



ČVUT

ČESKÉ VYSOKÉ
UČENÍ TECHNICKÉ
V PRAZE

Tvorba metodik a dokumentace v oblasti kybernetické bezpečnosti v prostředí VVŠ

Projekt fondu rozvoje CESNET

České vysoké učení technické

Technická univerzita Ostrava

Univerzita Pardubice

Česká zemědělská univerzita

Cíle projektu

Umožnit členům sdružení CESNET využít příležitost zvýšit úroveň kybernetické bezpečnosti a zvýšit tak prestiž celého sdružení

Dalším záměrem je nastolit zvyšující se trend úrovně kybernetické bezpečnosti

Vytvořit standardizovaný model vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti s možností vzájemného uznávání

Vysvětlit základy provádění analýzy rizik

U členů sdružení vznikne další prostor pro využívání služeb CESNETu

PROČ

Potřeby zavedení bezpečnosti informací – kybernetické bezpečnosti

Vnitřní - Protože chceme (a můžeme)

- Chceme chránit své hodnoty
- Konat s péčí řádného hospodáře (nový Občanský zákoník)
- Řídit a kontrolovat dodavatele
- ...

Vnější - Protože musíme

- Obecně závazné právní předpisy – ZoKB, GDPR
- Oborové požadavky a normy – např. finanční instituce
- Přímý nebo nepřímý požadavek jiné povinnosti

Předpoklady zavedení bezpečnosti informací

V první řadě,

vždy musí být jednoznačná podpora statutárních orgánů a vrcholového vedení!!!

Příprava dokumentace, která umožní vedení VŠ řídit rizika v kybernetickém prostoru, je nutný krok, bez kterého to nebude fungovat

Legislativa a normy

Obecné nařízení o ochraně osobních údajů (GDPR). V Česku přímo zákon č. 110/2019 Sb. o zpracování osobních údajů.

Zákon č. 181/2014 Sb., zákon o kybernetické bezpečnosti a vyhláška č. 82/2018 Sb., vyhláška o kybernetické bezpečnosti

Rodina norem ISO/IEC 27000, soubor mezinárodních standardů zaměřených na řízení informační bezpečnosti v organizacích

Vztah kybernetické bezpečnosti a GDPR

Obecné nařízení o ochraně osobních údajů (GDPR) nabylo účinnosti 25. května 2018.

Osobní údaj je jedním z typů informací v digitální podobě, tedy **AKTIVEM**, které musí být chráněno podle principů informační bezpečnosti

Dalším **AKTIVEM** jsou **informační služby nebo funkce nezbytné pro plnění povinností nezbytných pro zachování práv subjektů dle GDPR**

GDPR podle článku 32 přímo předpokládá bezpečnostní opatření ze systému řízení bezpečnosti informací, tedy kybernetické bezpečnosti, jak organizační, tak technická

Povinné subjekty dle ZoKB

Vysoká škola je orgánem veřejné moci, který není organizační složkou státu.

Pokud vysoká škola provozuje informační systém, který je podle vyhlášky č. 317/2014 Sb. významným informačním systémem, pak se tato VŠ automaticky stává správcem významného informačního systému (VIS).

Správce VIS je orgánem, kterému se ukládají povinnosti v oblasti kybernetické bezpečnosti dle zákona č. 181/2014 Sb.

Kroky ke splnění povinností ZoKB

Zavedení Systému řízení bezpečnosti informací

- Zaslat Úřadu seznam informačních systémů
- Nahlásit kontaktní údaje Úřadu pro kybernetickou a informační bezpečnost
- Zřídit bezpečnostní role a určit do nich osoby
- Ustavit Výbor kybernetické bezpečnosti
- Určit rozsah vlastního SŘBI
- Provést celou Analýzu rizik podle požadavků ZoKB nad určeným rozsahem SŘBI
- Provést návrh architektury Kybernetické bezpečnosti
- Vytvořit Bezpečnostní politiku
- Zavést bezpečnostní opatření v rozsahu svých povinností
- Zpracovat a aktualizovat Bezpečnostní dokumentaci
- Provést interní kontrolu a audit zavedeného SŘBI včetně testů zranitelnosti

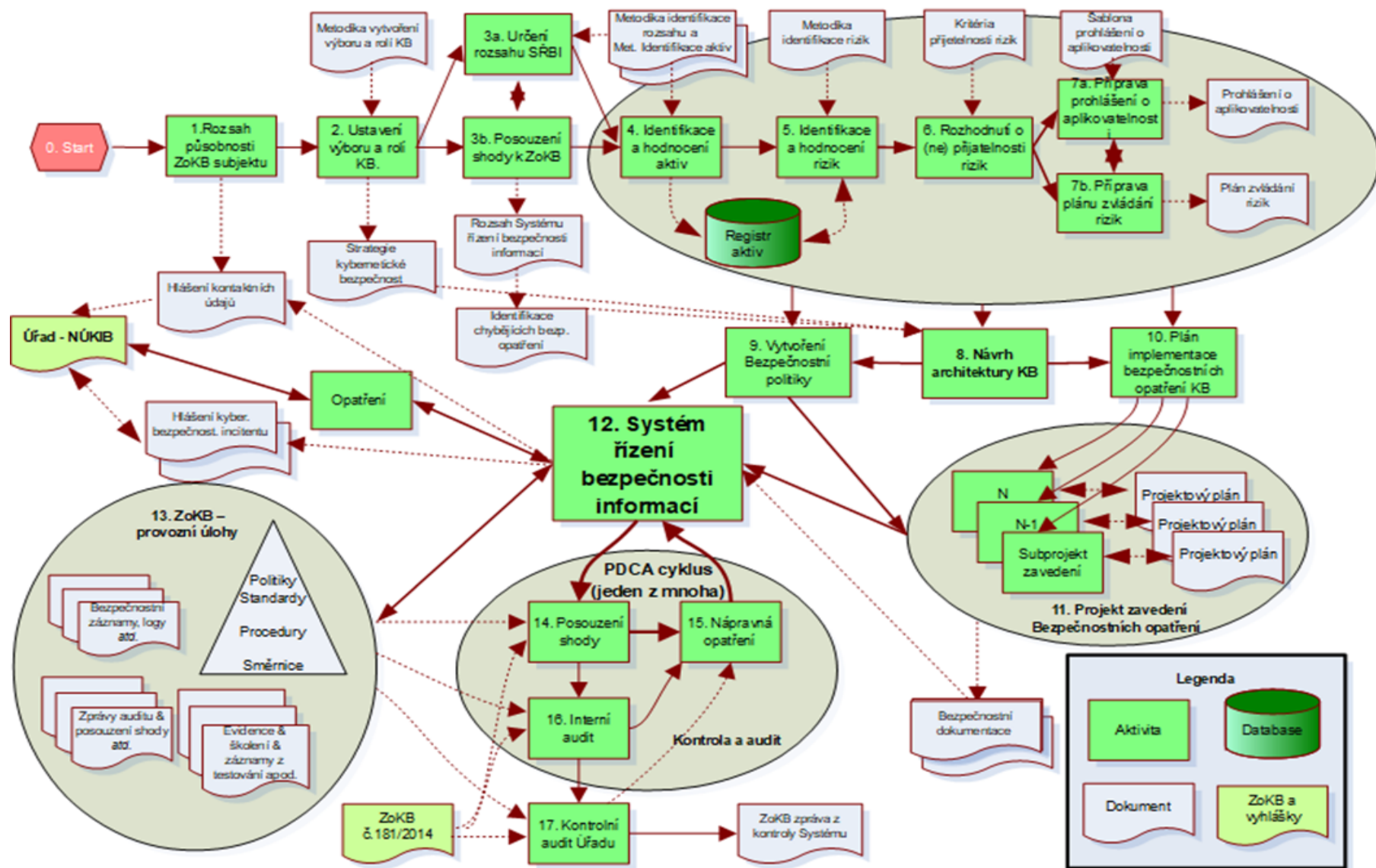
Oblasti řešené v SŘBI

- Organizační bezpečnost vč. definice jednoznačných odpovědností.
- Klasifikace a řízení aktiv určující způsob identifikace a ohodnocení aktiv, způsob klasifikace informací a způsob zacházení s nimi. Oblast postihuje i samotnou „Analýzu rizik“, včetně stanovení její struktury a kritérií hodnocení.
- Bezpečnost lidských zdrojů, jejímž cílem je, aby se s citlivými informacemi seznamoval pouze k tomu určený, prověřený a v oblasti informační bezpečnosti proškolený pracovník.
- Fyzická bezpečnost a bezpečnost prostředí předcházející neautorizovanému přístupu, poškození, znehodnocení, zničení či jiným zásahům do aktiv VŠ.
- Řízení komunikací a řízení provozu, které stanovuje postupy pro řádný a bezpečný provoz prostředků pro zpracování informací VŠ a služeb s tím souvisejících.
- Řízení přístupu, které definuje ochranu a kontrolu přístupu k informacím, službám a procesům.
- Akvizice, vývoj a údržba systémů, která definuje bezpečnostní pravidla vývoje a údržby systémů od fáze návrhu, vývoje, testování až po vlastní provoz a údržbu.
- Zvládání bezpečnostních událostí, které stanovuje postupy reakce na porušení pravidel, bezpečnosti a odolnosti SŘBI.
- Řízení kontinuity činností organizace, které stanovuje rámec prevence a reakce na krizové situace formou plnění plánů kontinuity.
- Zajištění souladu s požadavky, které rozpracovává konkrétní postupy v oblasti zajištění shody přijímaných opatření s legislativou a bezpečnostními i technologickými požadavky.



ČVUT

ČESKÉ VYSOKÉ
UČENÍ TECHNICKÉ
V PRAZE



Vzdělávání zaměstnanců

Dřívější zkušenosti ukazují

- **Různý zájem cílové skupiny „se školit“**
 - Vnímání školení coby
 - nepříjemné „povinnosti“, která „zdržuje od práce“
 - vs.
 - příležitost se dozvědět něco nového
- **Různé vnímání úlohy testů**
 - „zdržování od práce“ a „zpochybnění vlastní erudice“
 - vs.
 - odlišení „absolvování kurzu“ vs. „získané znalosti“
- **Různé pojetí školení (účast vs. znalost)**

Architektura řešení – I

- Modulárnost řešení
 - Sada **malých kurzů** na konkrétní témata
 - Snazší udržovatelnost
 - jednotlivé kurzy mohou mít různé autory
 - Snazší rozšiřitelnost
 - nová témata řešena jako nové kurzy
 - neovlivňuje již existující
 - **Kombinace** dílčích kurzů **do větších celků**
 - Znovupoužitelnost vytvořených materiálů
 - Např. pro další cílové skupiny
- Platforma Moodle

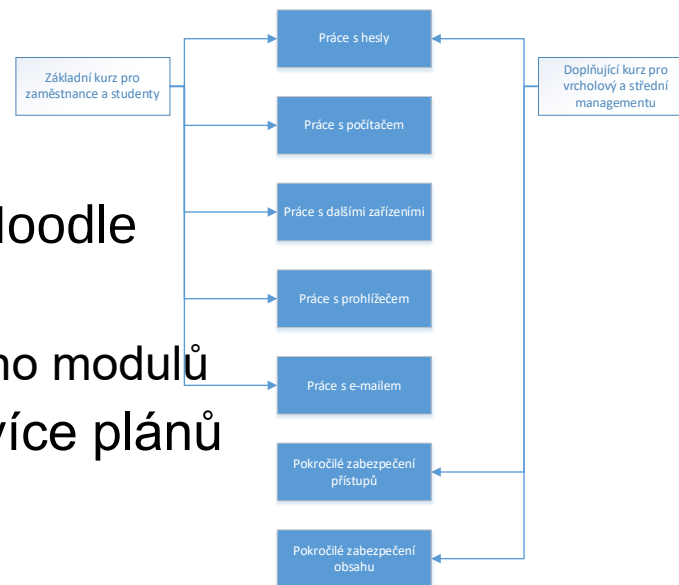
Architektura řešení – II

- Rozlišení „Plánu“ a „Modulu“

- V obou případech se jedná o kurz Moodle
- Plán se skládá z více modulů
 - Zápis do plánu = zápis do všech jeho modulů
- Jeden modul může být zařazen do více plánů

- Příklad

- Plány:
 - „Úvodní školení zaměstnanců“, „Opakované školení zaměstnanců“, „Pokročilá témata pro management“, ...
- Moduly:
 - „Používání e-mailu“, „Práce s hesly“, ...



Standardizace struktury modulů

- Každý modul se skládá ze tří částí
 - Textová část
 - Test
 - Certifikát

Struktura textové části

- Textová část
 - Skládá se z činností typu „Přednáška“
 - **Název** každé přednášky = jednoduché pravidlo, kterým se má školený řídit
 - Jednotlivé stránky přednášky = detailnější informace k danému pravidlu
 - **Co** pravidlo přesně znamená
 - **Proč** by se daným pravidlem měl školený řídit
 - **Jak** může dané pravidlo dodržet

Kurz: Práce s e-mailem

https://moodle.upce.cz/moodle/course/view.php?id=...

Moodle Moje stránka Kalendář Kontakty Mahara Kurzy Čeština (cs)

Práce s e-mailem

Titulní stránka / Moje kurzy / IT Modul - Práce s e-mailem

Navigace

- Titulní stránka
- Nástěnka
- Moje kurzy
 - IT Modul - Práce s e-mailem
 - Účastníci
 - Oznaky
 - Známky
 - IT Modul - Práce s prohlížečem
 - IT Modul - Práce s dalšími zařízeními
 - IT Modul - Práce s počítačem
 - IT Plán - Základní kurz ZMC/STU
 - IT Modul - Práce s hesly

Váš pokrok

Úvod

Tento kurz Vás seznámí se základními pravidly bezpečného používání elektronické pošty.

Elektronická pošta stále ještě představuje jeden z nejvýznamnějších komunikačních kanálů a ze strany útočníků představuje nejjednodušší způsob realizace útoku. Vychází z toho, že s elektronickou poštou pracuje běžný uživatel daleko častěji, než s jinými prostředky, a spoléhají na selhání lidského faktoru.

Je proto vhodné si základní pravidla chování v rámci tohoto kurzu připomenout.

Autorem vzdělávacího modulu je ...

Oznámení

Textová část

- Pracovní adresu využívejte jen pro pracovní účely
- Zkontrolujte, zda se jedná o očekávatelný e-mail
- Neklikejte a nezažívejte své heslo na neznámé adresy
- Při přeposílání ověřte historii e-mailu a adresáty
- Buďte opatrní při otevírání příloh

Skóre kurzu

1

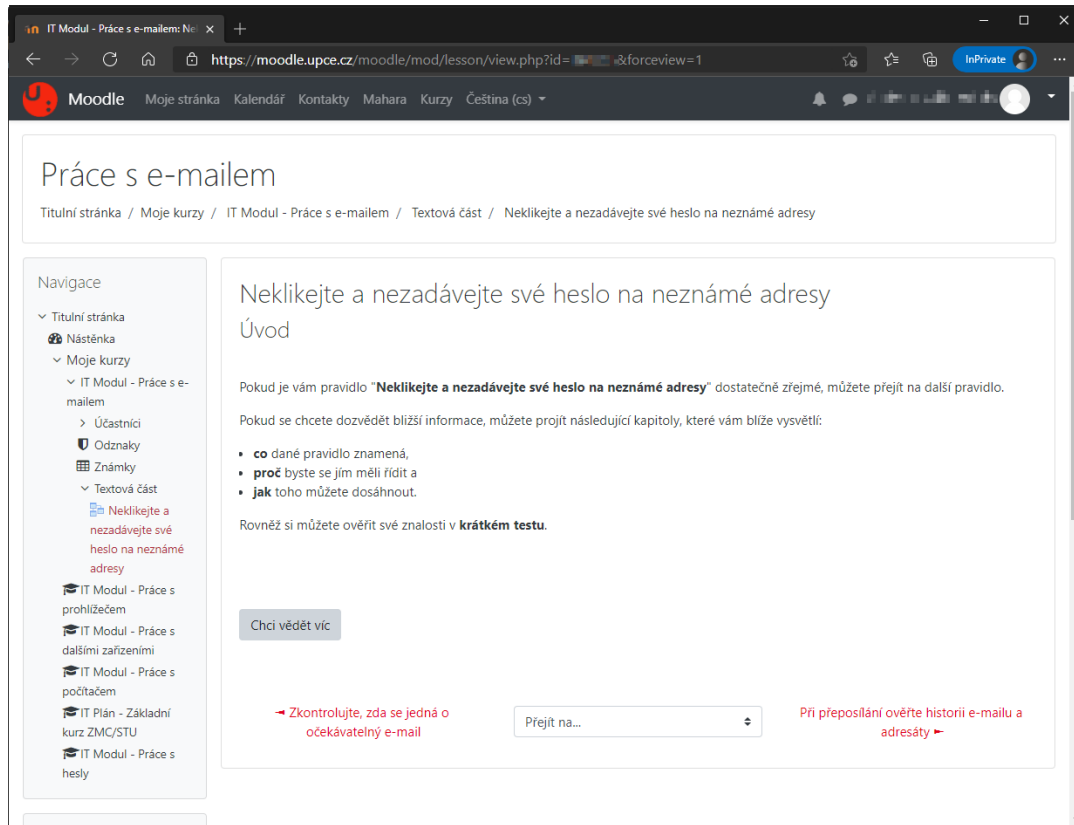
Novicius

3^{SP}

Absolvování kurzu

- Trojí možnost absolvování
 - **Rychlým proklikáním** úvodních stránek přednášek
 - = vychází vstříc těm, kteří „to chtějí mít rychle odbyté“
 - seznámí se jen s naprostým minimem informací
 - Chování v souladu s pravidly → bezpečné chování
 - **Pročtením podrobnějších stránek**
 - Vychází vstříc těm, kdo se chtějí dozvědět, co se za pravidlem skrývá
 - **Absolvováním testu**
 - Vychází vstříc těm, kdo potřebují prokázat znalost
- Vygenerování certifikátu odpovídající úrovni absolvování

Rychlý průchod



IT Modul - Práce s e-mailem: Ne x +

https://moodle.upce.cz/moodle/mod/lesson/view.php?id=...&forceview=1

Moodle Moje stránka Kalendář Kontakty Mahara Kurzy Čeština (cs)

Práce s e-mailem

Titulní stránka / Moje kurzy / IT Modul - Práce s e-mailem / Textová část / Neklikejte a nezaďávejte své heslo na neznámé adresy

Navigace

- Titulní stránka
- Nástěnka
- Moje kurzy
 - IT Modul - Práce s e-mailem
 - Účastníci
 - Oznaky
 - Známky
 - Textová část
 - Neklikejte a nezaďávejte své heslo na neznámé adresy**
 - IT Modul - Práce s prohlížečem
 - IT Modul - Práce s dalšími zařízeními
 - IT Modul - Práce s počítačem
 - IT Plán - Základní kurz ZMC/STU
 - IT Modul - Práce s hesly

Neklikejte a nezaďávejte své heslo na neznámé adresy

Úvod

Pokud je vám pravidlo "**Neklikejte a nezaďávejte své heslo na neznámé adresy**" dostatečně zřejmé, můžete přejít na další pravidlo.

Pokud se chcete dozvědět bližší informace, můžete projít následující kapitoly, které vám blíže vysvětlí:

- **co** dané pravidlo znamená,
- **proč** byste se jím měli řídit a
- **jak** toho můžete dosáhnout.

Rovněž si můžete ověřit své znalosti v **krátkém testu**.

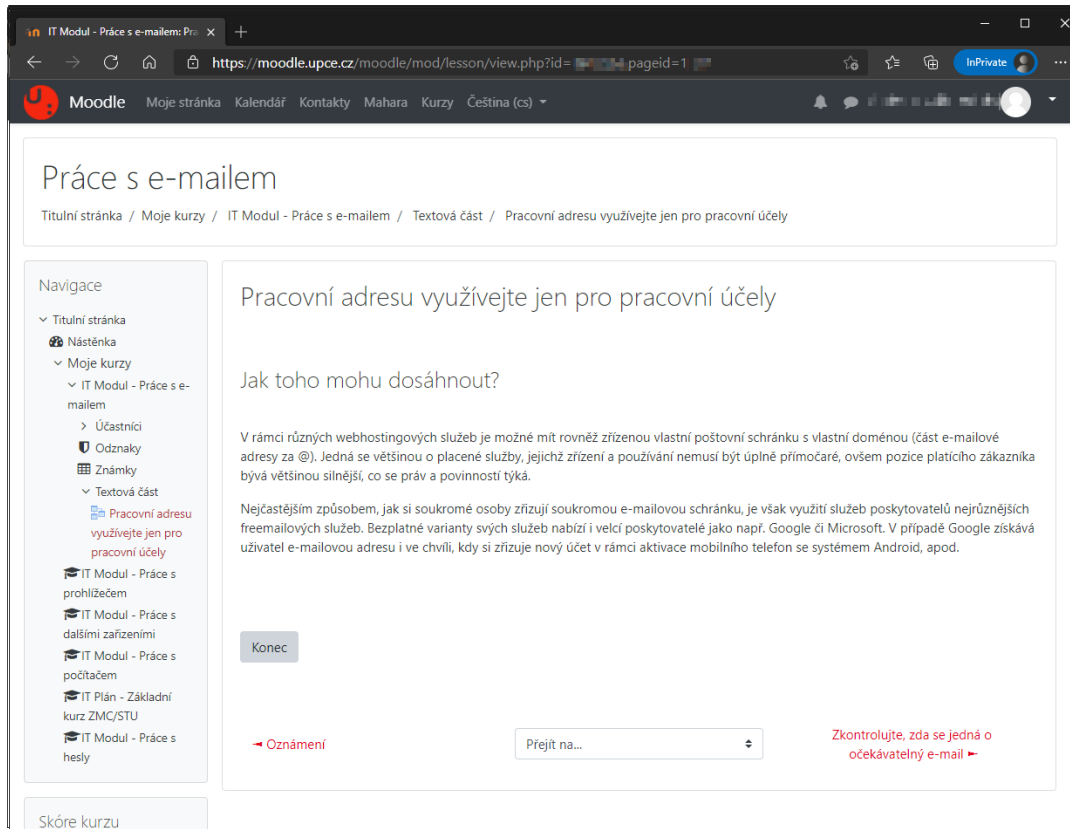
Chci vědět víc

← Zkontrolujte, zda se jedná o očekávatelný e-mail

Přejít na...

Při přeposílání ověřte historii e-mailu a adresáty →

Detailní průchod



IT Modul - Práce s e-mailem: Pr...

https://moodle.upce.cz/moodle/mod/lesson/view.php?id=... pageid=1

Moodle Moje stránka Kalendář Kontakty Mahara Kurzy Čeština (cs)

Práce s e-mailem

Titulní stránka / Moje kurzy / IT Modul - Práce s e-mailem / Textová část / Pracovní adresu využívejte jen pro pracovní účely

Navigace

- Titulní stránka
- Nástěnka
- Moje kurzy
 - IT Modul - Práce s e-mailem
 - Účastníci
 - Oznaky
 - Známky
 - Textová část
 - Pracovní adresu využívejte jen pro pracovní účely**
 - IT Modul - Práce s prohlížečem
 - IT Modul - Práce s dalšími zařízeními
 - IT Modul - Práce s počítačem
 - IT Plán - Základní kurz ZMC/STU
 - IT Modul - Práce s hesly

Pracovní adresu využívejte jen pro pracovní účely

Jak toho mohu dosáhnout?

V rámci různých webhostingových služeb je možné mít rovněž zřízenou vlastní poštovní schránku s vlastní doménou (část e-mailové adresy za @). Jedná se většinou o placené služby, jejichž zřízení a používání nemusí být úplně přímočaré, ovšem pozice platícího zákazníka bývá většinou silnější, co se práv a povinností týká.

Nejčastějším způsobem, jak si soukromé osoby zřídí soukromou e-mailovou schránku, je však využití služeb poskytovatelů nejrůznějších freemailových služeb. Bezplatné varianty svých služeb nabízí i velcí poskytovatelé jako např. Google či Microsoft. V případě Google získává uživatel e-mailovou adresu i ve chvíli, kdy si zřizuje nový účet v rámci aktivace mobilního telefonu se systémem Android, apod.

Konec

→ Oznámení

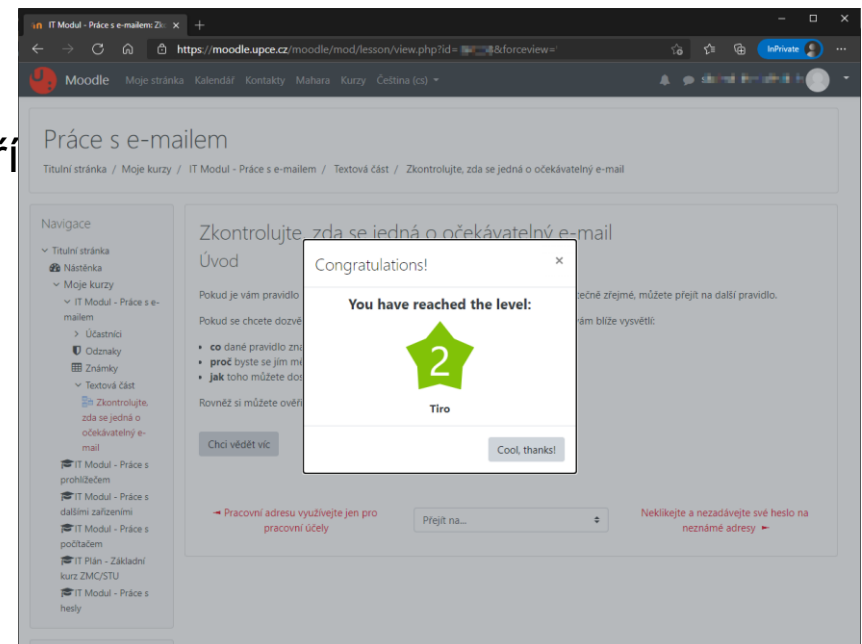
Přejít na...

Zkontrolujte, zda se jedná o očekávaný e-mail →

Skóre kurzu

Aktuální výzvy

- Snaha zatraktivnit kurzy s využitím gamifikace
 - Přičítání bodů za průchod kurzem
 - Free verze pluginu *Level up!*
- Opakované školení
 - Lze zatraktivnit školení pro ty, kteří jej již v minulosti absolvovali?





ČVUT

ČESKÉ VYSOKÉ
UČENÍ TECHNICKÉ
V PRAZE

Děkuji za pozornost

Ing. Jiří Richter