

Tvorba rizikových scénářů pro podporu reakce na incidenty

Bc. Lukáš Šťastný

Diplomová práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. Lukáš Šťastný
Osobní číslo:	A23397
Studijní program:	N1032A020003 Bezpečnostní technologie, systémy a management
Specializace:	Bezpečnostní technologie
Forma studia:	Kombinovaná
Téma práce:	Tvorba rizikových scénářů pro podporu reakce na incidenty
Téma práce anglicky:	Developing of Risk Scenarios to Support Incident Response

Zásady pro vypracování

- Popište problematiku a specifika řízení incidentů.
- Vypracujte teoretický přehled možností pro tvorbu rizikových scénářů.
- Analyzujte možné nástroje pro tvorbu scénářů.
- Navrhněte možné scénáře a vhodně je zapojte do vzdělávání a osvěty uživatelů.
- Realizujte interaktivní gamebook na základě navrženého scénáře.
- Provedte hodnocení a stanovte budoucí směřování.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. LUTTGENS, Jason T., PEPE, Matthew, a MANDIA, Kevin. Incident Response & Computer Forensics. 3rd ed. McGraw-Hill Professional, 2014. 624 s. ISBN 9780071798686.
2. BLOKDYK, Gerardus. Cyber Security Incident Response: A Complete Guide. 2019 Edition. 5STARCook, 2021. 317 s. ISBN 0655518479.
3. MARTIN-VEGUE, Tony. *How to Write Strong Risk Scenarios and Statements* [online]. [cit. 2024-10-25]. Dostupné z: <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-31/how-to-write-strong-risk-scenarios-and-statements>
4. STALLINGS, William. *Effective cybersecurity: understanding and using standards and best practices*. Upper Saddle River, NJ: Addison-Wesley, 2019. ISBN 978-0-13-477280-6.
5. STALLINGS, William. *Cryptography and network security: principles and practice*. Seventh edition, Global edition. Boston: Pearson, [2017]. ISBN 978-1-292-15858-7.

Vedoucí diplomové práce: **Ing. Lukáš Králík, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **29. listopadu 2024**

Termín odevzdání diplomové práce: **30. května 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 29. listopadu 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – diplomovou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na diplomové práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....

podpis autora

ABSTRAKT

Diplomová práce se zabývá problematikou tvorby rizikových scénářů pro podporu reakce na bezpečnostní incidenty. Teoretická část se věnuje řízení bezpečnostních incidentů, přehledu metod tvorby scénářů a analýze dostupných nástrojů, které tento proces podporují. Dále je zkoumán význam scénářů ve vzdělávání a osvětě uživatelů v oblasti kybernetické bezpečnosti. Praktická část práce zahrnuje návrh, tvorbu a realizaci interaktivních scénářů pomocí nástrojů jako H5P, Twine, Yo Scenario a PowerPoint. Výsledné scénáře jsou zaměřeny na běžné uživatele a mají za cíl zvýšit jejich povědomí o rizicích a správné reakci na incidenty prostřednictvím příběhového učení. V závěru je provedeno vyhodnocení efektivity tohoto přístupu na základě zpětné vazby od účastníků školení a nastíněny možnosti dalšího rozvoje.

Klíčová slova: bezpečnostní incidenty, rizikové scénáře, kybernetická bezpečnost, školení, interaktivní scénáře

ABSTRACT

This thesis addresses the development of risk scenarios to support incident response activities. The theoretical part focuses on incident management, an overview of scenario creation methods, and an analysis of available tools that assist in this process. It also explores the importance of scenarios in user education and cybersecurity awareness. The practical part involves the design, creation, and implementation of interactive scenarios using tools such as H5P, Twine, Yo Scenario, and PowerPoint. The developed scenarios target regular users and aim to increase their awareness of risks and appropriate incident responses through storytelling-based learning. The thesis concludes with an evaluation of the effectiveness of this approach based on participant feedback and outlines possibilities for future improvements.

Keywords: incident management, risk scenarios, cybersecurity, training, interactive scenarios

Rád bych vyjádřil upřímné poděkování vedoucímu mé diplomové práce, Ing. Lukáši Králíkovi, Ph.D., za odborné vedení, cenné rady, trpělivost a vstřícný přístup během celého zpracování této práce.

Zvláštní poděkování patří také mé ženě Kristýně Šťastné za její podporu, pochopení a trpělivost, kterou mi projevovala po celou dobu studia.

Mé poděkování směřuje i k mé dceři Patricii Šťastné, která mi svou přítomností dodávala motivaci a sílu překonávat náročné chvíle.

OBSAH

ÚVOD.....	13
I TEORETICKÁ ČÁST	14
1 ŘÍZENÍ BEZPEČNOSTNÍCH INCIDENTŮ.....	15
1.1 ÚVOD DO PROBLEMATIKY	15
1.2 DEFINICE A KLASIFIKACE BEZPEČNOSTNÍCH INCIDENTŮ.....	16
1.2.1 Základní rozdělení incidentů	17
1.2.2 Kategorizace podle dopadu a rozsahu	17
1.2.3 Modelové případy typických incidentů	18
1.3 PRÁVNÍ A NORMATIVNÍ RÁMCE ŘÍZENÍ INCIDENTŮ	19
1.3.1 ISO/IEC 27035	19
1.3.2 NIST SP 800-61	19
1.3.3 Evropské rámce a doporučení	20
1.3.4 Vztah k ochraně osobních údajů a hlášení incidentů	20
1.4 CÍLE A PŘÍNOSY ŘÍZENÍ INCIDENTŮ	21
1.4.1 Minimalizace dopadů incidentu	21
1.4.2 Zajištění provozní kontinuity	21
1.4.3 Ochrana informací a souladu s legislativou	21
1.4.4 Získání zpětné vazby a prevence budoucích incidentů	21
1.4.5 Zvyšování důvěry a reputace	21
1.4.6 Podpora školení a zvyšování připravenosti	22
1.5 FÁZE ŽIVOTNÍHO CYKLU ŘÍZENÍ INCIDENTU	22
1.5.1 Příprava	22
1.5.2 Detekce a identifikace	23
1.5.3 Analýza a klasifikace	23
1.5.4 Odezva a zmírnění dopadů	23
1.5.5 Obnova	23
1.5.6 Závěrečná analýza a poučení	23
1.6 ROLE TÝMŮ V ŘÍZENÍ INCIDENTŮ	24
1.6.1 Computer Security Incident Response Team	24
1.6.2 Interní spolupráce a zapojení dalších rolí	24
1.6.3 Externí partneři a outsourcing	24
1.7 NÁSTROJE A TECHNOLOGIE PRO ŘÍZENÍ INCIDENTŮ	25
1.7.1 Systémy SIEM	25
1.7.2 SOAR	25
1.7.3 Forenzní a monitorovací nástroje	26
1.7.4 Nástroje pro dokumentaci a koordinaci	26
1.8 VÝZVY A SPECIFIKA ŘÍZENÍ INCIDENTŮ	26
1.8.1 Lidský faktor a nepřipravenost uživatelů	26
1.8.2 Nedostatek zdrojů a kapacit	27
1.8.3 Krizová komunikace a řízení reputace	27

1.8.4	Právní a regulatorní nejistoty	27
1.9	TYPOLOGIE ÚTOČNÍKŮ A JEJICH MOTIVACE	28
1.9.1	Neorganizovaní útočníci.....	28
1.9.2	Interní hrozby	28
1.9.3	Kybernetičtí zločinci	28
1.9.4	Hacktivisté.....	28
1.9.5	Organizace podporované státem	29
1.9.6	Automatizované hrozby	29
2	TEORETICKÝ PŘEHLED MOŽNOSTÍ PRO TVORBU RIZIKOVÝCH SCÉNÁŘŮ	30
2.1	VÝZNAM SCÉNÁŘŮ V OBLASTI ŘÍZENÍ RIZIK A INCIDENTŮ	30
2.2	HISTORICKÝ VÝVOJ PŘÍSTUPŮ KE SCÉNÁŘŮM	31
2.3	TRADIČNÍ PŘÍSTUPY A MODEL Y PRO TVORBU SCÉNÁŘŮ	32
2.3.1	What-if analýza	32
2.3.2	Failure Modes and Effects Analysis.....	33
2.3.3	Analýza stromem poruch.....	33
2.3.4	Hazard and Operability Study a Structured What If Technique	33
2.4	MODERNÍ METODY TVORBY SCÉNÁŘŮ	33
2.4.1	STRIDE.....	34
2.4.2	Process for Attack Simulation and Threat Analysis.....	34
2.4.3	MITRE ATT&CK	34
2.4.4	Tvorba scénářů na základě CTI (Cyber Threat Intelligence)	34
2.5	TVORBA SCÉNÁŘŮ V KONTEXTU ŠKOLENÍ A SIMULACÍ	35
2.5.1	Tabletop cvičení a role-playing scénáře	35
2.5.2	Simulace útoků (Red Team / Blue Team)	35
2.5.3	Scénáře pro široké publikum – školení a osvěta	36
2.6	SOUČASNÉ TRENDY A VÝVOJ V OBLASTI SCÉNÁŘŮ	36
2.6.1	Automatizace a nástroje pro tvorbu scénářů	36
2.6.2	Využití umělé inteligence a predikce	36
2.6.3	Gamifikace a storytelling jako nové směry	37
2.6.4	Interaktivní příběhy a scénáře založené na rozhodování.....	37
2.6.5	Budoucí směřování.....	37
2.7	SCÉNÁŘE JAKO MOST MEZI TEORIÍ A REALITOU	37
3	ANALÝZA NÁSTROJŮ PRO TVORBU SCÉNÁŘŮ	39
3.1	KRITÉRIA PRO VÝBĚR NÁSTROJŮ	39
3.2	NÁSTROJE PRO SPRÁVU INCIDENTŮ A SIMULACÍ	40
3.2.1	TheHive.....	40
3.2.2	Request Tracker for Incident Response.....	40
3.2.3	Malware Information Sharing Platform	40
3.3	NÁSTROJE PRO VIZUALIZACI A PLÁNOVÁNÍ SCÉNÁŘŮ	40
3.4	NÁSTROJE PRO INTERAKTIVNÍ SCÉNÁŘE A ŠKOLENÍ.....	41

3.4.1	H5P.....	41
3.4.2	Twine.....	41
3.4.3	Yo Scenario	41
3.4.4	EdApp	41
3.4.5	Easygenerator	41
3.4.6	iSpring Suite.....	42
3.5	VÝHODY, OMEZENÍ A FINANČNÍ ASPEKTY NÁSTROJŮ PRO TVORBU SCÉNÁŘŮ	42
4	MOŽNOSTI VYUŽITÍ SCÉNÁŘŮ VE VZDĚLÁVÁNÍ A OSVĚTĚ UŽIVATELŮ	44
4.1	VZDĚLÁVÁNÍ POMOCÍ SCÉNÁŘŮ JAKO FORMA AKTIVNÍHO UČENÍ	44
4.2	FORMY VZDĚLÁVÁNÍ POMOCÍ SCÉNÁŘE	44
4.3	NÁSTROJE PODPORUJÍCÍ SCÉNÁŘOVÉ VZDĚLÁVÁNÍ	45
4.4	PŘÍNOSY VYUŽITÍ SCÉNÁŘŮ PRO ORGANIZACI	45
II	PRAKTICKÁ ČÁST.....	47
5	NÁVRH A PROSTŘEDÍ SCÉNÁŘE	48
5.1	CÍL PRAKTICKÉ ČÁSTI.....	48
5.2	METODIKA NÁVRHU SCÉNÁŘŮ	49
5.3	CÍLOVÁ SKUPINA A VZDĚLÁVACÍ PROSTŘEDÍ.....	51
5.3.1	Noví zaměstnanci jako hlavní cílová skupina	51
5.3.2	Začlenění do úvodního i opakovacího školení.....	52
5.4	POUŽITÉ NÁSTROJE PRO TVORBU SCÉNÁŘŮ	52
5.4.1	Twine – otevřený nástroj pro příběhové scénáře	53
5.4.2	Yo Scenario – profesionální nástroj pro rozvětvené scénáře	53
5.4.3	H5P – interaktivní obsah přímo v Moodle nebo pomocí programu Lumi	53
5.4.4	PowerPoint – klasická prezentace upravená pro e-learning.....	54
5.5	FIKTIVNÍ PROSTŘEDÍ A POSTAVY	54
6	TVORBA INTERAKTIVNÍHO SCÉNÁŘE	56
6.1	PROČ SCÉNÁŘE PRO BĚŽNÉ UŽIVATELE?	57
6.2	ZVOLENÉ FORMY: PŘÍBĚH, ROZHODNUTÍ, DŮSLEDEK.....	58
6.3	NÁSTROJE – SILNÉ A SLABÉ STRÁNKY	60
6.3.1	Moodle a H5P (prostřednictvím Lumi).....	60
6.3.2	Twine.....	61
6.3.3	Yo Scenario	61
6.3.4	PowerPoint	62
6.3.5	Publikace scénářů.....	62
6.4	PROPOJENÍ S LMS A FIREMNÍM ŠKOLENÍM	63
6.4.1	Vlastní server jako výuková platforma	63
6.4.2	Tematické rozdělení scénářů.....	63

7	REALIZACE INTERAKTIVNÍHO GAMEBOOKU NA ZÁKLADĚ NAVRŽENÉHO SCÉNÁŘE	65
7.1	MODUL H5P	65
7.2	TWINE	69
7.3	NÁSTROJ YO SCENARIO.....	72
7.4	POMOCÍ APLIKACE POWERPOINT.....	75
7.5	ZÁVĚREČNÉ SHRUTÍ A POROVNÁNÍ NÁSTROJŮ	79
8	VYHODNOCENÍ, PŘÍNOSY A DALŠÍ SMĚROVÁNÍ	80
8.1	VYHODNOCENÍ SCÉNÁŘŮ NA ZÁKLADĚ ZPĚTNÉ VAZBY	80
8.1.1	Jaký tip školení preferujete ?.....	80
8.1.2	Vyhodnocení zpětné vazby na gamebook s Janou (H5P)	81
8.1.3	Vyhodnocení zpětné vazby na gamebook s Radimem (Yo Scenario)	82
8.1.4	Vyhodnocení Radima pomocí Twine.....	83
8.1.5	Vyhodnocení Jany pomocí PowerPointu	84
8.1.6	Vyhodnocení Radima a aktualizace pomocí H5P	85
8.1.7	Vyhodnocení školení	86
8.2	PŘÍNOSY	90
8.3	DALŠÍ SMĚROVÁNÍ.....	91
	ZÁVĚR.....	92
	SEZNAM POUŽITÉ LITERATURY	93
	SEZNAM OBRÁZKŮ	95
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	97
	SEZNAM PŘÍLOH.....	99

ÚVOD

V dnešní digitální době čelí organizace rostoucímu počtu bezpečnostních hrozeb, které mohou vážně narušit jejich provoz, pověst i finanční stabilitu. Příprava na bezpečnostní incidenty se proto stává klíčovým prvkem celkového systému řízení rizik. Nejde přitom pouze o technická opatření – velkou roli hraje i schopnost zaměstnanců správně reagovat v krizových situacích.

V rámci této práce byly nejprve identifikovány, poté porovnány a následně vybrány vhodné nástroje a technologie, které umožňují inovativní formy školení a přípravy na bezpečnostní incidenty. Mezi tyto nástroje patří například H5P, Twine, Yo Scenario a PowerPoint, které podporují tvorbu interaktivních scénářů a simulací.

Pomocí těchto nástrojů byly vytvořeny vzdělávací scénáře zaměřené na běžné uživatele. Scénáře byly koncipovány tak, aby kombinovaly příběhový přístup, rozhodování a nabídku okamžité zpětné vazby. Jejich cílem je nejen zvýšit povědomí o kybernetických rizicích, ale především zlepšit připravenost uživatelů na reálné incidenty prostřednictvím aktivního a praktického učení.

Tato diplomová práce si klade za cíl nejen představit postup tvorby a implementaci těchto scénářů, ale také vyhodnotit jejich přínosy na základě zpětné vazby od účastníků školení a nastínit možnosti dalšího rozvoje tohoto přístupu.

I TEORETICKÁ ČÁST

1 ŘÍZENÍ BEZPEČNOSTNÍCH INCIDENTŮ

Bezpečnostní incidenty představují zásadní hrozbu pro stabilitu, důvěru a kontinuitu provozu firem kde využívají moderní techniku. Na druhou stranu s digitalizací a závislostí na informačních technologiích se zvyšuje i pravděpodobnost, že organizace bude dříve či později čelit situaci, kdy dojde k narušení její informační nebo komunikační infrastruktury. Taková situace může mít nejen technické, ale i právní, finanční a reputační dopady. [1][2]

Z těchto důvodů je řízení bezpečnostních incidentů chápáno jako nedílná součást systému řízení informační bezpečnosti. Jeho cílem je včasné rozpoznání incidentu, jeho analýza, omezení škod, rychlá obnova provozu a důsledná zpětná analýza. Proces řízení incidentů není improvizací v krizové situaci, ale řízeným a dokumentovaným souborem aktivit, které vycházejí z předem stanovených pravidel a scénářů. [3][4]

Efektivní řízení incidentů vyžaduje spolupráci napříč celou organizací. Kromě IT specialistů se často zapojují právníci a vedení firmy. Práce pod tlakem, rychlé rozhodování a nutnost přesné evidence všech kroků patří k základním charakteristikám incident response. [2]

Tato kapitola se věnuje problematice řízení bezpečnostních incidentů v širším kontextu. Jsou zde popsány definice a klasifikace incidentů, právní a normativní rámce (např. ISO/IEC 27035, NIST SP 800-61), jednotlivé fáze řízení, zapojené role a nástroje, stejně jako praktické výzvy. Dále je poukázáno na důležitost lidského faktoru a nutnosti trvalého vzdělávání, a to nejen v oblasti IT, ale i mobilní technice. [1][4]

Celý proces řízení incidentů je ve své podstatě pravidelný – s každým novým incidentem je systém revidován, aktualizován a lépe připraven na budoucí výzvy. Právě tato schopnost adaptace a učení se z vlastních i cizích chyb je považována za klíčový prvek úspěšné kybernetické bezpečnosti. [1][4]

1.1 Úvod do problematiky

V moderních organizacích, které jsou závislé na digitální infrastruktuře, je otázka kybernetické bezpečnosti považována za nezbytnou součást řízení provozních i strategických rizik. S rozšiřujícím se spektrem hrozeb, zahrnujících jak technické chyby, tak sofistikované útoky vedené útočníky zvenčí i zevnitř, vyvstává nutnost věnovat zvláštní pozornost zvládání incidentů, které tyto hrozby vyvolávají. [4]

Řízení bezpečnostních incidentů je definováno jako koordinovaný proces detekce, analýzy a reakce na události, které mohou ohrozit integritu, důvěrnost či dostupnost informačních aktiv. Tento přístup není vázán pouze na technologické nástroje, ale vyžaduje zapojení různých útvarů organizace a přesně stanovené kompetence jednotlivých rolí. Úspěšná reakce je podmíněna předchozí přípravou, zahrnující zavedení politik, stanovení odpovědností a technickou i organizační připravenost. [1][4]

Významnou roli sehrává rovněž schopnost rychlého rozhodování a efektivní komunikace, které jsou nezbytné v časově kritických situacích. Při zvládání incidentů bývá zároveň kladen důraz na dokumentaci průběhu, analýzu příčin a poučení, které slouží k posílení odolnosti do budoucna. [1]

Moderní přístupy k této problematice vycházejí z osvědčených rámců, jako jsou normy ISO/IEC 27035 nebo doporučení NIST SP 800-61, které poskytují strukturovaný model pokrývající jednotlivé fáze reakce – od identifikace až po závěrečnou revizi a optimalizaci procesů. Významné jsou také doporučení ENISA, která kladou důraz na praktickou použitelnost národních i evropských strategií a schopnost organizací adaptovat je na vlastní podmínky. [1][4]

Kromě samotné technologické připravenosti je nutné zohlednit i lidský faktor. Nedostatečné povědomí zaměstnanců, slabé politiky hesel, neschopnost rozpoznat phishing nebo selhání v krizové komunikaci bývají častými příčinami zhoršení situace. Právě proto je vzdělávání a školení považováno za nedílnou součásti účinného řízení incidentů. [1][2]

Na základě výše uvedeného lze konstatovat, že řízení bezpečnostních incidentů je víceúrovňový proces, který se neustále vyvíjí a musí být průběžně adaptován podle měnícího se prostředí i útočných technik. Jeho zvládnutí vyžaduje nejen investice do technologií, ale především jasně stanovené postupy, odpovědnosti a připravené lidské kapacity. [1][2][4]

1.2 Definice a klasifikace bezpečnostních incidentů

Bezpečnostní incident bývá v odborné literatuře definován jako událost, která narušuje nebo může narušit důvěrnost, integritu či dostupnost informací, systémů nebo služeb organizace. Taková událost vyžaduje zásah, protože představuje odchylku od běžného stavu, která může mít negativní dopad na chod organizace. [1][4]

Podle normy ISO/IEC 27035 je bezpečnostní incident chápán jako „jedna nebo více nežádoucích nebo neočekávaných bezpečnostních událostí, které pravděpodobně naruší provoz informačních systémů a ohrozí bezpečnost informací“. Americký rámec NIST SP 800-61 definuje incident jako „porušení bezpečnostních politik nebo opatření, které ohrožuje provozní schopnosti systému“. [1][4][5]

Pro účinnou reakci je nezbytné nejen incidenty identifikovat, ale také je systematicky třídit podle jejich povahy, míry závažnosti a potenciálního dopadu. Takovéto členění umožňuje stanovit adekvátní reakční kroky a určit, které týmy a role by měly být do řešení zapojeny.

1.2.1 Základní rozdělení incidentů

Incidenty lze rozdělit podle různých kritérií. Jedním z nejběžnějších způsobů je členění podle charakteru útoku:

- **Technické útoky** – například narušení firewallu, zneužití zranitelnosti systému, útoky typu DoS/DDoS, instalace škodlivého kódu (malware, ransomware). [4]
- **Sociálně-inženýrské útoky** – sem patří phishing, vishing, pretexting, kdy je uživatel přinucen k akci prostřednictvím manipulace. [1][4]
- **Fyzické incidenty** – ztráta zařízení, neoprávněný fyzický přístup k serverům, sabotáže.
- **Interní incidenty** – chyby nebo úmyslné jednání zaměstnanců (tzv. „insider threat“), např. únik dat nebo zneužití přístupových práv. [1][4]

1.2.2 Kategorizace podle dopadu a rozsahu

Způsobů, jak lze k dělení incidentů přistupovat je celá řada a neexistuje žádný konkrétní formální způsob. Dalším, často používaným dělením, je závažnost incidentu:

- **Nízká závažnost** – incidenty, které neovlivní provoz, např. pokus o neoprávněné přihlášení bez úspěchu.
- **Střední závažnost** – incidenty, které ovlivní část systému, ale lze je rychle vyřešit.
- **Vysoká závažnost** – incidenty s přímým dopadem na dostupnost služeb, ztrátu dat nebo ohrožení uživatelů, které vyžadují aktivaci krizového plánu. [1]

Z praktického hlediska bývá výhodné incidenty třídit i podle jejich četnosti (opakovaný vs. ojedinělý), způsobu detekce (automaticky vs. manuálně) nebo původu (externí vs. interní). Tato kategorizace umožňuje efektivnější nastavení metrik pro sledování, eskalaci a vyhodnocování incidentů. [4]

1.2.3 Modelové případy typických incidentů

V odborné literatuře bývají bezpečnostní incidenty často prezentovány prostřednictvím opakujících se scénářů, které umožňují efektivní kategorizaci a přípravu odpovídajících protipatření. Tyto typové případy slouží k ilustraci obvyklých hrozeb, se kterými se organizace setkávají napříč různými sektory. Jejich systematický popis přispívá k lepšímu porozumění dynamice útoků a podporuje tvorbu školicích a simulačních programů. [1][4]

Podle *Blokdyka* [2] a *Stallingse* [4] lze mezi běžně popisované incidenty zařadit následující schémata:

- **Scénáře založené na phishingu** – uživatel obdrží e-mail obsahující podvržený odkaz na přihlašovací formulář, jehož cílem je odcizení přístupových údajů. Tento typ incidentu je klasifikován jako sociálně-inženýrský útok a může mít za následek neoprávněný přístup k systémům nebo únik dat. [1][4]
- **Incidenty typu ransomware** – útočník pronikne do systému a zašifruje data, přičemž požaduje výkupné za jejich obnovení. Tento model se řadí mezi vysoce závažné incidenty s přímým dopadem na dostupnost klíčových služeb. [4]
- **Ztráta nebo odcizení zařízení** – například ztráta služebního notebooku bez odpovídajícího šifrování představuje riziko úniku citlivých informací. Jedná se o fyzický bezpečnostní incident, jehož důsledky lze částečně zmírnit pomocí technických opatření, jako je vzdálené vymazání. [4]
- **Únik dat způsobený chybou lidského faktoru** – neúmyslné zveřejnění souborů uložených v cloudovém prostředí nebo zaslání dat nesprávnému příjemci patří mezi časté příklady incidentů klasifikovaných jako neúmyslné porušení bezpečnostních pravidel. [3][4]
- **Vnitřní zneužití přístupových práv** – zaměstnanec zneužije oprávnění ke kopírování důvěrných dokumentů nebo k neoprávněné manipulaci s daty. Tento scénář je typickým příkladem interní hrozby (insider threat) a vyžaduje specifická preventivní opatření, jako je audit přístupů nebo separace pravomocí. [3][4]

Tyto modelové případy slouží nejen jako opora pro kategorizaci incidentů, ale zároveň jako základ pro návrh simulačních cvičení a scénářů určených k ověření připravenosti organizace. Literární zdroje doporučují jejich využití především při školení personálu, testování reakčních postupů a posuzování rizik. [3][4]

1.3 Právní a normativní rámce řízení incidentů

Pro efektivní řízení bezpečnostních incidentů je nezbytné, aby se organizace opírala o jednotný a uznávaný rámec, který vymezuje doporučené postupy, procesní fáze a odpovědnosti. Tato rámcová ukotvení se opírají o mezinárodní normy, národní strategie a oborové metodiky, které slouží nejen jako návod k praxi, ale často mají i právní nebo smluvní závaznost. [4]

1.3.1 ISO/IEC 27035

Základním dokumentem v oblasti řízení bezpečnostních incidentů je mezinárodní norma ISO/IEC 27035, která se zaměřuje na řízení bezpečnostních událostí a incidentů v rámci systému řízení informační bezpečnosti (ISMS). Tato norma poskytuje metodický přístup k detekci, hlášení, posuzování, zvládání a analýze incidentů a je členěna do několika částí, přičemž každá z nich se věnuje specifickým oblastem řízení událostí a reakcí. [4]

Norma klade důraz na systematické budování kapacit, plánování reakčních procesů a integraci incident managementu do širšího rámce řízení rizik. Důležitá je rovněž fáze post-incidentní analýzy, která umožňuje zlepšování procesů a zvyšování odolnosti organizace. [4]

1.3.2 NIST SP 800-61

Dalším široce uznávaným rámcem je dokument NIST SP 800-61 Revision 2, který byl vydán americkým Národním institutem pro standardy a technologie (NIST). Tento materiál nabízí praktický návod k zavedení a provozování týmu pro reakci na incidenty (IRT/CSIRT). Zaměřuje se především na čtyři základní fáze životního cyklu incidentu: přípravu, detekci, analýzu, odezvu a obnovu. [4]

Jedním z přínosů tohoto rámce je podrobnost a praktičnost jednotlivých kroků, které mohou být snadno přizpůsobeny potřebám konkrétní organizace. Současně je zde věnována pozornost technickým aspektům, jako je shromažďování důkazního materiálu, analýza záznamů a práce s logy. [1][4]

1.3.3 Evropské rámce a doporučení

V prostředí Evropské unie je oblast řízení kybernetických incidentů rámcově upravena směrnicí NIS2, která vymezuje požadavky na zabezpečení informačních systémů v klíčových odvětvích a u poskytovatelů digitálních služeb. Tato legislativa klade důraz na včasné odhalení, nahlášení a následné zvládnutí bezpečnostních událostí dle předem stanovených interních postupů [4]. Je však nezbytné zdůraznit, že směrnice NIS2 – podobně jako například nařízení GDPR – nemá bezprostřední právní účinek. Členské státy mají povinnost její obsah převést do vlastní legislativy tzv. transpozicí. V případě České republiky se předpokládá, že bude směrnice implementována formou nového zákona o kybernetické bezpečnosti, který nahradí současně platný zákon č. 181/2014 sb.

Důležitou podpůrnou roli v oblasti kybernetické bezpečnosti zastává Evropská agentura ENISA, která vytváří odborné materiály, metodiky a doporučení. Jejím cílem je posílit schopnosti členských států reagovat na kybernetické hrozby prostřednictvím školení, sdílení zkušeností a rozvoje odborných kapacit [4].

1.3.4 Vztah k ochraně osobních údajů a hlášení incidentů

V rámci evropského systému ochrany osobních údajů představuje významný právní nástroj nařízení (EU) 2016/679, známé jako GDPR. Toto nařízení stanovuje organizacím povinnost posoudit každý bezpečnostní incident, který by mohl vést k ohrožení osobních údajů, a v případě, že hrozí riziko pro práva a svobody fyzických osob, musí být incident nahlášen dozorovému orgánu do 72 hodin od okamžiku, kdy byl zjištěn [4]. Tato lhůta vytváří tlak na organizace, aby měly zavedena efektivní vnitřní pravidla pro včasné rozpoznání, posouzení a evidenci událostí, které se mohou dotýkat osobních údajů.

Součástí požadavků je rovněž povinnost vést záznamy o vzniklých incidentech a zabývat se jejich příčinami s cílem přijmout nápravná opatření a zabránit jejich opakování. Tímto způsobem se oblast řízení bezpečnostních incidentů přirozeně propojuje s celkovým systémem správy a ochrany osobních údajů [4].

Je však nutné upozornit, že nařízení GDPR nepředstavuje samostatně vykonatelný právní předpis na národní úrovni. V České republice se právní závaznost a praktické uplatnění jeho principů opírá o zákon č. 110/2019 Sb., o zpracování osobních údajů, který přináší konkrétní pravidla a výjimky přizpůsobené českému právnímu prostředí.[15]

1.4 Cíle a přínosy řízení incidentů

Řízení bezpečnostních incidentů je vnímáno nejen jako reakce na konkrétní hrozby, ale jako součást širšího rámce kybernetické odolnosti organizace. Jeho implementací jsou sledovány specifické cíle, které vycházejí jak z provozních potřeb, tak z požadavků právních předpisů a standardů řízení rizik. [4]

1.4.1 Minimalizace dopadů incidentu

Základním cílem řízení incidentů je omezení negativních důsledků, které mohou vzniknout v důsledku narušení informační bezpečnosti. Těmito dopady mohou být ztráta dat, výpadek služeb, poškození pověsti nebo finanční ztráty. Efektivní odezvou lze dosáhnout zkrácení doby trvání incidentu, omezení jeho šíření a rychlé obnovy provozu. [1][4]

1.4.2 Zajištění provozní kontinuity

Součástí cílů řízení incidentů je i udržení nebo obnovení klíčových funkcí organizace. Incidenty by neměly vést k dlouhodobým výpadkům či úplnému přerušení služeb. Reakční plán musí být sladěn s plány pro zajištění kontinuity podnikání (BCP) a disaster recovery (DR) strategií, aby bylo možné zajistit hladký přechod do nouzového režimu a zpětný návrat k běžnému provozu. [4][5]

1.4.3 Ochrana informací a souladu s legislativou

Dalším významným cílem je splnění povinností vyplývajících z legislativních požadavků a smluvních závazků. V evropském prostředí se jedná především o požadavky dané GDPR nebo NIS2, které stanovují pravidla pro detekci, hlášení a řešení bezpečnostních incidentů. [4] Nedodržení těchto pravidel může vést k sankcím nebo právní odpovědnosti.

1.4.4 Získání zpětné vazby a prevence budoucích incidentů

Řízení incidentů nemá pouze reaktivní charakter. Jedním z klíčových přínosů je možnost získat cenná data pro zpětnou analýzu, která napomáhá odhalit slabá místa v zabezpečení a navrhnout preventivní opatření. Dokumentací a vyhodnocením incidentů lze zvyšovat úroveň ochrany a efektivitu postupů. [4]

1.4.5 Zvyšování důvěry a reputace

Organizace, která dokáže transparentně a profesionálně zvládat bezpečnostní incidenty, působí důvěryhodně nejen vůči klientům, ale i vůči partnerům, investorům a regulačním

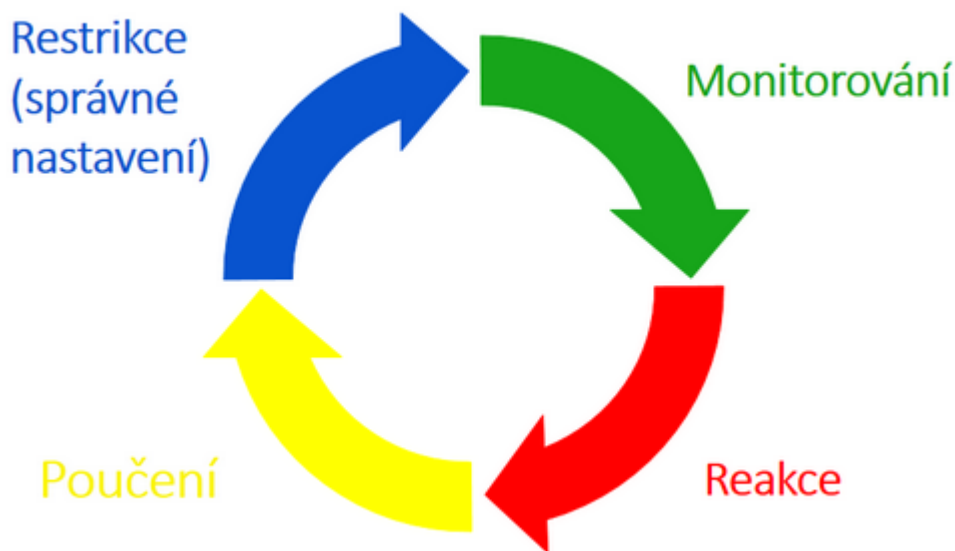
orgánům. Schopnost efektivně reagovat je považována za známku vysoké úrovně řízení a vyspělosti bezpečnostního systému. [4]

1.4.6 Podpora školení a zvyšování připravenosti

Incidenty a jejich zvládání mohou být využity jako zdroj reálných scénářů pro školení a trénink zaměstnanců. Tento přístup přispívá ke zvyšování bezpečnostního povědomí a připravenosti zaměstnanců čelit podobným situacím v budoucnu. Technické zdroje zdůrazňují význam realistických scénářů pro testování postupů a zvyšování kompetencí týmů. [1][4]

1.5 Fáze životního cyklu řízení incidentu

Proces řízení bezpečnostních incidentů bývá v odborné literatuře rozdělován do několika logických fází, které dohromady tvoří tzv. **životní cyklus incidentu**. Tento cyklus zajišťuje systematický přístup k řešení událostí od jejich vzniku až po uzavření a analýzu s cílem zamezit opakování. Přestože jednotlivé rámce se mohou v názvosloví lišit, základní struktura bývá zpravidla shodná. [1][4]



Obrázek 1 Životní cyklus incidentu

1.5.1 Příprava

Přípravná fáze představuje klíčový základ pro efektivní zvládnutí incidentu. V této etapě jsou definovány role a odpovědnosti, sestavují se reakční plány, nastavují se komunikační kanály a připravují se nástroje a postupy pro sběr důkazů. Dále je zajišťováno školení

zaměstnanců a testování reakčních scénářů. Příprava má zásadní vliv na rychlost a kvalitu následné reakce. [1][2][4]

1.5.2 Detekce a identifikace

Tato fáze zahrnuje rozpoznání bezpečnostní události, její analýzu a rozhodnutí, zda se jedná o incident. Detekce může být provedena různými způsoby – prostřednictvím bezpečnostního monitoringu (např. SIEM), upozorněním uživatele, nebo výskytem nestandardního chování systému. Klíčová je schopnost rychle vyhodnotit relevantnost a závažnost situace. [4]

1.5.3 Analýza a klasifikace

Po identifikaci následuje detailní analýza incidentu. Zjišťuje se, jakého systému se týká, jakého je původu, jaké mohou být jeho dopady a jaká data byla potenciálně kompromitována. Incident je zařazen do příslušné kategorie dle předem stanovené klasifikace (např. ransomware, phishing, vnitřní hrozba) a stanovuje se jeho priorita. [1][4]

1.5.4 Odezva a zmírnění dopadů

V této fázi jsou aplikována opatření ke zmírnění dopadu incidentu. Cílem je zastavit šíření útoku, odpojit infikované systémy, obnovit kontrolu a zabránit dalšímu poškození. Dále je možné zahájit odstranění škodlivého kódu, opravit zranitelnosti a obnovit provoz z bezpečných záloh. Tento krok bývá časově náročný a vyžaduje koordinaci různých týmů. [1][2]

1.5.5 Obnova

Jakmile je incident zastaven, přistupuje se k obnově provozu. Zasažené systémy jsou opětovně spuštěny, ověřuje se jejich funkčnost a provádí se závěrečná kontrola integrity. Součástí je i monitorování pro případný opakovaný výskyt incidentu. Obnova musí být provedena důkladně, aby nedošlo ke skrytému znovuoobjevení hrozby. [4]

1.5.6 Závěrečná analýza a poučení

Po uzavření incidentu je nutné provést jeho vyhodnocení. Dokumentuje se jeho průběh, způsob reakce, případné chyby a navrhuje se opatření pro budoucnost. Tyto výstupy se využívají pro aktualizaci politik, plánů i školicích programů. Fáze poučení bývá často opomíjena, přestože představuje významný nástroj pro posilování celkové bezpečnostní kultury. [1]

1.6 Role týmů v řízení incidentů

Efektivní reakce na bezpečnostní incidenty vyžaduje nejen dobře nastavené procesy a technologie, ale také **jasně definované role a kompetence jednotlivých týmů**. V praxi bývá řízení incidentů zajišťováno specializovanými útvary nebo externími partnery, přičemž je klíčová spolupráce napříč celou organizací. [1][4]

1.6.1 Computer Security Incident Response Team

Základní organizační jednotkou zodpovědnou za reakci na incidenty bývá tzv. CSIRT. Tento tým je obvykle zřízen interně v rámci organizace nebo na úrovni státní správy či akademické sféry. Jeho hlavním úkolem je příjem hlášení, analýza událostí, doporučení nápravných opatření a komunikace s dalšími subjekty. [1][4]

Role CSIRT může být dále rozdělena na operativní (monitorování, analýza), taktickou (koordinace zdrojů, reportování vedení) a strategickou (nastavení politik, tvorba scénářů, školení). Podle rámců NIST a ISO bývá doporučeno, aby CSIRT fungoval v režimu 24/7 a měl přímý přístup k vedení organizace. [4]

1.6.2 Interní spolupráce a zapojení dalších rolí

Kromě specializovaných týmů bývá do řízení incidentu zapojeno více organizačních jednotek. Mezi klíčové partnery patří:

- **IT oddělení** – technická podpora a obnova systémů,
- **právní útvar** – řešení dopadů na smluvní závazky a ochranu osobních údajů ve vztahu ke **GDPR a zákonu č. 110/2019 Sb., o zpracování osobních údajů**,
- **oddělení komunikace** – řízení interní a externí komunikace během krize,
- **vrcholové vedení** – rozhodování o eskalaci, rozsahu opatření a komunikaci s médii nebo regulátory. [1]

Efektivita reakce závisí na tom, zda byly tyto role předem definovány, zda existují komunikační scénáře a odpovědnostní matice (tzv. RACI model). [4]

1.6.3 Externí partneři a outsourcing

V některých případech bývá řízení incidentů částečně nebo zcela zajišťováno externími subjekty – např. dodavateli Managed Security Service Providers MSSP nebo právními kanceláři specializujícími se na kybernetické incidenty. Tento přístup může být výhodný

pro menší organizace nebo v situacích, kdy je incident natolik rozsáhlý, že přesahuje interní kapacity. [1]

Externí partneři by měli být součástí krizových plánů a smluvně zavázáni ke konkrétním lhůtám reakce (SLA), způsobu eskalace a odpovědnostem. Vhodná koordinace mezi interními a externími aktéry je klíčová pro zvládnutí komplexních útoků. [1]

1.7 Nástroje a technologie pro řízení incidentů

Řízení bezpečnostních incidentů je zajišťováno nejen procesně a organizačně, ale také za pomoci specifických technologií. Tyto nástroje podporují detekci, analýzu, dokumentaci, eskalaci a následnou obnovu provozu. Vzhledem k neustále se vyvíjejícím hrozbám je důležité, aby používané prostředky byly pravidelně aktualizovány a reflektovaly aktuální potřeby organizace. [4]

1.7.1 Systémy SIEM

Systémy typu SIEM slouží k shromažďování, korelaci a analýze bezpečnostních událostí z různých částí infrastruktury – síťových zařízení, serverů, koncových stanic i aplikací. Díky tomu je možné získat centralizovaný přehled o aktivitách v systému a včas detekovat anomálie nebo známky kompromitace. [4]

Pomocí pravidel nebo detekčních algoritmů je umožněno automatické označení podezřelého chování, které může signalizovat např. pokus o průnik, šíření malware nebo zneužití účtů. SIEM nástroje bývají základem SOC, odkud je incident dále řízen. [1][4]

1.7.2 SOAR

Technologie SOAR rozšiřuje možnosti klasických SIEM nástrojů o automatizaci reakce na incident. Pomocí předem definovaných scénářů může dojít k automatickému spuštění ochranných opatření – např. izolace napadeného zařízení, zablokování přístupu nebo vytvoření výstrahy pro analytika. [4]

SOAR zefektivňuje procesy tím, že zkracuje reakční dobu a eliminuje rutinní úkony. Díky napojení na databáze hrozeb a threat intelligence platformy je možné dynamicky reagovat na nové typy útoků. [4]

1.7.3 Forenzní a monitorovací nástroje

Součástí nástrojové výbavy by měly být také prostředky pro digitální forenzní analýzu, které umožňují zpětně zjistit průběh útoku, chování útočníka a případně shromáždit důkazní materiál pro další šetření nebo právní řízení. Používány bývají jak komerční nástroje (např. EnCase, FTK), tak open-source řešení (např. Autopsy). [1][4]

Mezi další podpůrné prostředky patří:

- **IDS/IPS systémy** (detekce a prevence průniku),
- **log management platformy,**
- **packet analyzátory** (např. Wireshark),
- **sandboxy pro analýzu podezřelých souborů.**

1.7.4 Nástroje pro dokumentaci a koordinaci

Pro správné řízení incidentu je nutné vést průběžnou dokumentaci. K tomu se využívají buď integrované moduly SIEM/SOAR systémů, nebo specializované nástroje pro správu incidentů (např. RTIR, TheHive). Tyto nástroje umožňují evidovat časové osy, úkony, odpovědnosti a výstupy z jednotlivých kroků řízení incidentu. [1]

Součástí podpory koordinace mohou být i nástroje typu issue tracker, collaboration platformy (např. MS Teams, Slack) nebo automatizované reportovací nástroje, které usnadňují sdílení informací mezi jednotlivými aktéry a pomáhají s eskalací incidentů směrem k vedení. [3]

1.8 Výzvy a specifika řízení incidentů

Ačkoli existují zavedené metodiky a nástroje, samotná realizace řízení bezpečnostních incidentů naráží v praxi na řadu výzev. Tyto výzvy se mohou týkat technologických, organizačních i lidských faktorů. Jejich zvládnutí je často klíčem k tomu, zda bude incident vyřešen rychle a s minimálními dopady, nebo zda přeroste v rozsáhlý bezpečnostní problém. [1][2]

1.8.1 Lidský faktor a nepřipravenost uživatelů

Jedním z nejčastějších problémů bývá nízké povědomí zaměstnanců o postupech při detekci a hlášení incidentu. Uživatelé si často nejsou jisti, zda situace představuje incident, a obávají

se, že jejich hlášení bude vnímáno jako selhání. [3] Tato váhavost může vést ke zpoždění reakce a zhoršení dopadů.

Současně se setkáváme s případy, kdy incident vznikl přímo vinou uživatele – např. kliknutím na škodlivý odkaz, použitím slabého hesla nebo odesláním dat neoprávněné osobě. Selhání jednotlivce se tak stává startovacím bodem pro celý incident. [4]

1.8.2 Nedostatek zdrojů a kapacit

V mnoha organizacích není zajištěno dostatečné personální a technické vybavení pro řízení incidentů. Chybějící nonstop dohled, nedostatek analytiků, slabé logování nebo chybějící procesy zpomalují reakci a znemožňují účinné zvládnutí události. Tato situace bývá běžná zejména u menších organizací bez vlastního SOC nebo CSIRT. [1]

Zdroje bývají navíc často soustředěny na prevenci a monitoring, zatímco schopnosti rychlé reakce a následné obnovy bývají podceňovány. Z toho důvodu bývá doporučováno pravidelné testování scénářů incidentů, tzv. tabletop cvičení, která pomáhají ověřit reálnou připravenost organizace. [1]

1.8.3 Krizová komunikace a řízení reputace

Komunikace během incidentu je kritickým prvkem celého procesu. Je-li realizována špatně – například zmatky v hlášení, nejasnosti v odpovědnosti nebo opožděná interní informovanost – dochází ke ztrátě důvěry, panice mezi zaměstnanci nebo dokonce k úniku neověřených informací směrem k médiím. [4]

Podcenění komunikační strategie může vést k výraznému poškození reputace organizace, a to i v případech, kdy samotný technický dopad incidentu byl relativně malý. Z tohoto důvodu se doporučuje vytvářet krizové komunikační plány jako integrální součást řízení incidentů. [1][2]

1.8.4 Právní a regulační nejistoty

Každý incident může mít i právní dopady – zejména pokud dojde k úniku osobních údajů, narušení smluvních povinností nebo ovlivnění zákazníků. V takových situacích je nutné postupovat v souladu s platnými předpisy, zejména s GDPR, NIS2 nebo se smluvními SLA. [2]

Často však bývá situace komplikována nejasností v odpovědnosti (např. mezi dodavatelem a zákazníkem), nejednotnými národními přístupy k hlášení incidentů nebo

nedostatkem právní expertízy přímo v organizační struktuře. Proto je doporučováno zapojení právních odborníků již při tvorbě plánů reakce. [4]

1.9 Typologie útočníků a jejich motivace

Pro správné nastavení řízení bezpečnostních incidentů je nezbytné porozumět tomu, kdo útoky provádí, jakými prostředky a s jakým cílem. Právě znalost typologie hrozeb a útočníků umožňuje lépe definovat preventivní opatření, reakční scénáře i následnou analýzu událostí. [1][4]

V odborné literatuře jsou útočníci členěni podle různých kritérií – nejčastěji podle motivace, technických schopností a dostupných prostředků. Tento přístup umožňuje kategorizaci aktérů do několika základních typů. [2]

1.9.1 Neorganizovaní útočníci

Tato skupina představuje jednotlivce s omezenými technickými znalostmi, kteří využívají veřejně dostupné nástroje a skripty k provádění jednoduchých útoků. Motivací bývá zvědavost, zábava nebo snaha o získání uznání v komunitě. Incidenty způsobené touto skupinou mívají nižší dopad, ale vysokou četnost. [4]

1.9.2 Interní hrozby

Zvláštní kategorii představují osoby působící uvnitř organizace – zaměstnanci, externisté nebo bývalí pracovníci. Může jít o úmyslné jednání (např. zneužití přístupových práv), ale i o neúmyslné pochybení (např. špatné nakládání s daty). Insider hrozby jsou obzvlášť závažné, protože útočník má přístup k systémům i znalost vnitřních procesů. [1][2]

1.9.3 Kybernetičtí zločinci

Tito aktéři využívají IT prostředky k finančně motivovaným útokům – např. pomocí ransomwaru, phishingu, zneužití platebních údajů nebo podvodných webů. Útoky jsou často dobře organizované, probíhají v rámci „kyberkriminality jako služby“ (CaaS) a zaměřují se na snadno zpeněžitelná aktiva. [1][4]

1.9.4 Hacktivisté

Hacktivismus kombinuje technické prostředky s ideologickou nebo politickou motivací. Cílem není nutně finanční zisk, ale vyjádření nesouhlasu, zviditelnění tématu nebo narušení

činnosti cílové organizace (např. státní instituce, nadnárodní firmy). Používané metody zahrnují DDoS útoky, defacement webů či úniky dat. [1][2]

1.9.5 Organizace podporované státem

Skupiny označované jako Advanced Persistent Threats (APT) disponují pokročilými prostředky a operují často s dlouhodobým strategickým cílem. Může jít o průmyslovou špionáž, destabilizaci infrastruktury nebo získávání citlivých informací. APT operace bývají dobře skrývané a obtížně detekovatelné. [4]

1.9.6 Automatizované hrozby

S nástupem automatizace a umělé inteligence dochází i k nárůstu incidentů způsobených robotizovanými systémy – např. botnety provádějící masivní útoky bez přímého zásahu člověka, nebo phishing generovaný pomocí jazykových modelů. Tyto hrozby kladou nové nároky na monitoring a reakční mechanismy. [4]

2 TEORETICKÝ PŘEHLED MOŽNOSTÍ PRO TVORBU RIZIKOVÝCH SCÉNÁŘŮ

Rizikové scénáře představují důležitý nástroj, který umožňuje simulovat potenciální bezpečnostní hrozby, vyhodnocovat jejich možné dopady a připravit organizaci na efektivní reakci. V oblasti informační bezpečnosti a řízení incidentů je tvorba scénářů využívána k identifikaci slabin, ověření připravenosti, testování odezvy a školení zaměstnanců. Scénáře tak tvoří most mezi teoretickým rámcem řízení rizik a praktickým zvládáním krizových situací. [2][4]

Pomocí vhodně sestaveného scénáře může být modelována konkrétní situace – například útok prostřednictvím phishingového e-mailu, zneužití oprávnění zaměstnance nebo výpadek cloudové služby – a následně mohou být analyzovány reakce jednotlivých aktérů. Tento přístup je v souladu s principy aktivního řízení rizik, kdy je důraz kladen nejen na prevenci, ale také na schopnost rychlé adaptace a zotavení. [1][3]

Využití scénářů není omezeno pouze na fázi plánování. Význam mají také při školení zaměstnanců, testování reakčních týmů (např. formou tzv. tabletop cvičení) a validaci nastavených politik. Scénáře rovněž podporují sdílení zkušeností, zvyšují bezpečnostní povědomí a pomáhají zviditelnit rizika, která by jinak mohla zůstat opomenuta. [3]

Tato kapitola se zaměřuje na systematický přehled metod, přístupů a trendů v oblasti tvorby rizikových scénářů. Nejprve je popsán jejich význam v kontextu bezpečnostního řízení, poté jsou představeny historické a tradiční metody, následně moderní přístupy reflektující současné hrozby a potřeby, a nakonec jsou analyzovány možnosti využití scénářů v oblasti školení a osvěty. Kapitola je uzavřena shrnutím aktuálních trendů a budoucího směřování tohoto nástroje v oblasti kybernetické bezpečnosti. [1][4]

2.1 Význam scénářů v oblasti řízení rizik a incidentů

Tvorba rizikových scénářů představuje základní nástroj pro pochopení, vizualizaci a řízenou simulaci potenciálních hrozeb. V kontextu řízení kybernetických rizik slouží scénáře k tomu, aby byly komplexní situace převedeny do konkrétních a uchopitelných modelů, které umožňují testování připravenosti a identifikaci slabých míst v systémech a procesech. [1][3]

Pomocí scénářů může být ověřeno, jak by organizace reagovala na incidenty různé závažnosti – od rutinních událostí až po krizové scénáře ohrožující kontinuitu provozu. Tím je podpořeno nejen plánování, ale i rozhodovací procesy na všech úrovních řízení. [1][4]

Využití scénářů se ukázalo jako mimořádně přínosné při zavádění bezpečnostních opatření, protože umožňuje simulovat situace, které ještě nenastaly, a přesto mohou mít zásadní dopad. Takto lze testovat připravenost nejen technické infrastruktury, ale také lidí – jejich reakce, schopnost spolupracovat, komunikovat a rozhodovat. [3]

Rizikové scénáře jsou rovněž nedílnou součástí rámců pro řízení informační bezpečnosti, jako jsou ISO/IEC 27001, ISO/IEC 27005 nebo NIST Risk Management Framework, které doporučují využívání modelových situací k vyhodnocování hrozeb a plánování odezvy. [4]

Při školení zaměstnanců a tréninku incident response týmů hrají scénáře klíčovou roli. Mohou být využívány v rámci tzv. tabletop cvičení, kde se účastníci bez reálného technického zásahu učí reagovat na modelové hrozby, nebo ve formě red teamingových aktivit, kdy jsou útoky simulovány co nejrealističtěji. [1]

Díky těmto vlastnostem lze tvorbu scénářů považovat za jeden z nejefektivnějších nástrojů pro propojování teorie a praxe v oblasti řízení rizik. Zatímco formální analýzy se zaměřují na pravděpodobnost a dopad, scénáře umožňují modelovat reálné dynamiky incidentu, včetně rozhodování, chování lidí a vlivu časového tlaku. [3]

2.2 Historický vývoj přístupů ke scénářům

Přístup k tvorbě scénářů se začal formovat již ve 20. století v oblastech vojenského plánování, krizového řízení a strategického rozhodování. První ucelené metody práce se scénáři byly rozvíjeny především ve vojenském prostředí, kde sloužily k přípravě na možné konfliktní situace s nejednoznačným vývojem. Již v této fázi byl kladen důraz na prediktivní simulaci možných událostí, jejich variant a dopadů. [4]

V 60. a 70. letech se tvorba scénářů rozšířila do oblasti strategického řízení v komerčním sektoru. Známým příkladem je využití scénářových metod v ropném průmyslu firmou Royal Dutch Shell, která díky této technice dokázala reagovat na ropnou krizi v roce 1973. Tím byla potvrzena efektivita scénářů jako nástroje pro podporu rozhodování v podmínkách nejistoty. [1]

V následujících desetiletích byly scénáře postupně adaptovány i do oblasti bezpečnosti. Nejprve šlo především o fyzické hrozby (např. požár, výpadek infrastruktury), později byly do scénářů začleňovány i technologické a informační rizikové faktory. S nástupem digitalizace, globalizace služeb a kybernetických útoků se scénářové techniky přesunuly do oblasti IT bezpečnosti a staly se součástí metodik pro řízení rizik. [1][4]

Zatímco dříve byly scénáře často statické a pracovaly s jednoduchým přístupem typu „co by se stalo, kdyby...“, dnešní metody scénářového modelování jsou výrazně pokročilejší. Využívají profilů konkrétních typů hrozeb (např. APT skupin) a umožňují větvení děje podle toho, jaké rozhodnutí zúčastněné osoby učiní. Významnou roli dnes hraje také lidské chování – tedy to, jak se jednotlivé role rozhodují v podmínkách stresu, tlaku na čas nebo v situacích s omezeným množstvím informací. [3]

V oblasti informační bezpečnosti je dnes tvorba scénářů považována za základní nástroj nejen v prevenci, ale i při samotném řízení incidentů a následném školení zaměstnanců. Vyvíjejí se nástroje pro automatizovanou generaci scénářů, využívá se prvků gamifikace a budují se interaktivní tréninková prostředí, která simulují reálné incidenty v bezpečném kontextu. [1][3]

2.3 Tradiční přístupy a modely pro tvorbu scénářů

Tradiční přístupy k tvorbě rizikových scénářů vycházejí převážně z průmyslového inženýrství, krizového managementu a systémové bezpečnosti. Tyto metody byly původně využívány pro analýzu provozních rizik, později však byly adaptovány i pro potřeby informační bezpečnosti. Jejich hlavním cílem je systematická identifikace rizikových faktorů, modelování jejich vzniku a navržení odpovídajících opatření. [1][4]

2.3.1 What-if analýza

What-if metoda je jedním z nejjednodušších a nejrozšířenějších nástrojů scénářové analýzy. Je založena na kladení otázek ve stylu „co by se stalo, kdyby..“, které umožňují simulovat potenciální problémy nebo havárie. Výhodou metody je její flexibilita a jednoduchá aplikovatelnost i bez složitých modelů. V oblasti informační bezpečnosti bývá využívána např. při analýze dopadů výpadků systémů, selhání přístupových kontrol či lidských chyb. [2]

2.3.2 Failure Modes and Effects Analysis

FMEA je strukturovaný postup, který slouží k odhalení možných chybových stavů systému, jejich příčin a odhadnutí, jaké následky mohou způsobit. Každé potenciální riziko se posuzuje podle tří hlavních hledisek: jak pravděpodobně může nastat, jak vážné dopady by mohlo mít a jak snadno se dá včas odhalit. Tyto faktory se následně využívají k výpočtu tzv. prioritního čísla rizika (RPN), které pomáhá určit, na které problémy je potřeba se zaměřit nejdříve. FMEA je vhodná především tehdy, když je potřeba detailně analyzovat konkrétní část systému nebo proces, a umožňuje tak včas odhalit slabá místa dřív, než dojde k jejich selhání. [2][4]

2.3.3 Analýza stromem poruch

Analýza stromem poruch (FTA) je grafická metoda, která znázorňuje logické vztahy mezi potenciálními chybami a konečným selháním systému. Využívá se především tam, kde je nutné pochopit kauzální vazby mezi jednotlivými událostmi. V kybernetické bezpečnosti může být FTA využita k modelování útoku – např. jakým způsobem by mohlo dojít k neoprávněnému přístupu do systému. [1]

2.3.4 Hazard and Operability Study a Structured What If Technique

Metody Hazard and Operability Study HAZOP a Structured What If Technique SWIFT byly původně určeny pro procesní průmysl, ale našly uplatnění i v oblasti IT. Využívají strukturovaných otázek a týmové práce k odhalování možných odchylek od očekávaného chování systému. Obě metody jsou vhodné tam, kde je třeba získat různé pohledy na systém a identifikovat nečekané kombinace rizik. [2][3]

2.4 Moderní metody tvorby scénářů

S vývojem kybernetických hrozeb a rostoucí složitostí IT prostředí bylo nutné rozšířit scénářové přístupy o nové rámce, které lépe reflektují specifika informační bezpečnosti. Moderní metody se zaměřují nejen na technické aspekty útoků, ale také na chování útočníků, fáze útoku a propojení s konkrétními zranitelnostmi. Jsou navrhovány tak, aby byly prakticky využitelné při plánování obranných opatření, tvorbě scénářů útoků i školení zaměstnanců. [1][4]

2.4.1 STRIDE

Model STRIDE je framework vyvinutý společností Microsoft pro klasifikaci hrozeb v oblasti softwarové architektury. Zkratka označuje šest typů hrozeb: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege. Tato klasifikace umožňuje systematicky analyzovat rizika na úrovni jednotlivých komponent a vytvářet scénáře simulující jejich zneužití. [4]

STRIDE je často využíván při modelování hrozeb v rámci tzv. threat modeling workshops, kde jsou společně s architekty, vývojáři a bezpečnostními specialisty tvořeny hypotetické útoky na konkrétní části systému. [2]

2.4.2 Process for Attack Simulation and Threat Analysis

Metodika PASTA představuje strukturovaný přístup k tvorbě scénářů zaměřených na útoky. Skládá se ze sedmi fází – od analýzy cílů organizace přes identifikaci zranitelností až po simulaci a kvantifikaci dopadů útoků. Výsledkem je sada scénářů, které odpovídají reálným možnostem útočníků s ohledem na specifika daného prostředí. [1]

PASTA je vhodná zejména pro větší organizace nebo projekty, kde je třeba propojit bezpečnostní analýzu s obchodními cíli, a kde je nutné zohlednit více typů hrozeb a vektorů útoku. [3]

2.4.3 MITRE ATT&CK

Databáze MITRE ATT&CK je celosvětově uznávaný rámec, který katalogizuje techniky a taktiky používané útočníky v různých fázích útoku. Umožňuje vytvářet scénáře založené na reálném chování hrozeb, jak bylo pozorováno v praxi. Scénáře mohou být vytvářeny podle jednotlivých útočných technik (např. spear-phishing, privilege escalation) a kombinovány do tzv. kill chains. [2]

Výhodou ATT&CK je vysoká granularita a možnost přímého propojení s nástroji pro detekci a monitoring (např. SIEM). Databáze je pravidelně aktualizována a podporuje i simulace útoků v rámci red teamingových aktivit. [4]

2.4.4 Tvorba scénářů na základě CTI (Cyber Threat Intelligence)

Moderní přístupy stále častěji využívají data z cyber threat intelligence (CTI) – tedy informace o aktuálních hrozbách, kampaních a aktérech. Tyto informace umožňují tvořit

scénáře, které odpovídají aktuálním trendům a technikám používaným útočníky. Scénáře tak nejsou statické, ale jsou průběžně přizpůsobovány nově zjištěným faktům. [3]

CTI scénáře se využívají nejen v technických týmech, ale také při školení zaměstnanců, kde se díky jejich aktualitě zvyšuje vnímání reálného rizika a relevance školených situací. [2]

2.5 Tvorba scénářů v kontextu školení a simulací

Scénáře nacházejí široké uplatnění nejen při plánování a analýze bezpečnostních hrozeb, ale také jako účinný nástroj při školení zaměstnanců a testování reakčních týmů. Jejich výhodou je možnost modelovat realistické situace, ve kterých si účastníci procvičí rozhodování, komunikaci i technické kroky potřebné pro zvládnutí incidentu. [2][3]

Použitím scénářů ve výcviku dochází k přenosu znalostí ze statických dokumentů do aktivního zážitku, což zvyšuje míru zapamatování a připravenosti. Při vhodně navrženém scénáři je zaměstnanci umožněno zažít dopady chybného rozhodnutí v kontrolovaném prostředí, aniž by došlo ke skutečné škodě. [1][3]

2.5.1 Tabletop cvičení a role-playing scénáře

Jedním z běžných formátů využití scénářů ve výuce jsou tzv. tabletop cvičení, během kterých je simulován bezpečnostní incident a účastníci (např. členové CSIRT, IT oddělení nebo vedení organizace) diskutují a rozhodují o vhodných krocích. Tyto scénáře nejsou technicky realizovány, ale zaměřují se na strategii, komunikaci a eskalaci. [1]

V některých případech je využíváno i role-playing formátu, kdy jsou účastníkům přiděleny konkrétní role (např. vedoucí IT, PR manažer, právník) a jejich úkolem je reagovat v souladu s odpovědnostmi a interními postupy organizace. [4]

2.5.2 Simulace útoků (Red Team / Blue Team)

V technicky orientovaných organizacích bývají scénáře využívány i v rámci tzv. red teamingových cvičení, kdy skupina (Red Team) simuluje útočníky a druhá (Blue Team) se snaží incident detekovat a zastavit. Tento typ tréninku umožňuje praktické prověření obranných schopností a poskytuje důležité poznatky o silných i slabých místech bezpečnostního systému. [2]

Simulace útoků může být také částečně nebo plně automatizována pomocí nástrojů, které napodobují chování útočníků podle rámce MITRE ATT&CK. Tím je možné testovat konkrétní techniky a vyhodnocovat reakční dobu i schopnosti týmu. [4]

2.5.3 Scénáře pro široké publikum – školení a osvěta

Scénáře nejsou určeny pouze pro technické specialisty. Naopak, jejich význam roste při školení běžných uživatelů, kteří často tvoří první linii obrany. Pomocí jednoduchých, ale realistických scénářů (např. příjem phishingového e-mailu, podezřelý USB disk) může být posíleno **bezpečnostní povědomí** a schopnost rozpoznat hrozbu. [3]

Důležitou roli hraje jazyk a forma scénáře – musí být srozumitelný, přiměřený cílové skupině a motivující k účasti. V tomto ohledu se osvědčuje využití **gamifikace, interaktivních příběhů nebo gamebooků**, které umožňují účastníkům ovlivňovat vývoj situace a zažívat přímé důsledky svých rozhodnutí. [3][4]

2.6 Současné trendy a vývoj v oblasti scénářů

S rostoucí potřebou přizpůsobit řízení kybernetické bezpečnosti rychlým změnám a novým hrozbám dochází k vývoji nových přístupů ke scénářům. Moderní scénáře se vyznačují vyšší mírou automatizace, přizpůsobivostí, propojením na reálná data a v neposlední řadě i důrazem na zážitkové vzdělávání a zapojení uživatele. [3][4]

2.6.1 Automatizace a nástroje pro tvorbu scénářů

Vývoj softwarových nástrojů umožňuje generovat scénáře automaticky, například na základě logů ze SIEM, dat z CTI platforem nebo detekovaných anomálií. Tyto scénáře pak mohou sloužit k tréninku analytiků nebo k testování připravenosti týmů. [2] Význam mají i nástroje podporující threat modeling a simulaci útoků podle rámců jako MITRE ATT&CK. [4]

2.6.2 Využití umělé inteligence a predikce

S příchodem nástrojů umělé inteligence (AI) dochází k posunu i v oblasti prediktivní tvorby scénářů. Pomocí AI je možné analyzovat předchozí incidenty, rozpoznávat vzorce chování útočníků a na jejich základě generovat hypotetické útoky nebo doporučení pro obranné strategie. Tento přístup se nachází v rané fázi, ale ukazuje potenciál k dynamickému přizpůsobení scénářů reálným podmínkám. [1]

2.6.3 Gamifikace a storytelling jako nové směry

Scénáře jsou stále častěji vytvářeny s důrazem na poutavost, interaktivitu a zapojení emocí. Zatímco dříve byly soustředěny na technickou přesnost, dnes je snaha vtáhnout účastníka do děje a vytvořit prostředí, kde je rozhodování spojeno s přímými důsledky.

Z tohoto důvodu bývají scénáře stylizovány do formy příběhů, využívají fiktivní postavy, mají dialogy a větvící se děj. Tato metoda je vhodná zejména pro školení běžných zaměstnanců, kteří nemají technické zázemí, ale musí umět rozpoznat hrozby a správně reagovat. [3][4]

2.6.4 Interaktivní příběhy a scénáře založené na rozhodování

Jedním z přístupů reflektujících výše uvedené trendy je také tvorba interaktivních příběhů, které vedou uživatele prostřednictvím simulovaného děje. V rámci této diplomové práce je tento přístup dále rozpracován v praktické části, kde slouží jako nástroj pro školení zaměstnanců v oblasti kybernetické bezpečnosti. Interaktivní forma umožňuje vyzkoušet různé možnosti reakce na incident a pochopit jejich důsledky v bezpečném prostředí.

2.6.5 Budoucí směřování

Do budoucna lze očekávat další rozvoj scénářových metod směrem k větší personalizaci, využívání behaviorálních dat, adaptivním simulacím a zapojení uživatelů pomocí rozšířené reality či virtuálních tréninkových prostředí. Scénáře tak stále více plní roli mostu mezi teorií, praxí a vzděláváním v oblasti kybernetické bezpečnosti. [2][4]

2.7 Scénáře jako most mezi teorií a realitou

Teoretické modely řízení rizik a incidentů, ať už vycházejí z mezinárodních standardů, akademických rámců nebo bezpečnostních směrnic, poskytují strukturovaný pohled na kybernetickou bezpečnost. Jejich výhodou je systematičnost, srovnatelnost a opakovatelnost. Jejich slabinou však často bývá odtrženost od reálného chování lidí v konkrétních situacích. [3][4]

V této souvislosti hrají scénáře jedinečnou roli – umožňují převést abstraktní zásady, pravidla a politiky do konkrétních modelových situací. V nich může být simulována nejen technická stránka incidentu, ale také lidská rozhodnutí, emoce, časový tlak a mezilidská komunikace, které jsou pro reálné zvládnutí bezpečnostních událostí často klíčové. [1][3]

Právě díky schopnosti spojovat formální strukturu s praktickým prožitkem jsou scénáře vhodné nejen pro školení, ale i pro testování, ověřování a ladění bezpečnostních opatření. Mohou sloužit jako zrcadlo, ve kterém si organizace ověřuje, zda její bezpečnostní strategie ob stojí i ve chvílích nejistoty a tlaku. [2]

Využitím scénářů lze také překlenout propast mezi IT a zbytkem organizace – protože právě skrze příběh, modelovou situaci nebo jednoduché rozhodování dokáží i netechnicky zaměřený zaměstnanec pochopit, jak jejich chování ovlivňuje bezpečnost celku. [3]

Tato schopnost přiblížit odborné koncepty běžným uživatelům činí ze scénářů cenný nástroj nejen analytický, ale i edukativní a transformační. V následující části práce bude představen návrh takového scénáře formou interaktivního příběhu, který kombinuje odborné poznatky s principy poutavého vyprávění a rozhodovací logiky.

3 ANALÝZA NÁSTROJŮ PRO TVORBU SCÉNÁŘŮ

Tvorba kvalitních a realistických scénářů v oblasti kybernetické bezpečnosti vyžaduje využití vhodných nástrojů, které umožňují jejich efektivní návrh, strukturování, vizualizaci a následné uplatnění v rámci školení nebo reakce na incidenty. Tato kapitola se zaměřuje na přehled konkrétních nástrojů, které se v praxi používají, a rovněž na kritéria, podle nichž je jejich výběr prováděn.

3.1 Kritéria pro výběr nástrojů

Při rozhodování o volbě nástroje pro tvorbu scénářů je třeba zohlednit řadu faktorů, které ovlivňují vhodnost daného řešení pro konkrétní prostředí. Obecně lze tato kritéria rozdělit do následujících kategorií:

- **Cílová skupina uživatelů**

Zda je scénář určen pro technické pracovníky, běžné zaměstnance, management nebo specializované týmy.

- **Typ scénáře**

Jestli se jedná o příběhový, simulační, školící nebo analytický scénář. Od toho se odvíjí požadavky na interaktivitu, rozhodovací logiku a zpětnou vazbu.

- **Možnosti distribuce a integrace**

Kompatibilita s existujícím LMS systémem (např. Moodle), podpora SCORM nebo xAPI, možnost webového nasazení.

- **Uživatelská přívětivost**

Důležitá zejména pro neprogramátory – editoři s intuitivním rozhraním snižují náklady na školení autorů.

- **Možnosti měření a vyhodnocení**

Podpora analýzy chování uživatele ve scénáři, sledování odpovědí, export dat.

- **Nákladovost a dostupnost**

Zda se jedná o open-source řešení (např. Twine, H5P), placenou platformu (např. některé LMS pluginy), nebo interně vyvíjený nástroj.

Správně zvolený nástroj zvyšuje efektivitu scénářového vzdělávání a umožňuje flexibilní přizpůsobení měnícím se hrozbám a cílovým skupinám.

3.2 Nástroje pro správu incidentů a simulací

Tyto nástroje umožňují zaznamenávání, modelování a vyhodnocování bezpečnostních incidentů. Využívají se především ve specializovaných týmech (např. CSIRT, SOC), ale své uplatnění nacházejí i při plánování tréninků a analýz.

3.2.1 TheHive

TheHive je open-source platforma pro správu incidentů, která umožňuje strukturovat případy (cases), zaznamenávat jednotlivé kroky, připojovat artefakty a sledovat reakce týmů. Nástroj je vhodný pro bezpečnostní analytiku a často bývá propojen s dalšími systémy jako MISP. [1][9]

3.2.2 Request Tracker for Incident Response

Request Tracker for Incident Response RTIR je modul systému RT zaměřený na evidenci a řízení bezpečnostních incidentů. I když je technicky náročnější, nabízí vysokou flexibilitu a možnost přizpůsobení pro tvorbu testovacích scénářů nebo vedení školení. [1]

3.2.3 Malware Information Sharing Platform

Platforma Malware Information Sharing Platform MISP je určena pro sdílení informací o hrozbách. Kromě této funkce umožňuje i vizualizaci vzorců útoků, na jejichž základě lze sestavovat realistické scénáře a analyzovat šíření hrozby v čase. [2]

3.3 Nástroje pro vizualizaci a plánování scénářů

Pro fázi návrhu a komunikace scénáře se využívají nástroje umožňující znázornění rozhodovacích větví, logiky incidentu nebo návaznosti jednotlivých kroků.

- **draw.io, Lucidchart** – vizuální editory pro tvorbu stromových struktur, které se hodí pro mapování větvících se scénářů.
- **BPMN nástroje** – jako je Camunda nebo Bizagi, umožňují popsat incident jako proces a napojit ho na další organizační struktury.

- **MindMup, XMind** – nástroje pro myšlenkové mapy, které podporují brainstorming a vývoj struktury scénáře. [3]

3.4 Nástroje pro interaktivní scénáře a školení

Jednou z nejdůležitějších oblastí využití scénářů je jejich začlenění do vzdělávacích programů, školení a interních kampaní. K tomuto účelu existuje řada nástrojů, které umožňují tvorbu větvících scénářů, interaktivních příběhů nebo rozhodovacích simulací.

3.4.1 H5P

H5P je open-source modul pro tvorbu vzdělávacích aktivit, který podporuje větvené scénáře, kvízy, prezentace nebo simulace rozhodnutí. Je kompatibilní s Moodle, WordPress a dalšími LMS. Díky přehlednému rozhraní je vhodný i pro netechnické autory. [6]

3.4.2 Twine

Twine je nástroj pro tvorbu interaktivních příběhů. Podporuje skriptování, proměnné i logické větvení. Uplatnění nachází při vytváření scénářů s důrazem na příběh a rozhodování – zejména v oblasti školení uživatelů na běžná rizika. [8]

3.4.3 Yo Scenario

Yo Scenario je cloudová platforma zaměřená na školení zaměstnanců pomocí scénářového rozhodování. Nabízí možnost zpětné vazby, export do SCORM/xAPI a integraci s LMS. Je vhodná pro jednoduché, ale účinné scénáře z běžného pracovního prostředí. [7]

3.4.4 EdApp

Mobilní microlearningová platforma, která umožňuje vytvářet krátké, interaktivní lekce. Podporuje gamifikaci, analytiku a scénářové otázky. Je vhodná pro rychlé interní školení v oblasti bezpečného chování, např. při práci s e-mailem nebo hesly. [9]

3.4.5 Easygenerator

Nástroj pro tvorbu e-learningových kurzů s možností větvení a zpětné vazby. Nabízí intuitivní rozhraní a export do SCORM. Vhodný pro menší a střední firmy hledající rychlé řešení bez nutnosti programování. [10]

3.4.6 iSpring Suite

Rozšíření PowerPointu určené pro tvorbu profesionálních e-learningových scénářů. Umožňuje simulace rozhovorů, větvené rozhodování a tvorbu školení, která lze snadno zařadit do stávajících interních systémů. [11]

3.5 Výhody, omezení a finanční aspekty nástrojů pro tvorbu scénářů

Volba vhodného nástroje pro tvorbu scénářů není závislá pouze na jeho technických parametrech, ale i na organizačních potřebách, uživatelské přívětivosti a finanční dostupnosti. V této podkapitole jsou shrnuty hlavní výhody a limity, které je třeba při implementaci nástrojů do vzdělávání a tréninku zvažovat.

Výhody nástrojů pro scénáře vzdělávání:

- **Interaktivita a zpětná vazba:**

Uživatel je aktivně zapojen do simulace incidentu, což zvyšuje míru zapamatování a porozumění. Možnost okamžité zpětné vazby podporuje reflexi rozhodnutí. [6][7]

- **Flexibilita přizpůsobení:**

Scénáře lze upravit podle cílové skupiny, pracovní role, typu útoku nebo organizační kultury. [7][8]

- **Podpora e-learningových standardů:**

Možnost exportu do formátů SCORM nebo xAPI umožňuje bezproblémovou integraci do většiny LMS systémů (např. Moodle, MS Viva Learning apod.). [11]

- **Rychlá tvorba a nasazení:**

Intuitivní editory umožňují rychlou tvorbu obsahu i bez pokročilých technických dovedností. [10]

Omezení a výzvy:

- **Technická náročnost pokročilých funkcí:**

U některých nástrojů (např. Twine nebo iSpring) může být potřeba základních znalostí programování, skriptování nebo práce s proměnnými. [8][11]

- **Závislost na kvalitě obsahu:**

Ani nejlepší nástroj nenahradí špatně napsaný scénář. Obsah musí být věcný, realistický a přizpůsobený uživatelům. [3]

- **Náročnost lokalizace:**

Některé platformy nemají plnou podporu češtiny, což může být komplikací při školení netechnických uživatelů. [10]

Finanční hledisko a licencování

Licenční modely jednotlivých nástrojů se liší podle rozsahu funkcí, způsobu nasazení i cílové skupiny:

- **Open-source řešení (např. Twine)** jsou zdarma dostupná a vhodná zejména pro vlastní nasazení. Vyžadují však technické zázemí a často chybí podpora. [8]
- **H5P** je open-source modul, jehož základní funkcionalita je zdarma dostupná pro lokální nasazení (např. v Moodle). Komerční cloudová verze H5P.com však nabízí rozšířené funkce jako analytiku, správu uživatelů či profesionální podporu, a je zpoplatněna dle počtu uživatelů. [6]
- **Yo Scenario, Easygenerator, iSpring Suite** nabízejí komerční licence, často formou ročních předplatných. Výhodou je jednoduché ovládání, podpora a integrace, nevýhodou vyšší pořizovací cena. [7][10][11]
- **EdApp** nabízí bezplatný plán pro malé organizace, ale pokročilé funkce (LMS, gamifikace, reporting) jsou dostupné pouze v placených variantách. [9]

Při výběru nástroje je nutné posoudit nejen pořizovací cenu, ale i celkové TCO (Total Cost of Ownership) – včetně školení autorů, správy obsahu a aktualizací.

4 MOŽNOSTI VYUŽITÍ SCÉNÁŘŮ VE VZDĚLÁVÁNÍ A OSVĚTĚ UŽIVATELŮ

Rizikové scénáře nejsou využívány pouze při technické analýze nebo plánování odezvy na bezpečnostní incidenty. Významnou roli sehrávají také při vzdělávání zaměstnanců a budování bezpečnostního povědomí v organizacích. Díky své názornosti a schopnosti simulovat reálné situace představují scénáře vhodný nástroj pro osvětu i trénink.

Tato kapitola se zaměřuje na konkrétní formy využití scénářů ve vzdělávání, školení a interních kampaních. Současně představuje výhody přístupu založeného na scénářích oproti tradičním metodám výuky a zohledňuje různé formy prezentace – od jednoduchých testů až po interaktivní příběhy.

4.1 Vzdělávání pomocí scénářů jako forma aktivního učení

Zatímco klasické školení často spoléhá na přednášku a pasivní příjem informací, scénářová výuka umožňuje aktivní zapojení účastníků. Uživatelé jsou postaveni do simulovaných situací, kde se od nich očekává rozhodování a zvažování důsledků.

Tento přístup podporuje:

- lepší zapamatování díky propojení s konkrétní situací,
- emoční angažovanost, která zvyšuje motivaci,
- kritické myšlení a analýzu rozhodnutí,
- přenesení zkušenosti do praxe. [3][6]

Učení se tak nestává jen teoretickou disciplínou, ale zážitkem, který formuje postoj uživatele k bezpečnosti.

4.2 Formy vzdělávání pomocí scénáře

Zaškolení nových zaměstnanců

Při nástupu do organizace lze využít základní scénáře (např. zacházení s hesly, práce s e-mailem, rozpoznání podvodu) pro rychlé seznámení s bezpečnostními pravidly.

Pravidelná školení

Scénáře umožňují připomenutí zásad bezpečného chování formou příběhu nebo simulačního testu. Lze je obměňovat dle aktuálních hrozeb. [6][10]

Tabletop cvičení a simulace

Pro pokročilé role (např. IT týmy) se využívají tzv. tabletop scénáře, kde se tým rozhoduje v simulované krizi. Tento přístup je běžně používán ve větších firmách nebo organizacích veřejné správy. [1][4]

Interní kampaně a osvěta

Během kampaní (např. Měsíc kybernetické bezpečnosti) se scénáře využívají jako edukační prvky – ve formě miniher, kvízů nebo krátkých animací. [7][9]

4.3 Nástroje podporující scénářové vzdělávání

Jak již bylo uvedeno v kapitole 3, tvorba a distribuce scénářů je dnes podporována širokou škálou nástrojů. Nejčastěji využívané jsou:

- H5P – tvorba větvených scénářů a interaktivních prezentací v LMS prostředí. [6],
- Twine – vývoj narativních příběhů pro školení i samostatné miniaplikace. [8],
- Yo Scenario – jednoduchý nástroj pro rozhodovací scénáře s hodnocením. [7],
- Easygenerator, EdApp, iSpring Suite – profesionální e-learningové nástroje vhodné pro větší organizace. [9][10], [11]

Volba konkrétní platformy závisí na cílové skupině, způsobu distribuce a požadavcích na zpětnou vazbu či měření výsledků.

4.4 Přínosy využití scénářů pro organizaci

Zavedení výuky pomocí scénářů přináší organizaci celou řadu benefitů:

- Zvýšení angažovanosti zaměstnanců – interaktivní přístup motivuje k účasti i opakovanému procvičování.
- Zlepšení rozhodovacích schopností – díky opakovanému tréninku konkrétních situací.
- Snížení rizika lidské chyby – protože uživatel ví, co může nastat, a rozpozná varovné signály.
- Možnost měření výsledků – pokročilé nástroje nabízejí analytické přehledy a hodnocení.

Scénáře navíc umožňují testování připravenosti na nové hrozby a jsou snadno aktualizované podle vývoje rizik v dané oblasti.

II PRAKTICKÁ ČÁST

5 NÁVRH A PROSTŘEDÍ SCÉNÁŘE

Praktická část této diplomové práce navazuje na poznatky shrnuté v předchozích kapitolách. Hlavním cílem bylo přenést teoretické principy řízení bezpečnostních incidentů a tvorby rizikových scénářů do praxe – konkrétně do prostředí firemního školení určeného pro nové zaměstnance. V první fázi byly vybrány vhodné nástroje a technologie, které umožňují vytvářet interaktivní a uživatelsky přívětivé formy vzdělávání. Důraz byl kladen na srozumitelnost, zapojení uživatele a možnost snadné integrace do LMS systému.

Na základě porovnání dostupných řešení byly vybrány čtyři nástroje – H5P, Twine, Yo Scenario a PowerPoint – které nejlépe vyhovují požadavkům na efektivní tvorbu scénářů. Pomocí těchto platform vznikly konkrétní modelové situace, jejichž úkolem je přiblížit zaměstnancům reálné bezpečnostní hrozby a naučit je správně reagovat. V následujících podkapitolách podrobně popisují návrh jednotlivých scénářů, jejich zaměření, cílovou skupinu, prostředí, ve kterém jsou realizovány, a zvolené nástroje. Vše bylo vedeno snahou vytvořit školení, které nebude jen formální nutností, ale zapamatovatelným a smysluplným zážitkem.

5.1 Cíl praktické části

Tvorba praktické části této diplomové práce pro mě představovala zásadní krok k tomu, jak překlenout mezeru mezi teorií a skutečným každodenním chováním uživatelů v oblasti kybernetické bezpečnosti. Teorie je bezesporu důležitá – vysvětluje pojmy, procesy i doporučené postupy. Ale jakmile uživatel sedí sám u počítače, rozhoduje se v reálném čase, často bez dostatečných informací, nebo naopak pod tlakem. A právě na tyto momenty jsem se chtěl v praxi zaměřit.

Hlavním cílem praktické části bylo vytvořit sadu scénářů, které budou uživatelům srozumitelně a názorně ukazovat nejběžnější situace spojené s bezpečnostními incidenty a to tak, aby si z nich opravdu něco odnesli. Nešlo mi o to vytvořit složitou simulaci pro IT specialisty, ale naopak praktický a lidsky napsaný trénink pro běžné zaměstnance, kteří se často s technologiemi potýkají jen jako uživatelé. Chtěl jsem vytvořit prostředí, kde se mohou bezpečně "spálit", pochopit následky špatného rozhodnutí a zároveň si zkusit, jak vypadá správný postup.

Vedle toho jsem měl ještě jeden osobní cíl: vytvořit školení, které nebude nudné. Kybernetická bezpečnost bývá vnímána jako suché, přísné a technické téma. Jenže většina

problémů vzniká kvůli chybám běžných lidí – a těm podle mě nepomůže tabulka plná technických termínů, ale příběh, se kterým se ztotožní, situace, kterou znají, a trochu humoru, který zjemní napětí.

Praktická část této práce, proto stojí na čtyřech základních pilířích:

- **Reálnost scénářů** – vychází z běžných situací, které se ve firmách opravdu dějí.
- **Interaktivita a větvení** – uživatel není pasivní, ale rozhoduje, co se stane dál.
- **Přenositelnost do osobního života** – školení ukazuje, že hrozby nekončí za dveřmi kanceláře.
- **Jednoduchost a přístupnost** – scénáře jsou psány jazykem, kterému rozumí každý.

V dalších podkapitolách popisuji, jak jsem jednotlivé scénáře navrhl, jaké nástroje jsem zvolil pro jejich realizaci a jak je celé školení technicky a organizačně usazeno do prostředí firemního vzdělávání.

5.2 Metodika návrhu scénářů

Při návrhu scénářů jsem se snažil přemýšlet očima člověka, který sedí v kanceláři, má za sebou krátké školení o bezpečnosti, a právě otevřel podezřelý e-mail. Přemýšlí, jestli ho má smazat, kliknout na odkaz, nebo to raději někomu předat. Přesně takové momenty rozhodují o tom, jestli firma zůstane v bezpečí, nebo ne. Proto jsem chtěl, aby každý scénář co nejvíce připomínal reálnou situaci, ve které se může uživatel skutečně ocitnout.

Metodiku jsem postavil na několika klíčových principech:

1. Výběr témat podle reálných incidentů

Nejdříve jsem si vytvořil seznam témat, která se opakují v běžné firemní praxi. Inspiroval jsem se jednak vlastní zkušeností z prostředí menších i větších organizací. Do výběru jsem zahrnul:

- situace s vysokou pravděpodobností výskytu (např. phishing, slabé heslo),
- témata s potenciálně vážnými následky (např. nalezené USB, veřejné Wi-Fi),
- oblasti, ve kterých je běžně vysoká míra chybovosti u běžných uživatelů.

Témata jsem zároveň konzultoval s několika známými z IT oddělení různých firem, abych měl jistotu, že opravdu odpovídají běžné praxi.

2. Strukturovaný přístup ke scénáři

Každý scénář jsem navrhl podle jednotného vzoru. To mi umožnilo zajistit srozumitelnost a zároveň konzistenci při zpracování. Každý scénář má:

- Úvod – krátký kontext (např. „Radim právě otevřel e-mail s přílohou“),
- Jádru – klíčový moment, kdy se uživatel rozhoduje,
- Rozhodnutí – obvykle dvě až tři možnosti chování,
- Důsledky – co se stane podle zvoleného postupu,
- Ponaučení – shrnutí + odkaz na správné chování.

Scénáře jsou navíc doplněny o poznámky typu „Jak by to ovlivnilo Tvůj osobní život?“ – tím chci ukázat, že kybernetická bezpečnost není jen firemní záležitost.

3. Jazyk a forma přizpůsobené běžnému uživateli

Cílovou skupinou nejsou IT specialisté, ale běžní zaměstnanci – účetní, skladník, administrativní pracovníci. Proto jsem volil jazyk, který je jednoduchý, srozumitelný, někdy trochu odlehčený. Příběhy jsou napsány v hovorovějším tónu, ale stále s odborným obsahem.

Namísto suché instrukce typu „Nikdy neotevírejte podezřelé přílohy“ říká scénář něco jako: „Radim chvíli přemýšlí, jestli má otevřít přílohu, která se tváří jako faktura. Přitom si není jistý, kdo je odesílatel...“

4. Propojení s interaktivitou

Všechny scénáře jsem navrhoval jako rozhodovací příběhy, které se větví podle uživatelského výběru. Použil jsem k tomu nástroje jako Twine nebo H5P (o tom více v následující kapitole). Díky tomu se uživatel může „projít“ scénářem a na vlastní kůži si vyzkoušet důsledky rozhodnutí.

Tento formát podporuje zapamatování, což potvrzuje i řada studií z oblasti e-learningu – zážitek si totiž pamatujeme lépe než pasivní výklad.

Scénáře jsem proto tvořil jako kombinaci reálného základu, jednoduchého jazyka, zapamatovatelného příběhu a jasné zpětné vazby. V další části popisuji, komu je školení určeno a jaké nástroje jsem použil k jeho realizaci.

5.3 Cílová skupina a vzdělávací prostředí

Při navrhování scénářů jsem se zaměřil především na to, **komu mají být určeny**. Školení kybernetické bezpečnosti totiž nebude fungovat, pokud nebude odpovídat tomu, jak lidé opravdu přemýšlejí, co zažívají v práci a jak se běžně chovají. Cílem tedy nebylo vytvořit trénink pro IT odborníky, ale **praktické a srozumitelné školení pro běžné zaměstnance**, kteří používají technologie jako nástroj ke své každodenní práci – a kteří často ani nevědí, že mohou být součástí bezpečnostního incidentu.

5.3.1 Noví zaměstnanci jako hlavní cílová skupina

Scénáře jsou určeny především pro nové zaměstnance fiktivní firmy, která má kolem šedesáti pracovníků – většina z nich pracuje v kancelářích, část ve skladu či logistice. Typově jde o běžnou organizaci, která využívá IT infrastrukturu napříč odděleními, ale její zaměstnanci nejsou nutně technicky orientovaní. A právě v tom je největší riziko: zaměstnanec neúmyslně klikne na škodlivý odkaz nebo připojí neprověřené zařízení a celý systém může být ohrožen.

Typický uživatel školení může být:

- účetní, která pravidelně zpracovává faktury z příloh e-mailu,
- asistentka, která spravuje dokumenty a přeposílá přístupy,
- skladník, který připojí vlastní USB disk kvůli tisku,
- pracovnice balírny zboží, která používá jedno heslo „na všechno“.

Pro takového uživatele je bezpečnost často neviditelná nebo matoucí. Proto jsem scénáře koncipoval tak, aby byly jednoduché, příběhové, a zároveň názorné – aby se v nich lidé poznali a pochopili, co může způsobit i malá nepozornost.

Školení i pro stálé zaměstnance – připomenutí, ne obviňování

Přestože hlavním cílem bylo oslovit nově příchozí zaměstnance v rámci onboardingu, myslím si, že stejně důležitou cílovou skupinou jsou i stálí zaměstnanci. Právě u nich se často objevuje tzv. falešný pocit bezpečí – „tohle už znám“, „mě se to netýká“, „takhle to dělám už roky“. A právě zde může scénář fungovat jako zrcadlo, které bez moralizování ukáže chyby, kterých se lidé dopouštějí. V příběhu se najdou, rozpoznají vlastní chování – a mohou ho změnit.

Díky příběhovému stylu nejsou scénáře vnímány jako kontrola nebo výslech, ale jako možnost zažít něco „nanečisto“, bez následků. A právě to může být užitečné i pro ty, kteří už firmu dobře znají a školeními dávno prošli.

5.3.2 Začlenění do úvodního i opakovacího školení

Každý scénář je navržen tak, aby mohl fungovat samostatně – jako krátký příběh, který si zaměstnanec projde, zamyslí se nad rozhodnutím a uvidí, co se stane. Právě díky tomu se dají scénáře snadno zařadit do různých typů školení.

Například:

hned po nástupu do firmy – během prvních dvou týdnů si nováček projde základní scénáře (např. hesla, e-mailly),

po několika měsících – může si znovu zopakovat důležité věci formou „refresheru“,

během roku – firma může využít scénáře jako součást kampaní nebo připomenutí (např. v rámci měsíce kybernetické bezpečnosti).

V některých případech – například u interaktivních příběhů vytvořených v Twine nebo Yo Scenario – může být scénář delší a rozdělený do více kapitol. Uživatel, ale nemusí projít vše naráz, může si postupně procházet jednotlivé části, třeba jednu kapitolu denně. Tento přístup pomáhá udržet pozornost a umožňuje přirozenější zapamatování informací.

Naopak školení připravená v PowerPointu jsou vždy zaměřena na jedno konkrétní téma. Jsou přehledná, strukturovaná jako klasická prezentace a hodí se tam, kde je potřeba stručně a rychle proškolit jedno konkrétní riziko.

Díky této variabilitě si může firma vybrat formu, která jí nejvíc vyhovuje – nebo je různě kombinovat podle cílové skupiny a dostupného času.

5.4 Použité nástroje pro tvorbu scénářů

Při sestavování výukových scénářů jsem se zaměřil na to, aby byly interaktivní, přehledné a dobře využitelné v praxi. Z tohoto důvodu jsem zvolil několik různých nástrojů, které se svými funkcemi navzájem doplňují. Každý z nich nabízí jiný způsob prezentace a odlišné výstupy, a proto jsou v následujícím textu rozděleny podle typu použití. Jejich společným cílem je umožnit uživateli prožít konkrétní situaci, samostatně se rozhodnout a získat tím praktickou zkušenost.

5.4.1 Twine – otevřený nástroj pro příběhové scénáře

Twine je bezplatný nástroj, který umožňuje tvořit interaktivní příběhy s rozhodnutími. Uživatel si během školení volí mezi různými možnostmi a každá volba vede jinam – k jinému pokračování, jinému výsledku. Taková forma scénáře připomíná herní knihu, kde si čtenář vybírá, jak se bude příběh vyvíjet.

Výhodou je, že Twine funguje i bez registrace a výstup je jednoduchý HTML soubor, který lze přímo vložit do Moodle. Uživatelsky přívětivé a flexibilní řešení pro tvorbu realistických scénářů. Pro lepší práci jde stáhnout i program TWINE, kde můžeme tvořit přímo z počítače

5.4.2 Yo Scenario – profesionální nástroj pro rozvětvené scénáře

Yo Scenario je online nástroj určený přímo k tvorbě vzdělávacích scénářů. Ve své bezplatné verzi umožňuje vytvořit klasické lineární školení – podobně jako prezentaci, kdy uživatel postupně prochází jednotlivými snímky a vybírá si z možností.

Pokud ale organizace přejde na placenou verzi, otevře se možnost vytvářet plnohodnotné Branching scénáře – tedy strukturované příběhy s větvemi, rozhodovacími uzly a propojením mezi kapitolami. To umožňuje tvorbu složitějších scénářů, které se chovají jako interaktivní hra s postupem. Pro rozsáhlejší témata (například recyklace zařízení nebo chování na služební cestě) je to ideální forma.

Yo Scenario má výhodu v přehledném rozhraní, možnosti sledování pokroku a snadném ovládání i pro méně technicky zdatné uživatele. Výstup může být vložen jako odkaz nebo iframe do Moodle.

5.4.3 H5P – interaktivní obsah přímo v Moodle nebo pomocí programu Lumi

H5P je nástroj pro tvorbu interaktivního výukového obsahu, který lze používat přímo v prostředí Moodle, nebo samostatně v programu Lumi. Umožňuje vytvářet celou řadu výukových prvků – od prezentací přes testy až po jednoduché rozhodovací úkoly. Díky tomu je velmi vhodný pro základní e-learningová školení.

H5P byl využit hlavně pro klasická školení, ve kterých uživatel prochází jednotlivými slidy, občas odpovídá na otázku nebo vybírá z možností. Typicky šlo o témata jako výběr hesla, bezpečné používání USB disků nebo chování na veřejné Wi-Fi. V této formě se jedná o přehledné, lineární školení, které je ideální pro stručné vysvětlení problému.

V této podobě však není možné vytvořit příběhový scénář s větvením děje, tak jak to nabízí Twine nebo Yo Scenario. Sám jsem se o to pokoušel, ale narazil jsem na limity standardních aktivit H5P dostupných v Moodle i Lumi.

Je však důležité dodat, že H5P jako nástroj tuto možnost v určité formě má – konkrétně pomocí typu aktivity „Branching Scenario“, který je dostupný v některých pokročilých integracích H5P nebo v placených verzích. Tento typ umožňuje větvení příběhu a už složitější interaktivní logiku. V mé práci ale nebyl k dispozici, a tak jsem jej zatím nevyužil.

Díky své jednoduchosti a rozšířenosti zůstává H5P ideálním nástrojem pro doplnění komplexních scénářů – například ve formě úvodu, shrnutí, nebo samostatného školení na jedno konkrétní téma.

5.4.4 PowerPoint – klasická prezentace upravená pro e-learning

Vedle interaktivních nástrojů jsem využil také klasický PowerPoint, který jsem upravil pro účely školení. Prezentace je vždy zaměřena na jedno konkrétní téma – například výběr hesla nebo instalaci aktualizací. Tento formát je vhodný tam, kde chceme stručně a jasně vysvětlit jednu věc bez větvení nebo příběhu.

V PowerPointu lze snadno vložit:

- firemní vizuál,
- postup krok za krokem,
- jednoduchá upozornění nebo doporučení.

Prezentace mohou být buď promítány naživo při školení, nebo vloženy do Moodle, jako doplňkový materiál ke scénářům.

5.5 Fiktivní prostředí a postavy

Při návrhu školení byl kladen důraz na to, aby bylo srozumitelné i pro uživatele bez technického zázemí. Proto byly připraveny příběhové scénáře zasazené do smyšleného, ale uvěřitelného firemního prostředí, které odráží každodenní činnosti typické pro středně velkou kancelář. V rámci příkladů se účastníci setkávají s úlohami jako je práce s elektronickou poštou, používání bezdrátových sítí, řešení situací na pracovní cestě nebo komunikace s technickou podporou.

Všechny scénáře jsou vystavěny okolo dvou hlavních postav:

Radim

Radim je fiktivní zaměstnanec, který nastoupil do firmy na administrativní pozici. V rámci scénářů prochází různými pracovními situacemi, ve kterých se musí rozhodovat – například jak naložit s podezřelým e-mailem, co dělat při ztrátě zařízení nebo jak reagovat na žádost o sdílení přihlašovacích údajů.

Radim je charakterizován jako běžný zaměstnanec bez výrazných IT znalostí, ale se snahou dělat věci správně – i když občas tápe nebo se nechá zmást okolím.

Jana

Jana je jeho kolegyně, která se objevuje zejména v příbězích zaměřených na recyklaci IT techniky, ochranu dat a udržitelnost. Její scénáře kladou důraz na odpovědnost při nakládání s hardwarem a na pochopení rizik spojených s neopatrnou manipulací s firemními zařízeními.

Obě postavy slouží jako nosiče příběhu – uživatel vstupuje do jejich role nebo je sleduje při rozhodování. Díky tomu se vzdělávací obsah stává přirozenější, snadněji zapamatovatelný a zároveň působí méně formálně než tradiční přednáškové školení.

Scénáře jsou psány s prvky jemného humoru a nadsázky, aby se uživatelé mohli s postavami ztotožnit a zároveň udrželi pozornost po celou dobu školení. Každé rozhodnutí má svůj důsledek – od pochvaly až po „fiktivní výpověď“, což dodává školení herní a motivující charakter.

6 TVORBA INTERAKTIVNÍHO SCÉNÁŘE

Cílem této části práce nebylo vytvářet technicky složité simulace pro profesionály v oblasti kybernetické bezpečnosti, ale naopak zaměřit se na běžné zaměstnance – tedy skupinu, která je v praxi často tou první a zároveň nejslabší linií obrany. Důraz byl kladen na každodenní rozhodování uživatelů v běžném firemním provozu, kde i zdánlivě drobná volba může rozhodnout o tom, zda ke kybernetickému incidentu vůbec dojde.

Zvoli jsem, proto formu interaktivních scénářů, které se svým pojetím blíží herním knihám – tzv. gamebookům. Tento přístup vychází z principů tabletop cvičení, ovšem převádí je do individuální a přístupné podoby: uživatel prochází příběh samostatně, z pohodlí své kanceláře nebo domova, a prostřednictvím různých rozhodnutí se dostává do různých situací, které mu názorně ukazují možné důsledky jeho voleb.

Pro realizaci byly využity čtyři nástroje s odlišnou úrovní složitosti a interaktivity – Twine, Yo Scenario, H5P (přes prostředí Lumi) a PowerPoint. Každý z těchto nástrojů má své výhody a limity, a právě tato různorodost mi umožnila nejen vytvořit pestrý vzdělávací obsah, ale zároveň porovnat vhodnost jednotlivých platforem pro konkrétní typy školení.

Scénáře jsou koncipovány tak, aby vycházely z reálného prostředí a situací, se kterými se zaměstnanci mohou běžně setkat: zapomenuté heslo, nález USB disku, podezřelý e-mail nebo problém s aktualizací systému. Díky větvení děje a okamžité zpětné vazbě si může uživatel bezpečně vyzkoušet různé varianty chování a pochopit, proč je některé jednání rizikové. Významnou roli přitom hrají fiktivní postavy – Radim a Jana – které působí jako průvodci příběhem a pomáhají vtáhnout účastníka do děje.

Jazyk zvolený ve scénářích je záměrně srozumitelný, lehce odlehčený a občas i humorný. To vše přispívá k tomu, aby školení nepůsobilo formálně či odtazité, ale bylo pro uživatele zapamatovatelné, přístupné a zároveň výchovné.

Při tvorbě jsem se snažil o to, aby každý scénář:

- vycházel z reálné situace, která se může snadno stát každému,
- nabízel rozhodovací momenty, které mají přímý dopad na vývoj děje,
- ukazoval důsledky špatného rozhodnutí, ale bez moralizování,
- a zakončil se shrnutím a poučením, které si uživatel odnese.

Tato výuková metoda působí na první dojem jednoduše, což je však jejím klíčovým přínosem. Namísto teorie přibližuje reálné situace a přirozeně ukazuje, proč je důležité chovat se v praxi bezpečně a zodpovědně.

Tvorba takových scénářů samozřejmě vyžaduje čas – napsat příběh, promyslet rozhodovací uzly, zohlednit různé varianty chování a přetavit to do interaktivního formátu není otázka pár minut. Ale ve srovnání s nákladnými simulacemi nebo školením na míru přináší tento přístup „hodně muziky za málo peněz“. Navíc umožňuje scénáře snadno aktualizovat, rozšiřovat nebo přizpůsobovat nové cílové skupině.

V následující části se zaměřím na jednotlivé nástroje, které jsem pro tvorbu scénářů použil, a popíšu jejich výhody, limity i vhodné využití v různých typech školení.

6.1 Proč scénáře pro běžné uživatele?

V rámci tvorby interaktivních scénářů jsem se záměrně rozhodl zaměřit na běžné uživatele, nikoliv na technicky zaměřené specialisty nebo krizové týmy. Důvod je jednoduchý – mnoho incidentů v organizacích vzniká právě vinou lidské chyby. Nejedná se o sofistikované útoky, ale o zdánlivé drobnosti: kliknutí na škodlivý e-mail, zaslání přístupových údajů, ztracený notebook bez šifrování nebo používání jednoho hesla pro všechno.

Právě běžní zaměstnanci bývají tou první linií, na které stojí prevence. Proto dává smysl věnovat pozornost tomu, jak přemýšlejí, jak se rozhodují a jakým způsobem jim můžeme pomocí scénářů zprostředkovat situace, které v nich vyvolají zájem i poučení.

Důležité pro mě bylo i to, aby scénáře nebyly jen moralizující nebo represivní. Naopak – jejich hlavním účelem je mluvit o chybách otevřeně, lidsky a s nadhledem. Mnoho lidí se totiž bojí přiznat, že něco udělali špatně. A právě strach z ostudy nebo potrestání často vede k tomu, že se incident nahlásí pozdě – nebo vůbec.

Cílem tedy bylo vytvořit prostředí, kde si může uživatel „bezpečně“ vyzkoušet různé situace:

- Zjistit, co by se stalo, kdyby kliknul na špatný odkaz.
- Jaké důsledky má odeslání hesla kolegovi.
- A proč je lepší zeptat se než něco zamlčet.

To vše formou jednoduchého příběhu, lehkého humoru a přehledné zpětné vazby. Žádné červené vykřičníky ani dlouhé přednášky, ale konkrétní situace, ve které se může najít

každý. A právě to je podle mě klíč – uživatelé si často nepamatují suché definice, ale pamatují si příběh, pocit a reakci postavy, se kterou se ztotožní.

Scénáře pro běžné uživatele tak nejsou náhradou za technická opatření, ale důležitým doplňkem bezpečnostní kultury. Pomáhají překonat bariéru mlčení, posilují důvěru v otevřenou komunikaci a ukazují, že chybovat je lidské – ale důležité je z chyby se poučit dříve, než bude pozdě.

6.2 Zvolené formy: příběh, rozhodnutí, důsledek

Každý scénář v této práci je postaven na jednoduché, ale účinné struktuře: co se stane, když...? Uživatel je postaven před konkrétní situaci, ve které se musí rozhodnout. Každá volba má svůj důsledek, ať už pozitivní nebo negativní, a scénář na ni bezprostředně reaguje.

Tato forma funguje velmi dobře z několika důvodů:

- Uživatel je aktivně zapojen do děje.
- Nejde jen o výklad, ale o zážitek.
- Každé rozhodnutí má okamžitou zpětnou vazbu.
- Výsledek není anonymní – týká se konkrétní postavy, se kterou se může ztotožnit.

Práce s postavami Radim a Jana

V rámci scénářů se opakovaně objevují dvě fiktivní postavy – Radim a Jana. Tyto postavy jsem záměrně vytvořil jako modelové reprezentace situací, se kterými jsem se osobně setkal při práci s běžnými uživateli. Nejde o reálné osoby, ale o fiktivní postavy složené z typických chování, chyb, zmatků i způsobů uvažování, které jsem v praxi mnohokrát viděl.

Radim reprezentuje typického zaměstnance, který se nebojí technologie, ale často jedná impulzivně nebo bez dostatečného uvážení. V jeho scénářích řeší například podezřelý e-mail, žádost o heslo nebo podivné zprávy na sociálních sítích.

Jana je více systematická a rozvážná, ale i ona se dostává do problémových situací – typicky při práci s daty, zařízeními nebo veřejnými sítěmi. Její scénáře jsou více zaměřené na udržitelnost, pořádek a dlouhodobější důsledky chování.

Postavy fungují jako prostředníci mezi reálným světem a scénářem. Uživatel se na ně může dívat zvenčí, ale zároveň v nich často pozná sám sebe – bez obviňování, zato s možností zažít dopady rozhodnutí v bezpečném prostředí.

Rozhodnutí, které mají důsledek

Důležitým prvkem každého scénáře je důsledkový systém. Uživatel po svém rozhodnutí dostane zpětnou vazbu, která není jen obecná, ale konkrétní a vázaná na firemní prostředí. Scénáře tak mohou vést například k:

- pochvale od nadřízeného,
- upozornění nebo výtce,
- nebo dokonce „vyhazovu“ – samozřejmě v nadsázce a simulaci.

Tento princip slouží nejen ke zvýšení zapamatovatelnosti, ale i k emočnímu zapojení. Když postava dostane pochvalu, uživatel má dobrý pocit. Když dojde k „fiktivnímu vyhazovu“, uživatel se zasměje – ale zároveň si uvědomí, že šlo o vážné pochybení. Vše je zasazeno do příběhového kontextu a doprovázeno komentářem, který vysvětluje, co bylo špatně (nebo správně) a proč.

Styl psaní: přístupný, někdy odlehčený – ale vždy se vzdělávacím cílem.

Všechny scénáře jsou psány tak, aby byly:

- srozumitelné pro každého – bez složité terminologie,
- stručné a přehledné – s důrazem na konkrétní děj,
- odlehčené – s jemným humorem nebo nadsázkou tam, kde to dává smysl,
- a hlavně poučné – každé rozhodnutí má jasné důsledky a doprovodné vysvětlení.

Cílem není uživatele nachytat nebo „usvědčit z chyby“, ale naopak vytvořit prostředí, kde si může bezpečně vyzkoušet různé varianty chování a uvědomit si, co by mohlo nastat v reálném světě. Tento zážitkový přístup má podle zkušeností mnohem větší dopad než klasické přednáškové školení.

6.3 Nástroje – silné a slabé stránky

Při tvorbě interaktivních scénářů jsem pracoval s několika různými nástroji, které se liší svými možnostmi, technickými nároky, výstupními formáty i mírou interaktivity. Výběr jednotlivých nástrojů nebyl předem daný, ale vznikal postupně – v reakci na možnosti a omezení, které jsem objevoval během vývoje.

Cílem bylo najít takové nástroje, které jsou:

- cenově dostupné (ideálně bezplatné),
- dostatečně flexibilní pro tvorbu různých typů scénářů,
- technicky zvládnutelné bez nutnosti pokročilých znalostí programování,
- a vhodné pro publikaci na vlastním serveru, případně v LMS prostředí.
- Níže uvádím jednotlivé nástroje v pořadí, v jakém jsem s nimi pracoval.

6.3.1 Moodle a H5P (prostřednictvím Lumi)

Na začátku jsem plánoval tvorbu scénářů v systému Moodle s využitím modulu H5P. Po nastavení jsem však zjistil, že vestavěná podpora H5P v Moodle neumožňuje vytvářet scénáře typu „Branching Scenario“, které by poskytovaly větvení a dynamické rozhodování. Tato funkce je dostupná pouze prostřednictvím placené služby H5P.com, což nebylo v souladu s cílem práce.

Později jsem objevil nástroj Lumi, který umožňuje offline i online tvorbu H5P aktivit a obsahuje i typ „Branching Scenario“. Tento nástroj jsem využil jak ve stáhnutelné verzi pro PC, tak i ve verzi online přímo na stránce lumi.education. Výhodou Lumi je také to, že automaticky kontroluje úplnost scénáře – upozorní například na chybějící přechody mezi snímky nebo nevyplněné větve. Díky tomu je práce s větvením intuitivní a bezpečnější.

Vytvořený scénář jsem exportoval ve formátu H5P i HTML a následně publikoval na vlastním serveru.

Výhody:

- jednoduché ovládání, rychlé vytvoření obsahu,
- dostupné bez nutnosti připojení k internetu (desktop verze),
- možnost využít také online editor bez instalace,

- automatická kontrola správného a kompletního propojení scénáře.

Nevýhody:

- omezené větvení a logika v běžném,
- menší flexibilita v grafickém zpracování a uživatelském zážitku.

6.3.2 Twine

V další fázi jsem se seznámil s nástrojem Twine, který slouží k tvorbě interaktivních příběhů a scénářů. Twine je open-source a umožňuje tvorbu přímo v prohlížeči nebo v offline desktopové verzi. Příběhy se vytvářejí pomocí systému uzlů a větvení, s možností použití proměnných, podmínek i vizuálních úprav pomocí CSS. V mém případě jsem pracoval s formátem SugarCube.

Twine umožnil vytvořit komplexní scénář s postavou Radima a větším množstvím rozhodovacích bodů. Výstup byl exportován do HTML a následně publikován na serveru.

Výhody:

- vysoká míra kontroly nad logikou a strukturou scénáře,
- podpora proměnných, větvení, podmíněných přechodů,
- možnost grafické úpravy prostřednictvím CSS,
- funguje zcela bezplatně.

Nevýhody:

- vyžaduje základní znalost práce s proměnnými a stylováním,
- složitější orientace v rozsáhlejších scénáři.
- Nefunguje kontrola propojení scénáře

6.3.3 Yo Scenario

Na základě doporučení vedoucího práce jsem se dále seznámil s online nástrojem Yo Scenario, který je určen pro tvorbu rozhodovacích scénářů. V bezplatné verzi umožňuje tvorbu scénářů s lineární strukturou, placené verze pak rozšiřují možnosti o větvení, export do SCORM, integraci s LMS a další funkce.

V rámci práce jsem využil bezplatnou verzi s tvorbou vlastního scénáře bez AI. Výsledný scénář byl publikován formou odkazu a zpřístupněn na serveru.

Výhody:

- intuitivní rozhraní, vhodné i pro netechnické autory,
- možnost exportu a snadného sdílení,
- podpora zpětné vazby u jednotlivých voleb.

Nevýhody:

- pokročilé funkce dostupné pouze v placených verzích,
- omezené možnosti grafické úpravy a přizpůsobení vzhledu.

6.3.4 PowerPoint

Jako doplňkový formát byl využit nástroj Microsoft PowerPoint, prostřednictvím kterého byl vytvořen jeden scénář ve formě interaktivní prezentace. Pomocí hypertextových odkazů mezi jednotlivými snímky bylo umožněno simulovat rozhodovací body a větvení děje. Tento scénář byl použit jako doplňkový prvek pro přehledné zpracování konkrétní kapitoly.

Výhody:

- široká dostupnost a znalost nástroje mezi uživateli,
- možnost začlenění firemního vizuálního stylu,
- vhodné pro jednoduché scénáře nebo úvodní shrnutí tématu.

Nevýhody:

- omezené možnosti logiky a proměnných,
- žádná přímá podpora analytiky ani LMS integrace bez dalších nástrojů.

6.3.5 Publikace scénářů

Všechny vytvořené scénáře byly publikovány na vlastním serveru, který slouží jako testovací a prezentační platforma. Scénáře zde byly zpřístupněny kolegům za účelem vyhodnocení, zpětné vazby a dalšího rozvoje. Díky tomu je možné scénáře jednoduše aktualizovat, porovnávat nástroje mezi sebou a vyhodnocovat, jak uživatelé reagují na různé formy školení.

6.4 Propojení s LMS a firemním školením

Jedním z hlavních cílů této praktické části bylo nejen vytvořit interaktivní scénáře, ale také ověřit jejich použitelnost v reálném vzdělávacím prostředí. Vzhledem k tomu, že pro školení zaměstnanců i testování obsahu využívám vlastní server s nainstalovaným systémem Moodle, byla všechna řešení navrhována tak, aby s tímto systémem byla kompatibilní, nebo na něj alespoň navazovala.

6.4.1 Vlastní server jako výuková platforma

Scénáře vytvořené v jednotlivých nástrojích byly publikovány na mém vlastním serveru, a to buď jako samostatné HTML stránky, nebo jako odkazy vedoucí na veřejně přístupný scénář (např. u Yo Scenario). Tento způsob umožňuje maximální flexibilitu při testování, zpřístupnění kolegům a sběru zpětné vazby.

Přístup k jednotlivým scénářům je zajištěn:

- buď přímo v Moodle jako odkazy nebo vložené HTML prvky (Twine, H5P),
- nebo přes strukturované menu scénářů na serveru (např. Yo Scenario, Lumi exporty),
- případně v rámci hybridního školení, které kombinuje více typů aktivit – například scénář vytvořený v PowerPointu jako statická prezentace s hypertextovými přechody, doplněná o interaktivní části v jiných nástrojích.

Tento přístup umožňuje jednoduše doplňovat nové scénáře nebo upravovat stávající obsah bez zásahu do LMS samotného. Scénáře tak mohou existovat nezávisle na konkrétní instalaci Moodle, což zvyšuje jejich přenositelnost i použitelnost v jiných kontextech.

6.4.2 Tematické rozdělení scénářů

Jednotlivé scénáře jsou rozděleny podle témat, která odpovídají nejčastějším problémovým oblastem v každodenní praxi uživatelů:

- práce s hesly a přihlašováním,
- rozpoznání podvodných e-mailů a phishingu,
- nakládání s nalezenými médii (např. USB disky),
- chování při připojení k veřejným Wi-Fi sítím,
- recyklace zařízení a odpovědnost při jejich vyřazení,

- sdílení přístupových údajů mezi kolegy,
- a další specifické situace z pracovního prostředí.

Tato tematická struktura usnadňuje začlenění scénářů do jednotlivých školicích modulů a umožňuje cíleně pracovat s konkrétní oblastí rizika podle role uživatele.

Využití scénářů ve vzdělávání a osvojení návyků

Scénáře byly navrženy tak, aby je bylo možné využít:

- jako samostatnou interaktivní aktivitu, například v rámci bezpečnostního týdne nebo firemní kampaně,
- jako doplněk k formálnímu e-learningu, kde slouží jako praktické cvičení,
- nebo jako zpětnou vazbu – například po školení ve formě „zkuste si, jak byste se zachovali v praxi“.

Výhodou takto vytvořených scénářů je jejich nízká technická náročnost, vysoká přístupnost a možnost opakovaného použití. Díky tomu se mohou stát součástí dlouhodobé strategie zvyšování bezpečnostního povědomí ve firmách – a to bez nutnosti investovat do nákladných řešení nebo složitých integračních procesů.

7 REALIZACE INTERAKTIVNÍHO GAMEBOOKU NA ZÁKLADĚ NAVRŽENÉHO SCÉNÁŘE

V praktické části diplomové práce jsem se rozhodl vytvořit interaktivní scénáře pomocí různých dostupných nástrojů. Cílem bylo vytvořit příběh, který bude mít scénář na různé incidenty. Výběr jednotlivých programů jsem nejen otestoval jejich možnosti, ale hlavně si vyzkoušet, jak se dají přizpůsobit konkrétním potřebám školení a vzdělávání. Věnoval jsem se úpravám vzhledu, příběhovému stylu i funkcionalitě.

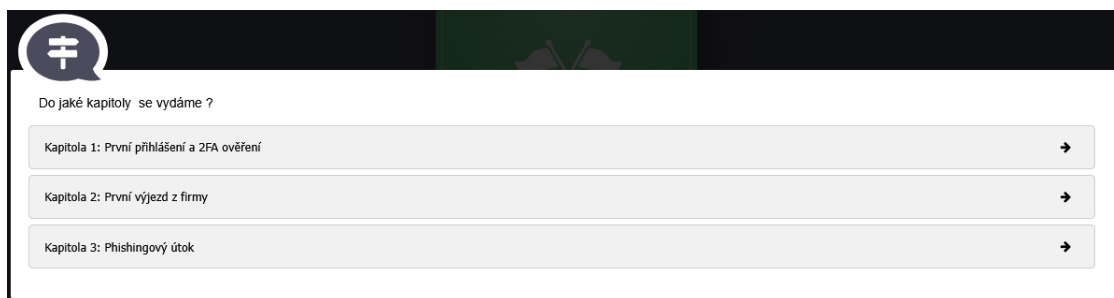
Postupoval jsem tak, že jsem nejprve navrhl základní podobu scénáře a poté jsem podle možností jednotlivých platforem provedl úpravy a doplnění. Každou platformu jsem hodnotil zvlášť, podle toho, jak snadno šla použít a kde se objevily limity. V neposlední řadě jsem hodnotil i cenu a další možnosti rozvoje.

Pro potřeby školení na uživatelích byl vytvořen server, kde byl nainstalován OS Linux Ubuntu a byl doinstalován systém Moodle.

Jednotlivá školení jsem psal zábavnější formou, ne nudou či rozkazovací formou, jako jsem už absolvoval stovky, ale aby se i zapojily.

7.1 Modul H5P

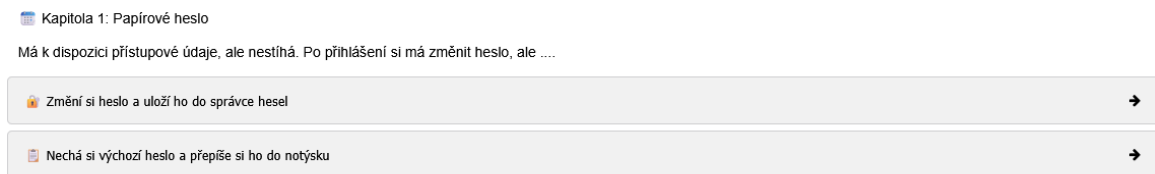
Po nainstalování systému Moodle byl využit open-source nástroj H5P. K tvorbě obsahu byl použit nástroj LUMI, který je dostupný jak jako desktopová aplikace, tak i ve webové verzi. V počáteční fázi nebyl umožněn přístup k rozšířenému scénáři, a proto bylo od této varianty upuštěno. Později však bylo zjištěno, že již bylo toto rozšíření zpřístupněno. Využil jsem středně dlouhé školení s Janou jako produkt manažerkou. Zde jsem použil hlavně scénáře na hesla, 2FA ověření, VPN a připojení k veřejné WI-FI a Phishingový útok.



Obrázek 2 Základní výběr kapitol s Janou pomocí H5P

(zdroj: vlastní)

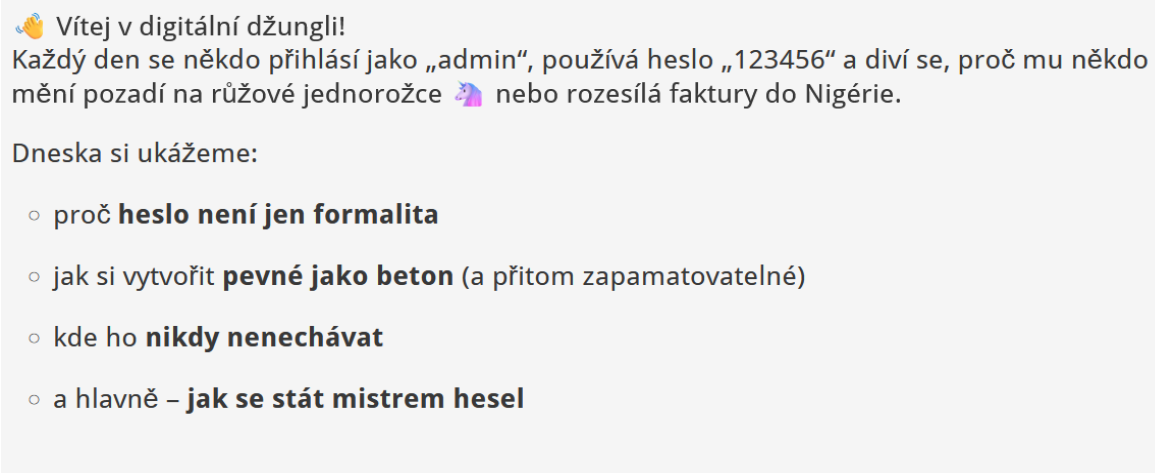
Možnosti rozhodování s Janou jsem vytvořil pomocí nástroje H5P v modulu Branching Scenario. Obrázek (Obrázek 3) ukazuje, jak byly jednotlivé volby v příběhu prezentovány uživateli. Každá volba vedla k jiné větvi příběhu a ovlivnila jeho další vývoj.



Obrázek 3 Možnosti rozhodování s Janou pomocí H5P

(zdroj: vlastní)

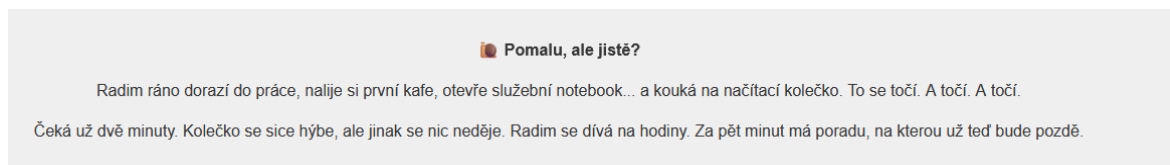
Obrázek (Obrázek 4) zachycuje ukázkou školení s postavou Jany vytvořeného pomocí H5P.



Obrázek 4 Ukázkou školení s Janou pomocí H5P

(zdroj: vlastní)

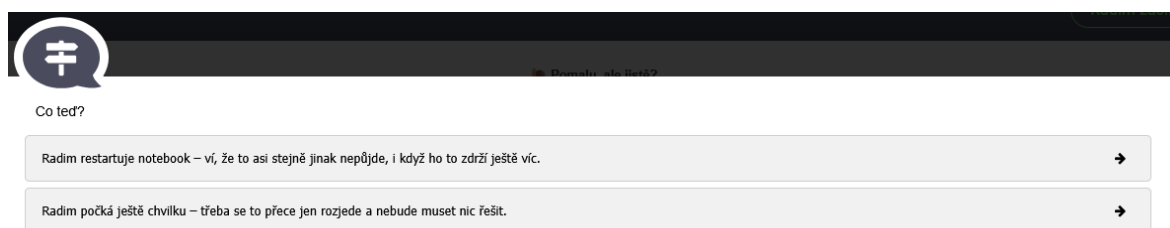
Kratší školení Radima a aktualizaci operačního systému. Zde jsem vytvořil jen jednu kapitolu, pro zjištění, co nato účastníci.



Obrázek 5 Úvod do školení s Radimem pomocí H5P

(zdroj: vlastní)

Obrázek (Obrázek 6) ukazuje kratší rozhodovací scénář s postavou Radima vytvořený v H5P. Uživatel si vybírá z nabízených možností a ovlivňuje tím další směr příběhu.



Obrázek 6 Rozhodovací scénář s Radimem pomocí H5P

(zdroj: vlastní)

Obrázek (Obrázek 7) zachycuje ponaučení s postavou Radima, zaměřené na důležitost aktualizací. Příběh ukazuje, že správné ponaučení je vždy důležité, a to nejen v pracovním, ale i v osobním životě.

Proč je důležité aktualizovat?

Aktualizace nejsou jen o nových funkcích nebo hezčích ikonách. Jsou hlavně o bezpečnosti. Vývojáři jimi opravují chyby, které by mohli zneužít útočníci. Bez aktualizací je tvůj počítač jako dům s otevřenými dveřmi – stačí, aby si toho někdo všiml.

Navic často zlepšují i výkon, stabilitu a kompatibilitu. Ano, někdy to chvíli trvá, ale lepší pár minut aktualizace teď než hodiny řešení průšvihů později.

Takže příště, až se ti objeví okénko s „Instalovat a restartovat?“...

👉 klikni **Ano**. Tvoje budoucí já ti poděkuje. A možná i IT oddělení 🍀.

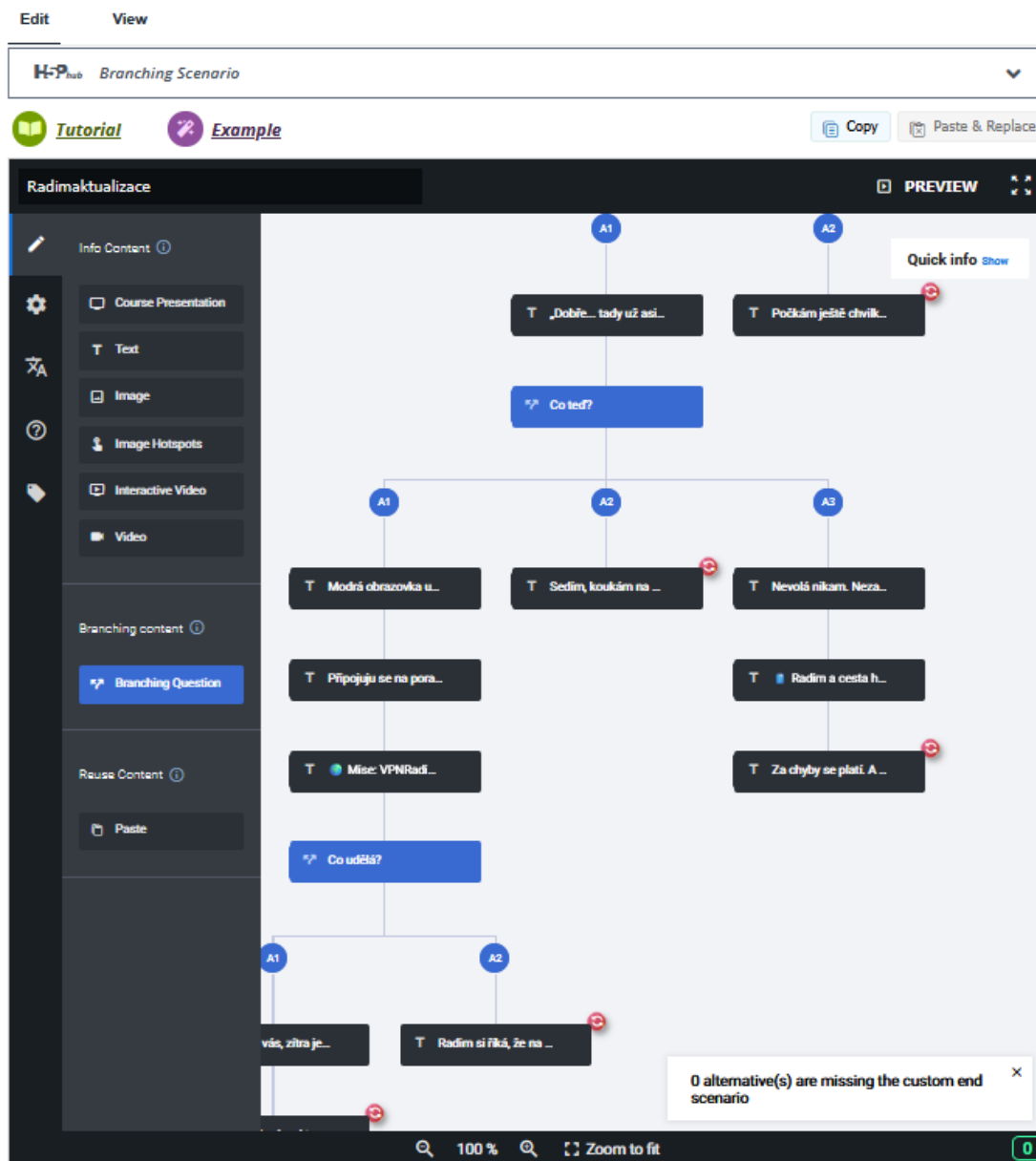
Uf, to byla doba... »

Obrázek 7 Ponaučení s Radimem pomocí H5P

(zdroj: vlastní)

Pro školení ať už s Janou či Radimem, bylo využito nelineární rozhodovací scénář. Obrázek (Obrázek 8) ukazuje, jak vypadá kontrola dokončení scénáře ve webové aplikaci Lumi. Aplikace přehledně zobrazí stav dokončení a u scénáře, který byl úspěšně dokončen,

je uvedena hodnota 0 chyb. Díky této funkci lze snadno ověřit, zda uživatel prošel celým scénářem správně.



Obrázek 8 Kontrola ukončení scénáře ve webové aplikaci Lumi [13]

Hodnocení modulu H5P.

Práce v H5P je velmi jednoduchá a intuitivní. Prostředí je srozumitelné i pro uživatele bez pokročilých technických znalostí, což výrazně urychluje tvorbu školení.

Velkou výhodou je integrovaný mechanismus kontroly dokončení scénáře – uživatel ,který při tvorbě nedokončí větve scénáře bude upozorněn

Hotový scénář lze snadno exportovat jako SCORM balíček nebo samostatný HTML soubor, což umožňuje jeho pohodlné nahrání do LMS systémů, například Moodle.

7.2 Twine

Po krátkém hledání jsem objevil nástroj Twine. Díky možnosti tvorby nelineárních scénářů a faktu, že je dostupný zdarma, se stal ideální volbou pro tvorbu interaktivních příběhů. Prvotní shlédnutí bylo trošku kostrbaté, ale po delší práci s ním mohu jen doporučit vlastní tvorbu.

V jednotlivých pasážích nebylo použito pouze ponaučení, ale také výtky. Pokud uživatel udělal závažnou chybu, příběh byl ukončen – například tím, že postava dostala vyhazov. Současně jsem ale nabídl možnost kliknutím na tlačítko „Zkusit znovu a lépe“ příběh restartovat na volbu kapitol a pokusit se situaci vyřešit správněji a dojít k lepšímu výsledku.

Nechtěl jsem, aby moje práce v Twine působila jako obyčejný černý text na obrazovce. Upravil jsem nejprve CSS styl tak, aby každá pasáž příběhu měla barevný rámeček, výrazný nadpis a přehledné rozcestníky na volby.

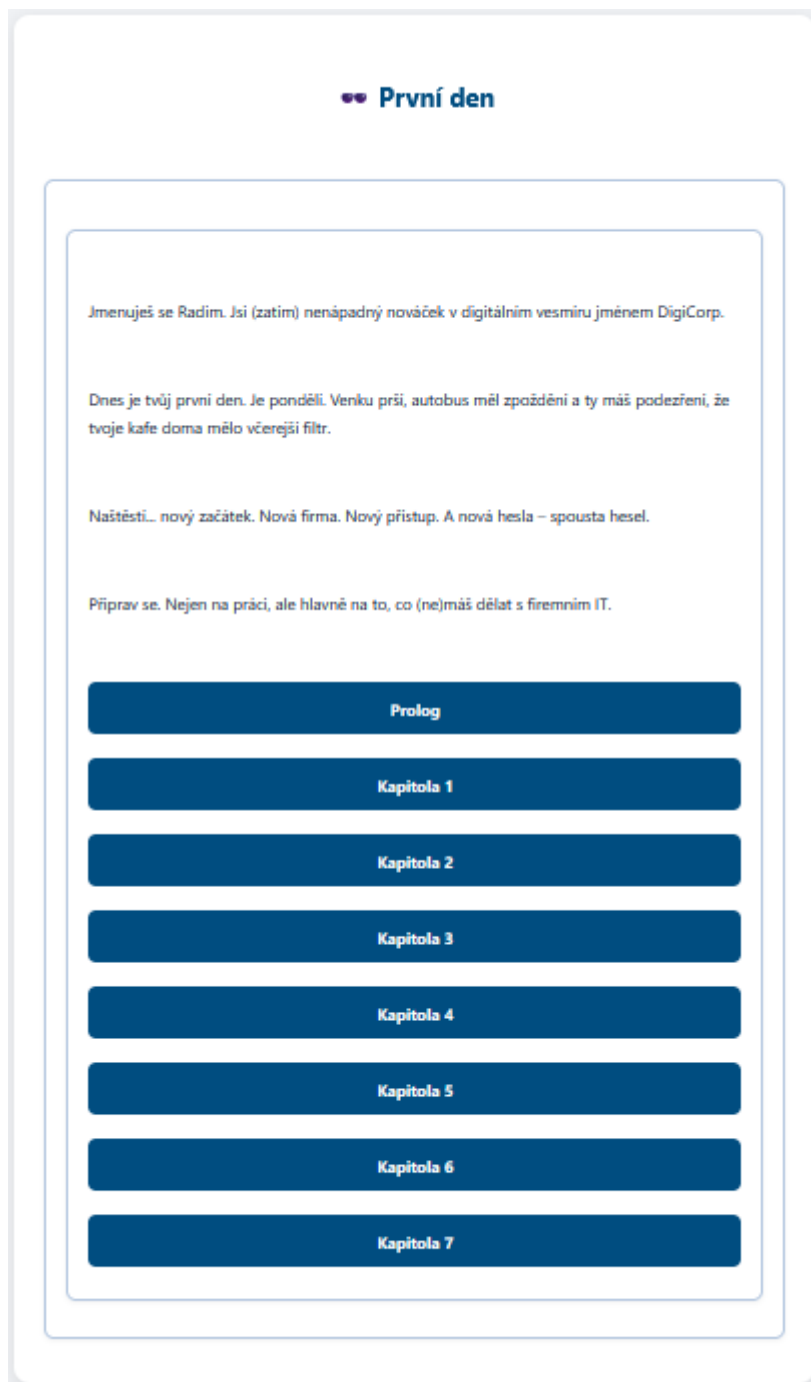
Kód CSS stylu použité pro gamebook s Radimem s vysvětlivkami je v příloze (Příloha P I.).

V Twine se jednotlivé části příběhu nazývají pasáže. Každá pasáž obsahuje kus textu, možnosti na výběr a někdy i jednoduchou logiku, která ovlivňuje, jak se bude příběh dál vyvíjet. Jednotlivé pasáže jsem označil P s číslem pro lepší dohledání.

K psaní pasáží jsem použil formát SugarCube, protože umožňuje snadné vkládání odkazů, úpravy stylu a dodání menších funkcí do příběhu.

Ukázka jedné jednoduché pasáže je v příloze (Příloha P II.):

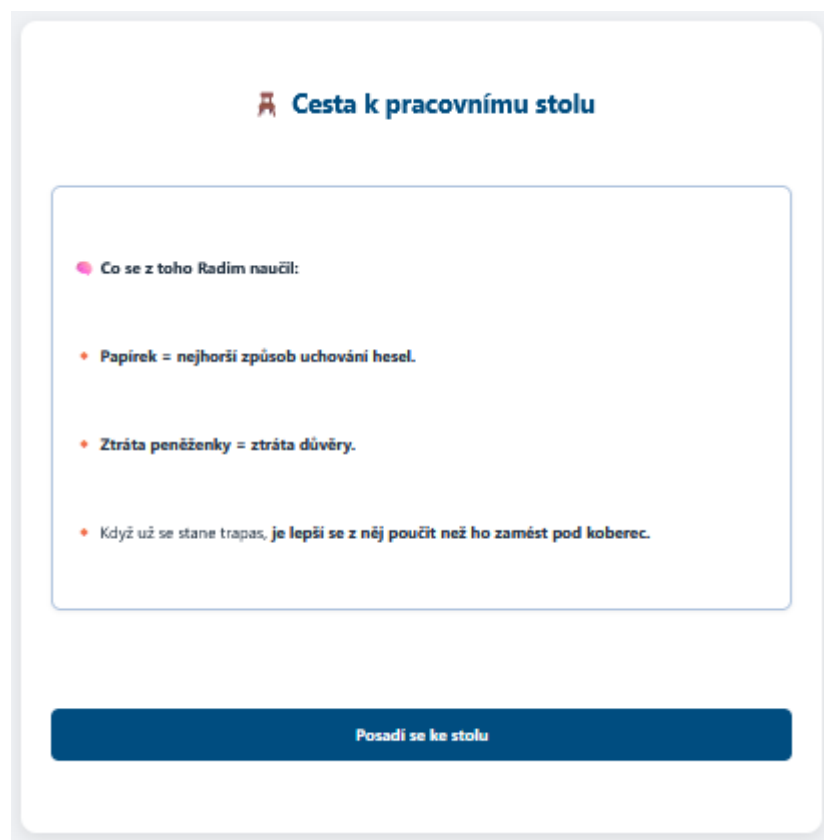
Po úpravě CSS stylu a formátování pomocí SugarCube získá výsledné zobrazení modernější a přehlednější podobu. Místo obyčejného černého pozadí a bílého textu se pasáže zobrazují v modrých rámečcích, s výraznými nadpisy a přehledně oddělenými volbami.



Obrázek 9 Rozdělení kapitol s Radimem pomocí Twine

(zdroj: vlastní)

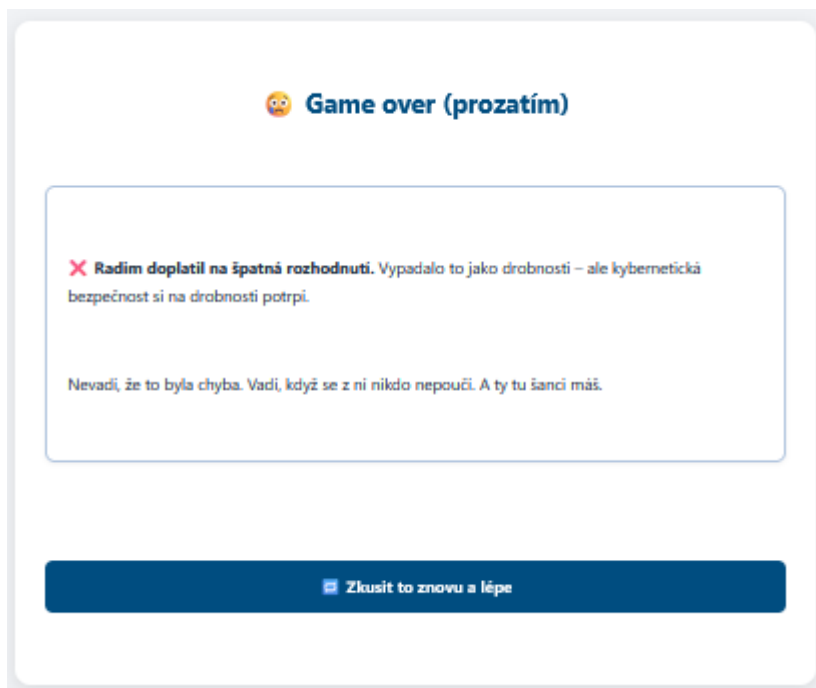
Na obrázku (Obrázek 10) zachycuje část příběhu s Radimem, kde bylo uživateli nabídnuto ponaučení. V Twine jsem využil možnost uzavřít jednotlivé kapitoly krátkým shrnutím a poučením, aby měl uživatel jasnou zpětnou vazbu ke svému rozhodnutí.



Obrázek 10 Ponaučení s Radimem pomocí Twine

(zdroj: vlastní)

Obrázek (Obrázek 11) ukazuje scénu, kde byla v příběhu s Radimem využita i možnost výpovědi. Tento prvek sloužil k tomu, aby si uživatel uvědomil vážnost špatného rozhodnutí a jeho možné důsledky.



Obrázek 11 Výpověď Radima pomocí Twine

(zdroj: vlastní)

Hodnocení nástroje Twine.

Práce v Twine pro mě byla na začátku složitější kvůli nastavování formátu, stylu a struktury příběhu. Jakmile jsem ale vše nastavil podle svých představ, další tvorba už byla zcela na mně a měl jsem plnou volnost v psaní i větvení příběhu.

Výhodou Twine je možnost exportu hotového scénáře jako HTML souboru nebo Twee kódu pro další úpravy.

Na druhou stranu, Twine nemá vestavěnou kontrolu dokončení větvení, takže jsem musel ručně hlídat, aby všechny cesty příběhu vedly ke správnému závěru a nebyly nikde slepé uličky.

7.3 Nástroj Yo Scenario

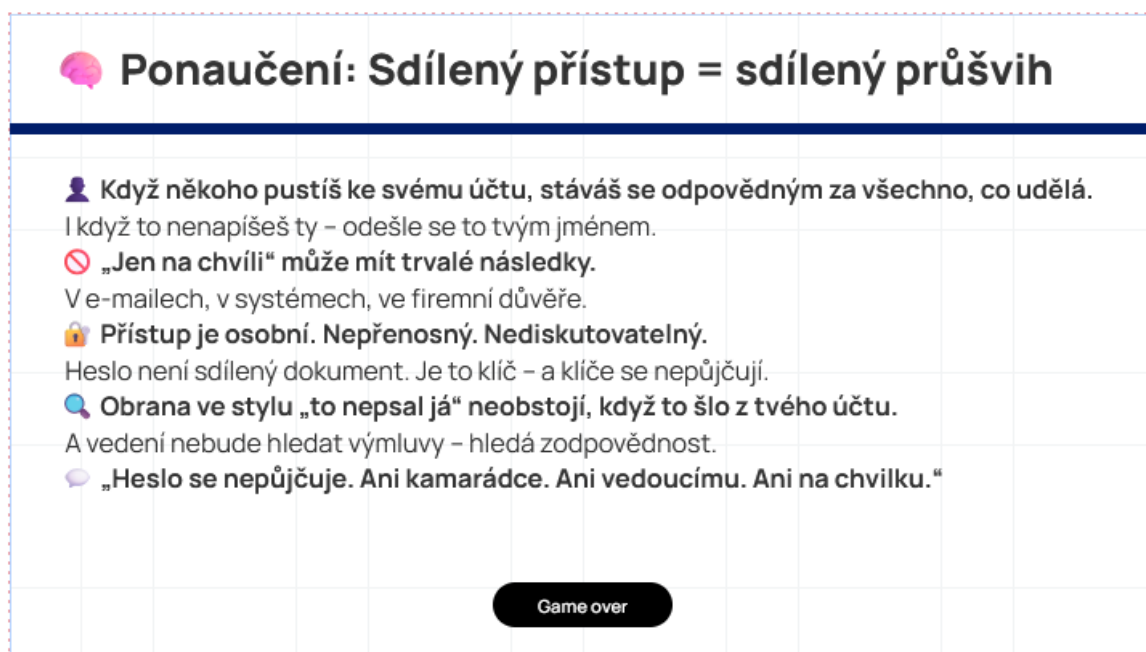
Pomocí nástroje Yo Scenario jsem vytvořil scénář podobný jako v Twine, kde představuje příběh Radima. Příběh, ale není stejný jen podobný. Jedná se o sedm kapitol. Formátování je předem nastaveno pomocí šablony.



Obrázek 12 Úvod do příběhu s Radimem pomocí Yo Scenario

(zdroj: vlastní)

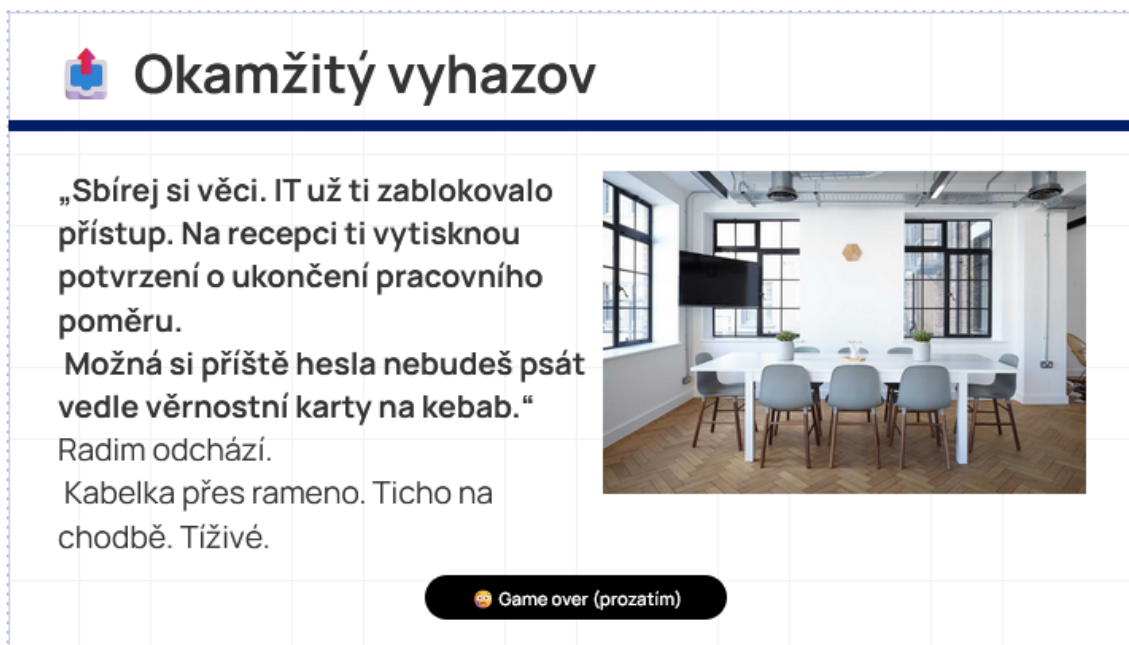
Obrázek (Obrázek 13) zachycuje ponaučení v příběhu s Radimem vytvořeném pomocí nástroje Yo scenario. Každé rozhodnutí má vlastní ponaučení.



Obrázek 13 Ponaučení s Radimem pomocí Yo Scenario

(zdroj: vlastní)

Obrázek (Obrázek 14) ukazuje scénu, kde Radim v důsledku špatného rozhodnutí obdržel výpověď. V rámci Yo Scenario jsem tak uživateli ukázal, že některé chyby mohou mít vážné a okamžité následky.



Obrázek 14 Výpověď s Radimem pomocí Yo Scenario

(zdroj: vlastní)

Hodnocení platformy Yoscenario

Yo scenario je v základní verzi dostupné zdarma a umožňuje vytvářet rozhodovací scénáře bez nutnosti programování. Tvorba scénářů je velmi intuitivní, jednotlivé části příběhu jsou rozděleny do přehledných obrazovek a větvení se nastavuje pomocí jednoduchého grafického editoru.

Výhodou je možnost exportu výsledků do formátů Excel a JSON. Export do Wordu je sice teoreticky podporován, ale nejde otevřít.

Pro svou práci jsem využil placenou verzi, která mi umožnila pracovat s více scénáři současně a využít některé rozšířené funkce. Pro mé potřeby by však v zásadě postačoval i základní balíček.

Vytvořený scénář jsem následně zveřejnil přímo pomocí platformy Yo Scenario, která umožňuje jednoduché publikování příběhu a snadné sdílení odkazu bez potřeby složitějších integrací.

Přednastavené šablony vzhledu urychlují práci, ale na druhou stranu omezují možnosti vlastních grafických úprav. I přes tato drobná omezení je Yoscenario vhodným nástrojem pro tvorbu kratších školení a rozhodovacích testů, kde je kladen důraz na jednoduchost a rychlé nasazení.

7.4 Pomocí aplikace PowerPoint

Pro scénář s Janou a příběhem o recyklaci jsem využil také PowerPoint. Tento nástroj jsem si vybral, protože je běžně dostupný, snadno se ovládá a umožňuje rychle vytvořit příběh s rozhodovacími body.

Použil jsem funkci akčních tlačítek, která po kliknutí přesunula uživatele na jiný snímek podle jeho volby. Tím jsem mohl simulovat rozhodovací příběh bez potřeby programování. Vypnul jsem možnost se pohybovat klasicky v prezentaci

Příběh s postavou Jany jsem postavil tak, že každé rozhodnutí vedlo na jiný snímek, kde uživatel viděl, co jeho volba způsobil.

Na obrázku (Obrázek 15) je znázorněna úvodní obrazovka příběhu Jany vytvořená pomocí aplikace PowerPoint. Obrázek ukazuje, jak byl příběh graficky uveden a jakým stylem byl uživatel do příběhu uveden.



Obrázek 15 Úvodní zobrazení příběhu s Janou pomocí PowerPointu

(zdroj: vlastní)

Na obrázku (Obrázek 16) zachycuje rozhodovací scénář vytvořený pomocí PowerPointu. Rozhodování je řešeno pomocí rámečků s odkazy, které vedou na jednotlivé snímky podle zvolené možnosti.

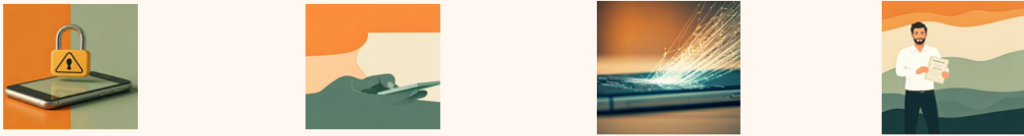


Obrázek 16 Rozhodovací scénář pomocí PowerPointu

(zdroj: vlastní)

Na obrázku (Obrázek 17) znázorňuje část příběhu, kde nechybí ponaučení nejen pro firemní prostředí, ale i pro osobní život uživatele.

Ponaučení



Ve firmě:

- ✗ Fyzické zničení zařízení není automaticky bezpečné – data mohou být stále obnovitelná
- ✗ Neautorizované zásahy mohou vést ke ztrátě důležitých informací a incidentu
- ⚠ Ztráta dat před zálohou = nevratná škoda
- ✓ Vždy kontaktuj IT – mají nástroje pro bezpečné mazání, zálohu a likvidaci
- ✓ Každá likvidace by měla být řízená a zdokumentovaná

V osobním životě:

- ✗ Rozbití starého telefonu neznamená, že tvá data zmizí
- 🔓 Kdo zařízení najde, může obnovit fotky, kontakty nebo přístupy
- ✓ Před likvidací smaž data, obnov tovární nastavení a ideálně přepiš paměť
- ✓ Používej aplikace pro vzdálené vymazání (např. „Najít iPhone“, „Najít moje zařízení“)
- 🔵 Zvaž předání telefonu k odborné ekologické likvidaci

Ponaučení Zpět na začátek

Obrázek 17 Ponaučení i pro osobní život v PowerPointu

(zdroj: vlastní)

Obrázek (Obrázek 18) ukazuje situaci, kdy byla postavě Jany udělena pouze výstraha, nikoliv okamžitá výpověď. Příběh tím upozorňuje na možnost nápravy chybného jednání.



Výstraha z pekla tabulek



Péťa z financí kývl. „Jo... ta růžová flashka byla moje.“



Jana ztuhla. „Taková... s nálepkou a... ehm, s Despacitem?“

Péťa: „Měla na sobě auditní podklady a výkaz ke čtvrtletí.“

Jana zbledla a pokračovala v práci

Obrázek 18 Výstraha Jany pomocí aplikace Powerpoint

(zdroj: vlastní)

Hodnocení platformy PowerPoint

PowerPoint je nástroj, který téměř každý zná a umí s ním základně pracovat. Díky tomu bylo vytvoření jednoduššího rozhodovacího scénáře velmi rychlé a intuitivní. Výhodou je jednoduchost práce s obsahem – snadno lze přidávat snímky, vkládat akční tlačítka a propojovat rozhodovací cesty. Na druhou stranu, při tvorbě delšího nebo složitějšího příběhu vzniká v prezentaci poměrně rychle chaos ve snímcích. Správa většího množství rozhodovacích větví se stává nepřehlednou a vyžaduje důsledné plánování. Dalším omezením je, že výsledný soubor lze uložit pouze jako .pptx, a není možné ho jednoduše importovat přímo do systémů typu Moodle bez dodatečných úprav nebo převodu. Přesto se PowerPoint ukázal jako dobrý nástroj pro rychlou tvorbu kratších rozhodovacích scénářů, kde není potřeba složité větvení a integrace.

7.5 Závěrečné shrnutí a porovnání nástrojů

Pro tvorbu interaktivních vzdělávacích scénářů byly využity čtyři nástroje: H5P, Yo scenario, Twine a PowerPoint. Každý z nich má svá specifika – H5P nabízí jednoduché začlenění do Moodle a širokou škálu šablon, je však omezenější v možnostech větvení děje. Yo scenario umožňuje vytvářet vizuálně přehledné a komplexní scénáře, ale je závislý na placeném přístupu. Twine je open-source nástroj s velkou flexibilitou a možností úprav stylu pomocí CSS, což z něj dělá ideální volbu pro rozsáhlé interaktivní příběhy. PowerPoint představuje tradiční nástroj, vhodný spíše pro lineární scénáře s omezeným větvením, ale je dostupný a známý široké veřejnosti.

Tabulka 1 Porovnání nástrojů

Nástroj	Výhody	Nevýhody	Licence	Vhodnost použití
H5P	Integrace do Moodle, jednoduchost, šablony, kontrola dokončení scénáře,	Omezené větvení, méně komplexní scénáře	Open-source / zdarma	Krátké scénáře, mikroškolení
Yo scenario	Pěkné UI, propracované volby, flexibilita	Placený přístup, cloudové řešení	Placený	Komplexní scénáře s rozhodováním
Twine	Flexibilita, vlastní CSS/JS, open-source	Vyšší náročnost na tvorbu, nutná znalost struktury	Open-source / zdarma	Interaktivní příběhy, gamebooky
PowerPoint	Známé prostředí, snadná dostupnost	Omezené větvení, nevhodné pro rozsáhlé scénáře	Komerční	Tradiční školení, lineární prezentace

(zdroj: vlastní)

8 VYHODNOCENÍ, PŘÍNOSY A DALŠÍ SMĚROVÁNÍ

V této kapitole shrnuji výsledky praktické části práce, tedy tvorby a realizace interaktivních scénářů pomocí různých nástrojů. Zaměřuji se na přínosy zvoleného přístupu, zpětnou vazbu z testování scénářů a identifikaci hlavních silných i slabých stránek jednotlivých řešení. Na základě získaných poznatků také navrhuji možnosti dalšího směřování, které by mohly vést ke zlepšení efektivity školení a rozšíření využití interaktivních příběhových scénářů v oblasti vzdělávání.

8.1 Vyhodnocení scénářů na základě zpětné vazby

Pro získání zpětné vazby na vytvořená školení jsem realizoval krátký průzkum mezi zaměstnanci společnosti, ve které dělám. Celkem odpovědělo 50 respondentů. Výsledky ukázaly, že většina respondentů preferovala gamebook s příběhem a rozhodováním před klasickým školením. Pomocí nástroje Google Forms jsem vytvořil formulář s názvem „Průzkum spokojenosti po absolvovaném školení“, který jsem připravil speciálně pro potřeby své diplomové práce.

Při vyhodnocení pěti otázek dotazníku (Obrázek 20, Obrázek 21, Obrázek 22, Obrázek 23, Obrázek 24), které se zaměřovaly na celkové vnímání školení, se opakovaně objevovala pozitivní zpětná vazba na poutavou formu výuky, celkovou atmosféru během školení a přehlednost a logickou strukturu scénářů. Tyto možnosti byly respondentům nabídnuty ve formě výběrových odpovědí, přičemž u všech uvedených otázek hrály uvedené aspekty klíčovou roli v celkovém hodnocení. Respondenti rovněž měli možnost doplnit vlastní komentář prostřednictvím volby „jiné“, která byla navržena pro zachycení individuálních dojmů a podnětů mimo předem definované oblasti.

8.1.1 Jaký tip školení preferujete ?

První otázka na zaměstnance, bylo zjištění pro prožití celkového školení, zda se jim líbilo školení pomocí klasického školení nebo novějšího pomocí gamebooku. Výsledky ukázaly, že většina účastníků preferovala právě formu interaktivního příběhu, která je více vtáhla do děje a nabídla možnost aktivně ovlivňovat průběh školení. Na obrázku (Obrázek 19) je patrné, že tento princip školení má potenciál pro další rozšíření.



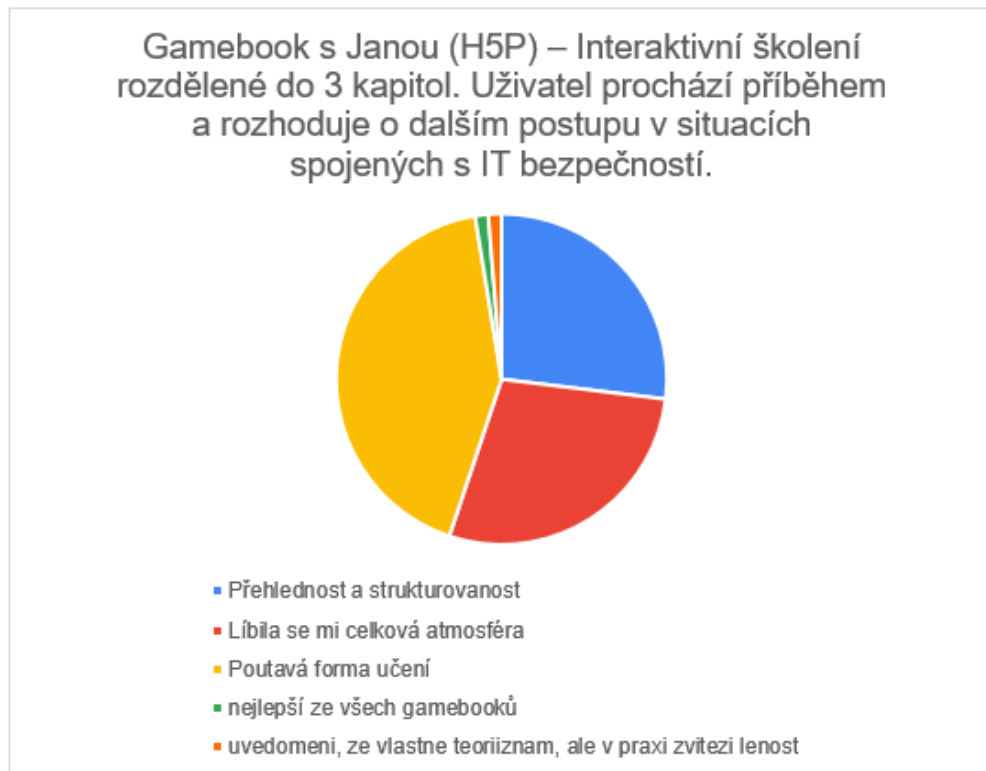
Obrázek 19 Jaký tip školení preferujete.

(zdroj: vlastní)

8.1.2 Vyhodnocení zpětné vazby na gamebook s Janou (H5P)

V rámci školení jsem vytvořil interaktivní příběh s postavou Jany pomocí nástroje H5P. Příběh byl rozdělen do tří kapitol a zaměřoval se na situace spojené s IT bezpečností.

Výsledky ukazují, že přehlednost a struktura byly oceňovány už při samotné tvorbě interaktivního příběhu, zejména v prostředí H5P, které umožňuje snadnou orientaci a logické členění obsahu. Pozitivní vnímání atmosféry a způsobu podání školení pak poukazuje na důležitost zvoleného přístupu ke vzdělávání, který kombinuje příběhové prvky s rozhodováním a vizuálně přehledným zpracováním.



Obrázek 20 Zpětná vazba na gamebook s Janou pomocí H5P

(zdroj: vlastní)

8.1.3 Vyhodnocení zpětné vazby na gamebook s Radimem (Yo Scenario)

Z průzkumu vyplynulo (Obrázek 21), že účastníci ocenili hlavně poutavou formu učení, přehledné větvení příběhu a logické návaznosti mezi rozhodnutími a následky.



Obrázek 21 Gamebook s Radimem pomocí Yo Scenario

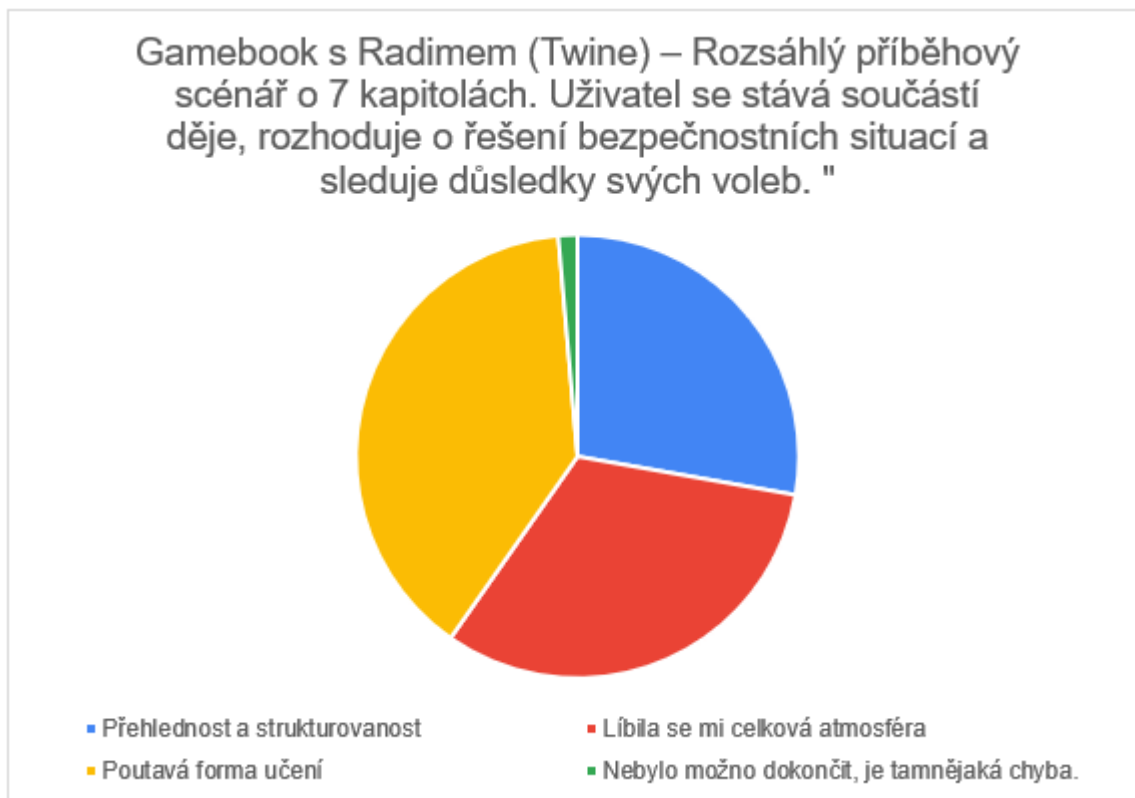
(zdroj: vlastní)

8.1.4 Vyhodnocení Radima pomocí Twine

Scénář s postavou Radima (Obrázek 22), vytvořený v nástroji Twine, zaujal uživatele svou interaktivní formou, humorem a možností samostatného rozhodování. V rámci průzkumu zpětné vazby byla opakovaně oceněna poutavá forma učení, což potvrzuje, že příběhový přístup výrazně přispěl k zapojení účastníků.

Zároveň se ale objevila připomínka „Nebylo možno dokončit, je tam nějaká chyba“. Tato chyba však nebyla způsobena nástrojem Twine samotným, ale vznikla v důsledku chyby v návrhu scénáře na straně autora – konkrétně chybějícím odkazem, který znemožnil dokončení jedné větve. Po identifikaci byla chyba odstraněna a scénář upraven tak, aby bylo možné jej kompletně projít.

Tato situace ukazuje důležitost důkladného testování při práci s otevřenými nástroji, které neobsahují automatické kontroly návaznosti mezi pasážemi. Přesto je Twine díky své flexibilitě a možnosti přizpůsobit vzhled i logiku příběhu velmi vhodným nástrojem pro tvorbu scénářů v oblasti kybernetické bezpečnosti.



Obrázek 22 Vyhodnocení gamebooku s Radimem pomocí Twine

(zdroj: vlastní)

8.1.5 Vyhodnocení Jany pomocí PowerPointu

Nejzajímavější bylo hodnocení na gamebook vytvořený pomocí aplikace Powerpoint (Obrázek 23). Jelikož se výhradně dělá jen prezentace zkusil jsem vytvořit i jeden s gamebookem.

Jeho hodnocení vyšlo nejvíce opět na formu učení, ale zde došlo i na názor, že se nelíbí vytvořený gamebok pomocí Powerpointu, ale příběh se líbí.



Obrázek 23 Příběh Jany pomocí PowerPointu

(zdroj: vlastní)

8.1.6 Vyhodnocení Radima a aktualizace pomocí H5P

Tento příběh (Obrázek 24) byl mezi účastníky hodnocen velmi pozitivně. Zpětná vazba často zmiňovala „poutavou formu a přehlednost“, což svědčí o tom, že jednoduchý, ale promyšleně navržený scénář dokáže efektivně předat klíčové sdělení.

Zaznamenány byly i neformální reakce od několika kolegů, kteří označili tento příběh za „ideální“ způsob školení – konkrétně kvůli jeho stručnosti, jasné struktuře a schopnosti přimět uživatele k zamyšlení, aniž by byl přetížen informacemi.



Obrázek 24 Vyhodnocení Radima a aktualizace systémů

(zdroj: vlastní)

8.1.7 Vyhodnocení školení

V závěru školení byli účastníci požádáni o zodpovězení několika otázek, které měly zjistit jejich spokojenost a vnímanou užitečnost školení. Většina účastníků odpověděla, že informace získané během školení považují za užitečné, a to buď zcela, nebo alespoň částečně. Tento výsledek ukazuje, že i když šlo o základní úvodní školení, podařilo se naplnit hlavní cíl – předat důležité informace srozumitelnou a praktickou formou.

Účastníci hodnotili užitečnost získaných informací velmi pozitivně. Většina uvedla, že získané poznatky mohou ihned využít v praxi. Jen jediná odpověď zmiňovala částečné využití.

Interaktivní prvky (Obrázek 25) školení byly hodnoceny na škále od 1 (nejhorší) do 5 (nejlepší). Průměrné hodnocení interaktivity bylo 4,45 bodu, což ukazuje na vysokou míru spokojenosti s tímto způsobem výuky.



Obrázek 25 Jak hodnotíte školení

(zdroj: vlastní)

Podle odpovědí na navazující otázku bylo školení vnímáno jako užitečné, interaktivní a dobře srozumitelné. Všichni respondenti by školení doporučili svým kolegům – ať už jednoznačně, nebo s drobnou výhradou. Žádný z účastníků nezvolil odpověď „ne“, což potvrzuje, že školení bylo hodnoceno výhradně kladně a splnilo očekávání většiny respondentů.

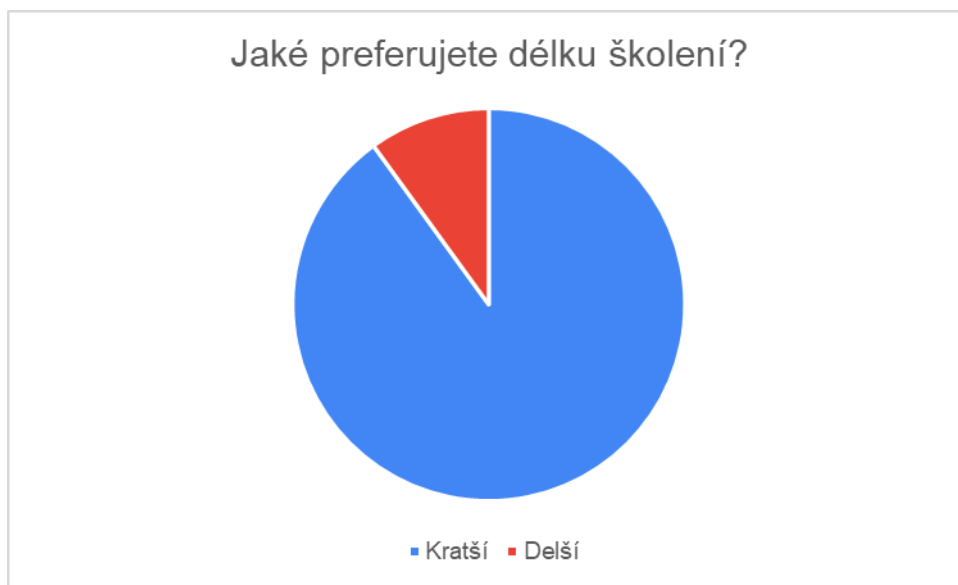


Obrázek 26 Užitečnost školení

(zdroj: vlastní)

Co se týká délky školení (Obrázek 27), respondenti častěji preferovali kratší formát školení. Tato preference se opakovaně objevovala i v otevřených odpovědích, kde někteří účastníci navrhovali zestručnění popisů situací nebo zkrácení celkové délky interaktivních scénářů.

Za „kratší školení“ lze v tomto kontextu považovat formát v délce do 50 minut, případně rozdělený na více kratších částí (např. 2×25 minut). Oproti tomu delší školení přesahuje 90 minut a vyžaduje vyšší míru soustředění, což – jak potvrzují i praktické zkušenosti – může vést ke snížení pozornosti a zájmu účastníků, zejména pokud není dostatek interaktivity nebo možností zapojení. Na základě této zpětné vazby a zkušenosti z pilotního nasazení lze za optimální délku školení považovat rozmezí 50–90 minut.



Obrázek 27 Délka školení

(zdroj: vlastní)

Účastníci hodnotili **užitečnost získaných informací** (Obrázek 28) velmi pozitivně. Většina uvedla, že získané poznatky mohou ihned využít v praxi. Jen jediná odpověď zmiňovala, že informace nejsou relevantní.

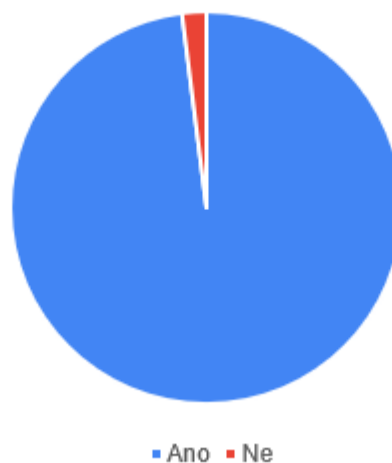


Obrázek 28 Použitelnost v praxi

(zdroj: vlastní)

Poslední otázka v dotazníku zjišťovala, zda by účastníci doporučili školení svým kolegům. Z celkového počtu 50 respondentů odpovědělo 49 kladně a pouze 1 negativně.

Doporučili by jsme toto školení kolegům



Obrázek 29 Doporučení kolegům

(zdroj: vlastní)

Na závěr dotazníku byli účastníci vyzváni, aby uvedli vlastní návrhy na možné zlepšení školení a také náměty na další témata nebo situace, které by bylo vhodné v budoucnu do školení zařadit.

V rámci otázky „Co byste navrhli ke zlepšení školení?“ účastníci uvedli několik podnětů, které se zaměřovaly především na:

- Občas tam byly chyby a rušilo to. Jinak super, zábavné.
- Dlouhé texty. Zaměřit se na formulaci slov, aby pochopili i ne IT.
- Nemít PowerPoint, je to na mě zastaralé. Preferuji ty ostatní varianty. Také by bylo přínosnější nemít tak jasná rozhodnutí, např. "Vymysli silnější heslo", raději bych tam viděla nějakou variantu, např. "RaD430WJ@86" apod.
- Velice pěkné edukativní školení.
- Lepší vysvětlení k průběhu kurzu a jak začít a co vše nás v kurzu očekává.

V rámci otázky „Máte nápad na další témata nebo situace, které bychom měli zařadit do školení?“ jsou otázky např.:

- telefon – instalace nových neověřených aplikací, PC – odhlašování, pokud odcházím od PC, vypínání, pokud jdu domů,
- rizika spojená s kryptoměnami,
- téma finančních podvodů a internetového bankovníctví,
- dětská bezpečnost na internetu.

Tímto způsobem byla sbírána zpětná vazba nejen na formu a obsah aktuálního školení, ale i inspirace pro jeho budoucí rozvoj.

8.2 Přínosy

Školení realizované formou gamebooků se ukázalo jako správná cesta, jak efektivně vzdělávat uživatele v oblasti bezpečnosti. Nasazení příběhů vycházejících ze skutečných situací bylo účastníky velmi dobře přijato a podpořilo jejich aktivní zapojení.

Délka jednotlivých scénářů byla vždy uzpůsobena potřebám příběhu a důležitosti předávané informace, což ovšem ne vždy plně odpovídalo očekávání všech účastníků. Někteří preferovali svižnější průběh.

Velkým přínosem byla také samotná forma školení, která díky uvolněnějšímu stylu a špetce humoru působila přístupněji a srozumitelněji než tradiční školení založená na strohých frázích.

Hodnocení probíhalo u zaměstnanců ve věkovém rozmezí od 21 do 63 let, což byl požadavek na hodnocení. Tento fakt potvrzuje vhodnost zvoleného přístupu napříč různými věkovými skupinami.

8.3 Další směřování

Jak bylo uvedeno v kapitole 8.1.6, účastníci v rámci zpětné vazby navrhovali rozšíření školení o další aktuální témata, například bezpečnost mobilních zařízení nebo ochranu dat při práci z domova či kryptoměny.

Je však důležité si uvědomit, že hrozby v oblasti kybernetické bezpečnosti se neustále vyvíjejí. Útočníci nikdy nespí a neustále hledají nové způsoby, jak zneužít slabá místa v systémech i v chování uživatelů.

Z tohoto důvodu je nutné školení pravidelně aktualizovat, doplňovat o nové typy útoků a přizpůsobovat je aktuálním trendům v oblasti bezpečnosti. Zachování příběhové formy, dynamického tempa a uvolněného stylu s prvky humoru se ukazuje jako vhodná cesta, jak i složitá témata předávat účastníkům srozumitelně a s trvalejším dopadem na jejich chování.

ZÁVĚR

Diplomová práce se zaměřila na inovativní přístup k přípravě na bezpečnostní incidenty prostřednictvím tvorby interaktivních vzdělávacích scénářů. V první fázi byly identifikovány a analyzovány dostupné nástroje, které umožňují efektivní tvorbu scénářového školení. Na základě porovnání jejich funkcí, náročnosti a vhodnosti pro cílovou skupinu byly vybrány nástroje H5P, Twine, Yo Scenario a PowerPoint.

S využitím těchto nástrojů byly následně vytvořeny interaktivní scénáře, které kombinují příběh, rozhodování uživatele a okamžitou zpětnou vazbu. Scénáře byly implementovány v prostředí LMS Moodle a testovány v rámci školení pro nové zaměstnance. Výsledky ukazují, že scénářového vzdělávání výrazně zvyšuje zapojení účastníků, zlepšuje jejich schopnost rozpoznat rizikové situace a podporuje rychlejší a správnější rozhodování při bezpečnostních incidentech.

Zpětná vazba od uživatelů potvrdila, že forma vzdělávání založená na příběhových scénářích je vnímána jako srozumitelná, poutavá a přínosná. V budoucnu je možné tento přístup dále rozvíjet například zapojením pokročilejších simulací, adaptivních scénářů nebo větší personalizace podle role uživatele ve firmě.

SEZNAM POUŽITÉ LITERATURY

- [1] LUTTGENS, Jason T., PEPE, Matthew, a MANDIA, Kevin. Incident Response & Computer Forensics. 3rd ed. McGraw-Hill Professional, 2014. 624 s. ISBN 9780071798686.
- [2] BLOKDYK, Gerardus. Cyber Security Incident Response: A Complete Guide. 2019 Edition. 5STARCook, 2021. 317 s. ISBN 0655518479
- [3] MARTIN-VEGUE, Tony. How to Write Strong Risk Scenarios and Statements. [online][cit. 2024-10-25] Dostupné z: <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-31/how-to-write-strong-risk-scenarios-and-statements>
- [4] STALLINGS, William. Effective cybersecurity: understanding and using standards and best practices. Upper Saddle River, NJ: Addison-Wesley, 2019. ISBN 978-0-13-477280-6.
- [5] STALLINGS, William. Cryptography and network security: principles and practice. Seventh edition, Global edition. Boston: Pearson[2017] ISBN 978-1-292-15858-7.
- [6] H5P. *Documentation – Create and reuse interactive HTML5 content in your browser*. [online][cit. 2025-04-03] Dostupné z: <https://h5p.org/documentation>
- [7] Yo Scenario. *User Documentation – Help Center*. [online][cit. 2025-04-03] Dostupné z: <https://app.yoscenario.com/help/docs>
- [8] Twine. *Twine Reference – Documentation for interactive story creation*. [online][cit. 2025-04-03] Dostupné z: <https://twinery.org/reference/en/>
- [9] EdApp. *Mobile LMS with Microlearning and Gamification*. [online][cit. 2025-04-03] Dostupné z: <https://www.edapp.com>
- [10] Easygenerator. E-learning authoring tool for workplace training. [online][cit. 2025-04-03] Dostupné z: <https://www.easygenerator.com>
- [11] iSpring Solutions. *iSpring Suite – Authoring Toolkit*. [online][cit. 2025-04-03] Dostupné z: <https://www.ispringsolutions.com>
- [12] Lumi Education. "Lumi – Create interactive and engaging H5P content." Dostupné z: <https://lumi.education/en/>

- [13] [online] In: LUMI. [cit. 2025-04-28] Dostupné z: <https://app.lumi.education/dashboard/content/67ef914a343318e48465fe4d/edit>
- [14] HALLER, Martin. Bezpečnost a její životní cyklus [online]. 2021 [cit. 2025-05-19]. Dostupné z: <https://martinhaller.cz/know-how/bezpecnost-zivotni-cyklus/>
- [15] Česko. Zákon č. 110/2019 Sb., o zpracování osobních údajů [online]. In: *Zákony pro lidi*. Zpracováno dle Sbírka zákonů [cit. 2025-05-19]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2019-110>

SEZNAM OBRÁZKŮ

Obrázek 1 Životní cyklus incidentu.....	22
Obrázek 2 Základní výběr kapitol s Janou pomocí H5P	65
Obrázek 3 Možnosti rozhodování s Janou pomocí H5P	66
Obrázek 4 Ukázka školení s Janou pomocí H5P	66
Obrázek 5 Úvod do školení s Radimem pomocí H5P	67
Obrázek 6 Rozhodovací scénář s Radimem pomocí H5P	67
Obrázek 7 Ponaučení s Radimem pomocí H5P	67
Obrázek 8 Kontrola ukončení scénáře ve webové aplikaci Lumi [13].....	68
Obrázek 9 Rozdělení kapitol s Radimem pomocí Twine	70
Obrázek 10 Ponaučení s Radimem pomocí Twine	71
Obrázek 11 Výpověď Radima pomocí Twine	72
Obrázek 12 Úvod do příběhu s Radimem pomocí Yo Scenario	73
Obrázek 13 Ponaučení s Radimem pomocí Yo Scenario	73
Obrázek 14 Výpověď s Radimem pomocí Yo Scenario.....	74
Obrázek 15 Úvodní zobrazení příběhu s Janou pomocí PowerPointu.....	75
Obrázek 16 Rozhodovací scénář pomocí PowerPointu	76
Obrázek 17 Ponaučení i pro osobní život v PowerPointu	77
Obrázek 18 Výstraha Jany pomocí aplikace Powerpoint	78
Obrázek 19 Jaký tip školení preferujete.	81
Obrázek 20 Zpětná vazba na gamebook s Janou pomocí H5P	82
Obrázek 21 Gamebook s Radimem pomocí Yo Scenario	83
Obrázek 22 Vyhodnocení gamebooku s Radimem pomocí Twine	84
Obrázek 23 Příběh Jany pomocí PowerPointu	85
Obrázek 24 Vyhodnocení Radima a aktualizace systémů	86
Obrázek 25 Jak hodnotíte školení	87
Obrázek 26 Užitečnost školení	88
Obrázek 27 Délka školení.....	88
Obrázek 28 Použitelnost v praxi	89
Obrázek 29 Doporučení kolegům	89

SEZNAM TABULEK

Tabulka 1 Porovnání nástrojů	79
------------------------------------	----

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI	Umělá inteligence
APT	Pokročilá perzistentní hrozba
ATT&CK	Databáze taktik a technik útočníků (MITRE)
BCP	Plán kontinuity podnikání
BPMN	Notace pro modelování podnikových procesů
CSIRT	Tým pro reakci na bezpečnostní incidenty
CaaS	Kyberkriminalita jako služba
CTI	Kybernetické zpravodajství o hrozbách
DDoS	Distribuované odepření služby
DR	Obnova po havárii
ENISA	Evropská agentura pro kybernetickou bezpečnost
FMAE	Analýza možných poruch a jejich dopadů
FTA	Analýza poruchových stromů
GDPR	Obecné nařízení o ochraně osobních údajů
HAZOP	Studie nebezpečí a provozuschopnosti
H5P	Open-source formát pro interaktivní vzdělávací obsah
IDS/IPS	Systém detekce a prevence průniků
ISO/IEC	Mezinárodní organizace pro normalizaci / Mezinárodní elektrotechnická komise
IRT	Tým pro řešení incidentů
LMS	Systém pro správu výuky
MISP	Platforma pro sdílení informací o hrozbách
MITRE	Výzkumná organizace spravující rámec ATT&CK
MS Teams	Komunikační platforma
MS Viva	LMS platforma od Microsoftu pro firemní vzdělávání

MSSP	Poskytovatel spravovaných bezpečnostních služeb
NIS2	Směrnice EU o kybernetické bezpečnosti
NIST	Americký národní institut pro standardy
PASTA	Proces simulace útoků a analýzy hrozeb
RPN	Číslo prioritizace rizika ve FMEA metodě
RTIR	Nástroj pro řízení incidentů
SCORM	Standard pro výměnu e-learningového obsahu
SIEM	Správa bezpečnostních informací a událostí
SLA	Smlouva o úrovni poskytovaných služeb
SOC	Bezpečnostní operační centrum
SOAR	Orchestrací řízená a automatizovaná reakce na bezpečnostní události
SP	Označení publikací NIST
STRIDE	Klasifikace typů hrozeb
SWIFT	Strukturovaná „co kdyby“ analýza
Tabletop	Scénáře cvičení „u stolu“ bez reálného technického zásahu
TCO	Celkové náklady na vlastnictví (nástroje, údržbu, školení apod.)
VPN	Virtuální privátní síť
xAPI	Standard pro sledování vzdělávacích aktivit

SEZNAM PŘÍLOH

Příloha P I: CSS styl ve Twine

Příloha P II: Ukázka kódu ve Twine

Příloha P III: Seznam elektronických příloh

PŘÍLOHA P I: CSS STYL VE TWINE

```
.sesit-list {  
    background: #ffffff; /* Bílé pozadí pro celý list */  
    border: 2px solid #d0e7ff; /* Světle modrý rámeček kolem celého listu */  
    border-radius: 12px; /* Zaoblení rohů (měkčí vzhled) */  
    padding: 25px; /* Vnitřní okraje obsahu od okrajů boxu */  
    margin-bottom: 30px; /* Vnější mezera pod listem */  
    box-shadow: 0 4px 12px rgba(0, 122, 204, 0.08); /* Jemný stín pod listem (modrý, poloprůhledný) */  
    font-family: "Segoe UI", sans-serif; /* Moderní bezpatkový font */  
}  
  
.sesit-nadpis {  
    font-size: 1.5em; /* Velikost písma nadpisu (1,5× základní velikosti) */  
    font-weight: bold; /* Tučný text */  
    color: #005b99; /* Tmavě modrá barva písma */  
    margin-bottom: 20px; /* Mezery pod nadpisem */  
    text-align: center; /* Zarovnání textu na střed */  
    border-bottom: 2px dashed #a3cfff; /* Spodní orámování nadpisu jako čárkovaná linka */  
    padding-bottom: 10px; /* Vnitřní mezera pod textem nadpisu a linkou */  
}  
  
.sesit-tab {  
    width: 100%; /* Tabulka se roztáhne na celou šířku boxu */  
    background-color: #ffffff; /* Bílé pozadí tabulky */  
    border: 2px solid #004b87; /* Tmavě šedomodrý rámeček */  
    border-radius: 8px; /* Jemné zaoblení rohů */  
    padding: 15px; /* Vnitřní mezera uvnitř tabulky */  
    margin-bottom: 25px; /* Vnější mezera pod tabulkou */  
}
```

```

    box-shadow: inset 0 0 6px rgba(0, 75, 135, 0.08); /* Vnitřní stín pro
plastický efekt */

    line-height: 1.7; /* Výška řádku pro čitelnost textu */
}

.sesit-tab td {

    padding: 20px; /* Vnitřní mezery kolem textu v buňce */

    font-size: 1.05em; /* Trochu větší text pro čitelnost */

    color: #002f54; /* Tmavě šedomodrá barva písma */
}

.odpoved-box {

    background-color: #364f6b; /* Tmavě šedomodré pozadí (aktuálně - ?)
*/

    border-radius: 8px; /* Zaoblení rohů pro vzhled tlačítka */

    padding: 12px 16px; /* Vnitřní mezery tlačítka (nahoru/dolů a po
stranách) */

    font-weight: bold; /* Tučný text pro zvýraznění */

    color: #004d80; /* Tmavě modrá barva textu */

    text-align: center; /* Zarovnání textu na střed */

    border: 2px solid #007acc; /* Modrý rámeček tlačítka */

    transition: background-color 0.2s, transform 0.2s; /* Animace při
najetí myši - změna barvy a velikosti */

    cursor: pointer; /* Kurzor se změní na "ručičku" při přejetí */
}

```

PŘÍLOHA P II: UKÁZKA KÓDU VE TWINE

```
<div class="pasaz">

<div class="pasaz-nadpis">P1</div>

<div class="pasaz-obsah">


<div class="text-box">

<p>Jmenuješ se Radim. Jsi (zatím) nenápadný nováček v digitálním
vesmíru jménem DigiCorp.</p>

<p>Dnes je tvůj první den. Je pondělí. Venku prší, autobus měl zpoždění
a ty máš podezření, že tvoje kafe doma mělo včerejší filtr.</p>

<p>Naštěstí.. nový začátek. Nová firma. Nový přístup. A nová hesla -
spousta hesel.</p>

<p>Připrav se. Nejen na práci, ale hlavně na to, co (ne)máš dělat s
firemním IT.</p>

</div>

</div>

<div class="pasaz-odkazy">

[ [Prolog->P46]]

[ [Kapitola 1->P2]]

[ [Kapitola 2->P38]]

[ [Kapitola 3->P67]]

[ [Kapitola 4->P121]]

[ [Kapitola 5->P153]]

[ [Kapitola 6->P161]]

[ [Kapitola 7->P185]]

</div>

</div>
```

PŘÍLOHA P III: SEZNAM ELEKTRONICKÝCH PŘÍLOH

Součástí této práce je také složka ve formátu ZIP, která obsahuje elektronické materiály vztahující se k praktické části. V této složce se nachází různé podklady, které dokumentují tvorbu a použití výukových scénářů, a také nastavení samotného školicího prostředí. Pro přehlednost jsou rozděleny na :

- /Dotazník spokojenosti – excelová tabulka s vyhodnocením
- / H5P Lumi – dva scénáře vytvořené pomocí platformy H5P
- / moodle – záloha databáze, konfigurační a podpůrné soubory
- / PowerPoint – jeden scénář vytvořený podle aplikace Powerpoint
- / Twine – jeden scénář vytvořený pomocí platformy twine
- /Videa – tři video návody pro H5P, Twine a Yo scenario
- /Yo scenario – jeden scénář vytvořený pomocí platformy Yo scenario