MUNI

Bezpečnost lidských zdrojů

Interpretace § 9 vyhlášky č. 82/2018 Sb.

Metodická inspirace

PS-3 Osvěta uživatelů

KYBER 21

CRP-KYBER21

Obsah materiálu

Cílem tohoto materiálu je sloužit jako metodická inspirace pro rozvahy o dalších podobách a postupech rozvoje kyberbezpečnostních dovedností a prohlubování kyberbezpečnostního povědomí (*cyber security awareness, CSA*) různých cílových skupin v rámci VVŠ. Dokument v úvodu obsahuje podrobnou interpretaci vyhlášky *č. 82/2018 Sb.*, o kybernetické bezpečnosti, s ohledem na naplnění požadavků bezpečnosti lidských zdrojů, zpracovanou JUDr. Mgr. Jakubem Haraštou, Ph.D.

1. Bezpečnost lidských zdrojů (*interpretace vyhlášky*)

S ohledem na naplnění požadavků vymezených v § 9 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti.

1.1 Přehled zohledněných dokumentů

A. Právní úprava:

→ Vyhláška Národního bezpečnostního úřadu č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) – dále jen „neúčinná VoKB“ nebo „neúčinná vyhláška“

→ Vyhláška Národního úřadu pro kybernetickou a informační bezpečnost č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) – dále jen „VoKB“ nebo „vyhláška“

Komentář: Textace § 9 VoKB a §9 neúčinné VoKB je velice podobná. V rámci přijetí VoKB došlo ke specifikaci některých požadavků stanovených vyhláškou. Neúčinná VoKB obsahovala v odst. 1 povinnosti pro orgány a osoby vymezené v §3 písm. c) až e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a v odst. 2 další povinnosti pro orgány a osoby vymezené v §3 písm. c) a d). VoKB nadále stanovuje povinnosti pouze „povinným osobám“, změna tak spočívala primárně v racionalizaci textace. Východiska se neměnila, proto je možné při plnění povinností dle VoKB vyjít z případného minulého plánu plnění povinností dle neúčinné VoKB.

B. Přípravné (nelegislativní) dokumenty:

→ Odůvodnění (další příloha materiálu) návrhu vyhlášky o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti. Dostupné z https://apps.odok.cz/veklep-detail?pid=KORN9MHFXCU5

→ **Komentář:** K VoKB bohužel neexistují žádné přípravné dokumenty (důvodová zpráva, závěrečná zpráva z hodnocení dopadů regulace). Vzhledem k podobnosti právní úpravy ve VoKB a v neúčinné VoKB je možné přihlédnout k dokumentům týkajícím se právě neúčinné vyhlášky.

C. Rozhodovací praxe:

→ Rozsudek Nejvyššího soudu ze dne 26. 10. 2006, sp. zn. 21 Cdo 182/2006

Komentář: Při obecné nedostupnosti rozhodovací praxe týkající se přímo zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a jeho prováděcích předpisů, zohledňuji rozhodovací praxi, která se týká problematiky stanovování povinností vnitřními předpisy (tedy obecně problematiky pracovněprávních předpisů). V uvedeném rozhodnutí Nejvyšší soud uvedl, že není předepsán žádný konkrétní způsob pro seznámení zaměstnanců s vnitřními předpisy – právní úpravy v této oblasti (pracovní právo) tak vychází z toho, že zaměstnavatel sám ví nejlépe, jakým způsobem by se jeho zaměstnanci měli seznamovat s vnitřními předpisy (např. bezpečnostní politikou).

D. Komentářová literatura:

→ KOLOUCH, Jan, BAŠTA, Pavel a kolektiv. *CyberSecurity*. Praha: CZ.NIC, 2019.

→ MAISNER, Martin a Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Praha: Wolters Kluwer, 2015.

Komentář: Kniha od Maisnera a Vlachové představuje jediný „klasický" komentář na českém trhu, který byl publikován v malém časovém odstupu od samotného zákona č. 181/22014 Sb. a od jeho prováděcích předpisů. Obecně se jedná o shrnutí důvodové zprávy s malou přidanou hodnotou. Druhá publikace pak je zařazena z důvodu, že autoři usilovali mimo jiné i o snahu poskytnout výklad ustanovení zákona č. 181/2014 Sb. a prováděcích předpisů. Kniha tak má komentářové prvky.

E. Další relevantní dokumenty

→ ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečností informací – Požadavky.*

→ ČSN ISO/IEC 27002. *Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací.*

→ LOUTOCKÝ, Pavel a Kamil MALINKA. Bezpečnost ICT ve vnitřních předpisech a školení zaměstnanců. *Revue pro právo a technologie*, 2016, č. 14, s. 45-64.

→ Minimální bezpečnostní standard – podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti. Dostupné z: https://archi.gov.cz/_media/dokumenty:2020-07-17_minimalni-bezpecnostni-standard_v1.0.pdf

→ Pomůcka k auditu bezpečnostních opatření podle zákona o kybernetické bezpečnosti. Dostupné z: https://nukib.cz/download/publikace/podpurne_materialy/vkbchecklistfinalv21rev.pdf

1.2 Interpretace požadavků vyhlášky

Ustanovení § 9 VoKB stanovuje povinné osobě (což je orgán nebo osoba, která je povinna zavést bezpečnostní opatření dle ZoKB) určité povinnosti v rámci oblasti řízení lidských zdrojů. S přihlédnutím k výše uvedeným dokumentům se v následujícím dokumentu pokusím nastínit, jakým způsobem lze jednotlivé povinnosti v této oblasti naplnit.[1]

Politika bezpečnosti lidských zdrojů je jednou ze součástí celkové bezpečnostní politiky organizace. V rámci existujících zákonných, podzákonných nebo podpůrných dokumentů není stanovena závazná struktura bezpečnostní dokumentace (a to jak v oblasti bezpečnosti lidských zdrojů, tak mimo ni). Důležité je tak zajištění obsahu dokumentace v souladu s požadavky ZoKB a prováděcích předpisů. Je důležité uvést, že požadavky se netýkají pouze existence příslušné dokumentace – podobně jako v případě certifikace podle norem ISO/IEC 27001 a 27002, je nutné v prvé řadě zajistit soulad vnitřní dokumentace s externími požadavky a ve druhé řadě zajistit, že praktický výkon je v souladu s touto dokumentací.

Vzhledem k tomu, že lidský faktor je považován za jeden z hlavních nedostatků v rámci jakýchkoli bezpečnostních opatření, klade si tato úprava za cíl zajistit existenci souvislého řetězce opatření.[2] Jeho existence (tedy příprava formou dokumentace a následné vynucování postupů v dokumentací zakotvených) směřuje ke snížení rizika, že dojde k selhání lidského faktoru. Zastřešujícím cílem tak je nikoli zcela eliminovat lidské chyby – to je pochopitelně nemožné – ale snížit jejich výskyt a v případě výskytu snížit jejich potenciální dopad. Bezpečnost lidských zdrojů je v tomto smyslu součástí organizačních opatření.[3]

---

[1] Přiblížení základních pojmů užívaných v dokumentu. *Plán rozvoje* = obsahuje procesy týkající se rozšiřování bezpečnostního povědomí. *Organizační opatření* = v rámci organizace se stanovují opatření mj. k zajištění realizace plánu rozvoje. *Institucionální školení* = jedna ze součástí (může být i jediná) plánu rozvoje.

[2] Tento souvislý řetězec opatření je možné naplnit vzdělávacími moduly, institucionálním školení, *best practice* dokumenty či praktickým testováním – Phishingator apod. Vždy je však nutné vše přizpůsobovat potřebám konkrétní organizace a znalostem cílové skupiny.

[3] Garantem rozsahu organizačních opatření je povinný subjekt – VVŠ.

Každá z následujících kapitol se skládá z popisu povinnosti (nebo povinností), kterou je dle příslušného ustanovení nutné splnit, vymezení způsobu, jakým je možné zajistit splnění povinnosti, a souborem otázek, jejichž zodpovězením v dokumentaci by měla být povinnost splněna.

A. Plán rozvoje bezpečnostního povědomí (§ 9 odst. 1 písm. a) VoKB)

V prvé řadě je povinná osoba povinná stanovit plán rozvoje bezpečnostního povědomí. Cílem tohoto plánu je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí zaměstnanců i dodavatelů (§ 9 odst. 1 písm. a) VoKB). Plán rozvoje bezpečnostního povědomí musí pokrývat minimálně dvě vyhláškou stanovené oblasti:

- stanovit formu, obsah a rozsah poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a bezpečnostní politice (§ 9 odst. 1 písm. a) bod 1 VoKB)[4];
- stanovit potřebná teoretická i praktická školení uživatelů, administrátorů a osob zastávajících bezpečnostní role (§ 9 odst. 1 písm. a) bod 2 VoKB).

Zřejmě nejdůležitějším krokem pro splnění povinností plynoucích z tohoto ustanovení je zajištění správného mentálního nastavení: povinnost vytvořit plán rozvoje bezpečnostního povědomí není možné splnit jednorázovým proškolením zaměstnanců ve zkušební době. Na rozdíl od problematiky bezpečnosti a ochrany zdraví při práci je oblast kybernetické bezpečnosti výrazně dynamičtější co do hrozeb, které mohou vést k bezpečnostním incidentům. Plán rozvoje bezpečnostního povědomí tak musí představovat systematický, promyšlený a srozumitelný plán vzdělávání v oblasti.[5] Konkrétní parametry tohoto plánu nejsou stanoveny, ale je nutné při jeho formulaci přistoupit k obecnému cíli legislativy, kterým je zajištění bezpečnějšího prostředí.

Způsob školení a vzdělávání směřující k zajišťování a zvyšování povědomí musí být zvolen s ohledem na pozici zastávanou konkrétním zaměstnancem. VoKB rozlišuje skupinu uživatelů, administrátorů, osob zastávajících bezpečnostní role (manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti, garant aktiva, auditor kybernetické bezpečnosti) a eventuálně také

[4] Povinné subjekty mají povinnost stanovit administrátory a osoby zastávající bezpečnostní role.
Jednotlivé vzdělávání se poté na ně vztahuje od doby, kdy jsou jmenováni (souvisí s účinností předpisů).

[5] Je nutné zajistit periodickou revizi existujících aktuálních plánů, což plyne i ze zákonných povinností.

skupinu dodavatelů. V rámci struktury organizace tak bude zřejmě nutné zvolit odlišný přístup ke školení od řídících struktur organizací až po řadové zaměstnance.[6]

Jak bylo uvedeno výše, součástí plánu rozvoje bezpečnostního povědomí je povinnost stanovit formu, obsah a rozsah poučení jednotlivých skupin osob o jejich povinnostech a o bezpečnostní politice. Tuto část je možné označit za plán zvyšování bezpečnostního povědomí. Cílem je informovat o struktuře bezpečnostní politiky organizace a zajistit, že jsou v ní stanovené povinnosti jednotlivým uživatelům známy. K tomu je nutné zvolit adekvátní formu a v jejím rámci zajistit, že se zaměstnanci se svými povinnostmi prokazatelně seznámili. Plán zvyšování bezpečnostního povědomí však necílí pouze na zaměstnance, ale jako adresáty musí zahrnout i dodavatele. I ti totiž mohou představovat bezpečnostní riziko. Důležité je zajistit, aby se odpovědnost zaměstnanců v oblasti bezpečnosti nestanovovala *ad hoc*, ale uvážlivě a v souladu s celkovou bezpečnostní politikou organizace.

Druhou částí plánu rozvoje bezpečnostního povědomí je povinnost stanovit potřebná teoretická i praktická školení pro jednotlivé skupiny osob. Tuto část je možné označit za plán profesního vzdělávání. Cílem je zajistit kontinuální předávání informací o kybernetické bezpečnosti jednotlivým skupinám osob tak, aby byli seznámeni s případným vývojem v pro ně relevantní oblasti. Uživatelé, administrátoři a osoby zastávající bezpečnostní role budou mít v tomto směru diametrálně odlišný obsah vzdělávání, stejně jako náklady či časovou dotaci s tímto vzděláváním spojené.

Není nutné jednotlivé součástí vzdělávacího procesu tvořit pro vlastní potřebu nebo proprietárně pouze pro potřebu konkrétní organizace. Pro splnění podmínek stanovených tímto ustanovením je možné postavit rozsáhlé části vzdělávacího plánu na veřejně dostupných zdrojích nebo informačních materiálech. Důležité však je, aby byl plán rozvoje bezpečnostního povědomí (a to v části zvyšování bezpečnostního povědomí i profesního vzdělávání) promyšleným a uvážlivě vytvořeným produktem. Jeho součástí tak nepochybně může být i identifikace důvěryhodných institucí, jejichž materiály budou uživatelům buď přímo předávány nebo zpracovávány tak, aby měly pozitivní dopad na jejich povědomí o povinnostech v oblasti bezpečnosti. Stejně tak není

[6] Obsah i formu školení je nutné přizpůsobit jednotlivým cílovým skupinám. Zaměřit se tedy nejen na prověřování základních uživatelů, ale testovat i např. administrátory jako technicky zdatnější jedince.

nutné, aby jakákoli součást plánu probíhala formou frontální přednášky. Pravidelná školení zaměstnanců je možné zajistit e-learningovými prostředky (a to synchronními i asynchronními) s přihlédnutím ke specifikům příslušné organizace.

Otázky:

- → *Jakým způsobem byli uživatelé, administrátoři, osoby zastávající bezpečnostní role a dodavatelé poučeni o bezpečnostní politice organizace?*
- → *Jakým způsobem byli uživatelé, administrátoři, osoby zastávající bezpečnostní role a dodavatelé poučeni o jejich povinnostech v oblasti bezpečnosti?*
- → *Jakým způsobem organizace vzdělává uživatele, administrátory a osoby zastávající bezpečnostní role po teoretické stránce?*
- → *Jakým způsobem organizace vzdělává uživatele, administrátory a osoby zastávající bezpečnostní role po praktické stránce?*

Odpověď na shora uvedené otázky musí obsahovat specifikaci formy (například synchronní online výuka, frontální přednáška, asynchronní e-learning na úložišti organizace), obsahu (vymezení obsahu jednotlivých vzdělávacích a osvětových aktivit) a rozsahu (časová dotace). Organizace musí být schopna doložit, že tyto vzdělávací aktivity proběhly a že se jich osoby, kterým byly určeny, zúčastnili.

B. Odpovědnost za realizaci plánu (§ 9 odst. 1 písm. b) VoKB)

Pro každé jednotlivé činnosti, které jsou obsažené v rámci plánu rozvoje bezpečnostního povědomí, musí být stanovena pověřená odpovědná osoba.[7] Není nutné uvádět odpovědnou osobu jménem, vymezení však musí obsahovat alespoň pracovní pozici, kterou odpovědná osoba zastává, a se kterou bude odpovědnost v oblasti zvyšování bezpečnostního povědomí spojena.

Z dikce ustanovení není jasné, zda se má jednat o osobu s fyzickou odpovědností za vykonání dané činnosti (R v rámci RACI matice) nebo o osobu, která má odpovědnost za fakt, že je daná činnost vykonávána, jak bylo předdefinováno (A v rámci RACI matice). Vzhledem k tomu, že plán rozvoje

[7] Odpovědná osoba není konktrétně zákonem stanovena. Mělo by se jednat o osobu, která zajistí, že vzdělávání bude organizačně dávat smysl a také bude probíhat s náležitou úrovní. Je nutné sledovat účel legislativy, ale další podmínky nejsou stanovené.

bezpečnostního povědomí může být s přihlédnutím k potřebám organizace realizován i za pomoci externích subjektů, lze důvodně očekávat, že se bude jednat o osobu odpovědnou za fakt, že je daná činnost vykonávána (A v rámci RACI matice). Cílem ustanovení je přiřadit ke konkrétním činnostem v rámci plánu konkrétní odpovědné osoby tak, aby byla zajištěna odpovědnost za jejich vykonání. Není tedy možné, aby se činnosti „nějak staly", ale opět je zdůrazněna jejich dopředu promyšlená a cílená povaha. Identifikace odpovědné osoby navíc přímo souvisí s požadavkem na to, aby byly plány podrobovány periodické revizi.

Otázky:

- → *Kdo odpovídá za to, že uživatelé, administrátoři, osoby zastávající bezpečnostní role a dodavatelé byli poučeni o bezpečnostní politice organizace?*
- → *Kdo odpovídá za to, že uživatelé, administrátoři, osoby zastávající bezpečnostní role a dodavatelé byli poučeni o jejich povinnostech v oblasti bezpečnosti?*
- → *Kdo odpovídá za to, že organizace vzdělává uživatele, administrátory a osoby zastávající bezpečnostní role po teoretické stránce?*
- → *Kdo odpovídá za to, že organizace vzdělává uživatele, administrátory a osoby zastávající bezpečnostní role po praktické stránce?*

C. Vstupní a pravidelná školení bezpečnostního povědomí (§ 9 odst. 1 písm. c) VoKB)

Kromě nutnosti stanovit plán rozvoje bezpečnostního povědomí je nutné, aby školení reálně a náležitým způsobem probíhala. Cílem školení podle tohoto ustanovení je zajistit informování o povinnostech ve vztahu ke kybernetické bezpečnosti a o bezpečnostní politice pro uživatele, administrátory, osoby zastávající bezpečnostní role a dodavatele.

Zaměstnanci mají být seznámeni s povinností ochrany informací a povinnosti mlčenlivosti v rozsahu, který je pro organizaci nezbytný. Povinnost řídit se bezpečnostní politikou může být zakotvena například přímo v pracovní smlouvě každého zaměstnance. Nicméně transparentní úpravou povinností a odpovědnosti v této oblasti se povinnost dle tohoto ustanovení nevyčerpává. Ustanovení přímo předpokládá kromě existenci vstupního školení v této oblasti i existenci pravidelných školení, která budou sloužit k oživování a upevňování zaměstnavatelem komunikovaných informací. Právní předpis předpokládají pravidelnost, nicméně nestanovují

periodicitu. V oblasti základů bezpečnosti, bezpečnostní politiky a povinností zaměstnance je vhodné uvažovat o pravidelném školení alespoň 1x ročně.

Otázky:

- → *Probíhá u zaměstnanců vstupní školení věnované povinnostem zaměstnanců a bezpečnostní politice organizace?*
- → *Probíhají u zaměstnanců pravidelná školení věnovaná povinnostem zaměstnanců a bezpečnostní politice organizace?*
- → *Je zvolená periodicita pro pravidelná školení dostatečná s přihlédnutím k bezpečnostním potřebám organizace?*
- → *Je organizace u všech uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů schopná doložit absolvování vstupních a pravidelných školení věnovaných povinnostem zaměstnanců a bezpečnostní politice organizace?*
- → *Jsou tato školení v souladu s plánem rozvoje bezpečnostního povědomí?*

D. Pravidelná školení profesního vzdělávání (§ 9 odst. 1 písm. d) VoKB)

Kromě povinnosti stanovit plán profesního vzdělávání pro osoby zastávající bezpečnostní role je nutné, aby tato školení reálně a náležitým způsobem probíhala. Cílem školení podle tohoto ustanovení je zajistit další rozvoj osob zastávajících bezpečnostní role tak, aby s vývojem v oblasti kybernetické bezpečnosti nedocházelo k relativnímu snižování kompetence těchto osob.[8]

Není stanoven žádný způsob, jakým by tato školení měla probíhat. Je však nutné přihlédnout k aktuálním potřebám organizace v oblasti kybernetické bezpečnosti. Lze tak předpokládat na jednu stranu značnou míru flexibility v oblasti stanovení obsahu vzdělávání dle tohoto ustanovení. Na druhou stranu je však nutné předpokládat, že obsah vzdělávání musí být navázán na bezpečnostní potřeby organizace, které tak musí být předem identifikovány.

Otázky:

- → *Probíhají u osob zastávajících bezpečnostní role pravidelná školení profesního vzdělávání?*

[8] Je nutné vycházet z požadavků cílových skupin. U odbornějších zaměstnanců je nutné sebevzdělávání a je možné ho v rámci plánu předpokládat a poskytovat k němu inciativy nebo ho i kontrolovat. Opět: jednou za rok může stačit, ale u některých organizací (nebo některých zaměstnanců některých organizací) to může být plánem vyžadováno častěji.

→ *Jakým způsobem se obsah a rozsah těchto pravidelných školení váže na identifikované bezpečnostní potřeby organizace?*
→ *Jsou tato školení v souladu s plánem rozvoje bezpečnostního povědomí?*

E. Ověřování bezpečnostního povědomí zaměstnanců (§ 9 odst. 1 písm. e) VoKB)

Toto ustanovení stanovuje povinnost zajistit pravidelná školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní. Cílem je zajistit, že s rozvojem oblasti kybernetické bezpečnosti bude docházet k systematickému dalšímu vzdělávání zaměstnanců tak, aby jejich bezpečnostní povědomí nekleslo pod určité nezbytné minimum.[9] Případné změny (například nové hrozby či změny v bezpečnostní politice) jsou zaměstnancům transparentně komunikovány. Toto ustanovení předpokládá značnou míru variability – důraz musí být kladen na adekvátní formu a zároveň musí být zaměstnanci vzdělávání v rozsahu, který je adekvátní jejich pracovní náplni. Nad rámec předcházejících ustanovení toto ustanovení stanovuje i nutnost ověřovat bezpečnostní povědomí zaměstnanců.

Vzhledem k relativně nízké účinnosti „tradičních" školení v oblasti bezpečnosti je nutné zajistit implementaci metod ověřujících skutečné pochopení komunikovaných pravidel a schopnosti zaměstnanců v souladu s těmito pravidly jednat. V úvahu připadají například šíření zdánlivých phishingových zpráv za účelem ověření bezpečnostního povědomí zaměstnanců.

Otázky:

→ *Probíhají pravidelná školení bezpečnostního povědomí, která jsou přizpůsobená pracovní náplni zaměstnanců?*
→ *Probíhá pravidelné ověřování bezpečnostního povědomí přizpůsobené pracovní náplni zaměstnanců?*
→ *Jsou tato školení a způsoby ověřování v souladu s plánem rozvoje bezpečnostního povědomí?*

[9] Minimum nezbytné pro výkon pracovní pozice v konkrétní organizaci. Stanovuje organizace v souladu s potřebami organizace a rozsahem pracovní smlouvy apod.

F. Mechanismus kontroly dodržování bezpečnostní politiky (§ 9 odst. 1 písm. f) VoKB)

Toto ustanovení stanovuje povinnou existenci mechanismu kontroly dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role. Povinnost vychází z úvahy, že ani v případě perfektního informování o povinnostech a bezpečnostní politice, zajištění odborného vzdělávání a ověřené bezpečnostního povědomí není možné rezignovat na kontrolu dodržování bezpečnostní politiky. V rámci organizace tak musí existovat mechanismy, které umožní odhalit, že zaměstnanci dodržují bezpečnostní politiku – tedy že u zaměstnanců nedochází k chybám a ve chvíli, kdy k nim dojde, tak je zaměstnanci řeší v souladu s postupy stanovenými v bezpečnostní politice.

Jakkoli bezpečnost lidských zdrojů představuje primárně sadu organizačních opatření, pro realizaci povinností plynoucích z tohoto ustanovení připadají v úvahu i některá technická opatření a nástroje.

Otázky:

- → *Je implementován mechanismus kontroly dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role?*
- → *Jaké technické nástroje a organizační postupy jsou ke kontrole dodržování bezpečnostní politiky implementovány?*

G. Předání odpovědnosti administrátorů a osob zastávajících bezpečnostní role (§ 9 odst. 1 písm. g) VoKB)

Dle tohoto ustanovení musí být v organizaci zajištěn proces předání odpovědnosti s administrátory nebo s osobami, které zastávají bezpečnostní role. Cílem je zajistit, aby nenastala situace, kdy organizace zůstane v této oblasti bez jasně odpovědného zaměstnance. Toto ustanovení přímo směřuje ke konci životního cyklu jednoho zaměstnance na těchto pozicích a počátku životního cyklu zaměstnance jiného. V ideální situace je dopředu stanoveným postupem zajištěna návaznost činností odcházejícího a přicházejícího zaměstnance, částečný překryv v jejich činnosti za účelem předání všech nezbytných materiálů a podobně. Bezpečnost lidských zdrojů totiž přímo souvisí i s ukončením pracovního poměru administrátora či osoby zastávající bezpečnostní role. Za tento

proces a jeho správný průběh musí nést konkrétní osoba v rámci organizace odpovědnost (s přihlédnutím k závažnosti doporučujeme R v rámci RACI matice), dohlédnout například na vrácení předmětů přidělených zaměstnanci nebo na zrušení jeho přístupových práv.

Otázky:

- → *Jaký je v organizaci stanoven postup pro předání odpovědnosti administrátorů a osob zastávajících bezpečnostní role?*
- → *Kdo je za tento postup odpovědný?*
- → *Jaký je stanoven postup pro předání odpovědnosti za situace, kdy původní zaměstnanec neodchází „v dobrém" a nelze tedy očekávat například návaznost a ideálně částečný překryv pracovních poměrů?*

H. Hodnocení účinnosti plánu rozvoje bezpečnostního povědomí (§ 9 odst. 1 písm. h) VoKB)

Toto ustanovení stanovuje povinnost hodnotit účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí. Stejně jako některá ustanovení VoKB předpokládají neustálý rozvoj individuálních kompetencí, ani plán rozvoje bezpečnostního povědomí nesmí být statický. Vyhláška nepředepisuje žádné další podmínky pro hodnocení účinnosti plánu rozvoje bezpečnostního povědomí. Podobně jako u některých dalších ustanovení výše je tak dána značná flexibilita umožňující přihlédnout k potřebám organizace a k povaze skupin zaměstnanců této organizace. Hodnocení účinnosti předpokládá formální proces s jednoznačně určenou odpovědnou osobou (A v rámci RACI matice).

Otázky:

- → *Jak často a jakým způsobem je hodnocena účinnost plánu rozvoje bezpečnostního povědomí?*
- → *Jakým způsobem může být plán rozvoje bezpečnostního povědomí měněn tak, aby reflektoval vývoj v oblasti kybernetické bezpečnosti?*
- → *Jakým způsobem dochází ke sběru připomínek k obsahu plánu rozvoje bezpečnostního povědomí?*
- → *Kdo je odpovědný za hodnocení účinnosti plánu rozvoje bezpečnostního povědomí?*

I. Pravidla a postupy při porušení bezpečnostních pravidel (§ 9 odst. 1 písm. i) VoKB)

Vedle procesu vzdělávání a kontrolu dodržování bezpečnostních politik organizace předpokládá vyhláška také existenci mechanismů, které umožní sankcionovat nežádoucí chování uživatelů, administrátorů a osob zastávajících bezpečnostní role. Zaměstnanci musí být od počátku informováni o tom, jaké následky může mít porušení pravidel bezpečnosti, pravidla při narušení bezpečnosti musí být formalizována (například formou pracovního nebo disciplinárního řádu organizace) a samozřejmě také vynucována. Vedení organizace dle tohoto ustanovení implementuje disciplinární procesy a opatření vůči zaměstnancům, kteří se dopustili narušení bezpečnosti informací. Pokud je v zájmu organizace mít porušení bezpečnosti stanovenou jako zvláště závažné porušení pracovních povinností, které je možné penalizovat například rozvázáním pracovního poměru, je vhodné toto zakotvit přímo v pracovní smlouvě.

Otázky:

- → *Jakým způsobem je formálně řešeno porušení bezpečnostních pravidel?*
- → *Jakým způsobem je formální řešení upraveno v interních předpisech organizace?*
- → *Jsou sankce za pochybení reflektovány v pracovních smlouvách?*

J. Vedení dokumentace o školeních (§ 9 odst. 2 VoKB)

O všech školeních, kterými byly v organizaci realizovány povinnosti dle různých písmen §9 odst. 1 je nutné vést přehledy. Tyto musí obsahovat přehled školení a seznam osob, které školení absolvovaly.

2. Cílové skupiny

Cílová skupina je skupina osob propojená společnými vlastnostmi. V našem kontextu jsou cílovými skupinami většinou univerzitní role – student, zaměstnanec, výzkumník, IT administrátor či manažer kybernetické bezpečnosti atp. Pro správné nastavení procesů a plánů zvyšování kyberbezpečnostního povědomí je však vhodné se v rámci jednotlivých rolí ponořit hlouběji, více si je pro účely vzdělávání segmentovat a následně tyto segmenty zastoupit skrze několik person, které nám pomohou lépe promýšlet plán vzdělávání a posilování CSA (*cyber security awareness*).

Persona je fiktivní zástupce cílové skupiny, který představuje jakýsi typický *exemplář*, archetyp současného nebo budoucího uživatele naší služby – tedy kyberbezpečnostního vzdělávání (*více o personách například na webu 100metod*). Přístupů k tvorbě person je mnoho, vyjít můžeme například z osobnostních charakteristik, z cílů typického uživatele, z jeho psychologických aspektů či sociálního zázemí. V rámci příprav plánu kyberbezpečnostního vzdělávání můžeme založit persony právě na jejich roli v rámci univerzity, ale obohatit je jak o socio-demografické pohledy, tak o širší pochopení vlastností, preferencí, přístupů či vzorců chování (*více k typům person viz např. Nielsen, 2013*).

Persona by neměla být jen odrazem naší představy typického zástupce cílové skupiny, ale je vhodné v rámci tvorby person vyjít **z dostupných dat či výzkumů**, např. z hloubkových rozhovorů se zástupci identifikovaných skupin nebo dalších rozličných metod pro výzkum uživatelů našich služeb. Osvědčilo se nám tak nejen pracovat např. s personou typu *„Aleš, profesor na Katedře románských jazyků“*, ale na základě pochopení dat a dalšího výzkumu určit např. Alešův věk; komunikační kanály a nástroje, které nejvíce využívá; jeho časové vytížení, preference a limity; jeho vzorce chování a osobnostní charakteristiky; nebo např. intenzitu stresu v zaměstnání či jeho pravděpodobnou ochotu se dále vzdělávat a spolupracovat s námi atp. (*více dalších charakteristik ke zvážení v rámci person založených na roli viz Adkisson, 2019*). Takto postavená persona nám pak umožní smysluplně navrhovat obsahy a kanály kyberbezpečnostního vzdělávání, které půjdou vstříc Alešovým preferencím a potřebám.

Persona bude do určité míry vždy limitovaným obrazem skutečných uživatelů, umožňuje nám ale nepřipravovat obsah pro neznámou *šedou masu* cílové skupiny, ale představit si fiktivní osobu, pro kterou dané vzdělávání připravujeme. Kvalita výstupů pak samozřejmě bude odvislá od kvality persony, tj. nakolik se nám skutečně povedlo z dostupných dat vytvořit smysluplnou a realistickou reprezentaci cílové skupiny.

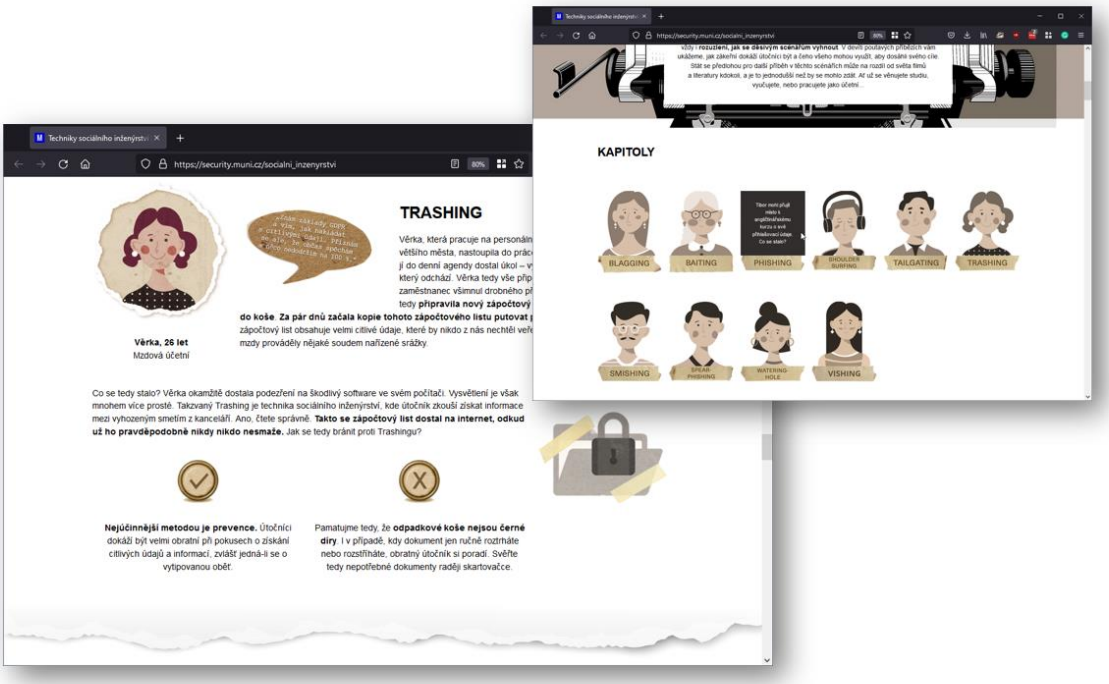
3. Typy obsahu a kanály

Mimo implementaci základního kyberbezpečnostního školení ve formě e-learningu či Moodle modulů, která bude z hlediska naplnění zákona většinou společná pro většinou cílových skupin a person, je vhodné do plánu vzdělávání a posilování kyberbezpečnostního povědomí zahrnout i další aktivity. Jejich rozsah a podoba (*zde vycházíme primárně z NIST členění dle Wilsona a Hashe, 2003, a z následného brainstormingu*) bude vždy odvislá od: a) person/skupin a jejich potřeb a preferencí; b) našich časových a lidských zdrojů.

3.1 Tradiční asynchronní metody

Využít je samozřejmě možné tradiční metody, a to jak v offline, tak online podobě. Své místo v prostoru univerzity stále mají běžné **tištěné a statické obsahy** (plakáty, letáky, bannery či brožury). Běžnými metodami jsou též metody založené na vlastním studiu, jako jsou **e-learningové moduly**, kterými dokážeme zajistit široký zásah, předat absolutní základy a naplnit povinnost díky jasně sledovatelným metrikám a indikátorům průchodu. Dopad těchto metod ale bude limitovaný a je vhodné, když jsou pouze jednou z částí celkového vzdělávacího mixu. Vhodné je většinou také zajistit jejich centralizaci do **kyberbezpečnostního webového portálu**, který poskytuje rozcestník na různé další vzdělávací obsahy, umožňuje efektivně informovat o novinkách v oblasti kyberbezpečnosti a zajišťuje jednotné kontaktní místo k nahlašování incidentů uživateli.

Příklad z praxe MUNI: *na Masarykově univerzitě pravidelně vznikají nové vzdělávací materiály pro uživatele cílené na různé oblasti kyberbezpečnosti a ochrany soukromí. Vychází často z aktuálních potřeb, které lze definovat skrze hrozby a incidenty. Například kurz Kyberkompas je rozsáhlý vzdělávací projekt základů kyberbezpečnosti, jehož cílem je srozumitelně a lidsky učit uživatele důležitým kyberbezpečnostním návykům. Kurz Technik sociálního inženýrství představuje nejčastější i méně známé podvodné techniky, které využívají psychologickou manipulaci k tomu, aby oklamaly oběť a ta se následně dopustila bezpečnostní chyby. Tyto techniky jsou demonstrovány na názorných příbězích, díky kterým si čitatel může situaci jednodušeji představit. Problematice ochrany osobních údajů se věnuje kurz GDPR, který vysvětluje základní pojmy, zásady zpracování osobních údajů a práva osob. Modulárnost kurzů umožňuje jejich snadnou aktualizaci a provázání s dalšími obsahy.*



Obrázek 1: Ukázka z kurzu Techniky sociálního inženýrství

Příklad z praxe: *centrální webové portály využívají jako bránu k veškerému kyberbezpečnostnímu obsahu mnohé zahraniční univerzity. Pro představu, jak může takový portál vypadat a co by mohl obsahovat, lze zamířit například na web Security Matters University of Toronto. Obsahuje* ***kyberbezpečnostní blog****, jasný a viditelný odkaz pro* ***hlášení incidentu, rozcestník*** *na vzdělávací zdroje i obecné informace k ISAT/CSAT (information/cyber security awareness training) procesům a povinnostem na univerzitě. Mnohé webové portály obsahují i takzvané* ***Phish bowls*** *– databáze zachycených phishingových e-mailů, podle kterých uživatelé mohou přijaté phishingové maily identifikovat. Podobnou databázi zveřejňují na svém kyberbezpečnostním portálu např. Cornell University, Princeton University nebo Carnegie Mellon University.*

Centrální webový kyberbezpečnostní portál není dostačujícím místem poskytování kyberbezpečnostních služeb v rámci VVŠ. Rozšiřování materiálů a komunikace obsahů by měly probíhat **více kanály**, jež budou odpovídat i mapování cílových skupin a identifikovaným personám: kde se daná persona nejvíce pohybuje, tj. kde a jakou cestou k ní náš obsah dokážeme dostat nejefektivněji i s ohledem na její další, např. časové preference a charakteristiky?

Obsah nemusí vždy přicházet v komplexní podobě. Mezi aktuální vzdělávací trendy patří tzv. **micro-learning**, kdy obsah dodáváme v malých kouskách, v různých kontextech a různými kanály.

Např. plakát tak nemusí obsahovat všechna doporučení najednou, příspěvek na Facebooku univerzity nemusí obsahovat odkaz na celou kyberbezpečností brožuru atp. Obsah, který chceme předat, se rozdělí na menší kousky a ty se následně komunikují postupně. Micro-learning reaguje především na realitu pracovních dní: zaměstnanci a další skupiny na VVŠ většinou nemají čas plně se věnovat vzdělávacímu obsahu během pracovního dne. Obsah designovaný na několik málo minut je pro ně stravitelnější a přístupnější. Menší kousky obsahu je také jednodušší kdykoliv doplňovat s ohledem na nové skutečnosti a nové hrozby v proměnlivém a dynamickém prostředí kyberbezpečnosti; micro-learning tak může základní komplexní školení kyberbezpečnosti vhodně doplňovat a aktualizovat.

Příklad z praxe MUNI: *v rámci prostorů Masarykovy univerzity jsou využívány např. digitální panely na chodbách, které se kromě oznámení a marketingu univerzitních akcí a aktivit využívají pro micro-learning v oblasti využívání informačního systému tzv. „po kapkách": skrze krátké tipy a triky. V zimě 2021 byl na portálu CSIRT-MU zprovozněn Adventní kyberkalendář, který každý prosincový den obsahoval jeden krátký tip nebo aktivitu vedoucí k navýšení kyberbezpečnosti uživatelů. Tento micro-learningový obsah, dostupný na webovém portálu, byl pak komunikován i dalšími kanály (sociální sítě atp.) s ohledem na využívané persony a cílové skupiny.*

Obrázek 2: Ukázka z Adventního kyberkalendáře

Mezi tradičnější způsoby posilování kyberbezpečnostního povědomí patří samozřejmě také videomateriály, jako jsou **videozáznamy** přednášek a kyberbezpečnostních seminářů, **videonávody** či motivační **spoty**. I zde je však vhodné uplatňovat principy *micro-learningu* a neočekávat, že cílové skupiny budou dobrovolně konzumovat např. hodinový záznam živé přednášky. Výzkumy efektivity a přínosů videoobsahů oproti textovým vzdělávacím obsahům pravidelně docházejí k odlišným výsledkům (hezké shrnutí viz např. v Wu et al., 2019).

Mezi důležité kanály pro komunikaci všech zmíněných kyberbezpečnostních obsahů patří samozřejmě i kampaně na **sociálních sítích**, bezpečnostní **newsletter** nebo **blog** kyberbezpečnostního týmu.

Příklad z praxe MUNI: *na Masarykové univerzitě vzniká například e-mailový newsletter ve formě komiksu, který vzdělává uživatele v základech kyberbezpečnosti a kyberhygieny prostřednictvím fiktivního světa. E-mailový newsletter může sloužit k informovaní zaměstnanců o nejnovějších kybernetických hrozbách či útocích, nebo jako pozvánka k souvisejícím vzdělávacím aktivitám či workshopům. Kyberbezpečnostní newsletter může být uchopen i pomocí gamifikačních technik, aby uživatele více zaujal. Tvorba newsletteru může být náročná, v případě nedostatku časových nebo personálních kapacit lze například využít pro důležité zprávy celouniverzitní newsletter, konkrétně zde vytvořit kyberbezpečnostní okénko se shrnutím nejdůležitějších zpráv a upozornění.*

Příklad z praxe MUNI: Kyberbezpečnostní tým Masarykovy univerzity *aktivně působí na sociálních sítích, kde prostřednictvím krátkých příspěvků informuje uživatele univerzity o aktuálním dění v kyberprostoru, hrozbách a útocích, a připomíná základy kyberhygieny vázané například k začátku nového semestru nebo letních prázdnin. Tato metoda mikro-learningu se velmi osvědčila právě proto, že má díky platformám sociálních sítí široký dosah, a svým krátkým a trefným obsahem je pro uživatele poměrně jednoduše pochopitelná. V případě komplexnějších záležitostí, například šifrování, je důležité shrnout v krátkém textu to klíčové a odkázat uživatele na další obsah, optimálně univerzitního charakteru. Před vstupem na sociální sítě a tvorbou osvětových činností skrze ně doporučujeme promyslet si, na koho míříme. Každá sociální síť disponuje jiným publikem, ať již se na to díváme věkově nebo profesně. Například na síti LinkedIn příliš studentů nezaujmeme, naopak skrze Instagram se příliš nepřiblížíme zaměstnancům a vyučujícím.*

I s ohledem na interpretaci zákona není nutné, aby byly výše zmiňované obsahy vždy založené výhradně na interních materiálech – je možné využít libovolné materiály, u kterých posoudíme

jejich **kvalitu** a **vhodnost**. Mezi základní zdroje českých materiálů paří materiály Národního úřadu pro kybernetickou a informační bezpečnost.

3.2 Synchronní metody

Mezi klasické synchronní formální metody patří např. běžná **školení** vedená interními nebo externími experty, a to jak v offline tak v on-line podobě. Výhodou je zde možnost uzpůsobit školení na míru operativně přímo přítomné skupině. Nemusí se jednat pouze o školení, ale též o formy jako je workshop, seminář či diskuse. Komplexní školení cílené na konkrétní skupiny zaměstnanců jsou efektivním způsobem výuky kyberbezpečnosti. Výhodou této metody je možnost zaměření na specifické problémy nebo nedostatky vázané k pracovní pozici nebo oblasti zájmu.

Mezi méně formální synchronní metody pak patří např. **filmové promítání** relevantních filmů s následnou debatou či neformální metody **zasahující do běžného provozu univerzity**, pojaté např. jako intervence do univerzitního prostoru.

Příklad z praxe: *v rámci programu Wellesley College "Security Gnome" procházeli studenti knihovnických oborů prostory univerzity a hledali např. nehlídané nezamčené notebooky v knihovně atp. U takových zařízení nechávali tištěné materiály s obsahem informujícím o bezpečnosti zařízení. Tam, kde zaznamenali dobrou praxi, nechávali malé figurky „bezpečnostních trpaslíků" vytištěné na 3D tiskárně. Aktivita byla samozřejmě komunikována mnoha kanály a dostatečně prezentována, což rozšířilo její dopad za několik málo desítek uživatelů, kteří byli intervenováni přímo v prostoru univerzity. Figurka trpaslíčka navíc měla potenciál stát se sběratelským objektem – celá aktivita tak do značné míry využívá i principy gamifikace.*

Příklad z praxe MUNI: *na Masarykově univerzitě se dbá o pravidelné školení administrativních, vědeckých, manažerských pracovníku i správců informačních systémů. Školení jsou většinou vedena lektorem jako online nebo prezenční přednáška/seminář, přičemž se účastníci školení aktivně zapojují do diskuse. Pozornost je věnována také kybervzdělávaní osob ohrožených nižší mírou digitální gramotnosti. Školení ve formě kurzů na míru pro Univerzitu třetího věku MU jsou cíleny na jedince v důchodovém věku a pokrývají výuku základů kyberhygieny a sebeobrany v kyberprostoru. Dalším příkladem je vzdělávaní dětí prostřednictvím MjUNI – univerzity pro děti, v které se učí digitální gramotnosti již od útlého věku.*

3.3 Herní a hands-on metody

Tyto metody představují hybridní aktivity, které mohou kombinovat teoretické i praktické cesty kybervzdělávání. Kyberbezpečnostní *hands-on* aktivity se také nazývají kyberbezpečnostní **vzdělávací hry** a slouží k praktickému procvičování kyberschopností uživatelů s různými úrovněmi technických schopností. Vzdělávaní může mít formu simulace kybernetického útoku nebo obrany prostřednictvím **deskových her, strategických scénářů**, diskusí nebo technicky orientované simulace (*k metodám založeným na simulaci viz dále v textu*). Výhodou této metody je spojení kybervzdělávaní se zábavou, protože *hands-on* aktivity často používají **gamifikační prvky** pro zaujetí účastníků. Taktéž jsou vhodná pro skupinové vzdělávaní zaměstnanců z různých oddělení a profesních zaměření. Kyberbezpečnostní *hands-on* vzdělávaní například učí zaměstnance řešit kybernetické incidenty na různých pracovních úrovních jako tým – od účetní, incident handlera, až po managera.

Herní metody vzdělávání a gamifikační prvky se osvědčují jako efektivní motivace pro posílení interakcí s kyberbezpečnostním obsahem a o gamifikační prvky (*odznáčky, odměny, sbírání bodů atp.*) můžeme obohacovat i naše již existující obsahy.

Příklad z Praxe: *University of Connecticut organizovala aktivitu nazvanou Husky Hunt. Šlo v podstatě o klasickou hru typu „scavenger hunt", tedy jakési hledání pokladu. Studenti univerzity pravidelně obdrželi bezpečnostní typy a kvízové otázky, jejichž správné zodpovězení je dovedlo na fyzickou lokaci v rámci univerzitního kampusu, kde nalezli další stopu. Sdílení kyberbezpečnostních tipů mezi spolužáky bylo hodnoceno body, držitelé nejvíce bodů pak obdrželi ceny včetně slev na skripta a učebnice. Hra je vetnuta do reálného prostoru univerzity a gamifikační prvky (sbírání bodů) pracují s motivací. Technicky a organizačně relativně náročný přístup umožňoval cíleně volit a posilovat aktuální kyberbezpečnostní témata podle momentálních potřeb kyberbezpečnostního týmu. Design hry navíc podporoval organické šíření obsahů např. do studentské komunity: obsah sdílený vrstevníky má vždy větší dopad, než komunikace shora – více k motivaci dále v textu. Husky Hunt se na UoC stále organizuje, podle dostupných informací ale nyní slouží primárně v procesu seznamování se s univerzitou a jejími službami. Podobné hry nejsou výjimečné, záleží samozřejmě na časových a lidských možnostech kyberbezpečnostních týmů, jelikož tento typ aktivit musí být vytvořen na míru každé organizaci. Obecnější přístup zvolila např. Florida State University, kde je součástí hry pouze jednoduchý test a hraje se o nový notebook.*

Hry mohou být i digitálního charakteru, jak to ukazuje například novozélandský projekt Education Arcade nebo česká hra Clashing. Půdorys vlajkové hry v hybridním prostředí pak využívá Carnegie Mellon University ve svém programu picoCTF.

Velká část zmíněného obsahu pokrývá teorii, a i když mluvíme v ukázkách a příkladech z praxe, nemusí být realita útoků pro některé cílové skupiny a jejich persony vždy plně představitelná a uchopitelná. Nejpřínosnějšími metodami z hlediska posilování CSA jsou tak ty, které **simulují reálné situace a útoky.** V praxi se samozřejmě jedná o simulační cvičení pro kyberbezpečnostní tým či IT administrátory, méně komplexní metody však lze aplikovat na celou škálu zaměstnanců, které můžeme chtít dostávat do kontrolovaných situací, v rámci kterých budou bezpečně budovat své reakce na různé typy útoků. Pokud k těmto metodám budeme sahat, je vhodné jejich využití zanést do **interních směrnic**: zkouška požárního poplachu je většinou předem oznamována jako zkouška; podobně je nutné, aby si byl zaměstnanec či student předem vědom, že k tomuto typu zkoušek může docházet. *Simulation-based metody* předávání dovedností patří mezi nejefektivnější a nejkomplexnější metody zvyšování CSA, jak se ukázalo např. i ve výzkumu Nachina et al. (2019). V rámci projektu CRP-KYBER připravila ZČU systém Phishingator, který byl již dříve prezentován a je možné ho jako *simulation-based delivery* metodu zavést do plánu vzdělávání.

3.4 Hledání optimální kombinace

Není v silách a časových možnostech žádného kyberbezpečnostního týmu pokrýt všechny možné kanály a obsahy. Součástí plánu vzdělávání a zvyšování kyberbezpečnostního povědomí by tak měla být i identifikace klíčových platforem a kanálů a jejich provázání do smysluplného vzdělávacího mixu. Kanály a obsahy volíme s ohledem na persony, a je vhodné si stanovit jejich cíle (tj. např. pokud se rozhodneme vytvářet kyberbezpečnostní newsletter, odpovědět si primárně na otázku *„Proč kyberbezpečnostní newsletter? Pro které persony tento typ obsahu a jeho dodávání dává smysl? Jaký je pro nás hlavní cíl newsletteru? Co v něm chceme komunikovat?“* atp.) či určit role a zodpovědnosti za ně – všechna tyto vodítka mohou být součástí vzdělávacího plánu.

4. Práce s motivací

Během přemýšlení nad správným návrhem kyberbezpečnostního vzdělávacího obsahu a nad jeho správnou komunikací je vhodné přemýšlet i nad motivací jednotlivých person se naším obsah a kyberbezpečností obecně zabývat. V praxi nám může významně pomoci **model MINDSPACE**: *Influencing behaviour through public policy* (Dolan et al., 2010), který se sice zaměřuje primárně na oblast vládních opatření, je však velmi dobře využitelný a užitečný i pro praxi zvyšování kyberbezpečnostního povědomí v rámci organizace.

Jednotlivá písmena modelu MINDSPACE označují několik zásadních faktorů, které příjemci berou v potaz, když se podvědomě rozhodují, zda je pro ně příchozí sdělení dostatečně motivační, nebo zda ho budou ignorovat. Různí lidé i v rámci různě definovaných cílových skupinách mohou odlišně

reagovat na různé podněty a motivace, je proto vhodné při nastavování plánů kyberbezpečnostního vzdělávání a posilování kyberbezpečnostního povědomí pracovat s faktory motivace šířeji. Jednotlivé body modelu MINDSPACE nyní velmi stručně shrneme a pokusíme se je překlopit do oblasti vzdělávání v kyberbezpečnosti a ilustrovat je příklady z oblasti CSA. Pro podrobnější studium je možné využít oficiální materiály k modelu MINDSPACE.

Messenger (*zdroj sdělení*): zdroj sdělení ovlivňuje naši motivaci, tj. např. zpráva předávaná expertem má u příjemce větší váhu, přínosem mohou být i demografické podobnosti mezi cílovou skupinou a zdrojem zprávy. Vhodné je také přemýšlet nad skutečností, že zpráva může být přijímána negativně jen proto, že přichází ze struktur spojených s univerzitním IT, kyberbezpečnostním týmem atp.

Příklad využití: *nemusíme být vždy tím, kdo komunikuje: můžeme využít externí hlas, využívat* ***storytelling*** (*podobně jako v e-learningových modulech, které byly dodány v rámci CRP-KYBER21*) *nebo pracovat s tzv.* ***peer message*** *– tedy využívat* ***ambasadory*** *z jednotlivých cílových skupin či různými cestami motivovat k organickému rozšiřování zprávy mezi vrstevníky/kolegy tak, jak to bylo využitu například v případě herní aktivity Husky Hunt zmíněné výše.*

Incentives (pobídky): interakce s CSA obsahem lze samozřejmě podmiňovat či podporovat různými typy pobídek. Model MINDSPACE zde pracuje především s finančními odměnami a pokutami, obecná doporučení však můžeme vztáhnout i do naší oblasti: vzdělávání a dobrá kyberbezpečnostní praxe může být spojena s odměnou, naopak špatná praxe a nedostatek iniciativy se ztrátou.

Dle zkušeností a výzkumů se ukazuje, že možné ztráty nás motivují více, než potenciální přínosy. Zmiňované výzkumy z oblasti veřejného zdraví např. ukazují tento rozdíl na příkladu možné finanční odměny (*pokud budete zdravě žít a zhubnete, dostanete finance navíc*), která se ukázala jako méně efektivní oproti představě potenciální ztráty (*např. skupina respondentů musela vložit své peníze na účet, odkud se jim vrátí i s navýšením o odměnu pouze v případě, že se jim podaří ve sledovaném období zhubnout*).

Příklad využití: *v oblasti kyberbezpečnostního vzdělávání nebudeme debatovat finanční pobídky, ačkoliv z rešerše se ukázalo, že některé zahraniční univerzity ustanovily kyberbezpečnostní školení jako prerekvizitu pro vyplácení jakýchkoliv finančních bonusů a odměn svým zaměstnancům – viz dále. Využít lze již zmíněnou gamifikaci, odznáčky atp., případně odměnu ve formě soutěže či losování. Wellesley College např. ke studiu v rámci měsíce kyberbezpečnosti motivovala losováním o iPad: ze všech uživatelů, kteří v rámci měsíce absolvovali e-learningový kurz a splnili závěrečný test,*

byl vylosován jeden výherce. Není vhodné komunikovat a vyvolávat přehnané obavy z potenciálních ztrát (jakkoliv to může být efektivnější než komunikace případných zisků), jelikož může docházet k tzv. security fatigue (popsáno např. v Stanton et al., 2016 nebo aktuálněji Cram et al., 2020) a následnému znecitlivění, popisovanému např. jedním z respondentů ve výzkumu Stantona et al.: „People get weary of being bombarded by 'watch out for this or watch out for that'." Půjde tedy o hledání harmonie, nikoliv jen o strašení.

Norms (normy): děláme to, co dělají ostatní. Pokud něco dělá většina, ostatní se přidají: to platí jak o negativních fenoménech, např. podvádění u zkoušek nebo vandalismu, tak stejnou mírou i u pozitivních podnětů – cokoliv je vnímáno a podáváno jako převažující sociální norma, bude povětšinou následováno.

Příklad využití: *lokální univerzitní normy mohou být velmi dobře použity např. k přesvědčení nepřesvědčených uživatelů v případě zavádění ochranných kyberbezpečnostních prvků: pokud např. 65 % uživatelů univerzity již chrání svoje O365 pomocí 2FA, je to vhodné komunikovat – takové sdělení odhaluje lokální normu, kterou budou mít ostatní uživatelé nutkání následovat. V oblasti kyberbezpečnosti se zatím těžko hledají příklady, kdy by bylo možné využít většinu: „47 % uživatelů internetu využívá blokování reklamy" však může být vhodné doplnění k dalším argumentů pro blokování reklamy. Stejně tak využití takových argumentů v určité fázi např. dobrovolného zavedení některých opatření může být efektivní (např. „podívejte, většina zaměstnanců již tento ochranný prvek využívá").*

Defaults (výchozí volby): možnosti, které jsou tzv. *výchozí*, předvybrané, prostě následujeme, a to bez výraznějších ohledů na dopady. Autoři modelu MINDSPACE ilustrují tento fakt na příkladech zemí, kde je nutné se k dárcovství orgánů přihlásit (jen malá procenta lidí to udělají) a naopak zemí, kde je nutné se od dárcovství orgánů odhlásit (většina obyvatel zůstane ve výchozím nastavení).

Příklad využití: *tato část motivačních prvků může být využitelná především pohledem nastavení systémů jejich administrátory. Pokud 2FA nastavíme jako výchozí variantu pro nově příchozí uživatele, můžeme kalkulovat s pravděpodobností, že většina uživatelů u této možnosti zůstane – a to i v případě, že k tomu není vedena žádnou interní směrnicí nebo povinností.*

Salience (*významnost*): pozornost lidí zasáhne to, co je pro ně nové, jednoduše přístupné, jednoduché (např. na kliknutí) nebo relevantní přímo pro ně jako jednotlivce. Problémem zde

například může být i příliš mnoho možností – výzkumy zmíněné v modelu MINDSPACE ukazují, že pokud máme příliš mnoho možností jak třídit, raději netřídíme vůbec. Vhodný design to často dokáže napravit.

Příklad využití: *s podobnými potížemi bojujeme v případě kyberbezpečnosti např. u doporučování vhodných nástrojů: instinktivně raději doporučujeme více nástrojů, tato možnost volby však často může vést k paralýze a apatii. Uživatelé mnohdy nechtěj vědět, jaké různé druhy správců hesel jsou na trhu a čím se liší, chtějí jednoduše dostupné a jednoduché řešení: chtějí slyšet, který nástroj mají využít a jak. Pomocí vhodného strukturování informací můžeme jednoduchostí uspokojit většinu uživatelů a podrobné přehledy nabídnout dále jen těm, kteří je vyhledávají.*

Příklad využití: *faktor významnosti mluví i pro vhodnou segmentaci kyberbezpečnostního obsahu a metod rozvoje kyberbezpečnostního povědomí: čím lépe budeme cílit na jednotlivé skupiny zastoupené našimi personami, tím větší šanci máme, že budeme úspěšní. Například newsletter o probíhajících phishingových kampaních hromadně na všechny zaměstnance je sice nejrychlejší cesta („Předmět: Zaměstnance univerzity opět ohrožuje phishing"), ale míra jeho otevření bude relativně nízká a pokud ho budeme posílat vždy plošně a všem, riskujeme posílení již zmíněného ‚security fatigue'. U stejného obsahu, personifikovaného a segmentovaného na nejohroženější skupiny (např. na účetní s předmětem „Účetní jako vy jsou ohroženy phishingem, víme jak se bránit") lze očekávat větší míru dopadu. Takový obsah je příjemcem přijímán jako významnější. Navíc se tak vyhneme tzv. ‚optimism bias', tedy víře, že špatné věci se s větší pravděpodobností dějí ostatním, nikoliv nám (dopady tohoto kognitivního zkreslení do oblasti kyberbezpečnosti popisují např. Heyun-Suk et al., 2008).*

Priming: Mnoho našich rozhodnutí je ovlivněno podvědomými vodítky (*cues*). Slova i obrazy, které používáme, mohou ovlivnit chování cílových skupin i nenápadnými cestami. Nenápadné podsunutí obrázku usměvavé tváře během pití alkoholu například v jedné z v modelu MINDSPACE zmiňovaných studií vedlo podvědomě k posílení přijmu alkoholu, a to oproti participantům, kteří mohli během pití zaregistrovat tváře zamračené. Využití fotografie knihovny v jednom z výzkumů pak např. mělo za následek tišší verbální projev participantů. Priming je dle autorů modelu MINDSPACE nejméně popsaný a pochopený ze všech zahrnutých faktorů, hraje však zásadní roli. Ukazuje se, že např. i pouhé umísťování běžeckých bot do prostoru osoby může vést k podpoře zdravého životního stylu.

Příklad využití: *tento fakt je možné např. skrze vhodně zvolenou ikonografii a fotografické podklady využít i v případě motivace ke zvyšování kyberbezpečnosti. Vhodně zvolené podklady např. v centrální počítačové studovně mohou vést k obezřetnosti. Například ikonografie hackerů může podvědomě vést k bezpečnějšímu chování. Na druhou stranu: stylizovaný obrázek hackera může podporovat nevhodné stereotypní představy o podobě kyberkriminality a kyberkriminálníků; příliš negativní a opakující se ikonografie i zde může vést k pocitu „bezpečnostní letargie". To souvisí i s aspektem emocí, viz dále.*

Affect (emoce): emoční asociace a nálady hají zásadní roli v našem chování a rozhodování. Každé sdělení, které (nejen) v rámci kyberbezpečnostního rozvoje lidských zdrojů předáváme, ponese emoci. Jako příklad můžeme uvést první z modulů distribuovaných v rámci projektu CRP-KYBER21: využíváme v něm *storytelling* obohacený o ilustrační obrázek persony. Tato ilustrace nese emoci a může během zlomku vteřiny měnit způsoby, jak budou uživatelé daný příběh přijímat nebo jak ho budou vnímat. Zkoumání emocí v oblasti kyberbezpečnosti je netriviální záležitostí, jak odhalují např. Renaudová et al. (2021) v čerstvém výzkumu, kde mimo jiné u uživatelů identifikují automaticky negativní přístup ke kyberbezpečnosti, ovlivněný nejspíše bezpečnostní letargií.

Příklad využití: *zásadní je primárně nevytvářet pouze negativní emoci. Specifickou emocí, se kterou pracujeme v oblasti CSA je* strach*. Výzkumy ukazují, že strach může být sice vyznaným motivačním faktorem, stejně tak významně ale může vést ke kontraproduktivnímu chování a již zmíněné bezpečnostní letargii (security fatigue). Více k využívání a zkoumání tzv. fear appeals v oblasti kyberbezpečnosti viz např. Renaudová a Dupuis (2020). Důležité je podávat kromě potenciálního rizika i jeho řešení a dívat se na situaci pohledem uživatelů.*

Příklad využití: *některé univerzity využívají pro komunikaci kyberbezpečnostních obsahů maskoty – ti jsou zmíněny i v dokumentu NIST. Maskot by s ohledem na aspekt emoce neměl být volbou jednoho člověka nebo kybertýmu, ale je třeba ho testovat s různými cílovými skupinami nebo ho alespoň interně subjektivně ověřovat vůči vystavěným personám: „Jak bude Aleš nejspíše reagovat na oranžového medvídka Bezpečňáčka? Bude ho považovat za příliš infantilní a jakmile ho uvidí, automaticky bude sdělení ignorovat? Jak bude reagovat na postavy v našem kyberbezpečnostním komixu? Nebude smysluplnější komixy primárně tvořit pro jinou personu/cílovku a s přihlédnutím k tomu pak volit i kanály pro jejich komunikaci?"*

Commitments (*závazky*): podle studií zmíněných v modelu MINDSPACE máme tendenci prokrastinovat a odkládat rozhodnutí, která nám budou k užitku v dlouhodobém dopadu (*např. přestat s kouřením*). Jednou z metod boje proti této skutečnosti je veřejné zveřejnění závazku – jeho nesplnění má pak pro jednotlivce i možné společenské dopady, a dle studií vede takto pojatý závazek ke změně v chování.

Příklad využití: *v případě systému kyberbezpečnostního vzdělávání může jít například o veřejné závazky k dosažení jakési „kyberbezpečnostní excelence", kterou předem definujeme skrze podmínky studia a aktivit, např. že se uživatel pravidelně zapojuje do vzdělávacích programů, dobrovolně odebírá univerzitní kyberbezpečnostní newsletter, zapojuje se do testovacích phishingových kampaní atp. Díky odznáčku, který se veřejně zobrazuje v jeho profilu v informačním systému, se k těmto aktivitám veřejně „zavazuje" - a odznáček se např. vybarvuje nebo plní podle toho, jak úspěšný uživatel v plnění svého závazku aktuálně je. Zde je tedy motivační faktor závazku propojen s různými podobami vzdělávacího obsahu i metodou gamifikace do jednoho motivačního celku.*

Ego: chováme se tak, abychom o sobě uvažovali lépe. Ilustrací může být například tzv. základní atribuční chyba: při hodnocení situace, která se nám povedla, chválíme sebe; při hodnocení selhání většinou viníme okolí a kontext. Autoři MINDSETu také ukazují, že se snažíme vystupovat konzistentně: pokud v rámci řešení naší kyberbezpečnosti narazíme na konflikt našeho chování (*např. nevyužívám 2FA*) a našeho přesvědčení (*např. věřím, že řešit kyberbezpečnost je důležité*), většinou máme tendenci měnit své přesvědčení a zachovat konzistenci v chování. Motivační faktor ega je nutné citlivě promítat do vzdělávacích materiálů.

5. Zapojení do procesů univerzity

Významnou motivací pro studium kybervzdělávacích materiálů je samozřejmě **povinnost** takového studia. Ta může nabývat různých podob a rozsahů, neměla by ale být jediným motivačním aspektem našeho CSA snažení: skutečnost, že všichni zaměstnanci či studenti povinně projdou e-learningovým kurzem ještě nic nevypovídá o skutečném dopadu takového opatření – i proto jsme dosud text o motivaci opírali o model MINDSET a povinnost řešíme až nyní. S povinností samozřejmě většinou na VVŠ pracovat budeme, blíže o ní vypovídá interpretace normy viz výše, zde pro úplnost připojujeme **několik vybraných ukázek** způsobů pojetí povinného školení na zahraničních univerzitách. Povinnost účastnit se školení je většinou dána interními směrnicemi.

Wellesley University (více zde ↗)

→ Školení povinně každý rok včetně externích zaměstnanců s přístupem do systému;
→ postupně rozšířeno i na studenty;
→ oběti phishingu povinně znovu do dvou týdnů po identifikaci problému;
→ noví zaměstnanci do 30 dnů od nástupu;
→ povinné distanční školení pro zaměstnance trvá cca 20-45 minut a obsahuje krátká videa a kvízy.

> *„SANS is our Cyber Security Awareness training. It is required by the Written Information Security Policy to be taken annually by all administrative staff and also, effective fall 2021, by all students. Any faculty, union, or contract employee that has access to PI or requests access to Secure VPN is also required to complete this yearly training. Additionally, users who are the victims of a phishing attack are required to complete this course within 2 weeks after LTS identifies the issue, regardless of whether or not they have already completed the training. If a user fails to complete the training within 2 weeks, his or her remote access to College resources will be disabled. Newly hired employees are give 30 days to complete the training. LTS maintains records of all such training.*

University of Wisconsin (více zde ↗)

→ Školení kyberbezpečnosti povinně každý rok společně se studiem nových směrnic;
→ uživatelé jsou k plnění motivováni mimo jiné negativní finanční pobídkou (v případě nesplnění kyberbezpečnostní odborné přípravy nemá takový zaměstnanec nárok na úpravy platu či příplatky stanovené jeho pracovištěm);
→ samostatná sekce interní směrnice ustanovuje povinnost cvičných phishingových kampaní;
→ při třech selháních v rámci cvičného phishingu je zaměstnanec zařazen do speciálního navazujícího školení technik phishingu; pokud ho nesplní do 30 dnů, může být zbaven přístupu k univerzitním systémům.

> *Cybersecurity Awareness Training is required for all faculty and staff and available for all students, per UWSA Policy 1032. Employees who do not complete the training will be deemed ineligible for pay adjustments and bonuses determined by their local schools, colleges, or divisions and ineligible for pay plan increases. Complete your training today to satisfy this requirement.*

University of Nevada (více zde ↗)

→ Povinné školení nových zaměstnanců do 30 dnů po nástupu;
→ každý rok aktualizace skrze povinné školení všech zaměstnanců, mimo studenty zaměstnané či jinak vypomáhající na univerzitě;

UNLV faculty and staff are required to complete the cybersecurity awareness training on an annual basis. Guidelines for employees to maintain cybersecurity skills are outlined in the university's Mandatory Cybersecurity Training Policy. Student workers are not required to take the training at this time.