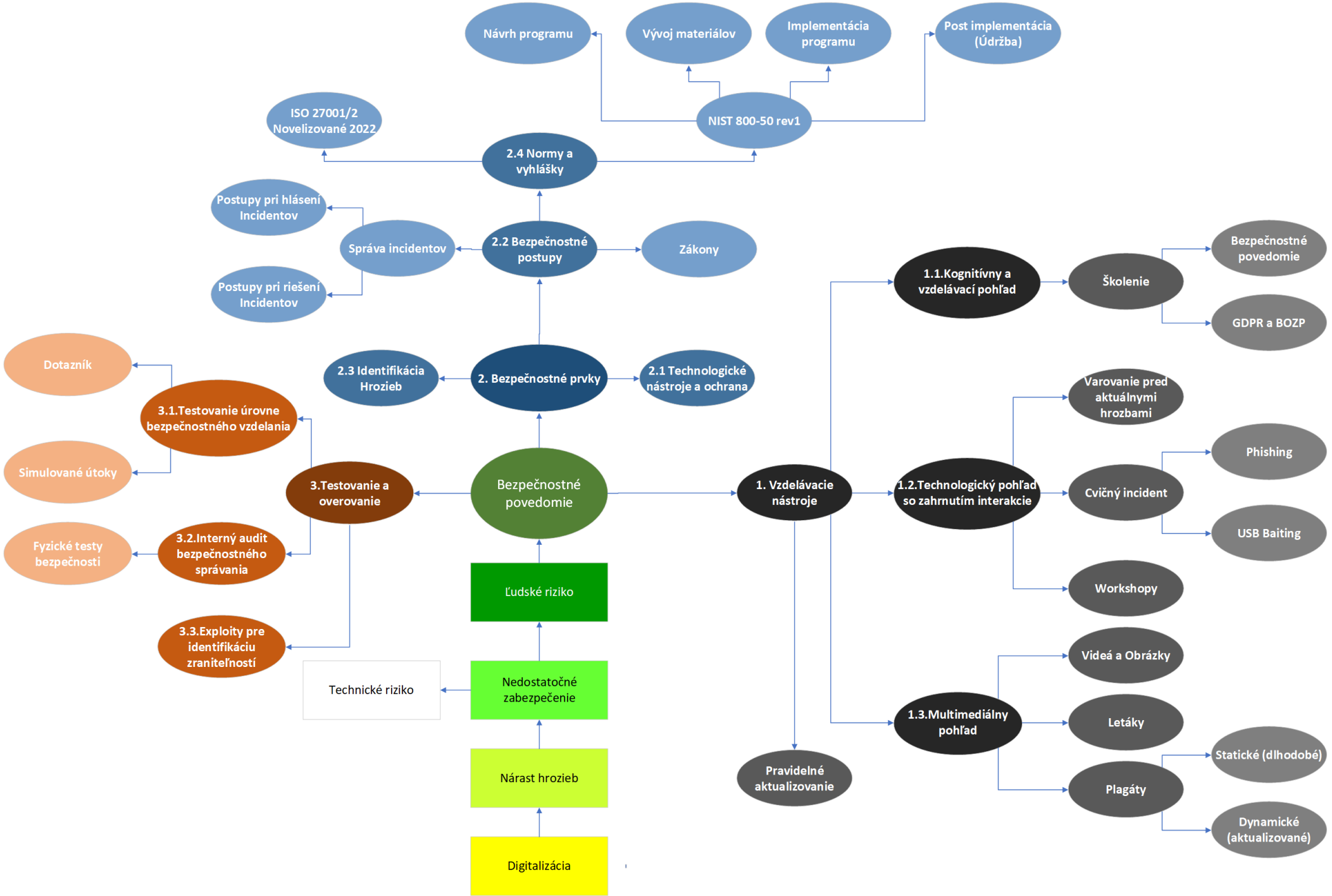
2. Bezpečnostné prvky

- **2.1. Technologické nástroje a ochrana**
  - Technické zabezpečenie
  - Ovládanie nástrojov
- **2.2. Bezpečnostné postupy**
  - Súbor pravidiel na ochranu dát
  - ISO, NIST
- **2.3. Identifikácia hrozieb**
  - Monitorovanie a vyhodnocovanie rizík
- **2.4. Normy a vyhlášky**
  - Chyba ľudského faktoru
  - Potreba vzdelávať zamestnancov

3. Testovanie a overenie

- **3.1. Testovanie úrovne bezpečnostného vzdelania**
  - Overenie znalostí
  - Dotazníky, testy
- **3.2. Interný audit bezpečnostného správania**
  - Praktické overenie znalostí
  - Simulácie
- **3.3. Exploity pre identifikáciu zraniteľností**
  - Odhalenie slabín v infraštruktúre




Návrh programu
Vývoj materiálov
Implementácia programu
Post implementácia (Údržba)
NIST 800-50 rev1
ISO 27001/2 Novelizované 2022
2.4 Normy a vyhlášky
Postupy pri hlásení Incidentov
Správa incidentov
2.2 Bezpečnostné postupy
Zákony
Postupy pri riešení Incidentov
Dotazník
2.3 Identifikácia Hrozieb
2. Bezpečnostné prvky
2.1 Technologické nástroje a ochrana
3.1.Testovanie úrovne bezpečnostného vzdelania
Simulované útoky
3.Testovanie a overovanie
Bezpečnostné povedomie
Fyzické testy bezpečnosti
3.2.Interný audit bezpečnostného správania
Ľudské riziko
3.3.Exploity pre identifikáciu zraniteľností
Technické riziko
Nedostatočné zabezpečenie
Nárast hrozieb
Digitalizácia
1. Vzdelávacie nástroje
Pravidelné aktualizovanie
1.1.Kognitívny a vzdelávací pohľad
Školenie
Bezpečnostné povedomie
GDPR a BOZP
1.2.Technologický pohľad so zahrnutím interakcie
Varovanie pred aktuálnymi hrozbami
Cvičný incident
Phishing
USB Baiting
Workshopy
1.3.Multimediálny pohľad
Videá a Obrázky
Letáky
Plagáty
Statické (dlhodobé)
Dynamické (aktualizované)

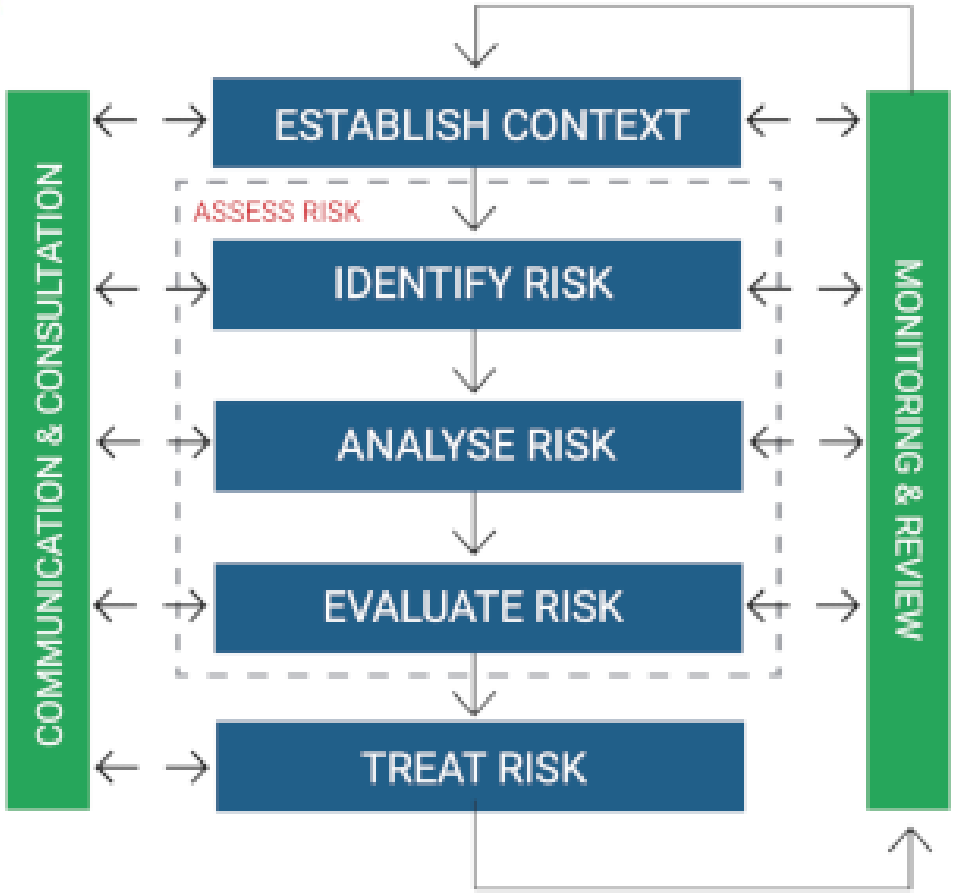
Rámce pre vzdelávanie v oblasti Kybernetickej bezpečnosti (KB)

Druhy rámcov

- NIST
  - Metodické rámce pre kybernetickú a informačnú bezpečnosť
  - NIST SP 800-50r1 pre vzdelávanie a riadenie rizík
- ISO/IEC
  - Medzinárodné normy pre systém riadenia informačnej bezpečnosti
  - ISO/IEC 27001, 27002, 27005 novelizované v roku 2022
- ENISA (European Union Agency for Cybersecurity)
  - Európska agentúra pre KB
  - Kampane a metodiky zamerané na zvyšovanie povedomia

ISO/IEC

- Uznávané vo verejnom aj súkromnom sektore
- Zameranie na systém riadenia informačnej bezpečnosti (ISMS) a kompetencie zamestnancov
- Kľúčové normy:
  - **ISO/IEC 27001:2022**
    - Certifikačná norma pre systém ISMS
  - **ISO/IEC 27002:2022**
    - Výkladová norma, ktorá poskytuje poradenstvo a usmernenia organizáciám
    - Norma poskytuje výklad bezpečnostných opatrení uvedených v ISO/IEC 27001, príloha A, ktoré sú v ISO 27002 referencované.
  - **ISO/IEC 27005:2022**
    - Poskytuje návod na splnenie požiadaviek vyplývajúcich z normy ISO 27001



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hlavný rozdiel novelizovaného ISO/IEC

Aktuálne + novo pridané opatrenia

ISO 27001 – 25.10.2022
ISO 27002 – 15.2.2022

Kategória	Počet opatrení	Skupina
Organizačné opatrenia	37	5
Riadenie ľudí	8	6
Fyzické opatrenia	14	7
Technologické opatrenia	34	8

ENISA – European Union Agency for Cybersecurity

- Agentúra pre podporu kybernetickej odolnosti a vzdelávania V EU
- Zameriava sa na praktické metódy, kampane, nástroje a odporúčania pre vzdelávanie
  - ENISA Cybersecurity Awareness Raising Framework
  - European Cybersecurity Month – každoročná kampaň v Októbri
  - Cybersecurity for SMEs – príručky pre malé a stredné podniky
- ENISA spája technickú a spoločenskú rovinu a tým pomáha formovať kultúru bezpečného správania v Európe

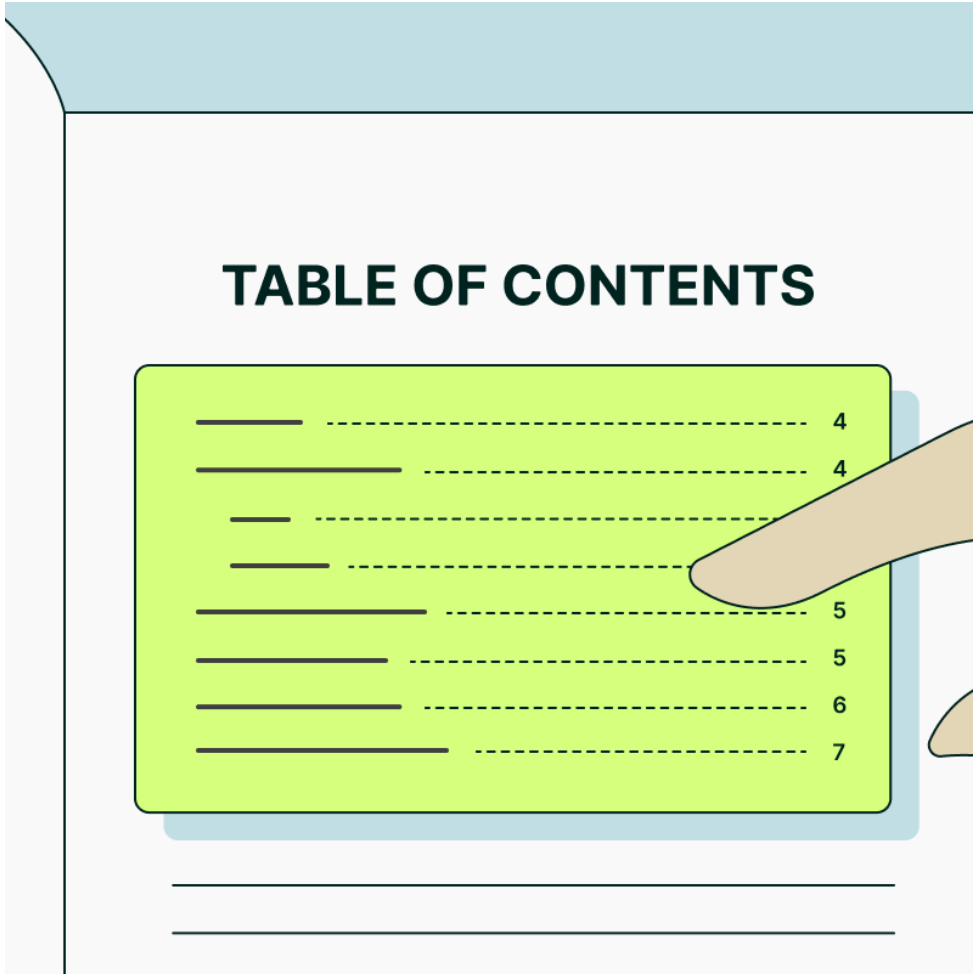
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

NIST SP 800-50r1 Building a Cybersecurity and Privacy Learning program

- Predošlé dokumety:
  - SP 800-50 rok 2003
  - SP 800-16 rok 1998
- Najnovšia revízia zo Septembra 2024
- Definuje koncept Cybersecurity and Privacy Learning Program (CPLP)
- Cieľom je podporiť dlhodobú kultúru bezpečného správania v organizáciách

Obsah NIST SP 800-50r1

- Sekcia 1
  - Úvod
- Sekcia 2
  - Plánovanie stratégie
- Sekcia 3
  - Analýza a návrh CPLP
- Sekcia 4
  - Vývoj a implementácia CPLP
- Sekcia 5
  - Hodnotenie a zlepšovanie



Sekcia 1 - Úvod

NIST SP 800-50r1 Building a Cybersecurity and Privacy Learning program

Vzdelávanie

- Kybernetické riziká a ochrana súkromia **(privacy)** si vyžadujú kontinuálnu pozornosť každého člena v organizácií
- Kľúčovou reakciou je **vzdelávací program (learning program) na KB**
- Cieľom je pochopenie rizík a úloh každého člena organizácie
- Hoci organizácia používa veľa rôznych typov školení, všetky by mali fungovať podľa spoločného rámca **CPLP (Cybersecurity and Privacy Learning Program)**

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Cybersecurity and Privacy Learning Program (CPLP)

- **Vzdelávací program kybernetickej bezpečnosti a ochrany súkromia**
- Zastrešuje
  - Aktivity na zvyšovanie povedomia
  - školenia
  - Simulácie
  - role-based tréningy
  - a dlhodobé vzdelávania
- Termíny **povedomie** (**awareness), školenie (training) a vzdelávanie (education)** sú zjednotené do jedného konceptu CPLP
- Pre každého účastníka programu sa používa pojem **learner**
- Prečo CPLP existuje ?
  - Riziká v oblasti kybernetickej bezpečnosti a súkromia sa dajú riadiť len vtedy, ak sú do toho zapojení všetci zamestnanci

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Účel a zameranie NIST

National Institute of Standards and Technology

- Poskytnúť organizáciám **usmernenia**, ako vytvoriť, riadiť a udržiavať komplexný CPLP
- Podporuje **budovanie** bezpečnostnej kultúry
- Programy musia byť počas celého životného cyklu **aktívne**, **riadené** a priebežne **upravované**

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Sekcia 2 – Plánovanie Stratégie

NIST SP 800-50r1 Building a Cybersecurity and Privacy Learning program

Budovanie strategického plánu CPLP

Čo musí obsahovať stratégia:

- Víziu a poslanie plánu
- Strategické ciele a merateľné výsledky
- Prístupy k učeniu a akčné plány
- Taktiky na dosiahnutie cieľov
- Metriku reportu
- Odrážať štruktúru a misiu organizácie
- Každá organizácia potrebuje vlastný prispôsobený program

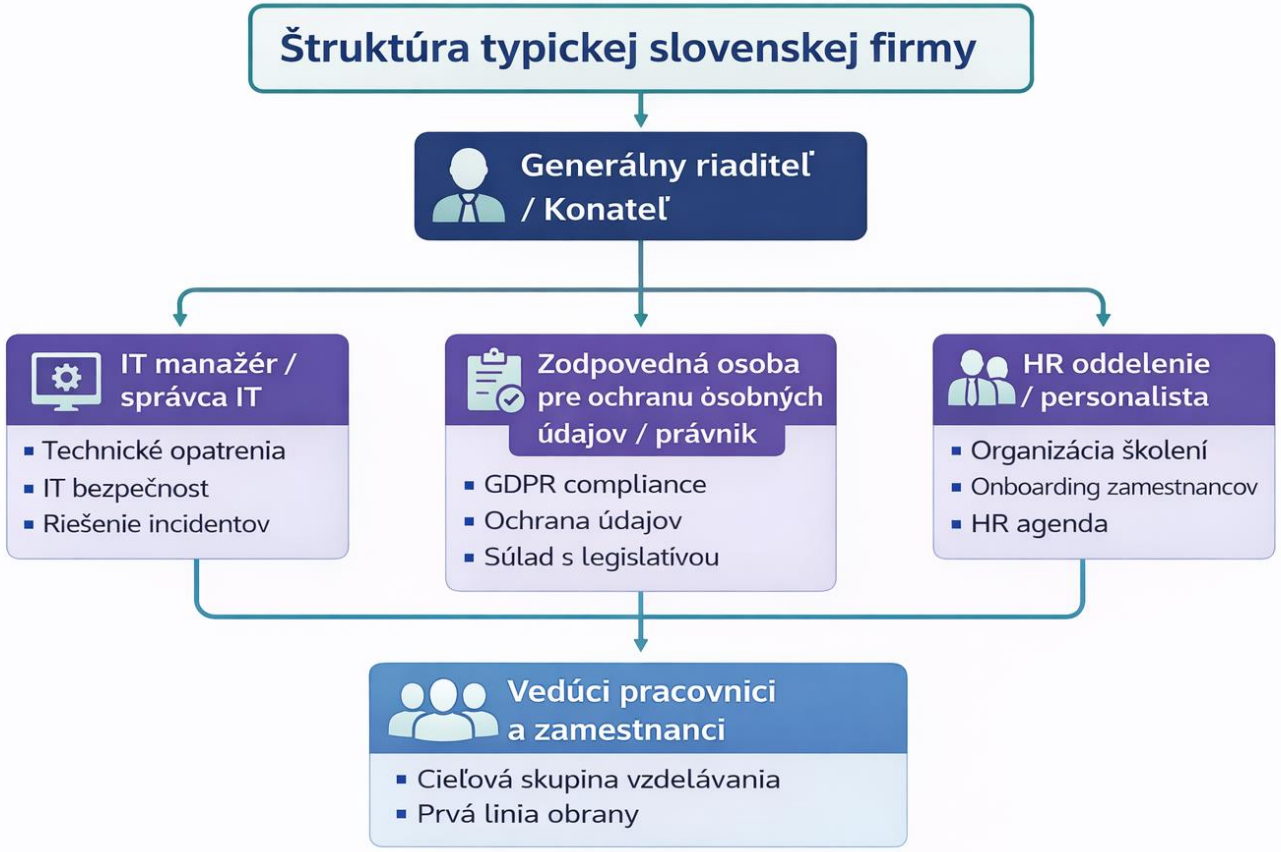
Čo musí spĺňať:

- Schvaľuje vrcholové vedenie (podmienka pre financovanie)
- Vychádzať z výsledkov posudzovania rizík a existujúcich stratégií
- Identifikácia kľúčových zainteresovaných strán
  - Vedenie organizácie, IT manažér,..
- Zahrnúť analýzu rozdielov (ak existuje starý program)
- Adresovať súlad s predpismi a legislatívne požiadavky
- Zohľadniť potreby rozmanitej pracovnej sily (na diaľku, cestujúci,..)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Budovanie strategického plánu CPLP

- CPLP musí vychádzať z organizačnej štruktúry firmy
- Vzdelávacie a bezpečnostné kompetencie sú rozdelené medzi pozície
- Strategický plán reflektuje zodpovednosti rolí
- Jasné rozdelenie úloh zvyšuje efektivitu vzdelávacieho programu
- CPLP je prispôsobené veľkosti a možnostiam organizácie



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

1. Príklady vyhlásení o politike vzdelávacieho programu

- **Čo môžu politiky obsahovať ?**
  - **Vedenie organizácie**
    - Zabezpečuje vytvorenie a schválenie vzdelávacieho programu v oblasti KB
  - **IT manažér/správca IT**
    - Pripravuje a koordinuje školenia v oblasti KB používateľov
  - **Zodpovedná osoba za ochranu osobných údajov (DPO)**
    - Zabezpečuje vzdelávanie v oblasti ochrany súkromia a osobných údajov
  - **Povinnosť používateľov**
    - Absolvovať úvodné KB a privacy školenia
    - Absolvovať pravidelné „refresher“ školenia
    - Splniť tieto požiadavky pred získaním prístupu k systémom

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

2. Príklady vyhlásení o politike vzdelávacieho programu

- **Role-based požiadavky a sprísnené požiadavky**
  - Používatelia so „significant security responsibilities“ musia:
    - Absolvovať „role-based training“ ešte pred prístupom k citlivým systémom
    - Mať „refresher“ školenia každý fiškálny rok
- **Aktivácia a deaktivácia účtov**
  - Účty používateľov musia byť zablokované, ak školenia nie sú dokončené
  - Výnimku môže schváliť vedenie organizácie / IT manažér
- **Povinnosti bezpečnostných a privacy manažérov**
  - IT manažér / správca IT a DPO sú zodpovední za:
    - Prípravu tréningových a metodických podkladov
    - Tvorbu tréningových plánov
    - Vyhodnocovanie zmien správania a postojov zamestnancov
  - IT manažér pravidelne prehodnocuje a aktualizuje tréningové programy
  - Poskytovanie metrík vedeniu organizácie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ako vytvoriť prehľadnú a merateľnú stratégiu CPLP ?

- Začať identifikáciou hlavných cieľov organizácie
- Stanoviť merateľné ciele ako napr.:
  - Percento preškolených
  - Kto potrebuje role-based tréning
- Používať SMART princípy
  - **S**pecific (Špecifické), **M**easurable (Merateľné), **A**chievable (Dosiahnuteľné), **R**elevant (relevantné), **T**ime-bound (Časovo obmedzené)
- Ku každému cieľu definovať taktiky (konkrétne aktivity)
  - (napr. phishing cvičenie, webinár, scenáre)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklad – Ochrana citlivých vytlačených dát

- **Situácia:**
  - Zamestnanci nechávajú citlivé tlačené dokumenty na stole. Politika ochrany súkromia vyžaduje zamknuté skrinky a čistý stôl. Riziko je neoprávnený prístup k citlivým údajom
- Mapovanie na stratégiu CPLP
- **Strategický plán:**
  - Splniť požiadavky ochrany súkromia
- **Strategický cieľ:**
  - Podporiť program ochrany súkromia
- **Zámery:**
  - Zamestnanci majú byť trénovaní a vedomí si povinností pri práci s citlivými dátami
- **Špecifické a individuálne úlohy:**
  - „Keep It Clean“ nálepky na priečinky v miestach, kde sa spracúvajú citlivé dokumenty

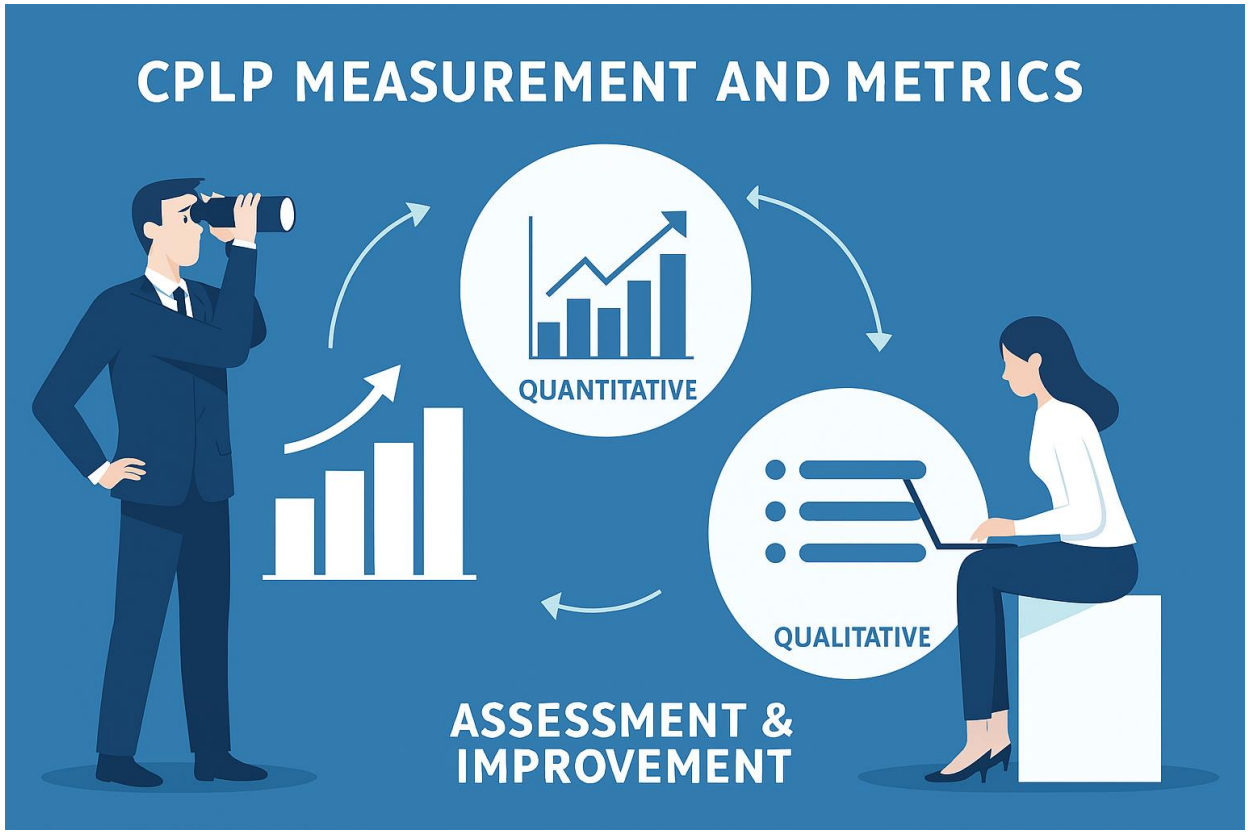
Príklad – Reakcia CPLP manažéra

- Navrhnúť nové awareness materiály
  - Letáky, plagáty a iné vizuálne pomôcky
- Využiť dostupný rozpočet od vedenia
- Následne zabezpečiť samotnú výrobu a distribúciu materiálov
- Koordinácia komunikácie s manažérmi a posilnenie dodržiavania politiky

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Merania a metriky CPLP

- Sú základom fázy Hodnotenie a zlepšovanie (sekcia 5) životného cyklu CPLP
- Pomáhajú hodnotiť efektívnosť a dopad programu
- Umožňujú robiť „data-driven“ rozhodnutia (rozhodnutie založené na dátach)
- Identifikujú oblasti, kde sú potrebné zmeny a zdroje
- Podporujú dodržiavanie požiadaviek (compliance), plánovanie a reportovanie
- Kvantitatívne meranie
  - Čísla, škály, kategórie
    - Napr. hodnotenia od 1 - 5
- Kvalitatívne meranie
  - Pozorovanie, rozhovory, otvorené odpovede



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklad ako merania poskytujú údaje pre metriky

- **Attendance (Účasť)**
  - **Merania**: Registračné a dochádzkové záznamy
  - **Metrika**: Percento registrovaných vs. účastníkov
  - **Analýza**: Trendy účasti
- **Completion (Dokončenie kurzu)**
  - **Merania**: Počet účastníkov + ich role
  - **Metrika**: Percento dokončených školení
  - **Analýza**: Rozdiel medzi účasťou a dokončením
- **Engagement (Zapojenie)**
  - **Merania**:
    - Kvantitatívne: počet zapojených
    - Kvalitatívne: spätná väzba, komentáre
  - **Metrika**: Úroveň interakcie (diskusia, otázky, úlohy)
  - **Analýza**: Trendy účasti
- **Cost per participant (Náklad na účastníka)**
  - **Merania**: Cena kurzu + účasť
  - **Metrika**: Cena programu / počet účastníkov
  - **Analýza**: Efektivita využitia zdrojov
- **Behavior change (Zmena správania)**
  - **Merania**: Počet testovacích phishing emailov a počet správnych reakcií
  - **Metrika**: Percento ľudí, ktorí vykonali želané správanie (napr. nahlásili phishing)
  - **Analýza**: Dopad tréningov na reálne správanie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

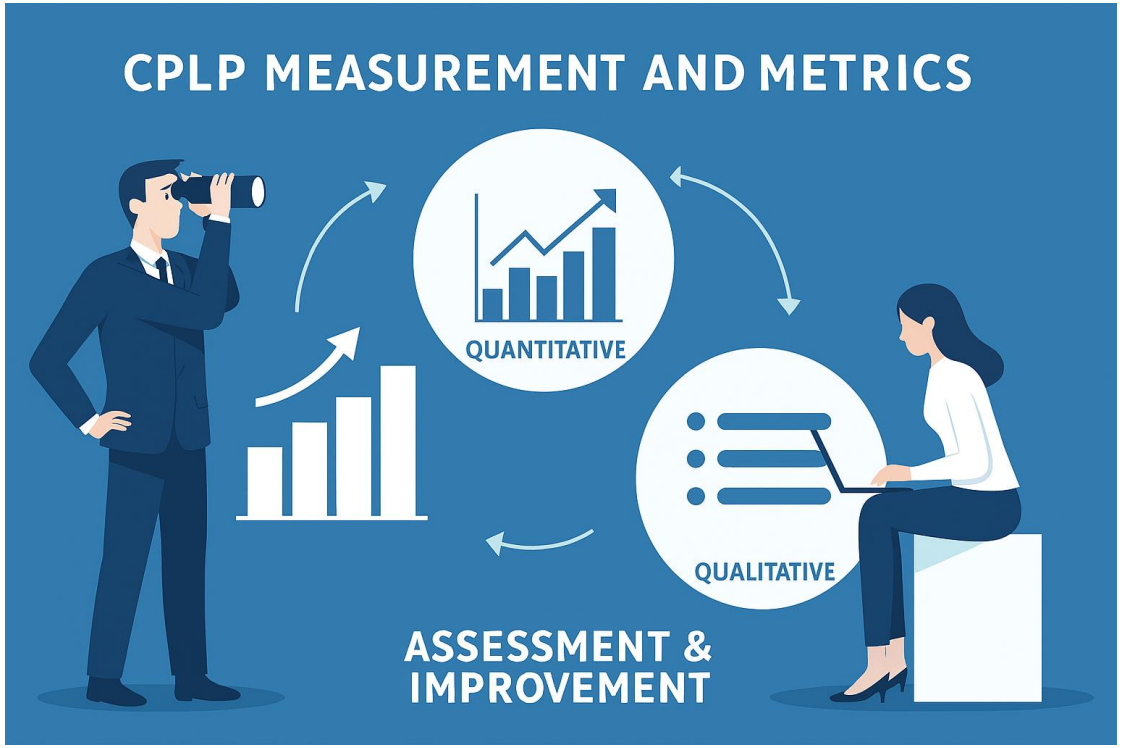
Definície Goals – Objectives - Outcomes

- **Goal (Cieľ)**
  - Všeobecné vyjadrenie toho, čo chce organizácia dosiahnuť
  - Zamerané na kompetencie a úlohy účastníkov
- **Objective (Konkrétny cieľ)**
  - Konkrétne, merateľné vyjadrenia toho, čo má účastník urobiť
  - Vzťahuje sa na konkrétny obsah tréningu
- **Outcome (Výsledok učenia)**
  - Zamerané na správanie účastníka
  - Popisuje ako sa overí, že účastník niečo dokáže
  - Príklad: Po absolvovaní bude účastník schopný ...

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MI INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnostné riziká pri zbere dát o učení

- Manažér CPLP musí riadiť:
  - Riziká spojené so systémom riadenia vzdelávania (Learning Management System - LMS) Ochrana osobných a citlivých údajov o tréningoch
  - Bezpečné ukladanie a reportovanie údajov

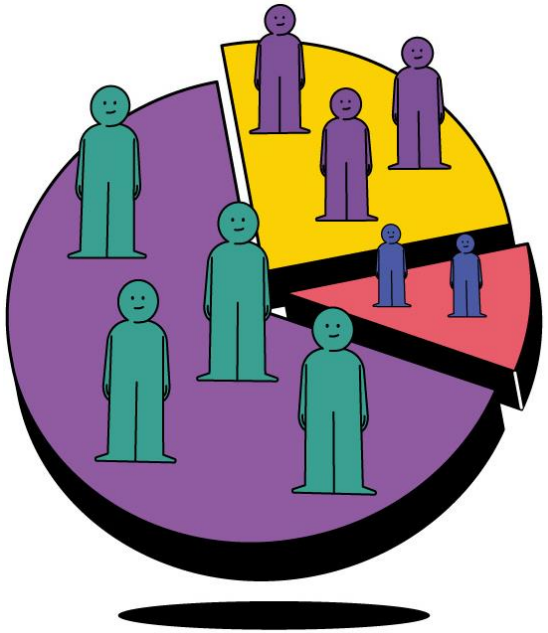


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Segmentácia publika

- **Segmentácia je dôležitá, lebo:**
  - Umožňuje prispôsobenie obsahu rôznym rizikám
  - Zabraňuje tomu, aby „všetci dostali rovnaký kurz“
  - Zabezpečuje, že vysokorizikoví používatelia dostávajú intenzívnejšie školenia
  - Podporuje efektívnejšie riadenie rizík a súlad s predpismi
  - Znižuje neúmyselné chyby pracovnej sily

- **All Users** (Všetci používatelia)
  - Témy: heslá, spracovanie dát, AI nástroje, vzdialený prístup,..
- **Privileged Access Account Holders** (Privilegovaní používatelia)
  - Vyžadujú dodatočný tréning, aby nevyvolali zraniteľnosti
- **Personnel with Significant Cybersecurity/Privacy Responsibilities** (Personál s významnými zodpovednosťami v oblasti KB a súkromia)
  - Vyžadujú role-based tréning (podľa SP 800-53 AT-3)
  - Školenia: technické, manažérske aj operačné povinnosti
  - Procesy, nástroje, metódy



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

CPLP prvky

- **Aktivity na zvyšovanie povedomia**
  - Kampane
  - Plagáty
  - Videá
  - Komunikácia s používateľmi
  - Mikro-obsah
- **Prakticky orientované vzdelávanie**
  - phishing simulácie
  - praktické cvičenia
  - scenáre
- **Školenia**
  - online kurzy
  - role-based kurzy
  - povinné tréningy

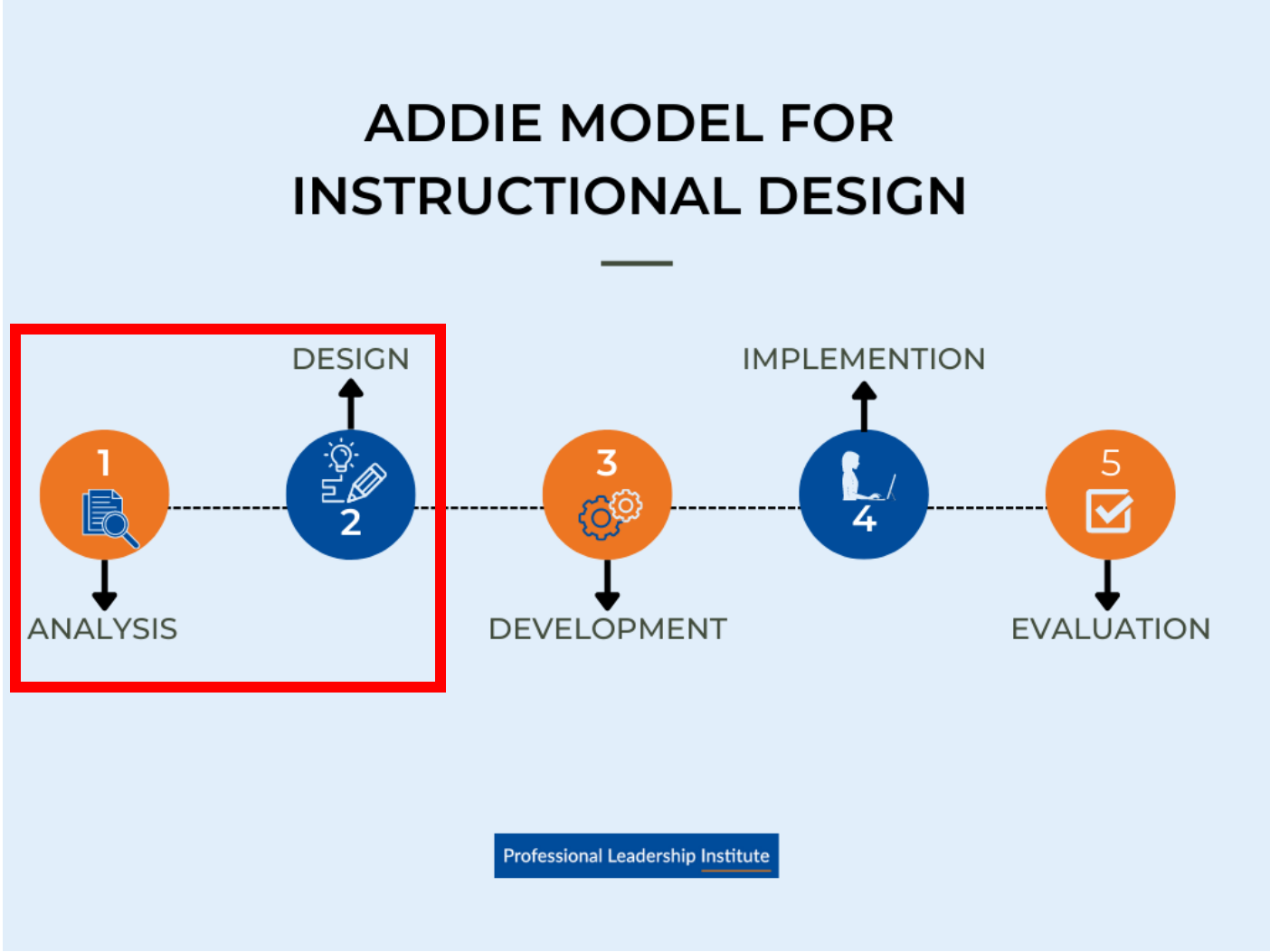
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Sekcia 3 – Analýza a návrh CPLP

NIST SP 800-50r1 Building a Cybersecurity and Privacy Learning program

ADDIE model

- ANALÝZA a NÁVRH
  - V rámci NIST popísaný v **sekcií 3** - CPLP Analysis and Design
- VÝVOJ a IMPLEMENTÁCIA
  - je **sekcia 4** - CPLP Development and Implementation
- HODNOTENIE A ZLEPŠOVANIE
  - je **sekcia 5** - CPLP Assessment and Improvement



1. Analýza (Analysis)

ADDIE

- **Zistenie vzdelávacích potrieb a výkonových medzier (learning gaps) organizácie**
- **Ak preskočíme túto fázu:**
  - Tréningy neriešia skutočné potreby
  - Nesprávne chápanie znalostí používateľov
  - Nesprávny obsah pre nesprávnych ľudí
  - Opakovanie neúčinného obsahu
- **Kto sa podieľa:**
  - Vrcholový manažment
    - nastavuje očakávania, pozná regulácie, podporuje smerovanie
  - Špecialisti KB, a GPDR špecialisti (pri SMEs)
    - dodávajú odborný obsah a znalosti
  - Vlastníci systémov
    - poznajú dopady tréningov na prevádzku
  - Learners
    - pomáhajú identifikovať potreby
- **Hlavné kroky analýzy (NIST):**
  - Identifikovať vzdelávacie potreby (podľa úloh a pracovných aktivít)
  - Určiť cieľové skupiny (all users, privileged users, significant responsibilities)
  - Priradiť potreby k jednotlivým skupinám
  - Zhodnotiť aktuálnu úroveň ich znalostí a zručností
  - Určiť konkrétne vzdelávacie medzery, ktoré treba z tréningov odstrániť

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

2. Návrh (Design)

ADDIE

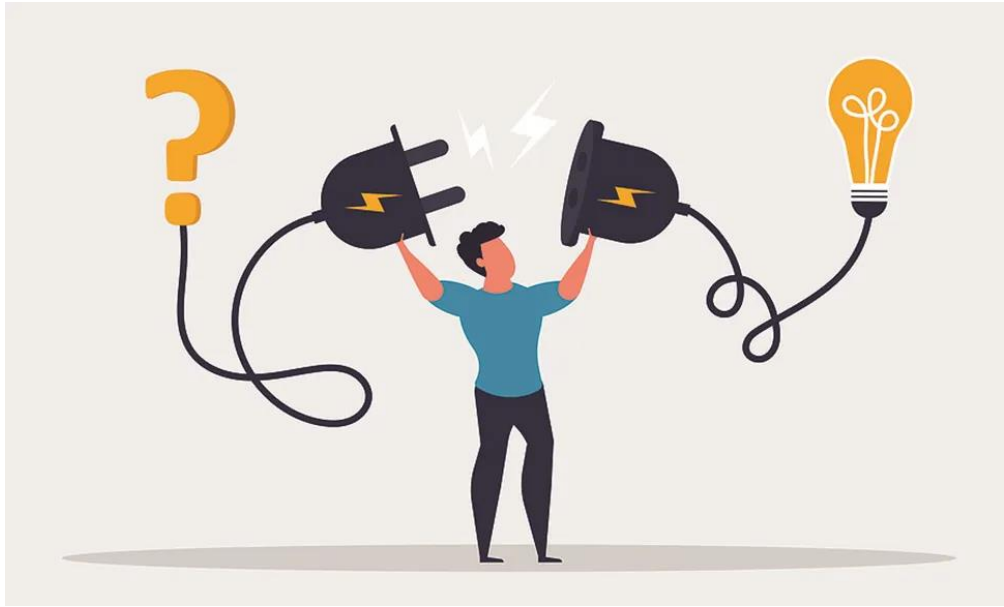
- **Vytvorenie Design Document (plán/dokument návrhu)**
  - Základný dokument, ktorý opisuje presný návrh tréningu:
    - Účel, ciele, pozadie
    - Cieľovú skupinu
    - Vzdelávacie ciele vzdelávacieho programu)
    - Rozhodnutie „build or buy“ (vlastné alebo kúpené riešenie?)
    - Osnovu kurzu
    - Výučbové metódy (video, simulácie, aktivity,..)
    - Spôsob doručenia (online, in-person)
    - Typy hodnotenia
    - Metriky a požadované výstupy

- **Survey – prieskum existujúcich tréningov**
  - Skontrolujú sa interné aj externé zdroje
    - Existujúce firemné kurzy
    - Federálne/agentúrne materiály
    - COST riešenia (vendor kurzy)
    - Nekomerčné a grantové zdroje
    - Podujatia
      - Cybersecurity Awareness Month,
      - Data Privacy Week,
      - Cybersecurity Career Week
    - Interné oddelenia, ktoré už majú tréningy
- **Identifikácia vzdelávacích cieľov**
  - Vzdelávacie ciele sa vytvárajú na základe medzier z fázy Analýza
  - Musí byť jasné
    - Čo má používateľ vedieť
    - Čo má byť schopný urobiť
    - Aké správanie sa má zmeniť

Identifikácia Learning Objectives

ADDIE

- **Fáza návrhu nadväzuje na fázu analýzy tým, že identifikované vzdelávacie medzery transformuje na konkrétne vzdelávacie ciele.**
- Stanovenie vzdelávacích cieľov CPLP manažérom
  - Zhromaždenie výsledkov analýzy a prehľadu dostupných materiálov
  - Definuje konkrétne ciele, ktoré odstránia zistené medzery vo vzdelávaní
  - Zabezpečí, aby boli v súlade s organizačnými potrebami



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklad zavádzania Multi-factor authentication (MFA)

- **Identifikovaná medzera:** Zamestnanci používajú iba heslo (single-factor)
- **Vzdelávacie ciele musia zabezpečiť, aby používatelia:**
  - Pochopili riziká single-factor autentifikácie
  - Rozumeli prečo organizácia zavádza MFA
  - Vedeli svoju rolu pri používaní MFA
  - Nainštalovali MFA aplikáciu a overili token
  - Používali token 100% času pre autentifikáciu do systému

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE
ADDIE

Požiadavky a odporúčania pred začiatkom Vývojovej fázy

- **Požiadavky na CPLP obsah, ktorý musí:**
  - Podporovať rôzne typy vzdelávania (online, osobne, opakovateľné, nahraté)
  - Byť priebežne aktualizovaný
  - Obsahovať jasné a merateľné vzdelávacie ciele pre každý modul
  - Byť zosúladený s úlohou organizácie (organizational mission)
  - Mať oddelené sekcie, pre každý cieľ vzdelávania
  - Obsahovať vizuálne prvky (grafika, video, tabuľky)
  - Obsahovať interaktívne prvky, ktoré podporujú prenos znalostí do praxe

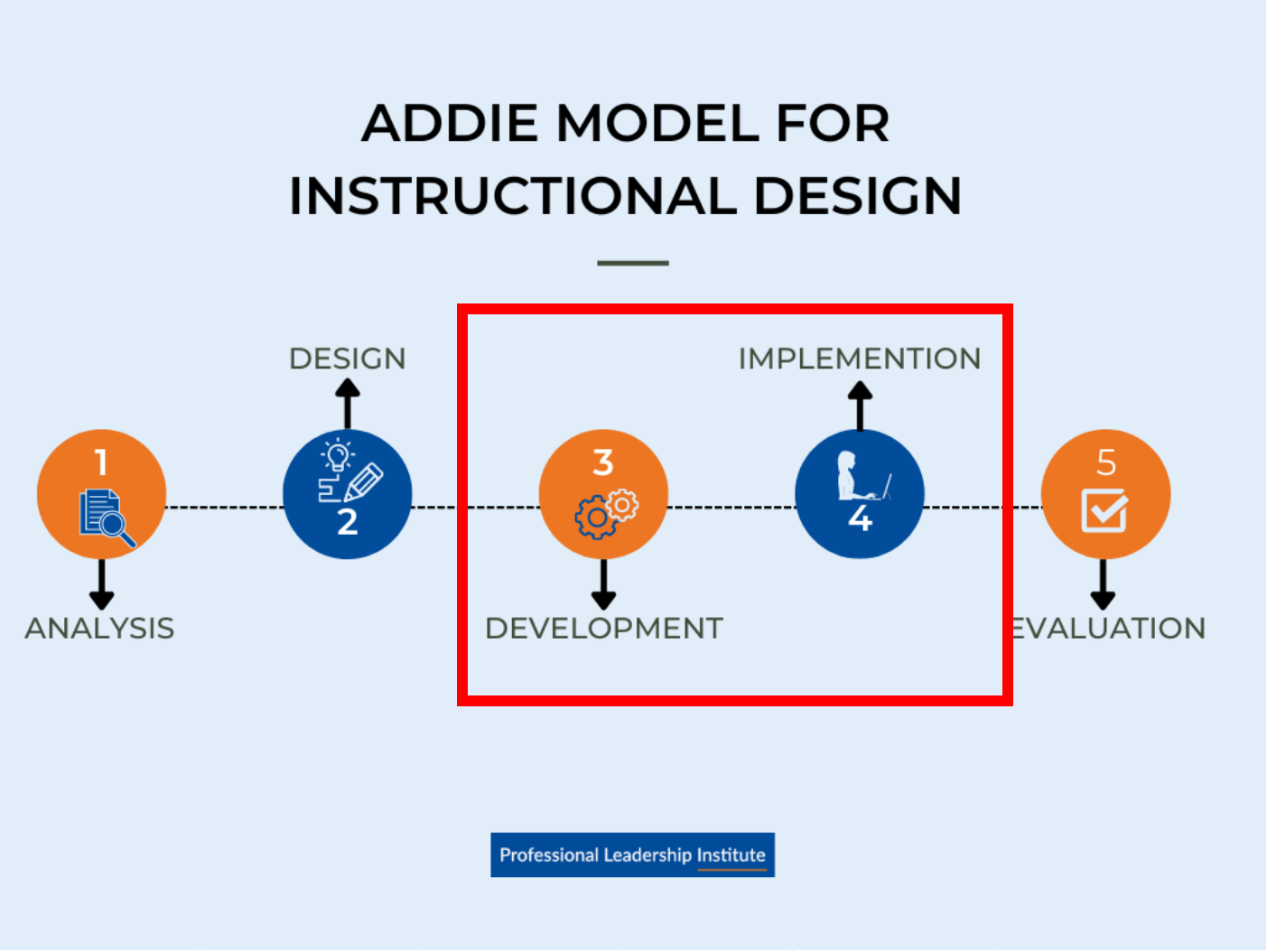
- **Technické a prevádzkové požiadavky:**
  - Manažéri a supervízori musia vedieť sledovať progres a reporty v LMS
  - Musí byť pokrytá povinnosť reportovania pre vrcholové vedenie
  - IT podpora musí byť pripravená podporovať CPLP
  - Ak sa používajú externé kurzy, poskytovateľ musí vedieť aktualizovať obsah aj LMS dáta

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE
ADDIE

Sekcia 4 - Vývoj a implementácia CPLP

NIST SP 800-50r1 Building a Cybersecurity and Privacy Learning program

ADDIE model


ADDIE MODEL FOR
INSTRUCTIONAL DESIGN
1
ANALYSIS
DESIGN
2
3
DEVELOPMENT
IMPLEMENTION
4
5
EVALUATION
Professional Leadership Institute

Vývoj (Development)

- Vyvíja sa obsah podľa požiadaviek z Analýza a Návrh
- Každý cieľový segment používateľov (all users, privileged users, significant responsibilities) sa rieši zvlášť
  - Obsah sa vyvíja podľa:
    - Vzdelávacích cieľov,
    - Identifikovaných vzdelávacích medzier,
    - Rozpočtu,
    - Dostupných zdrojov,
    - Osvedčených postupov.
- Na fáze vývoja sa podieľa:
  - **Vedenie organizácie:**
    - stanovuje priority, zdroje, dohliada na efektivitu tréningov
  - **Špecialisti KB a ochrany osobných údajov**:
    - určujú znalosti a zručnosti potrebné pre role, validujú obsah
  - **Vzdelávací špecialisti:**
    - vyvíjajú, upravujú a hodnotia tréningy
  - **Obstarávanie a rozpočet:**
    - riešia obstarávanie externých zdrojov

Všeobecné pokyny pre vývoj alebo získavanie nových CPLP materiálov

- **Dokument s požiadavkami má odpovedať na otázky:**
  - Pre akú cieľovú skupinu (audience segment) je obsah určený?
  - Aké riziká a správania má riešiť?
  - Aké znalosti/zručnosti má učiť?
  - Podporuje obsah bezpečnú kultúru?
  - Bude obsah pre publiku pútavý?
  - Aký je rozpočet a čas?
  - Kto schvaľuje a hodnotí obsah?
  - Ako bude prebiehať testovanie na používateľoch, aby sme sa ubezpečili, že program pokrýva ich potreby a je primeraný ich úrovni v danej oblasti?
  - Sú zahrnuté merania a metriky pre hodnotenie?

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

ADDIE

Všeobecné pokyny pre vývoj alebo získavanie nových CPLP materiálov

- **Ďalšie kritéria kvality obsahu:**
  - Obsah musí byť aktuálny (nie rýchlo zastarávajúci)
  - Musí podporovať používateľov na pracovisku aj vzdialených používateľov
  - Musí byť dostupný aj pre používateľov s podpornými technológiami (napr. čítače obrazovky, alternatívne ovládanie klávesnice, zväčšovanie,..)
  - Musí obsahovať merateľné hodnotenia
  - Musí byť špecifický pre príslušnú cieľovú skupinu používateľov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

ADDIE

Vývoj materiálov pre segment – All Users

- **Všetci používatelia**
- Materiály sa poskytujú počas celého roka (nie raz ročne)
- Obsah musí byť aktualizovaný podľa incidentov a udalostí (napr. phishingová kampaň)
- Kľúčové je udržať angažovanosť a preto treba používať rôzne formáty ako:
  - E-mail kampane
  - Plagáty
  - Informačné bulletiny (Newsletter)
  - Šetriče obrazovky
  - Neformálne vzdelávacie alebo informačné stretnutia (brown-bag sessions)
    - Napr. každý piatok pri obede
- Príklad tém:
  - Rôzne formy phishingu
  - Heslá, MFA
  - Bezpečná práca z domu a na cestách
  - Malware/ransomware
  - Bezpečné používanie cloudových služieb
  - Bezpečné mazanie dát

ADDIE

Vývoj materiálov pre segment - Privileged Access Account Holders

- **Používatelia s privilegovaným prístupom**
- Obsah podobný ako pre All Users segment
- Kľúčové otázky:
  - Čo by si mali držitelia účtov s privilegovaným prístupom uvedomovať z hľadiska kybernetickej bezpečnosti a ochrany súkromia?
  - Aké postupy musia zamestnanci dodržiavať na ochranu svojich účtov s privilegovaným prístupom?
- Odporúčané konzultovať s:
  - IT manažérom, KB špecialistom, DPO, interným / externým audítorom, manažmentom rizík

Vývoj materiálov pre segment - Significant Cybersecurity and/or Privacy Responsibilities

- **Zamestnanci so zvýšenými bezpečnostným a/alebo súkromnými zodpovednosťami**
- Vyžaduje si detailný a premyslený prístup k tvorbe vzdelávacieho programu
- Školenie musí byť prispôsobené individuálnym potrebám a úrovni zodpovednosti
- Môže byť potrebné vypracovať viacero dokumentov požiadaviek na nové prvky programu.
- CPLP manažér musí koordinovať činnosť s:
  - Manažérmi jednotlivých oddelení
  - **Zodpovednou osobou za vzdelávanie**
  - Tvorcami školení

Testovanie pred Implementáciou

- Pred implementáciou musí prebehnúť:
  - Testovanie vhodnosti obsahu pre každú cieľovú skupinu
  - Testovanie doručovacej metódy (online/in-person)
  - Testovanie jazyka, zrozumiteľnosti, hodnoty a užitočnosti
  - Iteratívna spätná väzba

Implementácia

- Skutočné doručenie a distribúcia CPLP materiálov
- Zameranie na prepojenie účastníka s obsahom
- Program sa implementuje cyklicky
- Možno implementovať až po komunikovaní a schválení managementom

- Kroky implementácie:
  - Komunikovať implementáciu CPLP
  - Stanovovať merania, metriky a reportovanie
  - Vytvoriť harmonogram poskytovania prvkov CPLP
  - Plánovať hodnotenia spätnej väzby (post-implementation)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

ADDIE

Komunikácia CPLP implementácie

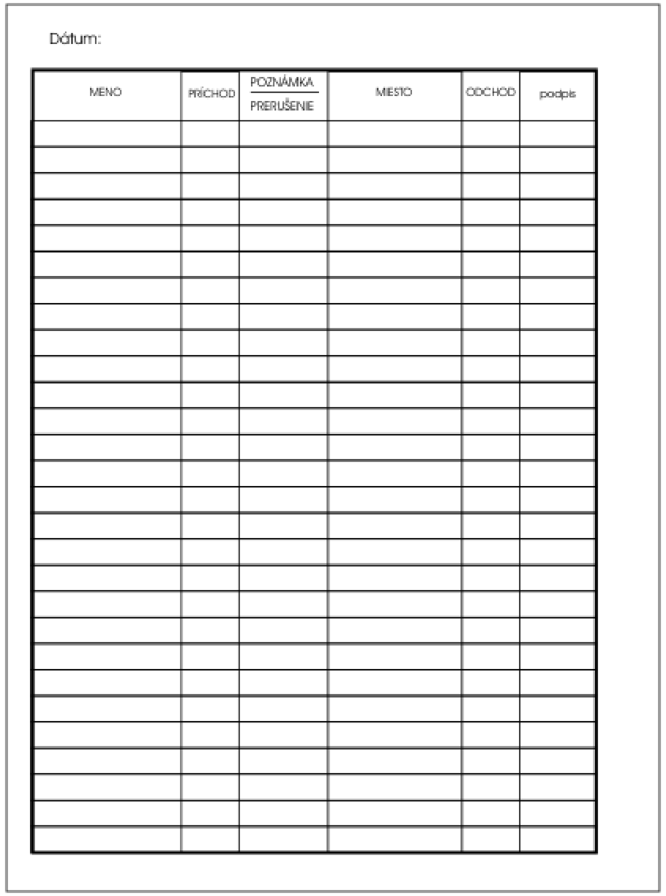
- **Manažéri CPLP musia:**
  - Vypracovať komunikačný plán pre každý prvok programu
  - Zapojiť tím organizačnej komunikácie
  - Určiť správny čas a frekvenciu oznámení
- **Obsah komunikácie:**
  - Názvy, popisy, účel a ciele školenia
  - Segment účastníkov (cieľová skupina)
  - Spôsob sledovania a dokončenia
  - Forma dodania: prezenčne, online, samostatne
  - Požadované/odporúčané prispôsobenia
  - Harmonogram a termíny
  - Overenie účastníkov s významnou zodpovednosťou

Povinnosti a odporúčania

- **Povinnosti:**
  - Vysvetliť povinnosti školenia
  - Uviesť prínosy účasti
  - Odkazy na zákony, predpisy a organizačné politiky
  - Informovať o dôsledkoch nedokončenia
- **Odporúčania**
  - Jedinečné názvy a čísla kurzov
  - Zabezpečiť jasné informácie o prístupe a termínoch

Zavádzanie meraní, metrík a reportovania

- Implementácia musí umožniť zbierať údaje pre:
  - Zabezpečiť, aby nové prvky CPLP umožňovali sledovanie výkonnosti a vyhodnocovanie
  - **Integrácia s LMS:** sledovanie registrácií, dochádzky a dokončenia školenia.
  - **Prvky mimo LMS:** manuálne alebo papierové sledovanie pre prezenčné, virtuálne alebo hybridné školenia.
  - **Meranie dopadu na kultúru:** hodnotiť, ako prvok zlepšuje správanie a podporuje kultúru KB a ochrany súkromia.


Dátum:

MENO	PRÍCHOD	POZNÁMKA PRERUŠENIE	MIESTO	ODCHOD	podpis

ADDIE

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Sekcia 5 - Hodnotenie a zlepšovanie

NIST SP 800-50r1 Building a Cybersecurity and Privacy Learning program

CPLP Hodnotenie(Assessment) a Zlepšovanie (Improvement)

- Môže sa líšiť podľa organizácie a dostupných zdrojov.
- Hodnotenie môže byť pre celý CPLP, pre konkrétnu skupinu účastníkov alebo pre jeden prvok CPLP.
- Je potrebné:
  - Vytvoriť správu o hodnotení CPLP
    - Analyzovať merania a metriky
    - Skontrolovať súlad s predpismi a reportovaním
    - Vyhodnotiť účinnosť CPLP cez spätnú väzbu
  - Preskúmať správu o hodnotení s vrcholovým vedením
    - Dohodnúť zmeny v CPLP
    - Posúdiť dopady na rozpočet a zdroje
  - Realizovať zlepšenia CPLP
    - Aktualizovať strategický a operačný plán CPLP

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

ADDIE

Obsah a štruktúra reportov

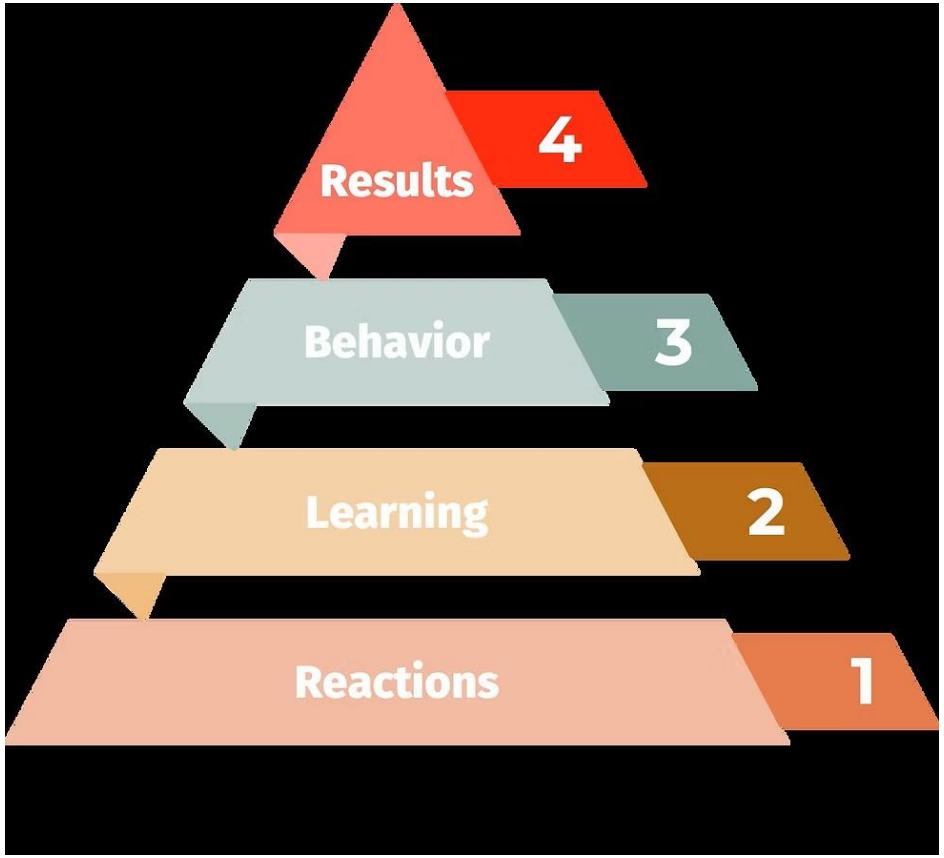
- Poskytnúť vedeniu sumarizovaný prehľad o výkonnosti programu
- Identifikovať problémy, zlepšenia a ďalšie kroky
- Vychádza z dát o: účasti na školeniach, miere dokončenia. Spätnej väzbe, meraných ukazovateľov
- **Merania a metriky**
  - Definované podľa cieľov a regulačných požiadaviek
  - Vyhodnocujú účinnosť, efektivitu, implementáciu
  - Zahŕňajú kvantitatívne aj kvalitatívne metriky
- **Informácie o súlade s predpismi**
  - Splnenie povinných školení
  - Pokrytie všetkých segmentov publika
  - Výsledky praktických cvičení
  - Overenie, či role s povinným tréningom splnili požiadavky
- **Hodnotenie účinnosti CPLP**
  - Manažéri zisťujú efektívnosť inštruktorov
  - Inštruktori poskytujú spätnú väzbu o učebných materiáloch

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

ADDIE

Kirkpatrick Model

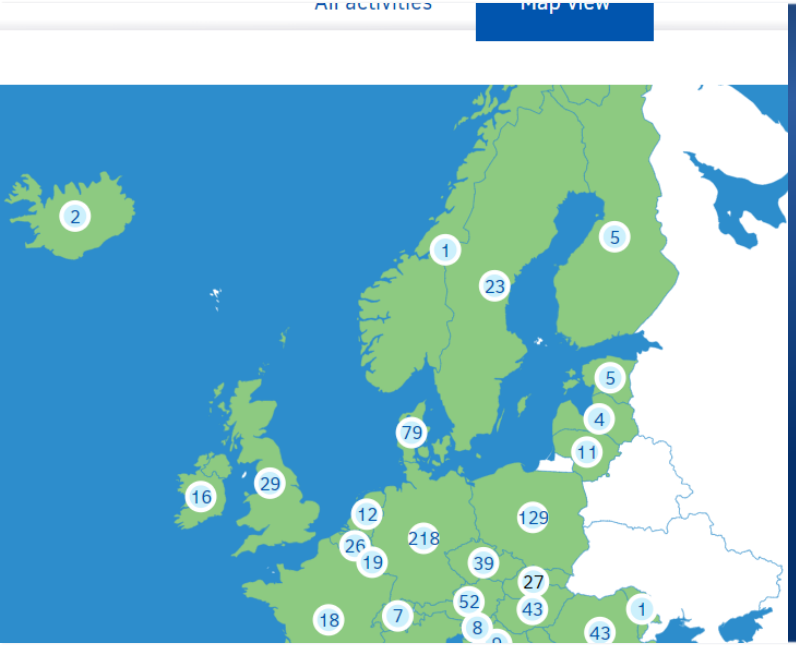
- Poskytuje 4 úrovne (levels) hodnotenia
- **Level 1 – Reakcia (Reaction)**
  - Ako účastník vnímal tréning?
  - Spokojnosť, angažovanosť, vhodnosť formy
- **Level 2 – Učenie (Learning)**
  - Čo sa účastník skutočne naučil?
  - Testy, praktické úlohy, simulácie
  - Zosúladené so vzdelávacími cieľmi a očakávanými výsledkami
- **Level 3 – Správanie (Behavior)**
  - Aplikácia naučených zručností v praxi
  - Spätná väzba od účastníkov, kolegov a nadriadených
  - Identifikuje prekážky v procese alebo organizácii
- **Level 4 – Výsledky (Result)**
  - Dopad tréningu na organizáciu
  - Prezentované vedeniu pri hodnotení programu



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ako na kontinuálne zlepšovanie?

- Založené na rámcoch NIST CSF, Privacy Framework a SP 800-53r5.
- Zahŕňa monitorovanie efektívnosti, identifikáciu problémov a aktualizáciu materiálov.
- Iteratívny proces – prebieha počas celého životného cyklu CPLP.



Príležitosti na rozvoj pre špecialistov KB

Príležitosti pre špecialistov KB

Zdieľanie hrozieb a budovanie povedomia o KB

- Vlády v súčasnosti aktívne podporujú KB
- Americká **agentúra pre kybernetickú infraštruktúru a bezpečnosť** (**CISA**)
  - vedie úsilie o automatizáciu bezplatného zdieľania informácií o KB s verejnými a súkromnými organizáciami.
  - používa systém **Automated Indicator Sharing** (**AIS**), ktorý umožňuje zdieľanie indikátorov útokov (**IOA**) medzi vládou USA a súkromným sektorom hneď po overení hrozieb.
  - NCAS (National Cyber Awareness System)
- Agentúra Európskej únie pre KB (**ENISA, *2004**) poskytuje poradenstvo a riešenia pre výzvy v oblasti KB členských štátov EÚ.
- CISA (Cybersecurity and Infrastructure Security Agency) a NCSA (National Cyber Awareness System) každoročne v októbri organizujú kampaň s názvom Národný mesiac povedomia o kybernetickej bezpečnosti (NCASM), ktorej cieľom je zvýšiť povedomie o kybernetickej bezpečnosti. https://www.cisa.gov/cybersecurity-awareness-month
  - Už aj ENISA (10 rokov): ECSM European Cybersecurity Month https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month

Príležitosti pre špecialistov KB

Zdieľanie hrozieb a budovanie povedomia o kybernetickej bezpečnosti (pokrač.)

- Témou NCASM na rok 2025 bolo **Secure Our World**
- Bezpečnostné témy poskytované prostredníctvom kampane:
  - Použitie silných hesiel a správca hesiel
  - Aktivácia viacfaktorovej autentifikácie
  - Pravidelná aktualizácia softvéru a systémov
  - Rozpoznávanie a nahlasovanie phishingových útokov
  - Zameranie na nové trendy: AI-hrozby, deepfake, simulácie phishingu, správa rizík spojených s ľudským správaním (human risk management)

ECSM by ENISA

European Cybersecurity Month

- V SR v roku 2022 – 7 akcií:

27 OCT 22 – 28 OCT 22

Slovakia

SecTec Security Camp 2022

Pozývame Vás na SecTec Security Camp, kde Vám na základe skúseností u nás, našich partnerov a zákazníkov poskytneme inšpiráciu na postup budovania kybernetickej bezpečnosti, ktorú sme upravovali roky podľa štatistík a charakteristík útokov. Dvojdňový produktový event sa bude konať v krásnom lesnom prostredí pri Modre. Odborný program, ktorým Vás prevedie Martin Matuška zo…

Business users

09 NOV 22 – 10 NOV 22

Slovakia

Qubit Conference Tatry 2022

Pozývame vás na druhý ročník jedinečného formátu komunitnej konferencie o kybernetickej bezpečnosti na Slovensku Qubit Tatry 2022. Po úspešnom minuloročnom podujatí sa opäť môžete tešiť na panelové diskusie, zdieľanie praktických skúseností profesionálov v oblasti informačnej a kybernetickej bezpečnosti, klubové stretnutia a obľúbený networking. Konferencia Qubit Tatry 2022…

Business users

09 NOV 22 – 09 NOV 22

Slovakia

ESET European Cybersecurity Day

A hybrid event for Government employees in the European Union discussing the challenges of cybersecurity in a digitised world, this time focusing on the topic of EU cyber resilience. Taking place in Prague NH Carlo IV and online.

All users

Cybersecurity Activities

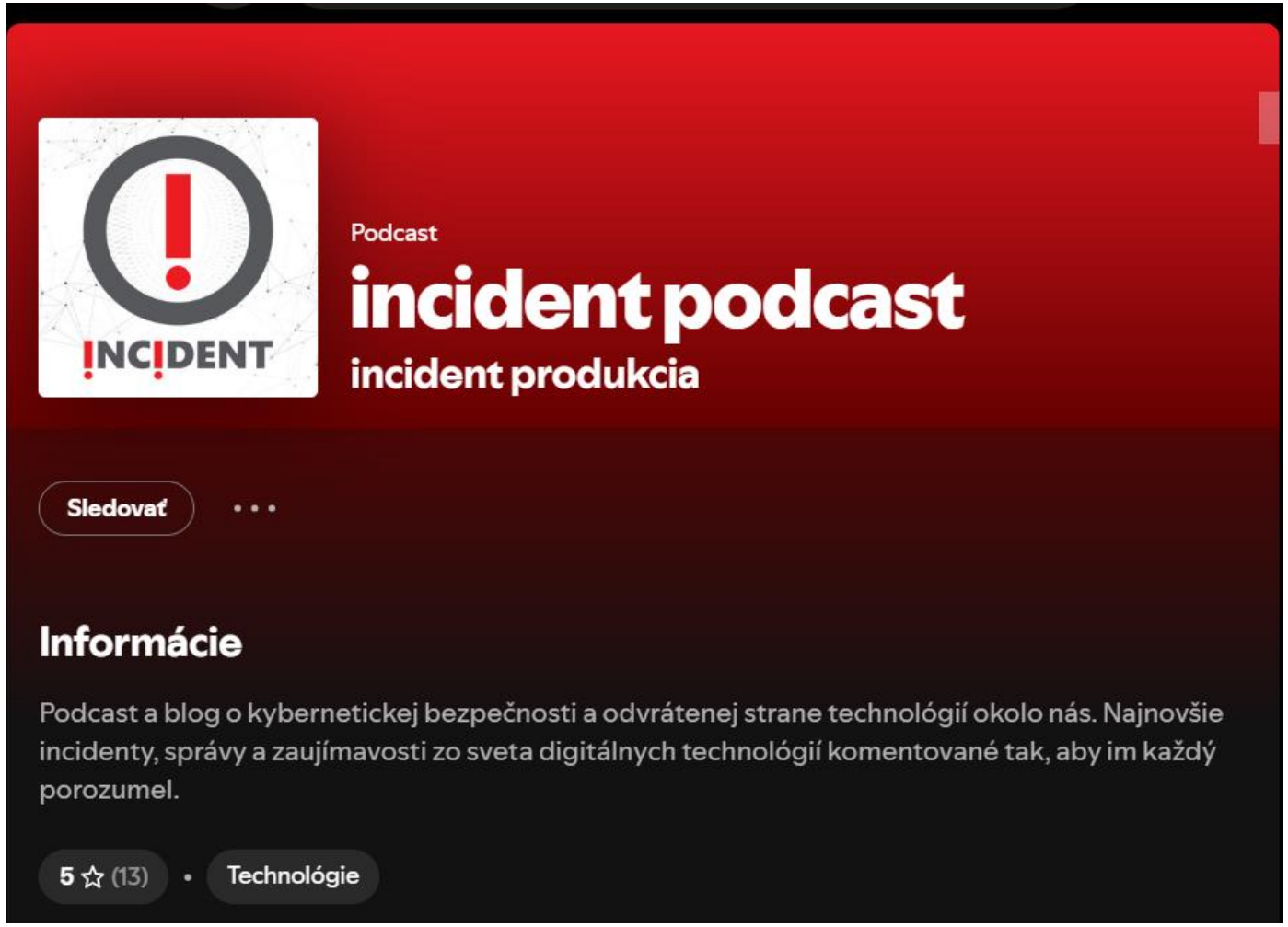
All activities | Map view

https://cybersecuritymonth.eu/@@activities-map

Príležitosti pre špecialistov KB

Ransomware referencie

- Everything you need to know about ransomware: Understand. Prevent. Recover https://ransomware.org/
- Pomoc s odomknutím digitálneho života bez platenia útočníkom https://www.nomoreransom.org
- Spotify Podcast: incident podcast https://open.spotify.com/show/1HVg09bOH46tXf3d1PD0LX



Návrh phishingovej kampane

Čo je simulovaná phishingová kampaň?

- simulovaný bezpečnostný test
  - organizácia rozposiela falošné, ale bezpečné e-maily, ktoré napodobňujú skutočné phishingové útoky

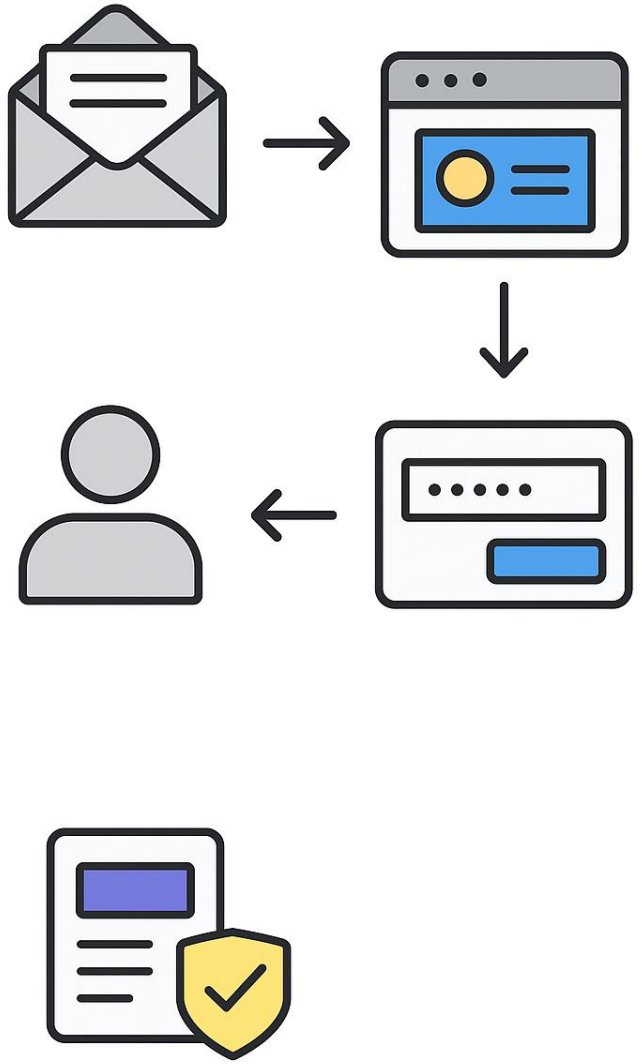
Ciele:

- **vyšovanie povedomia o bezpečnosti**
  Zamestnanci sa naučia rozpoznať podvodné e-maily, odkazy a techniky sociálneho inžinierstva
- **Identifikácia rizikových skupín**
  Meranie, kto kliká, kto zadáva údaje, kto nahlasuje podozrivé správy
- **Test procesov a pripravenosti organizácie**
  Overuje sa, či zamestnanci dodržia interné politiky (nahlásenie incidentu, kontaktovanie IT, neotváranie príloh)
- **Bezpečné učenie na reálnych scenároch**
  Používateľ je po chybe presmerovaný na edukatívnu stránku (landing page)
- **Zlepšovanie bezpečnostnej kultúry**
  Dlhodobé kampane budujú správne návyky a aktívny prístup k kybernetickej bezpečnosti

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Priebeh testovacej kampane

1) Používateľovi príde e-mail
2) Po kliknutí na link je užívateľ presmerovaný na doveryhodne vyzerajúcu web stránku - **landing page**
3) Užívateľa zadá svoje prihlasovacie údaje a klikne na tlačidlo (prihlásiť, zmeniť heslo...)
4) Užívateľ nasleduje politiky organizácie (prejde si školením, prezrie si vzdeávacie materiály...)



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Postup tvorenia kampane

A. **Príprava:** definovať cieľ, zoznamy, segmetnácia, schálenie vedenia...

B. **Tvorba obsahu:** e-maily, landing pages, formuláre (ochrana PII)

C. **Testovanie:** interné testy, doručenie na kontrolné mailboxy

D. **Spustenie:** spustiť kampaň podľa časového plánu

E. **Post-kampaň:** reporting, školenie/rekapitulácia

F. **Návrh zlepšení:** na základe výsledkov a priebehu kampane

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

A. Príprava

Kľúčové body

1) **Ciele kampane** (vzdelanie vs. testovanie odolnosti)
   - Jasne definovanujeme cieľ (napr. zvýšiť nahlasovanie o X %)
2) **Cieľové skupiny a segmentácia**
   - Vytvoríme zoznamy používateľov s atribútmi (oddelenie, rola, riziko)
3) **Zodpovednosti a schválenia**
   - Stanovíme si zodpovednosti za stav kampane, kamaň odkonzultujeme s vedením
4) **Etický a právny rámec**
   - Dbáme na dodržiavanie súkromia, zákonných limitov, GDPR
5) **Harmonogram a zdroje**
   - Stanovíme si harmonogram ďalších fáz kampane a nutné zdroje
6) **Posúdenie rizík**
   - Posúdime riziká (kto/čo, ak sa niečo pokazí)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

B. Tvorba obsahu

Kľúčové body

1) **Typy simulácií**
   - Vyberieme typ simulácie (spear-harpoon phishing, falošné faktúry, interné oznámenia)
2) **Komponenty e-mailu:**
   - Vytvoríme e-mail, ktorý budeme posielať (predmet, preheader, personalizácia, CTA (bez škodlivého obsahu)
3) **Landing page / formulár:**
   - Vytvoríme landing page, ktorá sa zobrazí po kliknutí na odkaz (bezpečná, bez zberu PII, obsah, ktorý má vzdelať)
4) **Jurisdikčné a kultúrne citlivosti**
   - Neútočíme na náboženstvo, kultúru a pod. Dodržujeme príslušné zákonné podmienky
5) **Revízie obsahu vedením a bezpečnostným tímom**
6) **Jasné interné značenie testu v prípade eskalácie** (skryté flagy pre IT)
7) **Pravidlá etiky**
   - **N**epoužívame škodlivé prílohy ani zbieranie hesiel a pod.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

C. Testovanie

Kľúčové body

1) **Interné testy**
   - V internom prostredí otestujeme doručiteľnosť, odkazy, zber analytických dát
2) **Kontrolné mailboxy na validáciu doručenia a obsahu**
   - Na kontrolu použijeme na to určené mailboxy, netestujeme v ostrej prevádzke
3) **Desktopové a smartfónové render testy**
   - Testujeme na počítačoch aj smartfónoch
4) **Spam filter testy, SPF check testy**
   - Otestujeme, či naša kampaň prejde cez náš mail server (doručiteľnosť, logy pre administrátorov)
5) **Bezpečnostné testy landing page**
   - Otestujeme, že landing page je bezpečná a slúži len na simuláciu

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

D.Spustenie kampane

Kľúčové body

1) **Harmonogram**
   - Máme presný časový plán pre každý krok (časové okná, časové pásma)
2) **Technické nasadenie**
   - Vyberieme si typ nasadenia/nástroja (napr. Gophish)
3) **Monitorovanie v reálnom čase**
   - Priebeh kampane pravidelne monitorujeme (doručenie, kliknutia/zadanie údajov)
4) **Plán pre nečakané udalosti**
   - V prípade eskalácie, predčasného ukončenia kampane, technických ťažkostí a pod.
5) **Kontingentná komunikácia pripravená**
   - Máme pripravenú komunikáciu s používateľmi, vedením, IT a bezpečnostným tímom (akdochádza k nejasnostiam)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

E. Post-kampaň

Kľúčové body

1) **Zber a analýza dát**
   - Dáta z kampane je nutné analyzovať, aby sme vedeli posúdiť úspešnosť (metriky, segmenty, behaviorálne vzorce)
2) **Metriky**
   - počet otvorení mailu, počet kliknutí na odkaz, počet nahlásení phishingov, počet zadaných údajov...
3) **Reporting pre vedenie a technický tím**
   - Report odovzdáme vededeniu a technickému tímu čo v najkratšom čase od ukončenia kampane
4) **Anonymizované reporty pre audit**
5) **Post-kampaň školenia**
   - Rizikoví používatelia by si mali prejsť školením, aby sa zmenšilo riziko, že znova kliknú na škodlivý odkaz
6) **Revizné stretnutie**
   - Kampaň zhodnotíme s vedením a IT tímom
7) **Uzavretie incidentu / dokumentácia**

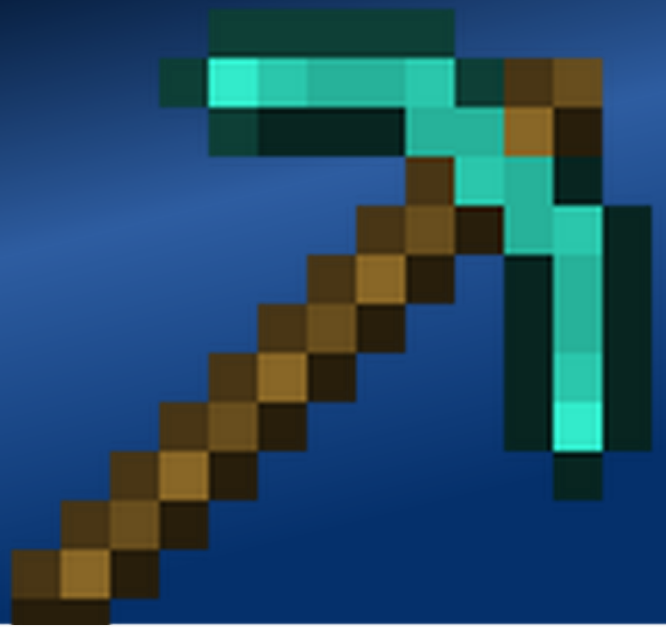
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

F. Návrh zlepšení

Kľúčové body

1) **Krátkodobé vs. dlhodobé opatrenia**
   - Definujeme, ako zlepšiť stav povedomia o phishingu (rázne školenia vs. zmena procesov)
2) **Návrh priorít na nasledujúce obdobie**
   - Čo potrebujeme prioritne? Viac kampaní? Dôverihodnejšie e-maily? A pod.
3) **Integrácia s bezpečnostnou stratégiou**
   - Ako výsledky ovplyvnia našu aktuálnu bezpečnostnú stratégiu? (MFA, least privilege)
4) **Kalendár ďalších kampaní**
   - Vytvoríme časový plán ďalších kampaní na najbližšie obdobie
5) **Plán pre iteratívne zlepšovanie obsahu**
   - monitoroujeme trendy a kontrolné skupiny, upravujeme obsah kampaní
6) **Úprava vzdelávacích materiálov**
   - Na základe výsledkov upravíme materiály aby sme vzdelali o rizikovejších segmentov
7) **Cieľ zlepšiť výsledky**
   - Ktoré metriky chceme zlepšiť a ako? (napr. Zníženie počtu kliknutí o X %)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



Nástroje súvisiace s bezpečnostným povedomím

Phishing nástroje

Nástroje na odhaľovanie phishingu / domén

Behaviorálne a školiteľské platformy

Phishing nástroje

- **Gophish**
  - Nasadený u nás
- **Phishingator**
  - Open-source nástroj zachovávajúci anonymitu používateľov, skvelý pre GDPR-friendly kampane
  - Veľmi jednoduchý rollout, populárny v Európe
- **King Phisher**
  - Pokročilejší open-source framework na kampane (credential harvesting simulácie, custom landing pages)
  - Vhodný pre technickejšie tímy
- **LUCY Security (HornetSecurity Awareness Platform)**
  - Silná komerčná platforma (phishing kampane, smishing, video lekcie, interaktívne testy)
  - Jedno z najkomplexnejších riešení

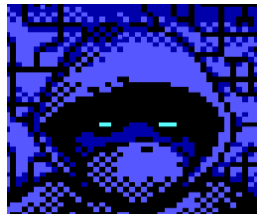
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Phishing nástroje (pokrač.)

- **KnowBe4 (KMSAT)**
  - Najrozšírenejšia komerčná platforma na svete (phishing simulácie, školenia, gamifikácia, awareness kampane)
  - Štandard v enterprise prostredí
- **Cofense PhishMe**
  - Enterprise komerčný nástroj pre veľké firmy, behaviorálne školenia, auto-response
  - Silná integrácia so SIEM a SOC
- **Microsoft Attack Simulator (Microsoft Defender)**
  - Súčasť M365 (phishing simulácie, credential-harvesting simulácie, fake malware attachments)
  - Výhodné, ak firma používa Microsoft 365

Nástroje na odhaľovanie phishingu / domén

- **Phishing Catcher**
  - Python skript – vie bežať lokálne, aj na vzdialenom servery
  - Detekcia phishingových domén podľa TLS certifikátov



- **Urlscan.io**
  - WEB stránka
  - Verejná reputácia a analýza URL adries

urlscan.io
A sandbox for the web

- **MXToolbox**
  - WEB stránka
  - Kontrola reputácie e-mailových domén, blacklistov, SPF/DKIM/DMARC

MX TOOLBOX®

- **MailSpoof**
  - WEB stránka
  - Kontrola možností spoofingu domén

- **DomainTools / RiskIQ PassiveTotal**
  - WEB stránka
  - Vyhľadávanie domén útočníkov, OSINT na kampane

DomainTools

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Nástroje súvisiace s bezpečnostným povedomím

Behaviorálne a školiteľské platformy

- **„behaviorálna platforma“**
  - vzdelávacia alebo bezpečnostná platforma, ktorá:
    - sleduje a vyhodnocuje správanie používateľov (napr. ako reagujú na phishing, podvody, podozrivé odkazy),
    - prispôsobuje tréning každému používateľovi podľa jeho chýb,
    - cielene mení správanie ľudí tak, aby sa vyhli rizikovým akciám.
    - teda nejde len o „kurz“, ale o **kontinuálne, praktické, personalizované učenie založené na reálnych reakciách používateľov**.
- **Hoxhunt**
  - Tréningová platforma postavená na personalizácii phishing simulácií a gamifikácii
- **Proofpoint Security Awareness Training**
  - Moduly na školenia, videá, phishing kampane, reporting
- **CyberRiskAware**
  - Behaviorálne školenia a kontinuálne vzdelávanie

- **„behaviorálne školenie“**
  - Ide o školenie, ktoré učí:
    - **ako sa správať bezpečne**,
    - **ako reagovať na hrozby**,
    - **ako rozpoznať rizikové situácie**,
    - nie iba čo je firewall alebo čo je phishing, ale čo *konkrétne používateľ urobí*, keď sa stretne s podvodom.

Príklad:
Namiesto teórie dostane používateľ falošný phishing email. Ak klikne, školenie mu okamžite vysvetlí, kde urobil chybu.

Gophish

Gophish

Účel nástroja

Popis

- Open-source framework pre simulované phishing kampane
- Vhodný pre interné bezpečnostné tímy a pen-testerov
- Webové rozhranie + REST API pre automatizáciu
- Oficiálna dokumentácia a repozitár
- WIN, Linux, macOS
- Často používaný nástroj na phishing testy

Kľúčové vlastnosti

- Admin web UI (vytváranie kampaní, šablón, landing stránok)
- SMTP / doručovanie emailov (konfigurácia servera alebo relay)
- Sledovanie udalostí (otvorenia, kliky, odoslanie údajov)
- API pre integráciu so SIEM, LMS alebo ticketing systémom
- Podpora certifikátov pre https
- Dashboard na sledovanie prebiehajúcich kampaní
- Jednoduché nasadenie a správa

Inštalácia pre WINDOWS a Linux

WINDOWS

- Stiahuť zip súbor z https://github.com/gophish/gophish/releases
- Extrahovať súbory do žiadaného priečinka

LINUX

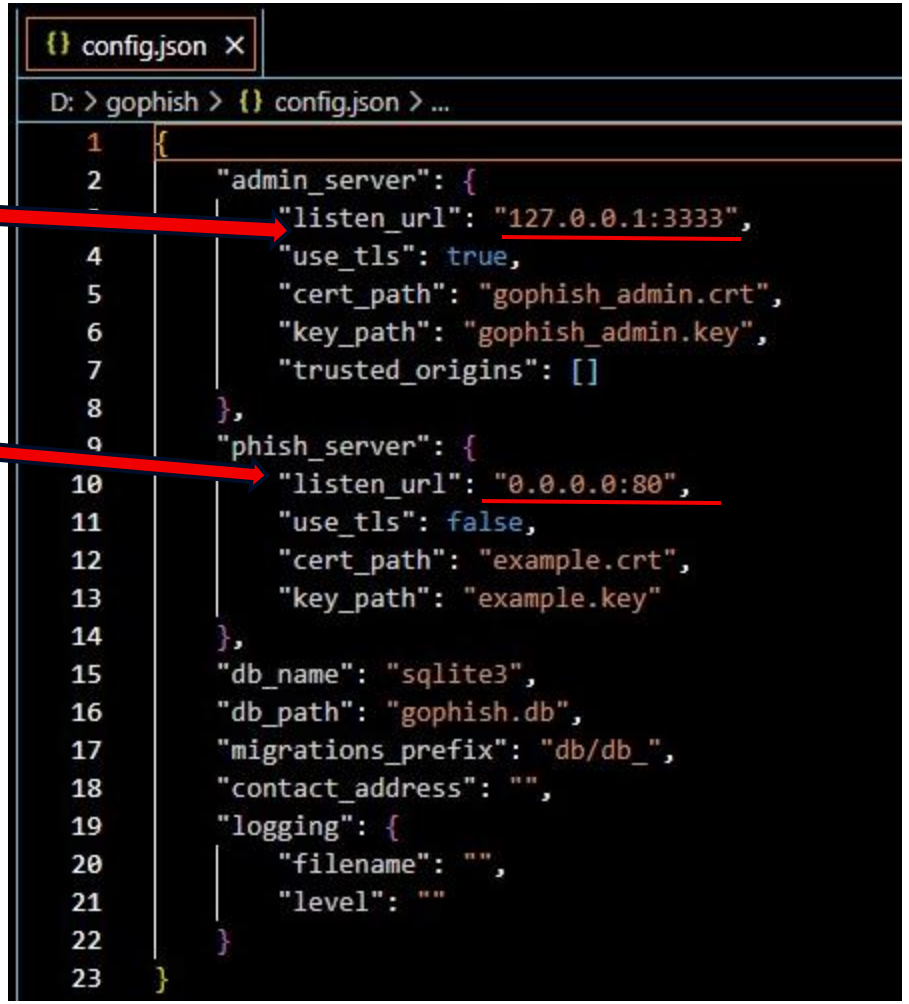
- Presunieme sa do priečinka, kde chceme mať Gophish nainštalovaný
- Spustíme nasledovný skript (môže sa líšiť v závislosti od distribúcie, tento príklad je pre Ubuntu, skript v podstate stiahne Gophish a rozbalí ho v danom priečinku):

```
sudo apt update && sudo apt install -y wget unzip
wget -O gophish-latest.zip "https://github.com/gophish/gophish/releases/download/v0.14.0/gophish-v0.14.0-linux-64bit.zip"
unzip gophish-latest.zip
cd gophish
chmod +x gophish
```

Gophish

Ďlašie kroky inštalácie (spoločné pre WIN aj Linux)

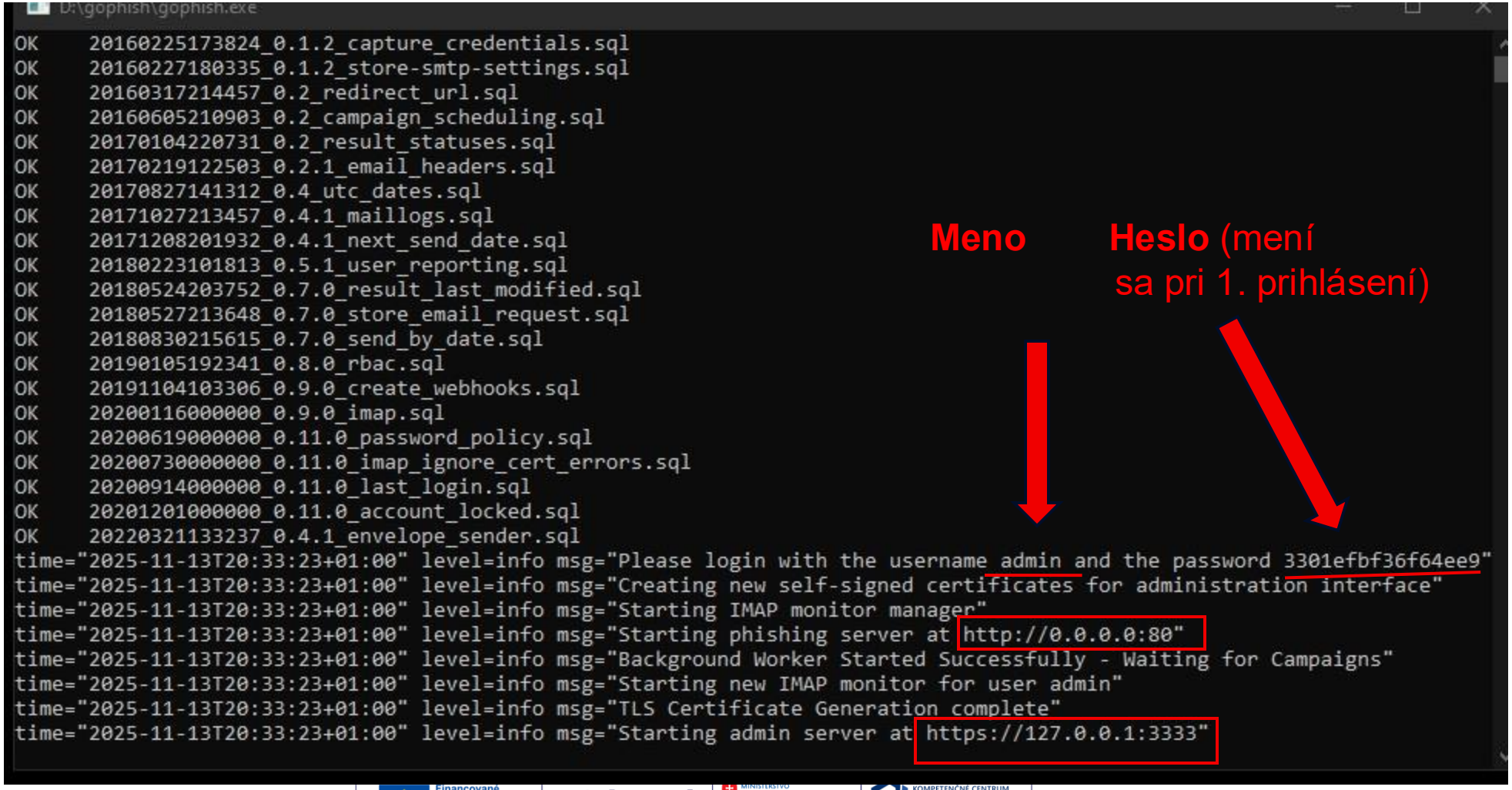
- Súbor config.json upraviť nasledovne:
  - Zmeniť ip na správnu IP nášho servera pre admin účely, aby sme sa mohli vzdialene pripojiť
    - Zmeníme aj port na aký chceme, pozor na overlap
  - Ak máme certifikát na doménu, upravíme port pre kampane na 443, inak necháme na 80
  - Súbor uložíme a zavrieme
- Zapneme gophish:
  - Pre WIN – rozklikneme gophish.exe
  - Pre Linux - príkaz ./gophish



Gophish

Prvé prihlásenie

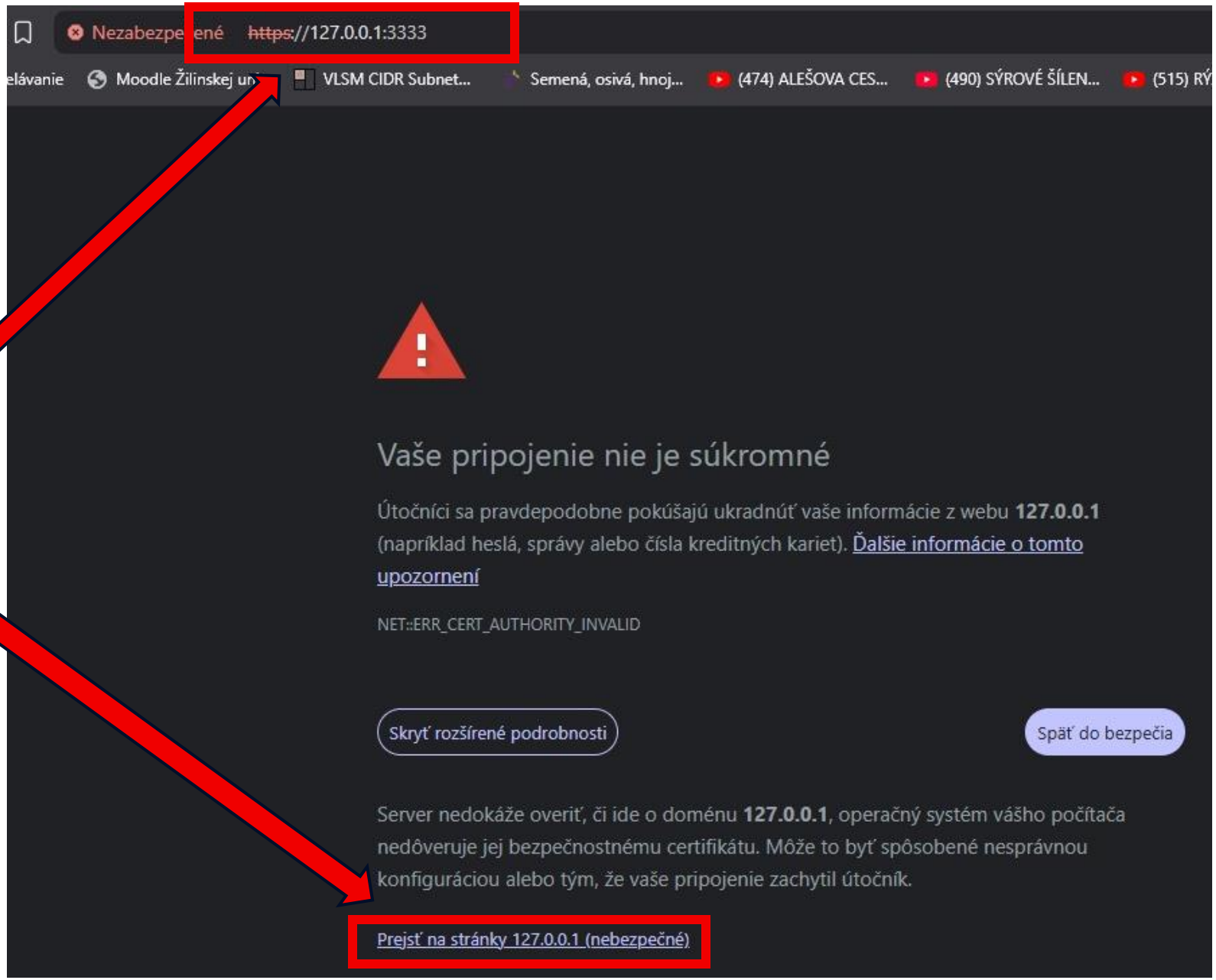
- Po zapnutí nám gophish zobrazí naše prihlasovacie údaje:



Gophish

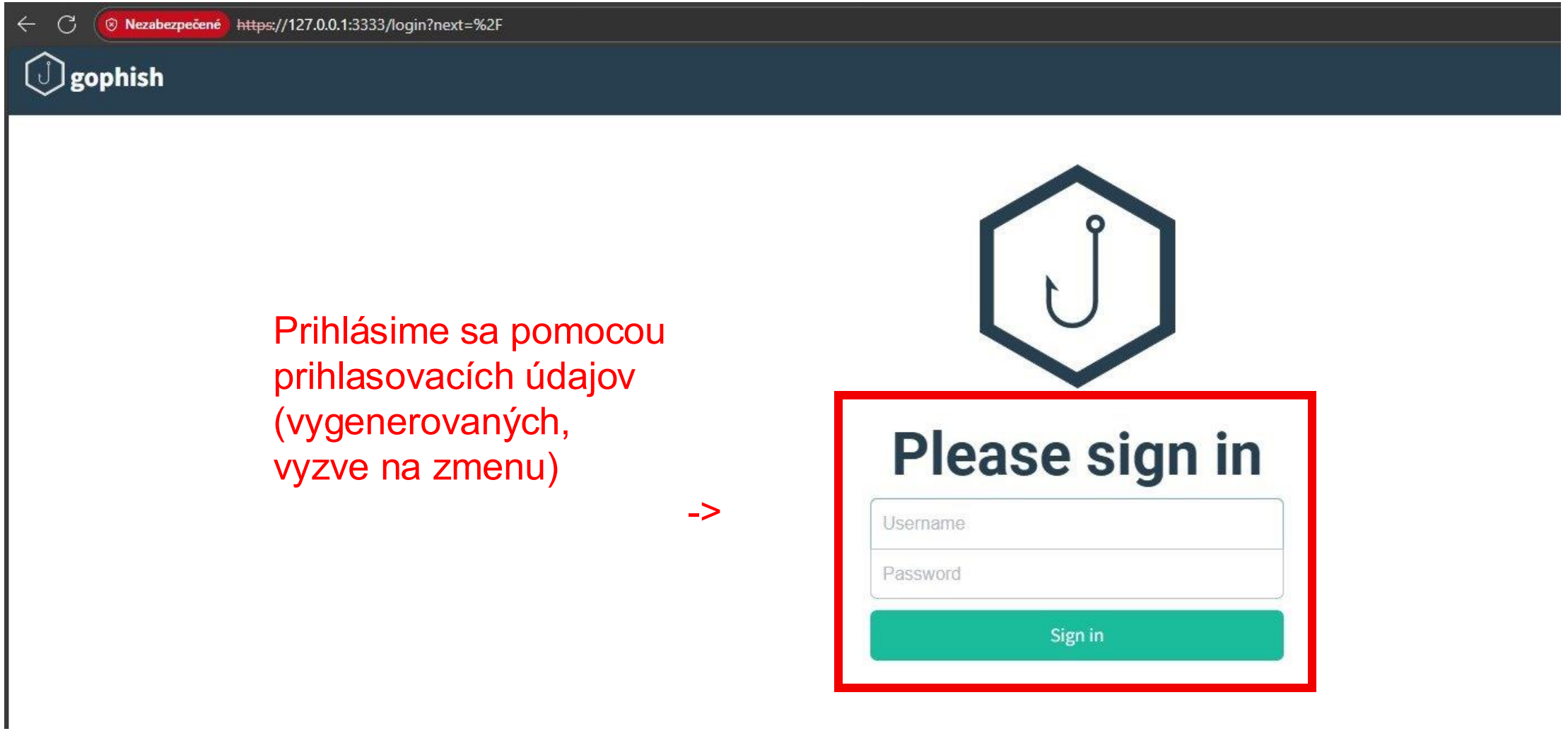
Prvé prihlásenie

- Pomocou zobrazených údajov sa teraz môžeme prihlásiť
- V prehliadači zadáme IP a port, ktoré sme nastavili pre admin server
- Prehliadač nám stránku zobrazí ako nebezpečnú, musíme ,,zobraziť napriek rizikám"
  - Tento ,,probém" sa dá vyriešiť nastavením certifikátov, funkčnosť však neovplyvní, dása doriešiť neskôr



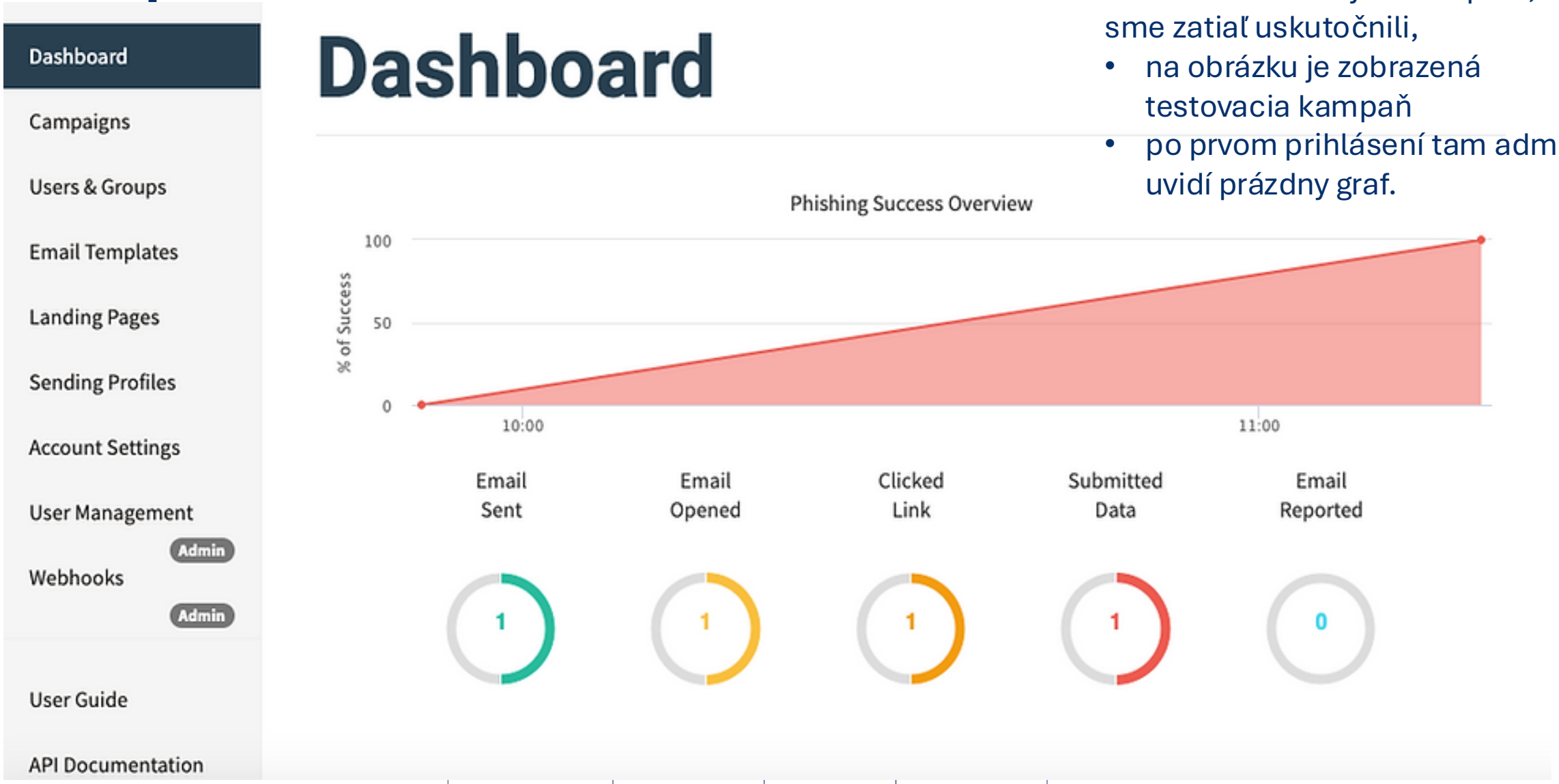
Gophish

Prvé prihlásenie



Gophish

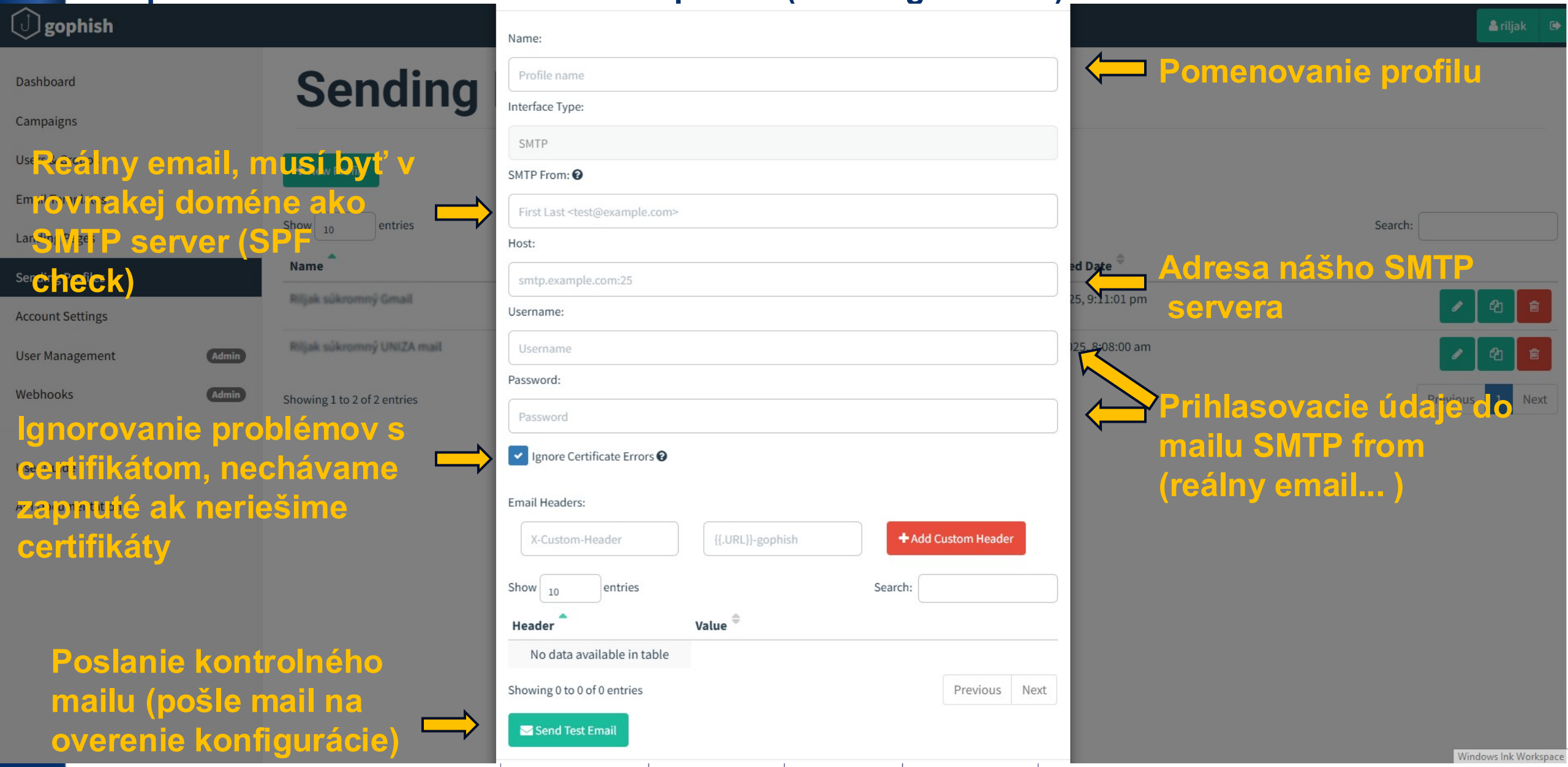
Prvé prihlásenie - úvodná obrazovka



Vidíme stav všetkých kampaní, ktoré sme zatiaľ uskutočnili,

- na obrázku je zobrazená testovacia kampaň
- po prvom prihlásení tam admin uvidí prázdny graf.

Gophish – nastavenie odosielacieho profilu (Sending Profiles)



Reálny email, musí byť v rovnakej doméne ako SMTP server (SPF check)

Ignorovanie problémov s certifikátom, nechávame zapnuté ak neriešime certifikáty

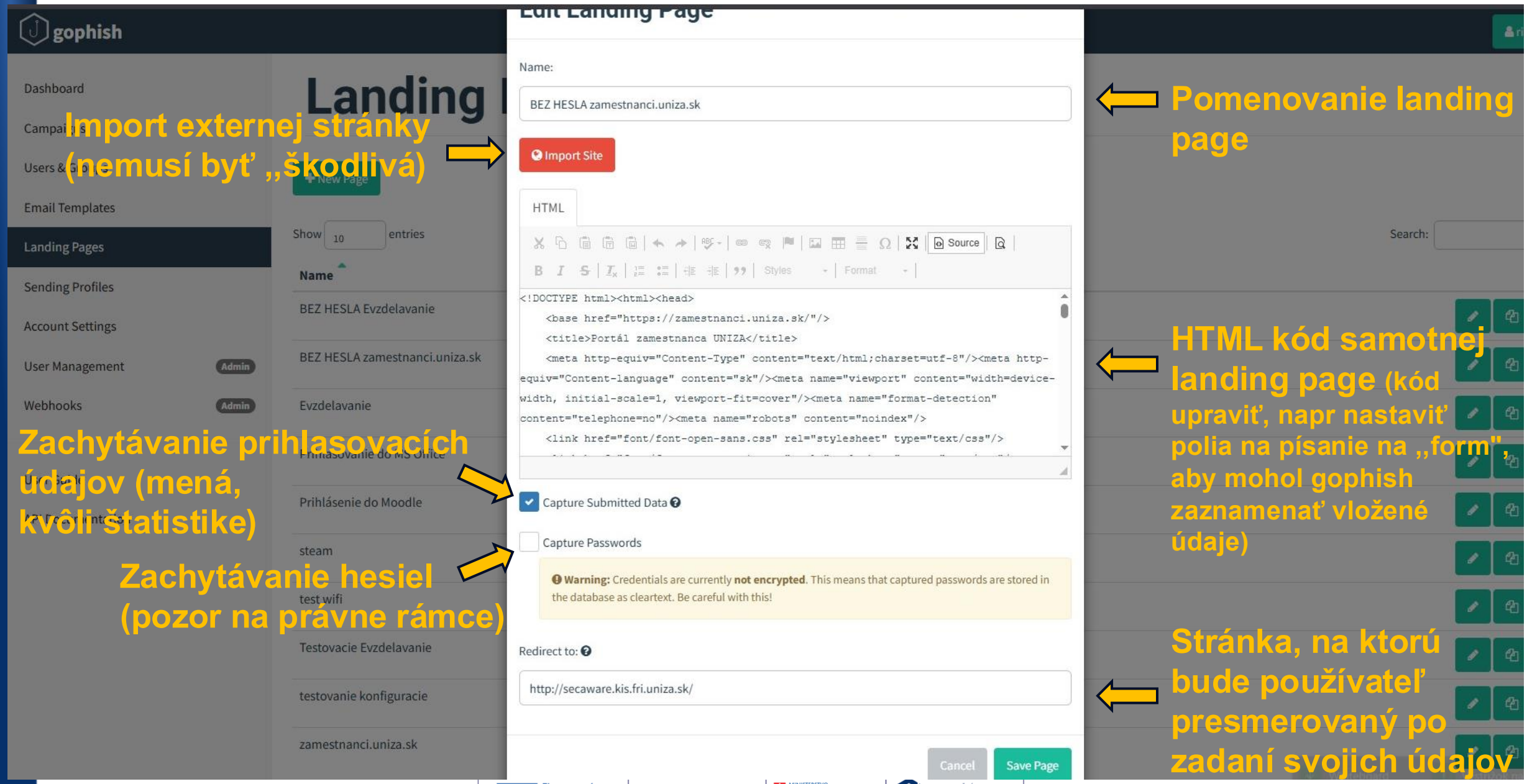
Poslanie kontrolného mailu (pošle mail na overenie konfigurácie)

Pomenovanie profilu

Adresa nášho SMTP servera

Prihlasovacie údaje do mailu SMTP from (reálny email...)

Gophish – nastavenie landing page (Landing Pages)



Import externej stránky (nemusí byť „škodlivá)

Pomenovanie landing page

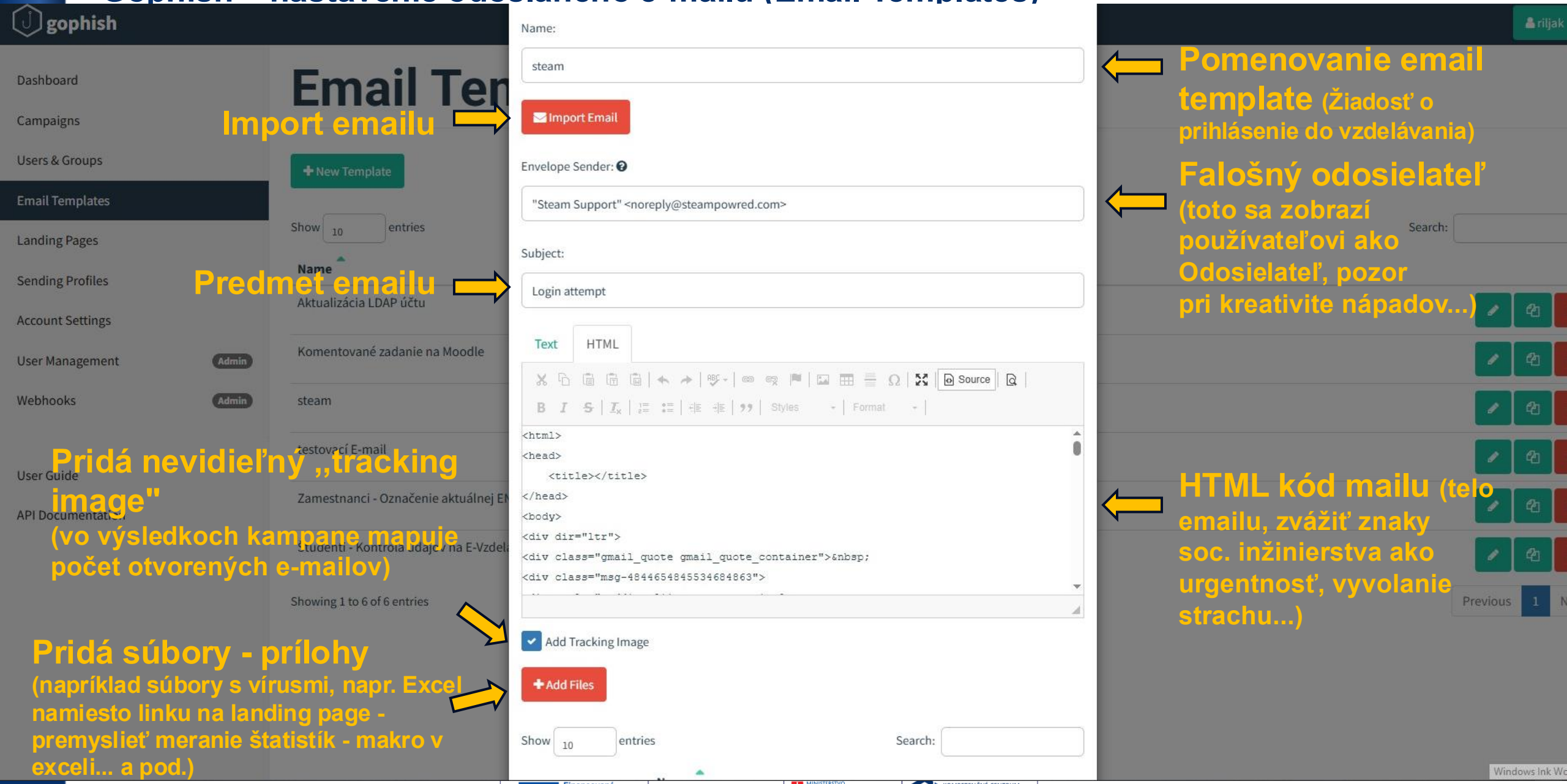
Zachytávanie prihlasovacích údajov (mená, kvôli štatistike)

HTML kód samotnej landing page (kód upraviť, napr nastaviť polia na písanie na „form", aby mohol gophish zaznamenať vložené údaje)

Zachytávanie hesiel (pozor na právne rámce)

Stránka, na ktorú bude používateľ presmerovaný po zadaní svojich údajov

Gophish – nastavenie odoslaného e-mailu (Email Templates)



Import emailu

Predmet emailu

Pridá nevidieľný „tracking image"
(vo výsledkoch kampane mapuje počet otvorených e-mailov)

Pridá súbory - prílohy
(napríklad súbory s vírusmi, napr. Excel namiesto linku na landing page - premyslieť meranie štatistík - makro v exceli... a pod.)

Pomenovanie email template (Žiadosť o prihlásenie do vzdelávania)

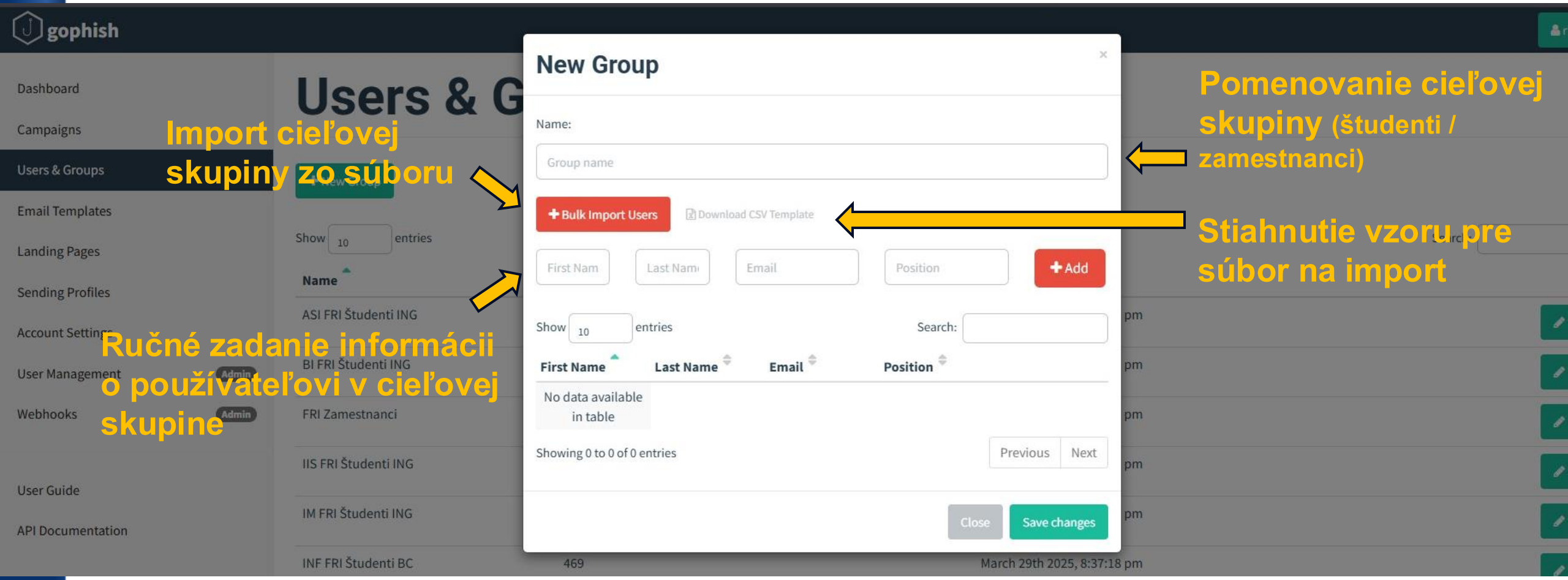
Falošný odosielateľ (toto sa zobrazí používateľovi ako Odosielateľ, pozor pri kreativite nápadov...)

HTML kód mailu (telo emailu, zvážiť znaky soc. inžinierstva ako urgentnosť, vyvolanie strachu...)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Gophish – vytvorenie cieľových skupín (New Group)

Komu ideme kampaň rozoslať...



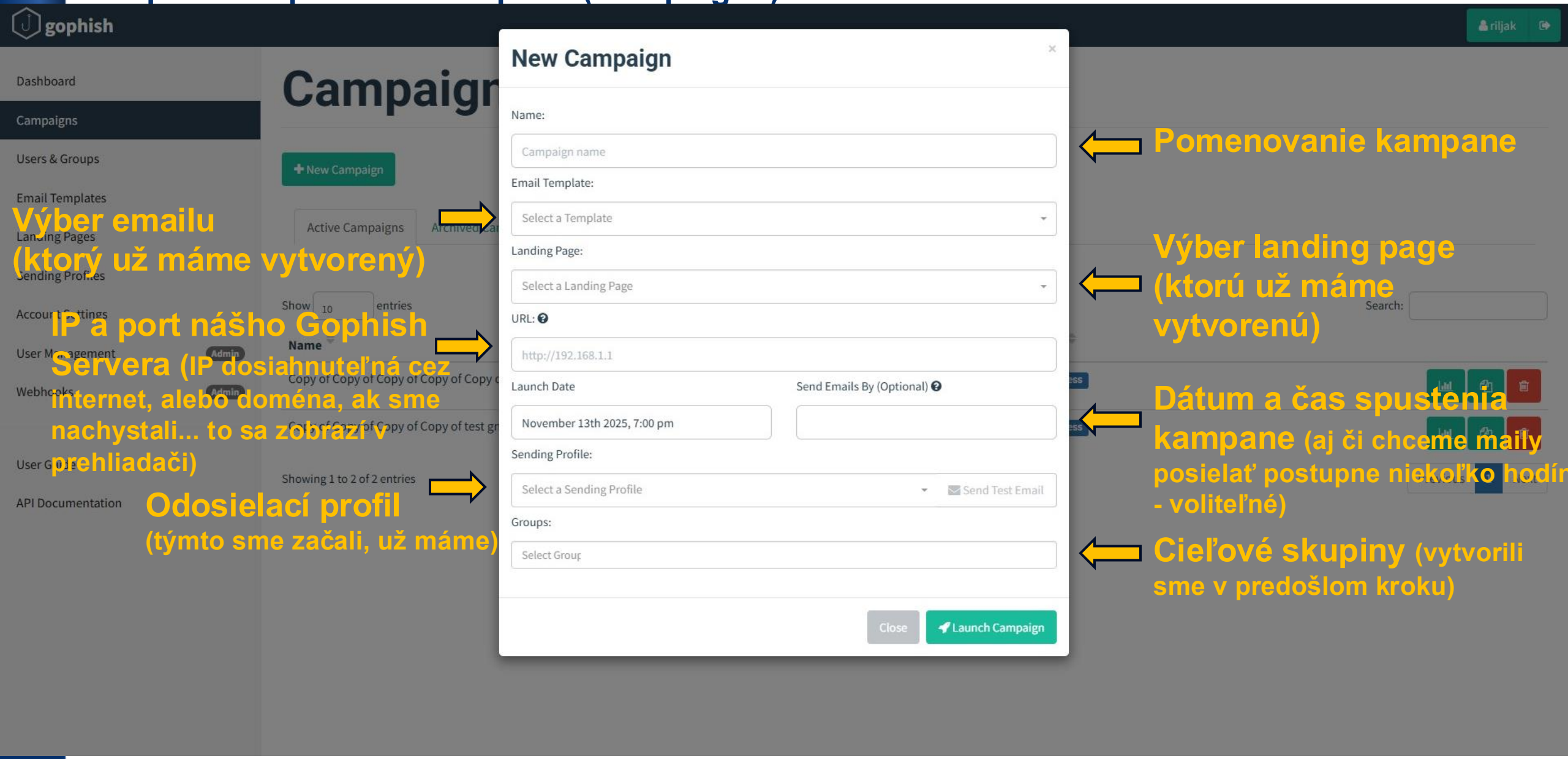
Import cieľovej skupiny zo súboru

Ručné zadanie informácii o používateľovi v cieľovej skupine

Pomenovanie cieľovej skupiny (študenti / zamestnanci)

Stiahnutie vzoru pre súbor na import

Gophish – spustenie kampane (Campaigns)



Výber emailu (ktorý už máme vytvorený)

IP a port nášho Gophish Servera (IP dosiahnuteľná cez internet, alebo doména, ak sme nachystali... to sa zobrazí v prehliadači)

Odosielací profil (týmto sme začali, už máme)

Pomenovanie kampane

Výber landing page (ktorú už máme vytvorenú)

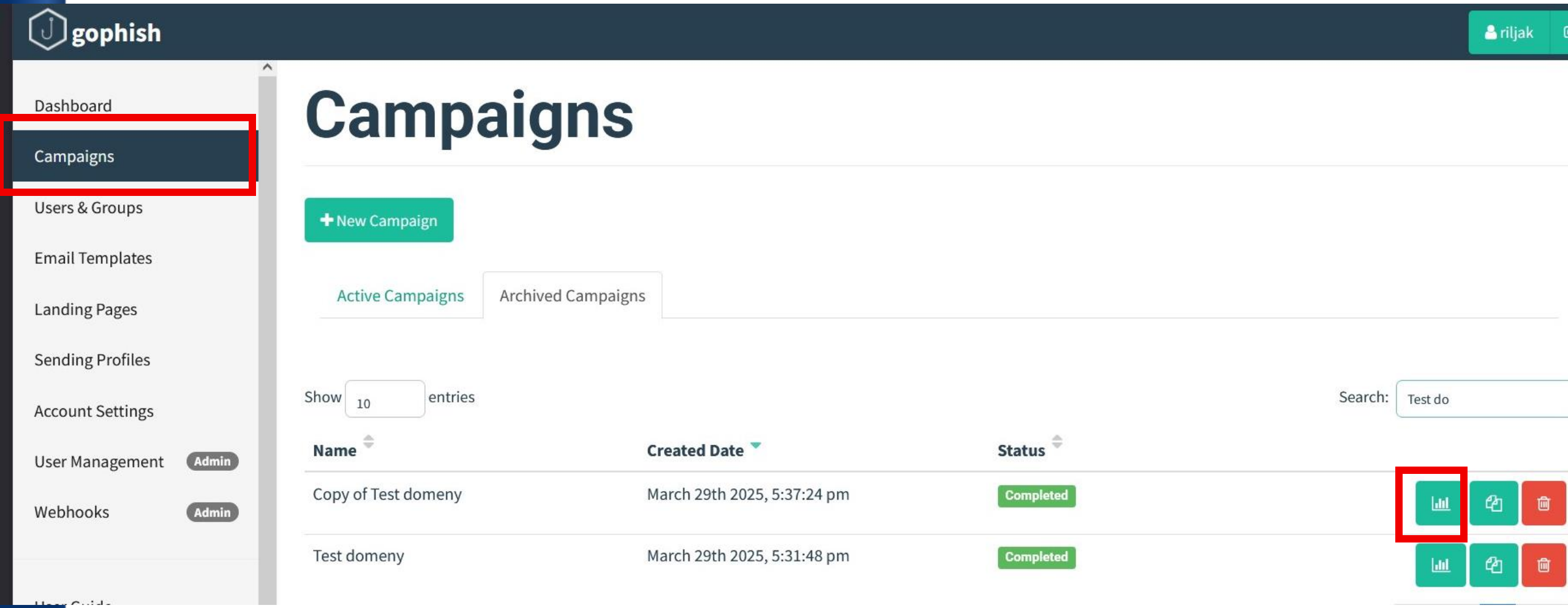
Dátum a čas spustenia kampane (aj či chceme maily posielať postupne niekoľko hodín - voliteľné)

Cieľové skupiny (vytvorili sme v predošlom kroku)

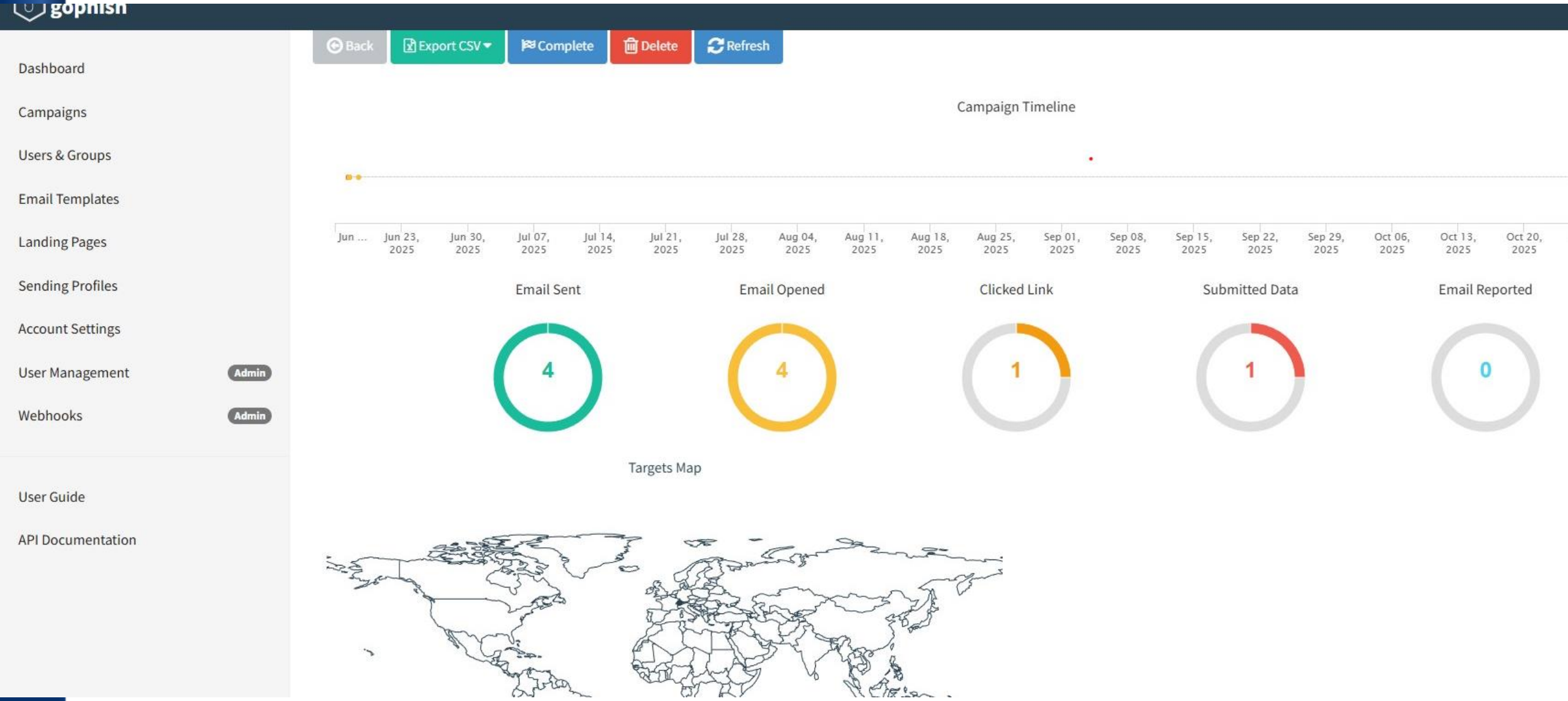
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Gophish – sledovanie kampane

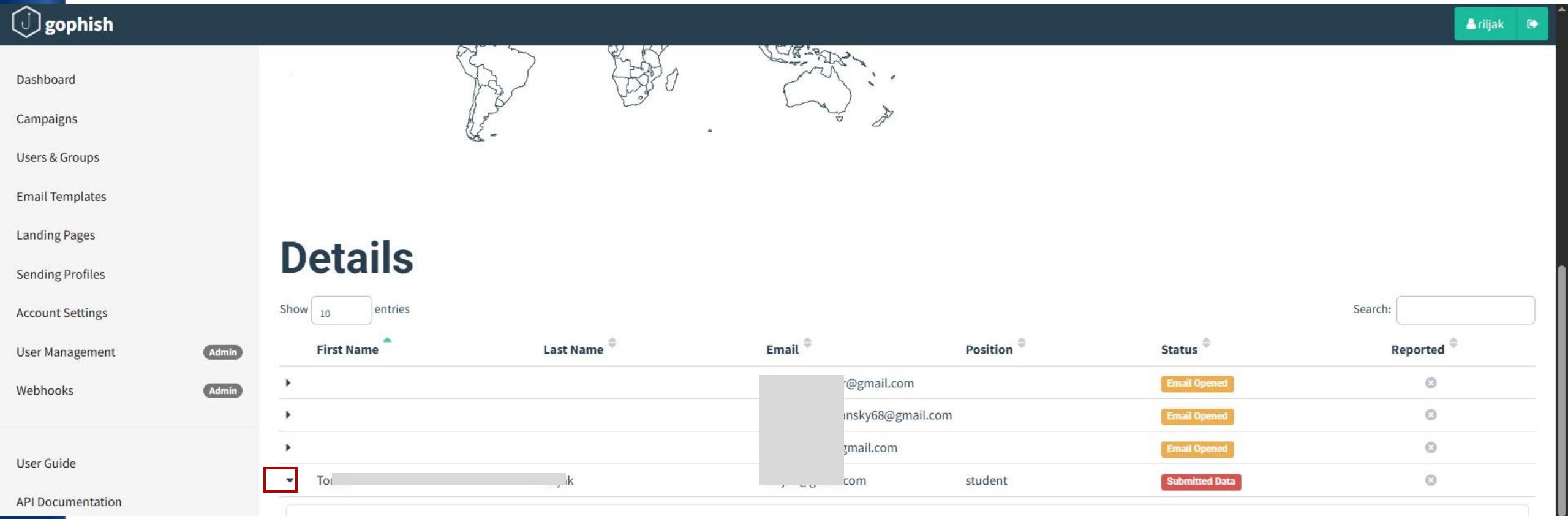
Zobrazenie si výsledkov...



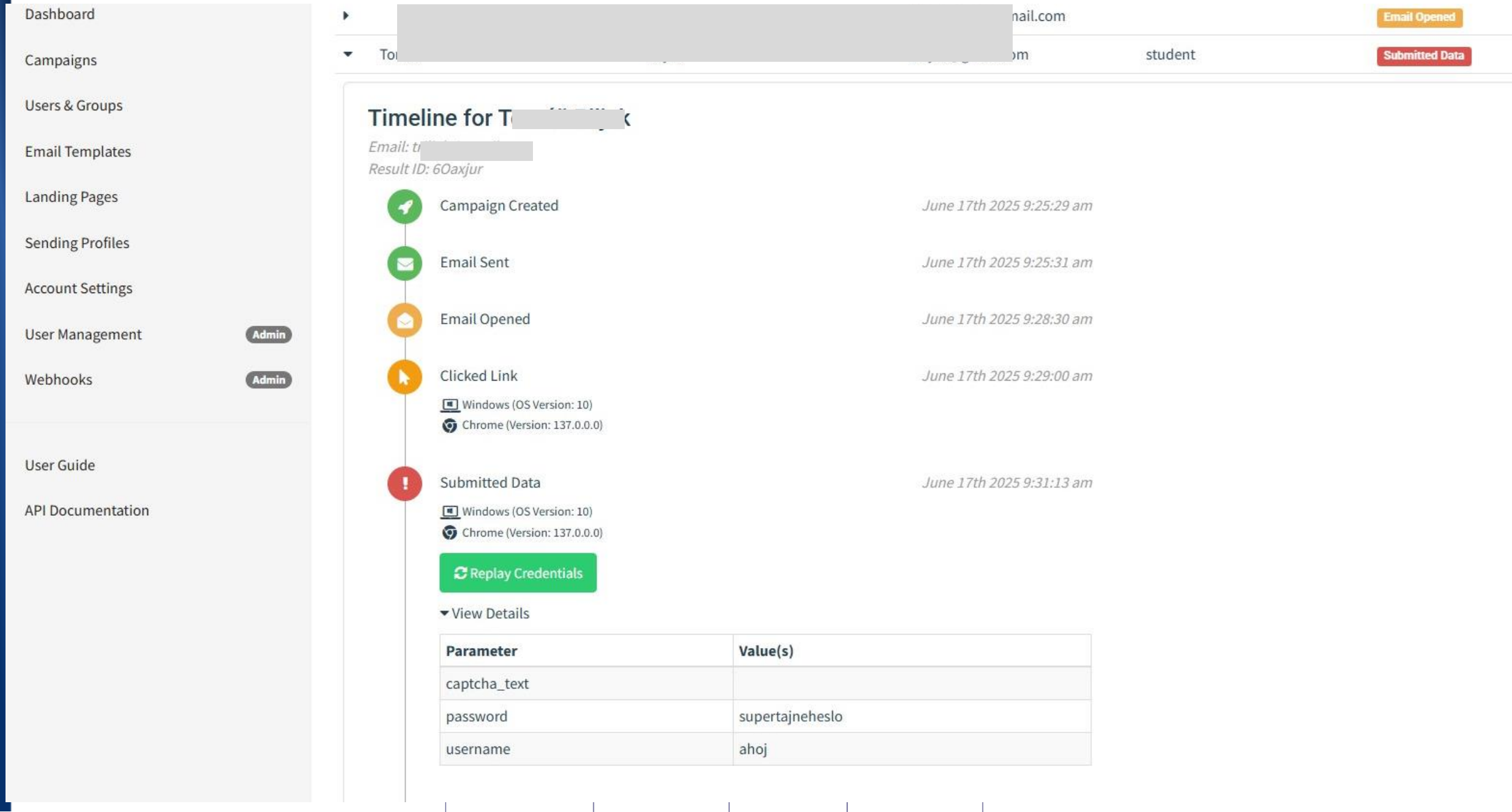
Gophish – sledovanie kampane



Gophish – sledovanie kampane (pokrač.)



Gophish – sledovanie kampane (pokrač., detaily pre používateľa)



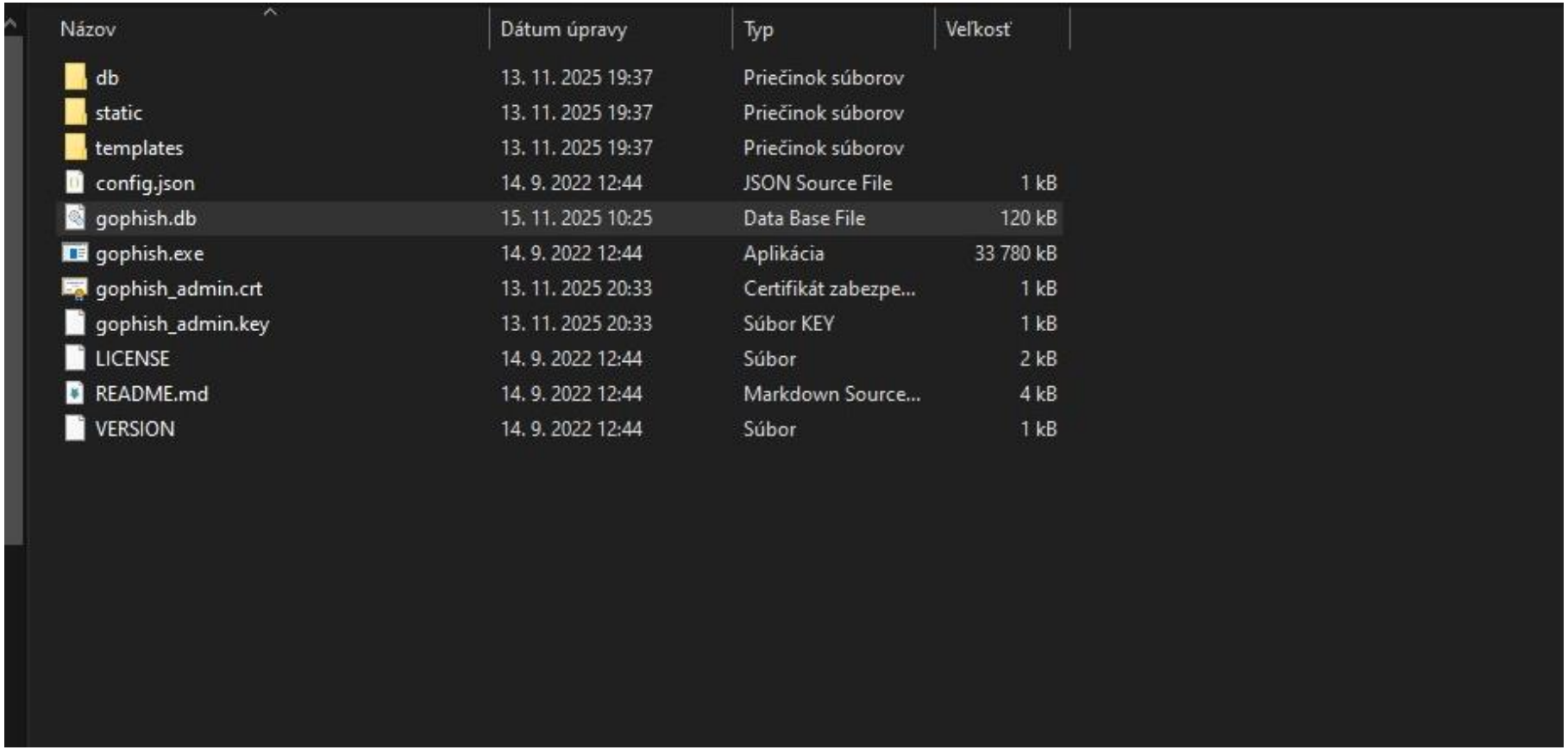
Gophish

Zálohovanie

- V priečinku, kde máme gophish (WIN aj Linux)
- Súbor **gophish.db**

Súbor obsahuje:

- Vytvorené e-maily
- Vytvorené landing pages
- Vytvorené kampane
- Výsledky a priebeh kampaní



Tuning gophish

- **TLS/SSL certifikáty**
  - Nahradenie self-signed certifikátu za Let's Encrypt alebo internú CA
  - Bezpečnejšie Admin UI a realistickejšie phishing landing pages (URL namiestio IP)
- **Webhooky & Integrácie**
  - Posielanie udalostí v reálnom čase (opened, clicked, submitted)
  - Prepojenie so SIEM, ticketing systémami, automatizované reporty
- **Externá databáza (Napr. PostgreSQL)**
  - Gophish používa implicitne SQLite, ktorú môžeme nahradiť externou DB
  - Stabilita pri veľkých kampaniach
  - Jednoduchší backup, audit a správa údajov
- **Reverse Proxy (nginx/apache)**
  - Skrytie interných portov, jednoduchšie nasadenie TLS
  - Podpora viacerých domén a realistických landing stránok

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Bezpečnostné povedomie a tréningy zamestnancov

Zvyšovanie povedomia o KB a testovanie bezpečnosti (Blok VIII)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Jana.Uramova@fri.uniza.sk