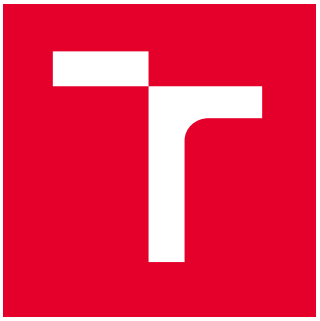


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

VZDĚLÁVACÍ HRA NA PLATFORMĚ BUTCA SE ZAMĚŘENÍM NA BEZPEČNOST V MICROGRIDU

EDUCATIONAL GAME ON THE BUTCA PLATFORM WITH A FOCUS ON MICROGRID SECURITY

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — **Radek Trávníček**

AUTHOR

VEDOUCÍ PRÁCE — **Ing. Antonín Bohačík**

SUPERVISOR

BRNO 2025

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Radek Trávníček ***ID:*** 247621

Ročník: 3 ***Akademický rok:*** 2024/25

NÁZEV TÉMATU:

Vzdělávací hra na platformě BUTCA se zaměřením na bezpečnost v microgridu

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce bude vytvoření virtualizované struktury microgridu na bázi virtuálních strojů, která bude simulovat komunikační síť mezi jednotlivými prvky (elektrárny, domácnosti apod.). Tato struktura bude implementována s využitím průmyslových a energetických protokolů. Na této struktuře bude následně vytvořena vzdělávací CTF hra s napojením na platformu BUTCA. Hra bude zábavnou formou učit studenty o fungování distribuce elektrické energie, microgridu a jeho bezpečnosti.

V teoretické části se student seznámí s konceptem microgridu, využívanými komunikačními protokoly (např. IEC 60870-5-104 či Modbus), bezpečnostními standardy a principy tvorby CTF her. V rámci praktické části práce proběhne volba nástrojů pro virtualizaci microgridu a simulaci komunikačních protokolů. Student navrhne a implementuje virtualizovanou strukturu microgridu v rámci virtuálních strojů, která bude simulovat komunikaci mezi jednotlivými prvky sítě a bude využívat ověřené bezpečnostní mechanismy. Následně bude vytvořena CTF hra na platformě BUTCA, která bude využívat tuto virtualizovanou strukturu microgridu. Hra bude zahrnovat úkoly zaměřené na pochopení provozních a bezpečnostních stavů, které mohou v rámci microgridu nastat. Na závěr bude provedeno testování jak samotné virtualizované sítě, tak CTF hry, včetně vyhodnocení funkčnosti a vzdělávacího potenciálu.

Výsledkem bakalářské práce bude plně funkční virtualizovaná struktura microgridu a CTF hra na platformě BUTCA, která bude sloužit jako vzdělávací nástroj pro studenty. Součástí práce bude rovněž dokumentace všech provedených kroků, detailní popis vytvořené hry a důkladné testování výsledného řešení.

DOPORUČENÁ LITERATURA:

Podle pokynů vedoucího práce.

Termín zadání: 10.2.2025 ***Termín odevzdání:*** 3.6.2025

Vedoucí práce: Ing. Antonín Bohačík

prof. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Bakalářská práce se zabývá návrhem a realizací vzdělávací hry v prostředí platformy BUTCA, s tématikou kybernetické bezpečnosti v mikrogridu. Cílem je vytvořit virtualizovanou strukturu mikrogridu, ve které se budou simulovat útoky. Scénář zasazuje hráče do role etického hackera, jehož cílem je odhalit slabiny systému a čelit výzvám od fiktivního útočníka ShadowBeacona. Hra byla také otestována na několika skupinách testerů.

KLÍČOVÁ SLOVA

Mikrogrid, BUTCA, Kybernetická bezpečnost, CTF hra

ABSTRACT

The bachelor's thesis focuses on the design and implementation of an educational game within the BUTCA platform, centered around cybersecurity in microgrids. The goal is to create a virtualized microgrid structure where attacks can be simulated. The scenario places the player in the role of ethical hacker tasked with uncovering system vulnerabilities and facing challenges from fictional attacker named ShadowBeacon. The game was also tested on several groups of testers.

KEYWORDS

Microgrid, BUTCA, Cyber security, CTF game

TRÁVNÍČEK, Radek. *Vzdělávací hra na platformě BUTCA se zaměřením na bezpečnost v microgridu*. Bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2025. Vedoucí práce: Ing. Antonín Bohačík

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Radek Trávníček
VUT ID autora:	247621
Typ práce:	Bakalářská práce
Akademický rok:	2024/25
Téma závěrečné práce:	Vzdělávací hra na platformě BUTCA se zaměřením na bezpečnost v microgridu

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu Ing. Antonínu Bohačíkovi, za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Úvod

Distribuční systémy elektrické energie tvoří základ moderní společnosti. S rostoucím významem obnovitelných zdrojů energie roste i potřeba efektivní správy decentralizovaných energetických sítí, známých jako mikrogridy. Tyto systémy umožňují optimalizaci distribuce energie a přizpůsobení měnícím se podmínkám, včetně odolnosti vůči výpadkům. Jejich komplexní struktura a propojení fyzických a kybernetických systémů činí mikrogridy náchylnými ke kybernetickým útokům, které mohou mít závažné důsledky pro stabilitu a bezpečnost energetické sítě.

Tato práce se zaměřuje na návrh a realizaci vzdělávací hry na platformě BUTCA, která umožňuje praktické pochopení kybernetické bezpečnosti v mikrogridu. Hra kombinuje simulaci provozu mikrogridu s úkoly typu Capture the Flag, přičemž účastníci získají praktické dovednosti v oblasti ochrany energetické infrastruktury před kybernetickými hrozbami. Práce zahrnuje návrh architektury hry, implementaci virtualizovaného prostředí mikrogridu a testování vzdělávacího potenciálu vytvořeného scénáře.

Práce je rozdělena do dvou částí. V první teoretické části je popsán mikrogrid a to, jak fungují Cyber Range platformy a teorie Capture the Flag her. Také jsou zde popsány dva komunikační protokoly z oblasti energetiky, a to protokol Modbus a protokol IEC 60870-5-104. Praktická část obsahuje návrh jednotlivých úkolů včetně jejich testování. Výsledky jsou nakonec vyhodnoceny z hlediska funkčnosti, vzdělávacího přínosu a možného dalšího rozvoje. V rámci bakalářské práce bude celý návrh scénáře implementován do platformy BUTCA, včetně struktury scénáře a jednotlivých úkolů.

Motivace

Cílem práce je navrhnout a zrealizovat scénář na téma kyberbezpečnosti v mikrogridu. Účelem tohoto scénáře je edukovat studenty o možném kybernetickém nebezpečí v energetických sítích. Znalosti slabin protokolů a obecně kritické infrastruktury jsou pro budoucí správce energetických sítí důležité. Hráči mají příležitost nahlédnout do rizik, se kterými se mohou setkat v kybernetickém prostoru mikrogridu. Tímto způsobem scénář přispívá k lepší připravenosti studentů na reálné kybernetické hrozby v oblasti energetiky.

1 Mikrogrid

Tradičně má rozvodná síť podobu centralizované elektrické sítě neboli makrogridu. Celý systém je založen na centralizované výrobě elektrické energie s velkým množstvím různých elektráren a distribučních uzlů. Tato energie je následně distribuována na velké vzdálenosti přes rozsáhlou přenosovou soustavu ke koncovým zákazníkům. Tento přístup má však své limity, tím největším je odolnost proti výpadkům. Pokud by došlo k poruše některého z klíčových uzlů, došlo by k rozsáhlým výpadkům dodávek energie [1].

V posledních letech však nastal trend decentralizace elektrické sítě. Důvody tohoto trendu jsou udržení ceny elektrické energie, výměna stárnoucí infrastruktury, zlepšení odolnosti a spolehlivosti, snížení produkce CO_2 a nebo zajištění spolehlivého přístupu k elektrické energii v oblastech bez potřebné infrastruktury. Ačkoliv se hnací faktory a detaily mohou lišit, je mikrogrid velmi flexibilní architektura pro nasazení DER (Distributed Energy Resources), které dokáží uspokojit širokou škálu komunit od metropolitních po venkovské [2].

Distribuční systém, který funguje jako mikrogrid, má dostatečnou výrobu blízko zatížení, a tak může udržet dodávku energie v případě poruch na makrogridu. Kromě toho, pokud má mikrogrid přebytek výrobní kapacity, může poskytnout makrogridu zdroje pro obnovu systému, čímž snižuje frekvenci a délku výpadků. Takové funkce přidávají flexibilitu zmíněné architektuře a činí z mikrogridu obrovský přínos pro zlepšení odolnosti sítě vůči selháním makrogridu [3].

Oproti tomu mají staré energetické sítě architekturu shora dolů, od výroby přes přenos po distribuční systémy. Tato struktura nabízí omezenou odolnost vůči poruchám a selháním v přenosovém systému, protože tyto poruchy mohou potenciálně vést ke ztrátě mnoha distribučních systémů. Mikrogrid je oproti tomu definován jako koordinovaná skupina jednotek DER, které obsluhují sadu zatížení prostřednictvím distribučního systému s těmito možnostmi [3]:

1. fungovat připojeny k konvenční energetické síti (tj. makrogridu),
2. fungovat odděleně od makrogridu,
3. poskytovat plynulý přechod mezi režimy připojení k makrogridu a odděleného provozu.

Obnovitelné zdroje hrají klíčovou roli v generování elektrické energie pro mikrogrid. Větrné a fotovoltaické elektrárny jsou využívány více než jiné typy obnovitelných zdrojů díky vysokému stupni vývoje a nízkým investičním nákladům. Ale vzhledem k nejistému chování těchto zdrojů jsou také součástí i konvenční generátory, jako jsou například ty dieselové. Kromě generování energie je také důležité tu přebytkovou někde ukládat pro pozdější použití, což zvyšuje spolehlivost systému a k tomu slouží baterie [2].

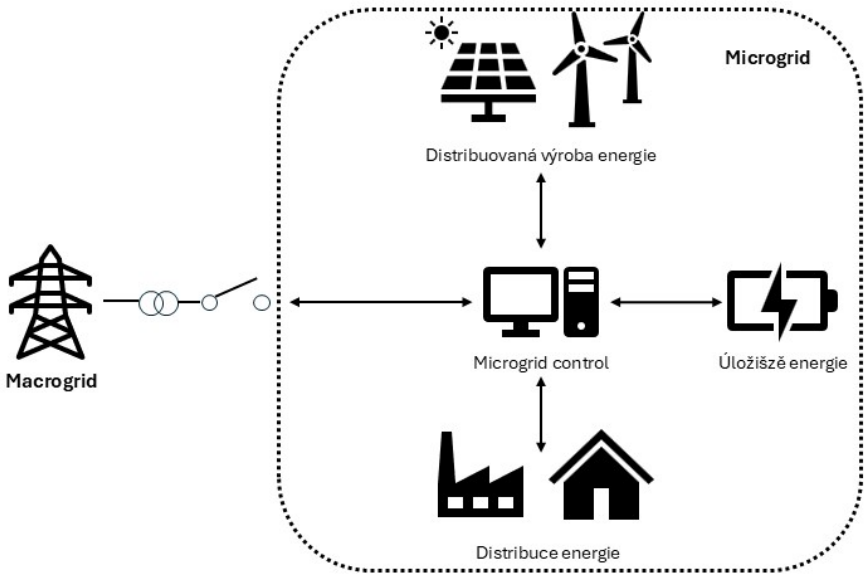
Další součástí je EMS (Energy Management System), jedná se v podstatě o „mozek“ mikrogridu, který zajišťuje optimalizaci výroby a spotřeby energie. Umožňuje vyrovnávat výkyvy v poptávce a výrobě energie, to je obzvlášť důležité u obnovitelných zdrojů, které jsou závislé na počasí. Může například rozhodnout o tom, kdy je vhodné přepnout na záložní zdroj a nebo začít čerpat energii z baterií. Kromě těchto funkcí je také zodpovědný za přepínání mezi různými provozními režimy [8].

Další složkou jsou chytré měřiče a IoT (Internet of Things). Chytré měřiče umožňují detailní sledování spotřeby elektrické energie a to od jednotlivých domácností po samotná zařízení, tato data se sbírají v reálném čase a díky tomu poskytují důležité informace o výrobě a spotřebě energie. IoT pak zajišťuje komunikaci mezi různými zařízeními, jako jsou třeba právě chytré měřiče, řídící jednoty nebo baterie. Tato komunikace je důležitá pro efektivní fungování mikrogridu [9].

Poslední částí jsou zákaznické sektory, které se dají rozdělit na obytné, průmyslové, komerční zóny a kritickou infrastrukturu. Obytné oblasti z pravidla zahrnují rodinné nebo bytové domy, mohou využívat solární panely na střechách, bývají zde obvyklá malá úložiště energie v podobě baterií. Průmyslové nebo komerční oblasti často mívají vyšší poptávku po energii než třeba oblasti obytné. Pro kritickou infrastrukturu je důležité zajistit nepřetržitou dodávku energie, a proto bývá vybavena záložními generátory nebo většími bateriemi. Schéma fungování tohoto systému je na obrázku 1.1.

Největšími firmami, které se v dnešní době zabývají stavbou mikrogridů, jsou AlphaStruxure, Anbaric, Bloom Energy, BoxPower nebo třeba Siemens. V České republice jde o Schneider Electric. Každá z těchto firem se zajímá o trochu jiné využití mikrogridů.

Mikrogrid je ale jako každé moderní zařízení náchylný ke kybernetickým útokům. Pokud by nějaký takový útok byl úspěšný, tak může dojít i na nejhorší scénář, jako je blackout (kolaps celé energetické sítě). Z tohoto důvodu je nutné mikrogrid co nejlépe zabezpečit jak proti fyzickým, tak i kybernetickým útokům [3].



Obr. 1.1: Schéma fungování mikrogridu

1.1 Typy mikrogridu

V kontextu typů můžeme mikrogridy rozdělit podle několika kritérií. Hlavními těmito kritérii jsou charakteristika, vlastnosti vedení a umístění. Z jejich pohledu určujeme 3 primární kategorie, a to městský, venkovský a osamostatněný mikrogrid.

Městský mikrogrid

Je mikrogrid, který se nachází v zastavěné nebo koncentrované průmyslové oblasti. Z tohoto důvodu jsou hlavní vedení a odbočky poměrně krátké a stupeň nesymetrie není vysoký. Krátkosvazkový poměr městského mikrogridu na jeho PCC (Point of Common Coupling) je obvykle vyšší než 25. Proto, když je připojený k makrogridu, tak napětí a frekvenci určuje makrogrid [3].

Venkovský mikrogrid

Je mikrogrid, který se nachází v řídce osídlené oblasti, a proto je zatížení rozptýleno. Z tohoto důvodu jsou hlavní vedení a odbočky značně dlouhé a krátkosvazkový poměr není nutně tak vysoký jako u městského mikrogridu. V tomto druhu mikrogridu může být značná nerovnováha a kolísání napětí [3].

Osamostatnělý mikrogrid

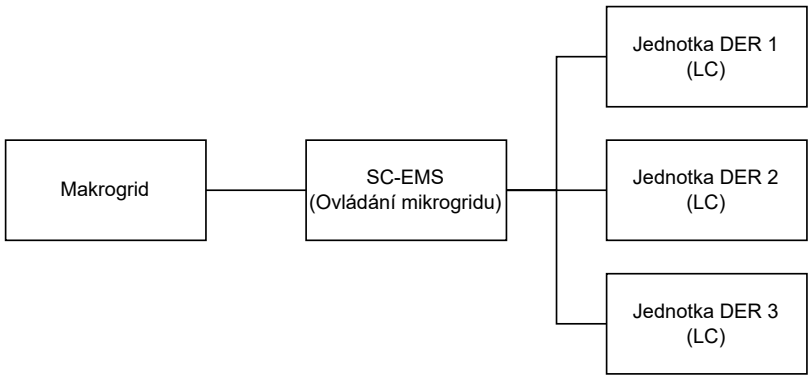
Osamostatnělý mikrogrid je buď geograficky umístěn ve vzdálené oblasti bez možnosti připojení k makrogridu, nebo obklopen obtížným terénem pro připojení k přenosovému vedení. Podle definice vždy osamostatněná mikroenergie pracuje v osamostatněném režimu a proto nesplňuje přísnou definici mikrogridu [3, 4].

1.2 Řízení mikrogridu

Strategie řízení mikrogridu zahrnují distribuované, centralizované a hierarchické řízení. Některé inherentní vlastnosti, jako je vysoký stupeň nesymetrie a rozmanitost jednotek DER, představují výzvu pro vytvoření funkčního řízení pro všechny provozní scénáře. Kromě toho přizpůsobení dvou odlišných provozních režimů (tj. osamostatněného a připojeného k makrogridu) a požadavek na přechod mezi těmito režimy dále zvyšuje složitost řízení mikroenergetické sítě. Proto je důležité znát jejich rozdělení [3].

Režim připojení k makrogridu

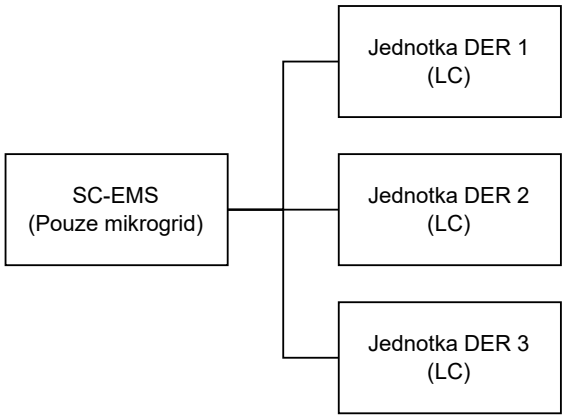
V tomto režimu každá jednotka DER obsahuje LC (Local Controller), který operuje s jednotkou podle lokálně měřeného napětí a dalších vedlejších produktů. SC-EMS (Supervisory Controller and Energy Management System) mikrogridu generuje referenční signály, které jsou potřeba pro koordinaci operací jednotek DER. Při připojení k makrogridu má SC-EMS také možnost přijímat informace z makrogridu pro efektivnější operování mikrogridu. Schéma mikrogridu, který je připojen k makrogridu, je na obrázku 1.2 [3, 5].



Obr. 1.2: Schéma režimu připojeno k makrogridu

Ostrovní režim

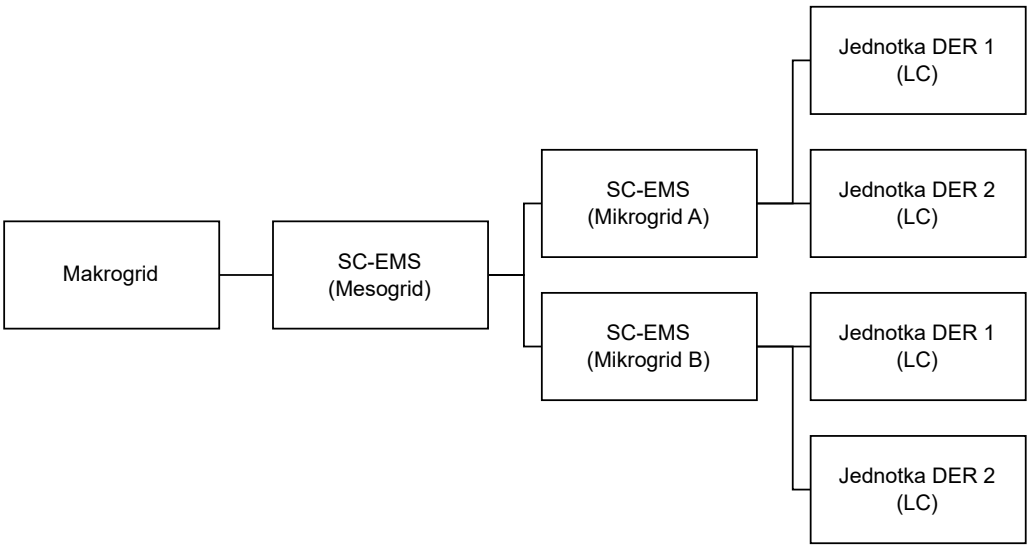
V tomto režimu jsou LC a SC-EMS odpovědné pouze za interní operace mikrogridu. Strategie kontroly pro ostrovní režim a režim připojení k makrogridu jsou často rozdílné, např. v režimu připojeno k makrogridu mohou všechny jednotky DER potenciálně pracovat v režimu PQ-řízení, zatímco po přechodu do ostrovního režimu musí určitá sada jednotek DER pracovat v režimu řízení napětí-frekvence a takový přechod řízení musí být určen a řízen SC-EMS. Schéma mikrogridu, který je v ostrovním režimu, je na obrázku 1.3 [3, 6].



Obr. 1.3: Schéma ostrovního režimu

Režim mesogridu

Je definován jako shluk mikrogridů, přičemž každý obsahuje LC a SC-EMS, které jsou připojené jako hostitelské mikrogridy a operují v předem specifikovaném koordinovaném způsobu. Každý mikrogrid v mesogridu operuje jako virtuální elektrárna na základě řídicích příkazů, které jsou generovány jejím SC-EMS a komunikovány LC v rámci mikrogridu. Druhou (vyšší) vrstvou SC-EMS, tj. mesogrid SC-EMS, přijímá informace od makrogridu a od každého jednotlivého mikrogridu. Na tomto základě specifikuje kontrolní/provozní odpovědnosti každého mikrogridu vzhledem k jeho PCC. Schéma mikrogridu, který je v režimu mesogridu, je na obrázku 1.4 [3, 7].



Obr. 1.4: Schéma režimu mesogrid

1.3 Bezpečnost mikrogridu

V mikrogridu, tak jako v každé moderní infrastruktuře, hrají informační a komunikační technologie klíčovou roli, jak v jejich provozu, tak i řízení. Jelikož jsou kybernetické systémy a fyzické procesy úzce propojeny, mohou jakékoli kybernetické incidenty ovlivnit jejich spolehlivý provoz. Provoz mikrogridu závisí na efektivním a spolehlivém toku dat v kybernetickém systému. Jakékoli zpoždění nebo poškození dat může ovlivnit hladký chod fyzického systému a ohrozit účinnost, stabilitu a bezpečnost chytrých sítí [10].

1.3.1 Typy kybernetických útoků

Kybernetické útoky můžeme rozdělit na různé druhy na základě určitých kritérií. Těmi můžou být například cíl útoku, motivace útočníka, použitá metoda nebo rozsah útoku. Z tohoto hlediska lze pak tyto útoky rozdělit následovně [11, 12, 13, 14]:

Útoky na integritu dat

Integrita dat znamená, že data jsou přesná, úplná a spolehlivá. Útok na integritu má za cíl data poškodit a tím majiteli způsobit škodu nebo útočníkovi získat výhodu. Může jít například o tyto útoky [11]:

- **Ransomware:** Jedná se o virus, který má za účel zašifrovat data, která se nachází v napadeném zařízení. Za dešifrování těchto dat je pak požadované

výkupné. Nejčastějšími cíli tohoto útoku jsou velké instituce, například nemocnice nebo velké firmy.

- **FDI (False Data Injection):** Jde se o typ útoku, při kterém jsou záměrně měněna reálná data za falešná nebo upravená. Cílem je ovlivnit chování, rozhodování a výstupy systému. Pro tento typ útoku je nejčastější cíl kritická infrastruktura jako je například mikrogrid.

Útoky na důvěrnost dat

Důvěrnost dat znamená, že informace jsou soukromé a přístup k nim mají jen určité osoby. Útok na důvěrnost pak má za cíl získat přístup k těmto informacím, ke kterým by normálně přístup mít neměl. Důvod pro tento útok může být například získání hesla uživatele. Může jít například o tyto útoky [12]:

- **Data Breach:** Tento útok je definován jako neoprávněný přístup k citlivým datům s cílem jejich odcizení. Nejčastěji jde o osobní údaje nebo finanční informace.
- **Phishing:** Jedná se o pokus získání citlivých informací od jednotlivce nebo i firmy, jako jsou například přístupové údaje. Při tomto útoku je využíváno sociálního inženýrství.

Útoky na dostupnost dat

Dostupnost dat znamená, že se k informaci, kterou chceme vědět, můžeme dostat kdykoliv, a bez obtíží. Útok na dostupnost má pak za cíl této věci zamezit. Důvod pro tento útok může být způsobení chaosu. Může jít například o tyto útoky [12]:

- **DDoS (Distributed Denial of Service):** Jde o typ útoku, při které je cílem přetížit server obrovským množstvím požadavků, například pomocí bot netu. To znemožňuje přístup ke službám pro legitimní uživatele.
- **Malware:** Jedná se o obecné označení škodlivých programů. Tyto programy pak mají za cíl provádět v počítači činnost, o které uživatel buď neví, a nebo by s ní nesouhlasil. Může se jednat o krádež dat, narušení sytému nebo o získaní neautorizovaného přístupu k důvěrným informacím.

Útoky na autentizaci

Autentizace znamená, že k přístupu k určitým službám je potřeba se prokázat, aby bylo jisté, že se jedná opravdu o daného uživatele. Útok na autentizaci má pak za cíl získat neautorizovaný přístup. Důvod pro tento útok může být získání citlivých informací. Může jít například o tyto útoky [13]:

- **Brute Force Attack:** Je snaha o prolomení hesla, přihlašovacích údajů nebo šifrovaných dat pomocí automatizovaných nástrojů. Tyto nástroje postupně zkouší všechny možné kombinace, dokud ochranu neprolomí.
- **Keylogger:** Jde o program, který snímá veškeré stisky jednotlivých kláves. Tímto způsobem se může útočník pokusit získat hesla nebo přihlašovací údaje.

Útoky na důvěru

Tento typ útoku má za cíl narušit důvěru mezi lidmi, organizacemi nebo systémy. Může jít například o útoky [14]:

- **MitM (Man-in-the-Middle):** Podstatou tohoto útoku je odposlouchávání a manipulace s komunikací mezi dvěma stranami tak, že se stane aktivním prostředníkem. To může poškodit integritu předávaných informací a tím pádem i důvěru.
- **DNS Spoofing:** Při tomto útoku jsou zmanipulovány záznamy DNS serverů tak, aby přesměrovaly uživatele na falešné webové stránky. Uživatel si pak myslí, že přistupuje na normální web, ale ve skutečnosti je na webu útočníka.

Útoky aplikovatelné na mikrogrid

Všechny tyto vyjmenované útoky mohou být použity na mikrogrid, ale některé jsou více aplikovatelné než jiné. Těmi nejnebezpečnějšími jsou FDI, DDoS, Malware a MitM. Jelikož je mikrogrid závislý na přesných datech o výrobě a spotřebě energie, může vložení falešných dat při FDI útoku, vést k výpadkům dodávek nebo k celkovému kolapsu systému. DDoS útok je obzvlášť účinný, jelikož některé řídící jednotky komunikují prostřednictvím sítě. To znamená, že pokud by botnet zahltil řídící servery požadavky, tak by tím mohl vyřadit tyto komponenty z provozu. Malware může mít celou škálu různých dopadů od krádeže citlivých dat po vyřazení klíčových jednotek. To může mít za následek narušení provozu mikrogridu. Posledním útokem je pak MitM, útočník pomocí tohoto útoku může manipulovat s informacemi o toku energií nebo celkovém stavu jednotlivých částí mikrogridu [15].

1.3.2 Obrana proti kybernetickým útokům

Defenzivní strategie proti kybernetickým útokům obsahují různé technologie a přístupy. Největší firmy, které se starají o kybernetickou bezpečnost, jsou například Cloudflare, který se zajímá o bezpečnost sítí a cloudů, nebo Rapid7, která se zabývá bezpečností IoT a detekcí hrozeb. Strategie lze rozdělit na základě jejich funkce při obraně do následujících kategorií [16]:

- **Prevence útoků:** Cílem této strategie je útokům zabránit ještě předtím, než se stanou. Příkladem může být dvoufaktorová autentizace, šifrování komunikace, správné nastavení firewallu nebo pravidelné aktualizace [16, 17].
- **Detekce a monitorování:** Tyto strategie mají za cíl odhalit potencionální útok pomocí hledání anomálií a podezřelé aktivity v systému či komunikaci. K tomu se používají různé systémy jako je například IDS (Intrusion Detection System) nebo SIEM (Security Information and Event Management). IDS analyzuje síťový provoz a hledá v něm potenciální hrozby. SEIM je systém, který kombinuje analýzu bezpečnostních informací a událostí, které se dějí reálném čase pro identifikaci hrozeb [16, 18].
- **Reakce na incidenty:** Pokud se nějaký incident stane, tak je důležité mít rychlou reakci, aby napáchané škody byly co nejmenší. Může se jednat například o rychlou izolaci napadených systémů [16].

V kontextu mikrogridu jde pak o strategie založené na ochraně a detekci. Ochranné strategie mají za cíl předejít nebo alespoň ztížit útočníkům jejich útok. Naopak ty, založené na detekci, se soustředí na brzkou detekci útoků a zmírnění jejich dopadů.

Defenzivní strategie založené na ochraně

V obranných strategiích, které jsou založené na ochraně, jsou měřiče/senzory chráněny proti kybernetickým útokům. Jelikož v nově vznikajících mikrogridech existuje mnoho senzorů a měřičů, není ochrana všech měřičů finančně efektivní. Z tohoto důvodu se obvykle chrání pouze pár kritických senzorů a měřičů [19].

Je důležité zmínit, že počet napadených měřičů/senzorů je základním kritériem při detekci FDI útoků. V některých případech se počet senzorů navyšuje pro lepší viditelnost, to ale zvyšuje zranitelnost. V ochranných strategiích se počet chráněných senzorů dá dosáhnout s ohledem na rozpočet a citlivost systému [10].

Defenzivní strategie založené detekci

V detekčních strategiích jsou naměřená data analyzována pro detekci útoků a následující zmírnění jejich následků. Tyto strategie lze rozdělit na statické a dynamické:

- **Statická detekce útoků**

  Tato defenzivní strategie se v mikrogridu zaměřuje na identifikaci útoků, které cílí na stabilitu v ustáleném stavu systému. Jedním z nejznámějších statických detektorů je detektor na útoky odhad stavu sítě. Pro detekci a zmírnění útoků FDI na odhad stavu sítě vzniklo již několik strategií jako jsou například sparse optimization (řídká optimalizac), state forecasting (predikce stavu) nebo network theory (teorie sítí). Tyto strategie jsou vhodné pro FDI útoky na odhad stavu stejnosměrného proudu. Naopak v systémech se střídavým

proudem, nejsou tyto strategie dostatečně uspokojivé. Z tohoto mohou být do regulátorů výkonových měřičů distribuované výroby přidány doplňkové řídící smyčky, které mají bránit velkým odchylkám napětí způsobeným útokem [10].

- **Dynamická detekce útoků**
  Tato defenzivní strategie využívá informace o dynamice systému k identifikaci útoků. Různé dynamické detektory byly v posledních letech studovány, ale zaměřují se primárně na lineární systémy. Z důvodu nelinearity reálných energetických systémů nejsou tyto metody pro detekci útoků velmi praktické. Příkladem dynamické detekce může být detekce FDI útoku na řízení frekvence zátěže, jelikož je řízení frekvence zátěže závislé na dynamice energetického systému. A právě proto jsou detekovány dynamickými metodami. [10].

2 Cyber Range platformy

Cyber range (dále jen CR) platformy jsou nástroj pro výuku, trénink nebo vědeckou práci v oblasti kybernetické bezpečnosti. Nabízí kontrolované, bezpečné a izolované prostředí taktéž známé jako sandbox. Díky tomu je zde možné simulovat kybernetické útoky a obranu. Jedná se tedy o efektivní prostředek vzdělávání v mnoha ohledech [20].

2.1 Využití Cyber Range platforem ve výuce

V dnešní době se kybernetická bezpečnost převážně vyučuje tradičními způsoby, jako jsou přednášky, workshopy nebo semináře. CR platformy jsou důležitá součást výuky a tréninku v oblasti kybernetické bezpečnosti, jelikož dávají možnost testovat, experimentovat a procvičovat. Díky tomu si mohou studenti tuto problematiku „osahat“. CR platformy mají potenciál efektivně přispívat k řešení globálního nedostatku dovedností a aktualizaci znalostí v oblasti kybernetické bezpečnosti [21].

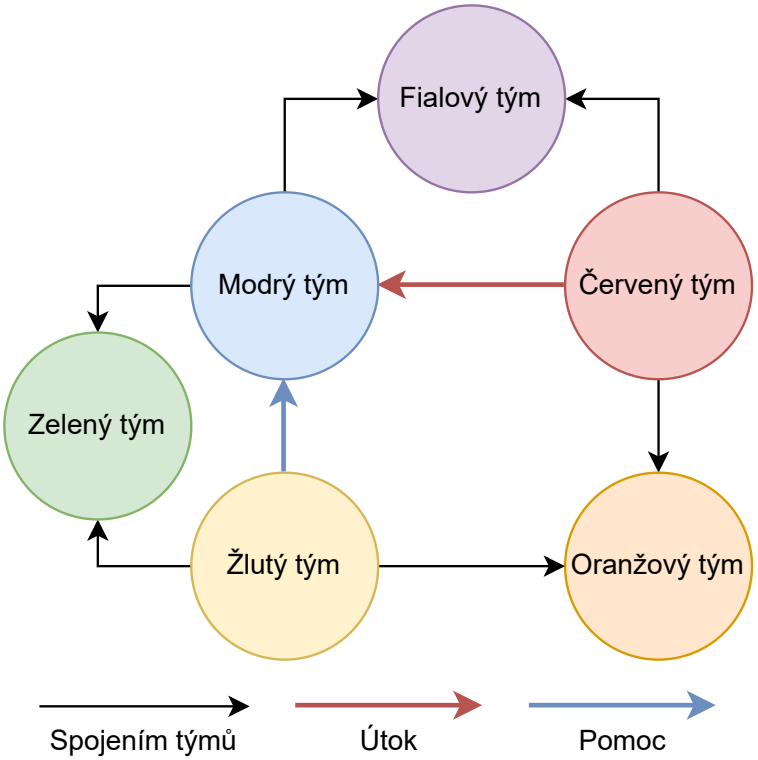
CR platformy zaměřené na vzdělávání má kromě studentů i instruktory. Ti mají za úkol sledovat studenty v jejich práci a pomoci jim, pokud si nebudou vědět rady. Účastníci scénáře mohou také mít různé role, které se dělí do 3 základních barevných týmů [22]:

- **Modrý tým** – bránící strana, která obsahuje veškeré defenzivní techniky jako je třeba reakce na incidenty a nebo zajištění obrany
- **Červený tým** – útočící strana, do které řadíme všechny ofenzivní techniky etického hackingu, jako je např. penetrační testování, odposlech síťové komunikace nebo sociální inženýrství.
- **Žlutý tým** – vývojáři, softwaroví architekti a další osoby, které se podílejí na bezpečném návrhu, vývoji, integraci a nasazení softwarových řešení.

Toto rozdělení ale již nedokáže pokrýt složitost dnešní kybernetické bezpečnosti, a z tohoto důvodu vznikly další rozšiřující týmy, které mažou bariéru mezi původními třemi týmy [22]:

- **Fialový tým** — spojení červeného a modrého týmu pro zvýšení efektivity bezpečnostního testování a následného odstraňování nalezených zranitelností.
- **Zelený tým** — spojení modrého a žlutého týmu pro zajištění interakce mezi členy obou týmu s hlavním cílem zlepšit obranu výstupů žlutého týmu.
- **Oranžový tým** -– spojení červeného a žlutého týmu za účelem edukace (např. možný dopad zneužití zranitelnosti) a podpoření žlutého týmu při zajišťování nápravy na základě nálezů červeného týmu.

Jednotlivé týmy mohou být začleněny do jednoho scénáře, ve kterém se navzájem ovlivňují (např. červený tým útočí na modrý tým). Nemusí se ale nutně jednat o zapojení více osob, ale scénář může být zaměřen pouze na jednotlivce. V tomto případě lze pak roli jiného týmu nahradit jiným způsobem. Barevné rozdělení týmů je znázorněno na obrázku 2.1.



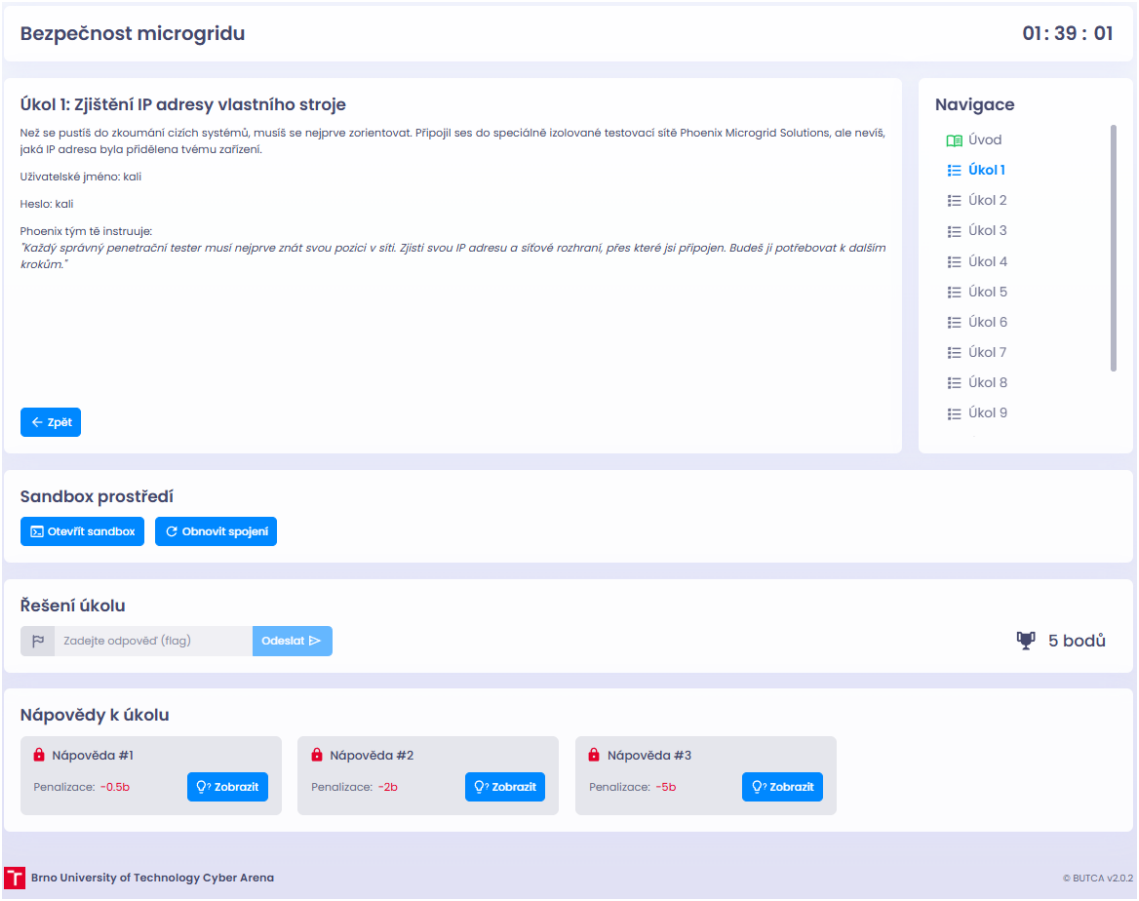
Obr. 2.1: Barevné rozdělení kyberbezpečnostních týmů

2.2 BUTCA

BUTCA neboli *Brno University of Technology Cyber Arena* je hybridní cyber range platforma vytvořená VUT v Brně. Platforma je navržena pro studenty středních a vysokých škol. Scénáře jsou zaměřeny na modrý a červený tým. Z toho plyne, že scénáře jsou zaměřeny primárně na ofenzivní a defenzivní operace. Platforma obsahuje výukové scénáře z oblasti ICT, průmyslu a energetiky [23].

Interaktivní prostředí stojí na uživatelském rozhraní, kde má uživatel přístup ke všem částem scénáře. Každý výukový nebo tréninkový scénář obsahuje řadu úkolů,

které uživatel řeší, ukázka úkolu je na obrázku 2.2. Pokud jsou v rámci scénáře obsaženy virtuální stroje, uživatelé k nim mají přístup přímo skrze webový prohlížeč. Všechny scénáře pak začínají úvodem, po kterém již následují jednotlivé úkoly. Průchod scénářem je lineární, to znamená, že úkoly nelze přeskakovat, pokud nejsou volitelné. Uživatelé také mohou používat podpůrné materiály, jako mohou být například návody. Součástí všech úkolů je také nápověda, její využití je penalizováno určitou ztrátou bodů, je možné využít i 100% nápovědu, která odhalí správnou odpověď. Jakmile je dokončen poslední úkol, tak se zobrazí závěr scénáře. Poté uživatele ještě čeká kontrolní test. Účel testu je ověřit získané znalosti z praktické části scénáře [23].



Obr. 2.2: Ukázka úkolu v BUTCE

Technická stránka

BUTCA je webová aplikace využívající virtualizační prostředí OpenStack. To umožňuje provoz výukových scénářů bez nutnosti instalace jakýchkoli programů. Díky tomu je možné scénáře hrát i na méně výkonných zařízeních. Celá infrastruktura je tvořena třemi hlavními vrstvami [23]:

1. **Databázova vrstva** uchovává veškerá data o uživatelích, úkolech a výsledcích jednotlivých scénářů.
2. **Virtuální stroje** jsou základem scénářů. Ve scénářích plní různé role jako jsou například klient nebo server.
3. **Služby** pak zahrnují zbylé věci jako například webové rozhraní, autentizační mechanismy a další funkce, které potřebné pro chod platformy.

2.3 Hra o vlajku

CTF (Capture the Flag) je gamifikovaný způsob výuky v oblasti kybernetické bezpečnosti, ve které se uživatelé snaží získat vlajku (flag). Vlajka představuje správné řešení daného úkolu. Vlajkou může být cokoliv v rámci řešeného úkolu, např. IP adresa nebo heslo. Toto řešení pak zadávají do hodnotícího systému. Některé CTF hry poskytují během řešení i nápovědy, které ale mohou být penalizovány ztrátou určitého počtu bodů. Mezi hlavní výhody CTF her patří zábavnější a poutavější učení, praktické zkušenosti a systém automatického bodování. Existují následující druhy CTF her [24]:

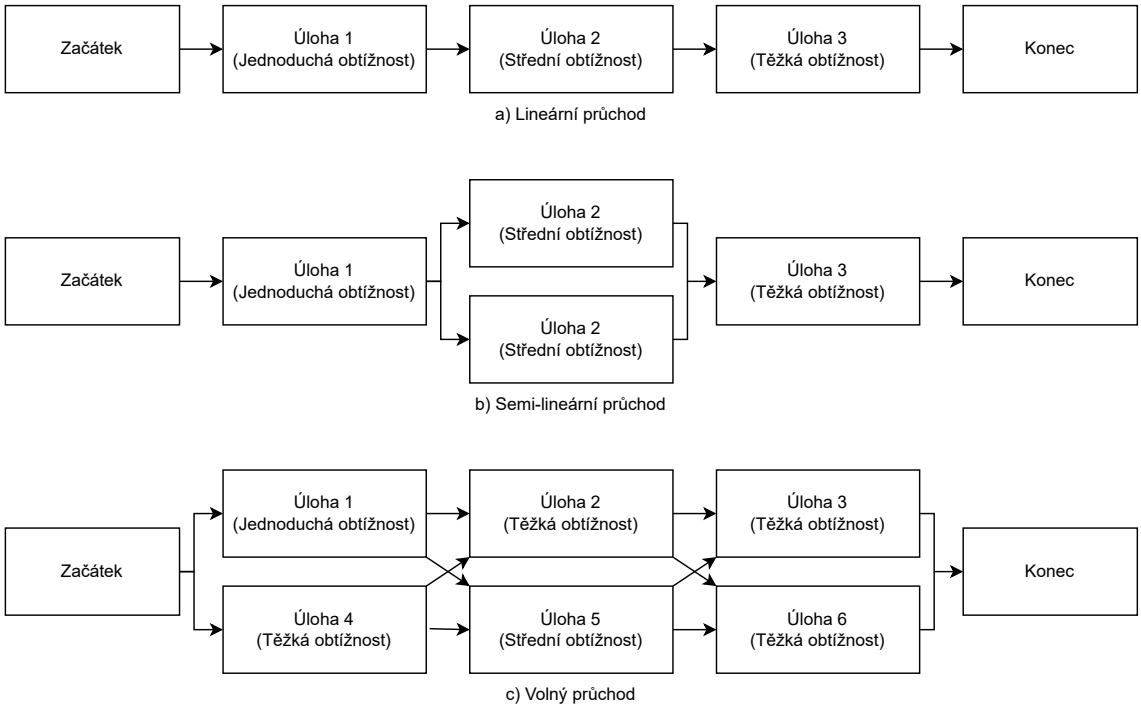
- **Jeopardy** je tím nejčastějsím typem CTF hry. Jednotlivci a nebo týmy zde řeší sérii úkolů z různých odvětví kybernetické bezpečnosti jako je například kryptografie, reverzní inženýrství a nebo webová bezpečnost. Za každou vyřešenou úlohu dostávají body podle její obtížnosti přičemž obtížnost úloh se postupně zvyšuje. Pro ověření správné odpovědi odešle uživatel specifický řetězec, čímž se prokáže, že úkol úspěšně splnil, a může pokračovat na další. Cílem je získat co nejrychleji nejvyšší možný počet bodů. Lze si zahrát přes BUTCU nebo FBCTF platformu [25].
- **Attack-Defence** je typ CTF ve kterém týmy současně útočí a brání jim přidělené virtuální stroje. Týmy postupně zabezpečují své systémy a hledají slabiny v systémech jiných týmů. Hra se dá udělat složitější pomocí přidání funkce omezených zdrojů. Jakékoliv rozhodnutí, co buď útočník nebo obrance udělá musí být v rozsahu zdrojů. Finálním cílem je získat vlajku jiného týmu a tím vyhrát. Tento typ si lze zahrát skrze platformu TryHackMe [25].
- **Kink of the Hill** je kompetetivní typ CTF. Cílem je obsazení předem určeného systému a udržet ho co nejdéle. Toho mají hráči docílit pomocí analyzování systému a jeho zranitelností, které poté využijí pro získání kontroly nad systémem. Čím déle jeden tým systém drží pod svou kontrolou, tím více bodů získává. Tento typ si lze zahrát na platformách FBCTF nebo RootTheBox [25].
- **Smíšené** jsou kombinace jiných typů CTF her, nejčastěji jde o jeopardy a attack-defence. Tento typ nabízí flexibilitu při řešení scénářů zaměřených na kybernetickou bezpečnost. Lze si zahrát skrze platformu 247CTF.

Průchody scénářem

Různé scénáře mohou mít různé průchody závislé na typu, zaměření a struktuře daného CTF. Pokud je scénář založený na předem daných úlohách, může být rozdělen na lineární, semi-lineární a volný, viz obrázek 2.3.

- **Lineární** – postup je přesně daný a uživatel řeší úkoly lineárně.
- **Semi-lineární** – úkoly se mohou větvit
- **Volný** – postup není předem daný a závisí na uživateli

Každý z těchto přístupů má výhody a nevýhody. Lineární průchod je vhodný pro nováčky, jelikož má jasnou strukturu, takže hráč přesně ví, co je dalším úkolem. U tohoto přístupu je taktéž jednodušší kontrolování obtížnosti řešených úkolů, jelikož úkoly se postupně ztěžují. Nevýhodou pak může být malá flexibilita, když se hráč zasekne na úkolu, tak nemůže postupovat dál. Semi-lineární průchod scénářem pak tento problém mít nemusí, hráči si totiž mohou vybírat mezi několika úkoly ve stejné úrovni. Tento přístup již ale může být trochu komplikovaný pro nováčky. Tvorba takového scénáře navíc může být složitější skrze udržení stejné obtížnosti napříč úkoly ve stejné úrovni. Scénář s volným průchodem je pro tvůrce jednodušší na vytvoření než předešlé dva, nabízí hráči různorodé strategie a může si také volit libovolné úkoly. Nevýhodou tohoto typu je pak velká obtížnost udržení obtížnosti a náročnost pro začátečníky.



Obr. 2.3: Schéma všech průchodů scénářem.

3 Energetické komunikační protokoly

V energetice dnešní doby jsou automatizace a řízení na dálku klíčové. Důvody jsou prosté, spolehlivé a bezpečné monitorování a ovládání zařízení elektrické infrastruktury. K tomu se využívají specializované komunikační protokoly. Tyto protokoly umožňují přenos dat napříč řídícími systémy a fyzickými zařízeními [26].

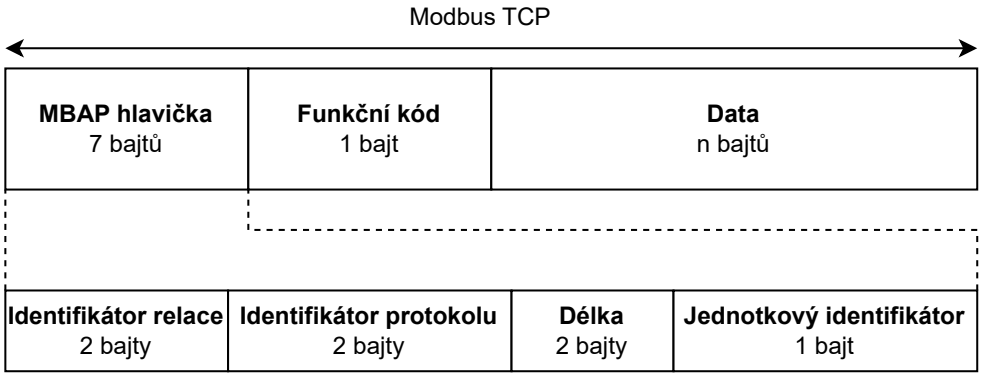
Průmyslové protokoly, na rozdíl od běžných IT protokolů, jsou optimalizovány pro spolehlivost a jednoduchost. Většina z těchto protokolů vznikla v době, kdy se na bezpečnost přenášených dat moc nemyslelo. To přineslo výzvy v odvětví kybernetické bezpečnosti [27].

3.1 Protokol Modbus

Modbus je komunikační protokol pracující na aplikační vrstvě, který umožňuje komunikaci mezi klientem a serverem. Existují dvě možnosti komunikace, a to dotaz/odpověď a broadcast. Při formě komunikace dotaz/odpověď probíhá komunikace mezi master (hlavní zařízení) a slave (ostatní zařízení). U broadcast komunikace posílá master příkaz všem slavům. Modbus transakce obsahují jeden rámec dotazu, odpovědi a nebo broadcastu. Modbusový rámec obsahuje adresu příjemce, příkaz, který má příjemce uskutečnit, a data pro jeho uskutečnění [28].

Jak již bylo zmíněno, většina průmyslových protokolů byla navržena před desítkami let. Právě protokol Modbus byl publikován v roce 1979 pro multidrop sítě s architekturou master/slave. Jelikož byly původně Modbusové sítě izolovány, tak jim nehrozilo téměř žádné nebezpečí, a proto aspekty, jako je integrita, autentizace a nepopiratelnost, nebyly brány v úvahu při návrhu protokolu. Z tohoto důvodu je potřeba tento protokol provozovat pouze na chráněných sítích a za použití firewallů, pravidel pro řízení přístupu a nebo také VPN [26, 28].

Pro využití protokolu Modbus v moderních sítích vznikla varianta s názvem Modbus TCP. Ta zapouzdří Modbusový rámec do TCP/IP protokolu. Standardně je pak využíván komunikační port 502. Zprávy pak obsahují MBAP (Modbus Application Protocol Header) hlavičku, která obsahuje některé prvky z původního rámce a doplňuje je informacemi, jako je identifikátor relace, délka zprávy nebo jednotkový identifikátor viz obr. 3.1. Díky této formě protokolu je možné ji využít s běžnou síťovou infrastrukturou [28].



Obr. 3.1: Modbus TCP rámec

MBAP hlavička obsahuje standardní Modbus zprávy. Přesněji se skládá z identifikátoru relace, identifikátoru protokolu, délkou a jednotkovým identifikátorem. Dále je zde pak funkční kód. Poslední část tvoří data, která mají proměnlivou délku.

Protokol Modbus definuje několik funkčních kódů, každý z nich odpovídá konkrétnímu příkazu. Patří mezi ně například:

- **Read Coils (0x01)** – Tento funkční kód se používá ke čtení stavu cívek ve vzdáleném zařízení. Požadavek specifikuje počáteční adresu a počet cívek. Cívky v odpovědi jsou v datovém poli zabaleny jako jedna cívka na bit. Stav je indikován jako 1 = ZAPNUTO a 0 = VYPNUTO.
- **Read Holding Registers (0x03)** – Tento funkční kód se používá ke čtení obsahu souvislého bloku registrů ve vzdáleném zařízení. Request specifikuje počáteční adresu registru a počet registrů. Data registrů v odpovědi jsou zabalena jako dva bajty na registr.
- **Write Single Register (0x06)** – Tento funkční kód se používá k zápisu do jednoho registru pro uchovávání dat ve vzdáleném zařízení. Registr s číslem 1 je proto adresován jako 0. Normální odpovědí je ozvěna požadavku, vrácená po zapsání obsahu registru.

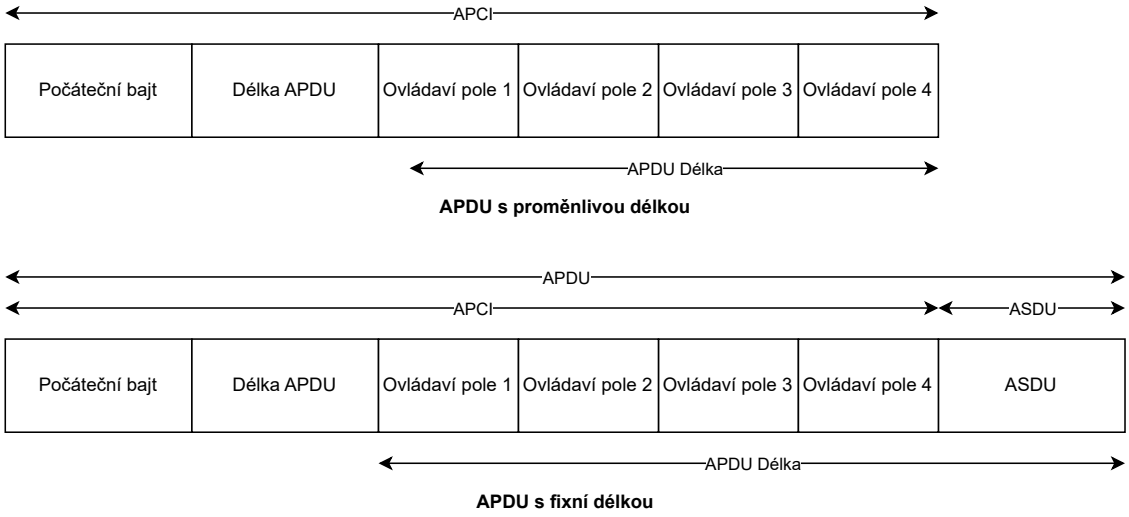
3.2 Protokol IEC 60870-5-104

IEC 60870-5-104 je komunikační protokol patřící do rodiny standardů IEC 60870. Komunikace probíhá na principu asymetrického modelu klient-server. Zde řídící centrum vystupuje jako klient a ostatní zařízení jako servery. Tento protokol je rozšířením staršího protokolu IEC 60870-5-101. Novější verze, tedy IEC 60870-5-104, využívá přenos skrze TCP/IP sítě. Výhodou této verze je možnost využití běžných ethernetových sítí [29].

Komunikace standardně probíhá skrze port 2404. Rámec protokolu má pak několik vrstev, z nichž ta nejdůležitější je ASDU (Application Service Data Unit). Ta obsahuje informace o tom, co daná zpráva přenáší, může se jednat například o měření, řídící příkaz či změnu stavu. Samotné rámce jsou pak rozděleny na informační, potvrzovací a řídící [30].

- **Informační (I-format)** – Používá se k přenosu číslovaných informací mezi řídicí a řízenou stanicí. Délka je proměnná.
- **Potvrzovací (S-format)** – Používá se k provádění číslovaných dohledových funkcí. Délka je pevně daná.
- **Řídící (U-format)** – Používá se k provádění nečíslovaných řídicích funkcí. Délka je pevně daná.

Struktura APCI rámce, ve kterém se tyto formáty využívají, je na obrázku 3.2.



Obr. 3.2: APCI rámce

APCI (Application Protocol Control Information) rámce začínají počátečním bajtem, který má hodnotu 0x68. Dále pokračují délkou APDU (Application Protocol Data Unit) o délce 8 bitů a dalšími čtyřmi 8 bitovými ovládacími poli. Dělí se na rámce s fixní délkou a variabilní délkou [30].

Protokol IEC 60870-5-104 je navržen pro spolehlivost a robustnost. Stejně jako u starších protokolů nemá v základní verzi implementovanou autentizaci nebo šifrování. Z tohoto důvodu je třeba při jeho používání využít jiných bezpečnostních mechanismů. Těmi mohou být firewall, VPN nebo síťová segmentace [27].

3.3 Porovnání protokolů

Protokoly Modbus a IEC 60870-5-104 patří mezi nejrozšířenější komunikační protokoly, které se využívají v oblasti energetiky a průmyslové automatizace. Slouží k výměně dat mezi řídícími systémy a podřízenými zařízeními. Jejich primární rozdíl je původ a funkcionalita, viz tabulka 3.1.

Modbus je protokol původně vytvořený pro sériovou komunikaci, ale později převedený i do prostředí TCP/IP. Funguje na jednoduché struktuře dotaz/odpověď. Jeho silnou stránkou je jednoduchost, snadná implementace a podpora široké škály zařízení. Nejvíce se využívá v lokálních sítích, například u měřících zařízení.

Na druhé straně protokol IEC 60870-5-104 je navržen pro dálkové řízení v prostředí TCP/IP. Funguje na principu asynchronního přenosu dat. Dále využívá různé typy rámců a je více vhodný pro dispečerské systémy. Oproti Modbusu není komunikace pouze dotazová, řízené stanice mohou sama posílat data bez toho, aniž by dostaly požadavek.

Z bezpečnostního hlediska jsou na tom oba protokoly podobně, v základní verzi nepodporují autentizaci ani šifrování. IEC 60870-5-104 nabízí standardizované způsoby zabezpečení dle normy IEC 62351. Ta přidává například autentizaci rámců.

Tab. 3.1: Tabulka porovnání protokolů

Vlastnosti	**Modbus**	**IEC 60870-5-104**
Původní účel	Sériová komunikace	Dálkové řízení
Síťové prostředí	Sériové linky, později TCP/IP	TCP/IP
Druh komunikace	Dotaz/odpověď	Asynchronní
Struktura rámce	Jednoduchá	Komplexní (více typů rámců)
Vhodné využití	Měřící zařízení, lokální sítě	Dispečerské systémy, dálkové řízení
Podpora zařízení	Velká	Omezená
Zabezpečení v základní verzi	Bez zabezpečení	Bez zabezpečení
Standardizace zabezpečení	Není standardizováno	Standardizováno dle IEC 62351

4 Návrh scénáře

V této kapitole bude popsán návrh vzdělávacího scénáře zaměřeného na kybernetickou bezpečnost v rámci mikrogridu. Cílem tohoto scénáře je seznámit hráče s principy fungování mikrogridů a jejich bezpečnostními mechanismy. Scénář je navržen tak, aby simuloval reálné hrozby a pomocí poutavého příběhu je hráči představil. Celý scénář je součástí přílohy práce.

4.1 Výběr nástrojů

Pro realizaci výukové hry byly zvoleny dva virtuální systémy, a to Kali Linux a Ubuntu Server. Tyto stroje reprezentují různé role v rámci simulovaného prostředí informační bezpečnosti. Výběr těchto platforem byl záměrný, jelikož Kali Linux je považován za standard v oblasti penetračního testování a etického hackingu. Ubuntu Servery slouží jako oběti jednotlivých útoků.

Kali Linux byl zvolen zejména díky předinstalovaným nástrojům, které se zaměřují na síťovou analýzu, testování zranitelností a simulaci útoků. V rámci hry byly využity konkrétně následující nástroje:

- **Skenování sítě** — pro zjišťování dostupných zařízení a jejich otevřených portů.
- **Komunikaci s Modbus zařízeními** – pro demonstraci fungování protokolu Modbus TCP/IP a jeho možná zneužití.
- **MITM útoky** — pro demonstraci odposlechu síťového provozu a manipulace s daty.

Nástroje, které se dají využít pro skenování sítě, mohou být například ZMap, Angry IP Scanner a Nmap. Z těchto nástrojů jsem zvolil Nmap, jelikož se jedná o velice obsáhlý nástroj, díky kterému lze provádět více typů průzkumů bez nutnosti kombinování s jinými nástroji. Také je považován za standard. Oproti tomu například ZMap je určen spíše pro masivnější skenování, což nebylo ve scénáři potřeba.

U komunikace s Modbus serverem byla volba mezi dvěma nástroji a to mbpoll a Modpoll. Oba nástroje fungují podobně a splnily by požadované vlastnosti pro využití ve scénáři, i když Modpoll je více robustní. Nakonec byl vybrán nástroj mbpoll. Důvod k této volbě byl takový, že nástroj Modpoll na virtuálním stroji nefungoval.

Pro MIMT útoky lze využít také několik nástrojů jako například ettercap nebo bettercap. Bettercap je nástupce ettercapu. Podporuje více druhů útoků, jako například DNS spoofing, ale je složitější na konfiguraci. Ettercap je spíše jednodušší na použití, a proto i vhodnější pro výukovou hru. Z tohoto důvodu byl také využit.

Na druhé straně byl Ubuntu Server použit jako cílový stroj, na kterém běží simulované služby dostupné na lokální síti. Další důvod výběru serveru nad klientem je menší zátěž systému, na kterém virtuální stroje běží.

Výběr zmíněných nástrojů a platforem byl snahou o realistické prostředí, které studentům umožní osvojit si nebo otestovat své znalosti techniky síťové analýzy, principy zranitelnosti a obrany v síťových infrastrukturách.

4.2 Návrh komunikační soustavy

Celý systém se skládá ze tří virtuálních strojů, přičemž každý z nich plní jinou funkci v systému mikrogridu. Virtuální stroj s Kali Linux (hráč) komunikuje přímo s Modbus serverem za účelem testování jeho zabezpečení. Modbus server dále spolupracuje se stanicí, která simuluje komponenty mikrogridu. Tato komunikace probíhá po síti a zahrnuje protokol Modbus TCP. Hráč může tuto komunikaci monitorovat, analyzovat nebo narušovat v rámci přidělených úkolů. Schéma tohoto systému je na obrázku 4.1.

Virtuální stroj s Kali Linux

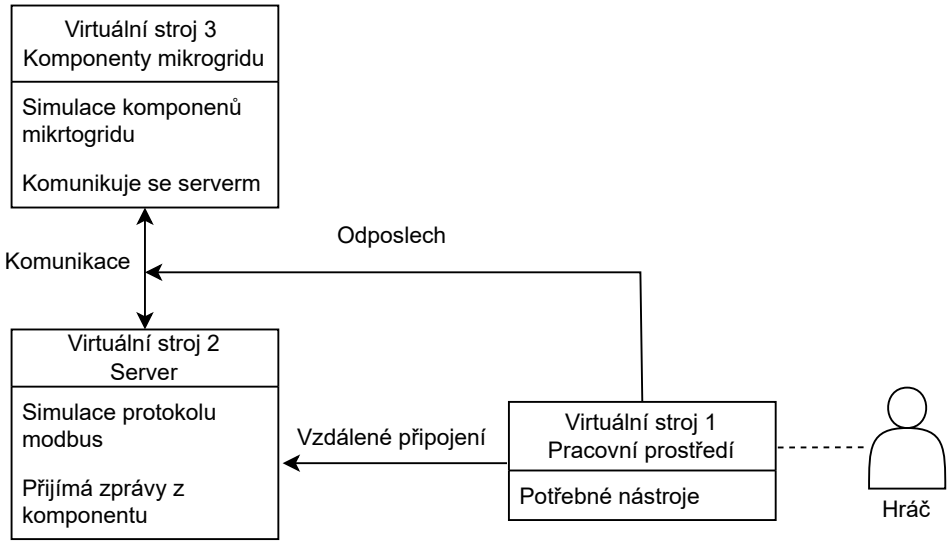
Tento stroj slouží jako pracovní prostředí hráče. Kali Linux byl zvolen z důvodu předinstalovaných nástrojů pro penetrační testování. Díky nim je komunikace se simulovanou infrastrukturou jednodušší, bez nutnosti instalování velkého množství dalších nástrojů. Již předinstalovanými nástroji, které budou ve scénáři využívány, jsou: nmap, ettercap a Wireshark. Kromě standardní výbavy byl do systému nainstalován ještě nástroj mbpoll. Tento nástroj umožňuje komunikaci s Modbus serverem. IP adresa tohoto stroje v komunikační soustavě je *192.168.56.20*. Hráč bude tento stroj využívat k provádění všech úkolů, včetně čtení registrů, injekce dat a dalších útoků na mikrogrid.

Virtuální stroj s Ubuntu Linux (Modbus server)

Tento stroj simuluje Modbus server, který implementuje protokol Modbus a poskytuje tak data a služby klientovi, je přístupný na portu 502. Server hostuje registry, které hráč zkoumá, manipuluje s nimi nebo je jinak ovlivňuje během průchodu scénářem. Dále naslouchá na portu 605 na příchozí zprávy z druhého serveru. Tento stroj slouží jako hlavní cíl hráčových aktivit. IP adresa tohoto stroje v komunikační soustavě je *192.168.56.10*.

Virtuální stroj s Ubuntu Linux (Komponenty mikrogridu)

Tento stroj simuluje ostatní části mikrogridu, které komunikují s Modbus serverem. Může se například jednat o senzory, aktuátory nebo řídicí jednotky. Na tomto stroji běží jednoduchá simulace procesů, které komunikují s Modbus serverem. Hráč má za úkol narušit jejich komunikaci pomocí technik, jako je například ARP spoofing nebo záměna dat při přenosu. IP adresa tohoto stroje v komunikační soustavě je *192.168.56.11*.



Obr. 4.1: Schéma komunikační soustavy

4.3 Návrh jednotlivých úkolů

Scénář je vytvořen jako soubor deseti na sebe navazujících úkolů. Celý scénář začíná prologem, ve kterém je hráči představen mikrogrid a hrozby, kterým může čelit. Samotné úlohy jsou tematicky rozděleny do tří hlavních kategorií:

- Síťová analýza
- Útoky na Modbus server
- Man-in-the-Middle útoky

Každá z těchto kategorií obsahuje několik úkolů, u kterých se postupně zvyšuje obtížnost. Scénář je zakončen epilogem a závěrečným testem. Celý scénář, včetně zadání, úkolů a bodového ohodnocení, se nachází v příloze A.1.

Úloha jedna a dvě

Tyto dvě úlohy se zaměřují na síťovou analýzu. První funguje spíše jako uvedení hráče do platformy BUTCA a seznámení se s operačním systémem Kali Linux. Cílem hráče je najít IP adresu zařízení, na kterém se právě teď nachází. V druhé úloze má hráč zjistit IP adresu Modbus serveru. Toho má dosáhnout pomocí znalosti síťového rozsahu a známého portu, na kterém Modbus obvykle operuje. V této úloze má k dispozici nástroj nmap, pomocí kterého může skenovat síť na základě určitých parametrů.

Celková obtížnost úloh je malá a očekává se, na základě testování, že hráčům obě úlohy nezaberou více než 10 minut. Na základě obtížnosti jsou úkoly ohodnoceny 5 a 6 body.

Úloha tři a čtyři

V těchto dvou úlohách se hráč seznámí s nástrojem mbpoll. Tento nástroj slouží ke komunikaci s Modbus serverem a čtením jeho registů. A bude potřebný v následujících úkolech.

Ve třetí úloze hráč otestuje připojení k serveru, čímž ověří jeho dostupnost. Ve čtvrté úloze pak přečte data uložená v registrech, čímž získá přehled o struktuře a obsahu Modbus komunikace.

Úlohy jsou opět relativně jednoduché, na základě testování je čas na tyto dvě úlohy 15 minut. Bodové hodnocení je pro obě úlohy 8 bodů.

Úloha pět a šest

Tyto úlohy se zaměřují na první typ útoku na mikrogrid. Tímto útokem je útok FDI. V prvním úkolu má hráč změnit data, která se nacházejí v jednom z deseti registrů. Tím se demonstruje, jak útok FDI může ovlivnit správnost dat, která jsou základem pro rozhodování o řízení mikrogridu. Druhým úkolem je pak záměna dat v několika registrech najednou. Tato úloha má hráči pomoci pochopit, jak může útočník ovlivnit více parametrových hodnot současně, což může mít vážné důsledky pro rozhodovací procesy v mikrogridu.

Úlohy jsou již těžší než předešlé, na základě testování je čas na tyto dvě úlohy 15 minut. Bodové hodnocení těchto úloh je 10 bodů pro pátý úkol a 8 bodů pro šestý úkol.

Úlohy sedm, osm a devět

Tyto tři úlohy se zaměřují na útok zvaný Man-in-the-Middle. Díky nim má hráč pochopit, jak může útočník získat přístup k citlivým datům přenášeným mezi dvěma

zařízeními, aniž by si obě strany byly vědomy jeho přítomnosti. V sedmé úloze je hráči představen nástroj ettercap, pomocí něhož je možné útoky simulovat. Úkolem je odposlouchávat komunikaci, která probíhá mezi dvěma zařízeními, serverem a komponentem mikrogridu, a zjistit, na jakém portu jsou data přijímána. Úloha osm pak dává hráči za úkol zjistit, jaká data jsou přenášena. Toho má docílit pomocí analýzy dat, která se přenášejí. K tomu využije další nástroj jménem Wireshark. Tento nástroj, ale v úloze není jinak vysvětlován a předpokládá se, že hráč jím umí zacházet. V poslední deváté úloze má hráč za úkol udělat injekci dat, která se přenášejí. K tomu opět využije nástroj ettercap. Tyto úlohy hráči ukazují, jak funguje útok Man-in-the-Middle a jak tyto útoky mohou ovlivnit fungování mikrogridu.

Celkově se jedná o nejtěžší úlohy a dle testování se očekává, že hráči dohromady zaberou přibližně 30 minut. Tyto úlohy mají následující bodové hodnocení: sedmá úloha 10 bodů, osmá úloha 12 bodů, devátá úloha 15 bodů.

4.4 Testování

Testování bylo provedeno ve třech fázích. V první fázi byla hra testována na malém počtu hráčů, jako test funkčnosti. Při druhém testování byla hra umístěna na platformu BUTCA a testování proběhlo na větším počtu hráčů. Ve třetím testování byla hra opět testována na menším počtu hráčů. Cílem bylo zjistit, zda provedené úpravy vedly k očekávanému výsledku. Celkově se testování zúčastnilo 35 hráčů středoškolského a vysokoškolského vzdělání.

4.4.1 První testování

Testování této verze hry proběhlo přes vzdálené připojení k počítači. Tato metoda byla zvolena z důvodu probíhající aktualizace platformy BUTCA, ta proto nebyla dostupná.

Testování se zúčastnili tři studenti oboru Informační bezpečnost z Fakulty informačních technologií VUT. Tato skupina byla vybrána záměrně, jelikož odpovídá jedné z možných cílových uživatelů hry. Testování proběhlo individuálně a ne skupinově z již dříve zmíněných důvodů.

Tetovaným byly poskytnuty instrukce o účelu hry a jejím samotném hraní. Během testování byl průchod hrou sledován a na základě tohoto sledování byly vytvořeny poznámky ohledně jejich interakcí se hrou a případných problémů.

Nakonec vyplnili dotazník se zpětnou vazbou. Z tohoto testování vyplynulo, že některé nápovědy je potřeba rozšířit nebo přepracovat. Podrobnější rozbor jednotlivých připomínek a návrhů vzešlých z tohoto testování je uveden v kapitole 4.5.

4.4.2 Druhé testování

Na základě poznatků získaných z prvního testování byla hra upravena. Byly přeformulovány a doplněny nápovědy, které původní testující hodnotili jako nejednoznačné. Také byla upravena zadání vybraných úkolů, které byly nejednoznačné. Po těchto úpravách byla nová verze hry nahrána na platformu BUTCA.

Tato verze hry byla testována na Střední škole průmyslové v Jedovnicích a zúčastnilo se jí 26 studentů třetího ročníku oboru Informační technologie. Cílem bylo zjistit, jak si s hrou poradí skupina s nižší úrovní odborných znalostí než v případě vysokoškolských studentů. Také bylo cílem odhalit potenciální slabá místa a chyby, které se potenciálně mohou objevit při hraní.

Testování proběhlo v rámci výuky za přítomnosti vyučujícího učitele, který měl k dispozici návod k řešení, a tvůrce hry. Studenti si scénářem prošli samostatně bez výrazné vnější pomoci. Většina hráčů se dostala ke čtvrtému úkolu, přičemž malá část dosáhla úkolu pět.

Největším problémem byla časová dotace, hráč má mít na tento scénář dvě hodiny času, ale bohužel další navazující výuka tento čas zkrátila na jednu hodinu a deset minut. Dále byl velký problém ten, že většina studentů se potkala s operačním systémem Linux poprvé, z tohoto důvodu jim bylo potřeba vysvětlit, jak v něm pracovat. Z celého testování vyplynulo, že obtížností je hra spíše pro studenty vysokých škol, a nebo pro studenty středních škol se specifickým zaměřením. Více v kapitole 4.5.

4.4.3 Třetí testování

Dle poznatků ze druhého testování byl scénář mírně upraven. Byly přepracovány vybrané úlohy. Také proběhla změna zadání některých úkolů, aby bylo jasnější, co je po hráči požadováno. Nápovědy byly taktéž přepracovány. Testování samotné pak opět probíhalo skrze platformu BUTCA. Tentokrát již bez přítomnosti tvůrce.

Tuto iteraci hry hrálo šest lidí. Oproti minulým testováním šlo nejen o lidi, kteří studovali nebo studují IT. Přesněji šlo o dva hráče, zbylí čtyři jsou pak studenti vysokých škol se zaměřením na IT. Všichni hráči měli na dokončení hry dvě hodiny a před začátkem byli instruováni o tom, co je to mikrogrid a penetrační testování.

Po tomto testování se prokázalo, že upravená verze hry je skrze pochopení zadání a užitečnost nápověd lepší než předchozí iterace hry. Přesto se objevilo pár problémů, zejména u hráčů, kteří, jak již bylo zmíněno, nestudují IT. Největším problémem bylo hlavně virtualizované prostředí a práce v příkazové řádce. Podrobněji je zpětná vazba popsána v kapitole 4.5.

4.5 Zpětná vazba

Součástí vývoje vzdělávací hry bylo zhodnocení její hratelnosti a vzdělávacího přínosu. Zpětná vazba byla získávána v průběhu tří testování prostřednictvím dotazníků, analytických dat z platformy BUTCA a také přímé komunikace s hráči. Každá z fází testování poskytla nové poznatky, které vedly k úpravám herního designu a obsahu. Následující podkapitoly shrnují výsledky a postřehy z jednotlivých testování. Stručně je zpětná vazba v tabulce 4.1. Všechny odpovědi respondentů jsou součástí přílohy B.

Tab. 4.1: Tabulka zpětné vazby

Parametr / Testování	**1. testování**	**2. testování**	**3. testování**
Počet hráčů	3	26	6
Věkový průměr	22,3 let	17,8 let	22 let
Průměrná herní doba	∼60 minut	68 minut	64 minut
Hodnocení příběhu	1,7	2,57	2,8
Hodnocení nápověd	3,3	2,36	2
Subjektivní obtížnost	3	4,28	3,8
Úspěšnost dokončení	100%	35,7%	66,7%

Poznámka: Hodnocení je formou známek, kde 1 představuje nejlepší hodnocení a 5 nejhorší.

4.5.1 Zpětná vazba z prvního testování

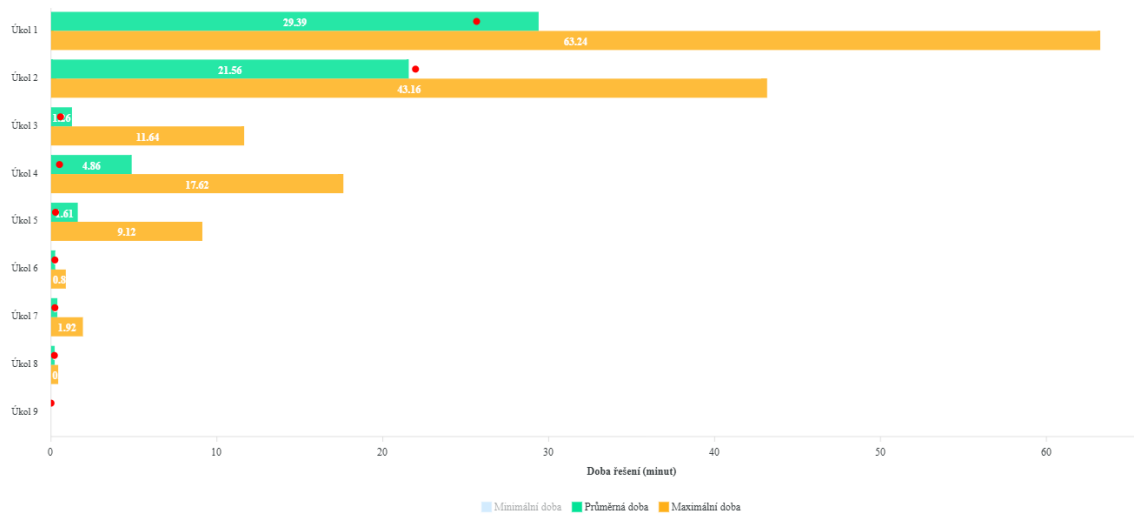
Výsledky dotazníku, ve kterém byli hráči tázaní na hodnocení příběhu, obtížnosti, nápovědy a herní dobu, jsou následující. Příběh byl průměrně ohodnocen známkou 1,7. Z toho vyplývá, že příběh by měl projít úpravou. Průměrné hodnocení obtížnosti úkolů je známka 3. Z toho můžeme usoudit, že zadání v této fázi patří spíše do kategorie středně těžkých. Vzhledem k zaměření scénáře je tato hodnota odpovídající a chtěná. Užitečnost nápověd byla hodnocena známkou 3,3 – nápovědy tedy budou muset být přepracovány, aby jejich využití a s tím spojený bodový postih byl v rámci scénáře adekvátní. Průměrná herní doba byla přibližně 60 minut, což je odpovídající obtížnosti. U pochopení zadání dotazovaní hráči uvedli, že zadání chápali, ale u některých úloh si nebyli jistí tím, co je po nich požadováno. Z toho plyne, že zadání některých úloh bude muset být přepracováno.

Testování hry přineslo cenné poznatky o její celkové hratelnosti a vzdělávacím přínosu. Testeři ocenili zajímavý příběh scénáře a možnost prakticky si vyzkoušet fungování mikrogridu. Nástroje, které hráči využívali, si osvojili relativně rychle, až na pár výjimek. Pozitivně také hodnotili postupně se zvyšující obtížnost úloh.

Na druhou stranu se objevilo několik návrhů na zlepšení. Někteří hráči měli problém s technickou složitostí samotných úloh nebo nepochopením zadání, což zpomalovalo postup ve hře. Dále bylo doporučeno změnit některé z nápověd, aby lépe pomohly hráči, který se zasekl. Tyto poznatky sloužily jako základ pro další iteraci vývoje.

4.5.2 Zpětná vazba z druhého testování

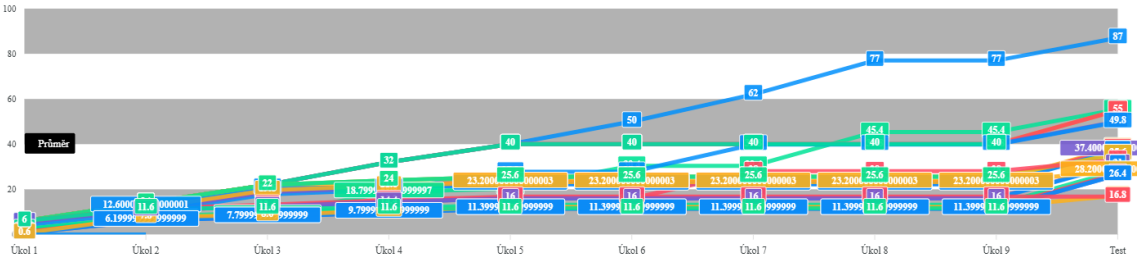
Výsledky dotazníku pro druhé testování, ve kterém byli hráči tázaní na hodnocení příběhu, obtížnosti, nápovědy, herní dobu a srozumitelnost, jsou následující. Příběh byl průměrně hodnocen známkou 2,56. Z toho vyplývá, že zábavnost příběhu je spíše průměrná a hráče velmi nezaujala. Obtížnost úkolů hráči hodnotili následovně: 50 % těžká obtížnost, 28,6 % pokročilá obtížnost a 21,4 % střední obtížnost. Z toho lze usoudit, že scénář je spíše těžký a to ve vztahu ke středoškolskému vzdělání. Užitečnost nápověd byla hodnocena průměrnou známkou 2,2, přičemž 22 % dotazovaných nápovědy nevyužili. Herní doba byla u všech hráčů 70 minut, to ale z důvodu nedostatku času. Doba řešení jednotlivých úkolů je v grafu 4.2. Srozumitelnost zadání ohodnotilo 64,3 % hráčů tak, že zadání chápali a věděli, co je požadováno, ale u maximálně jednoho úkolu si nebyli jistí. 21,4 % hráčů si u více než poloviny úkolů nebyli jistí a zbylých 14,3 % nevěděli, co je po nich požadováno. Celkový žebříček úspěšnosti jednotlivých hráčů je v grafu 4.3.



Obr. 4.2: Doba řešení jednotlivých úkolů druhého testování

Z grafu lze vyčíst, že průměrně nejvíce času hráči strávili na úkolech jedna a dva. Tyto úkoly nebyly nejlépe vysvětleny a také byly značně obtížné v porovnání vůči dalším úkolům. Dále je vidět, že úloha pět byla poslední, kterou hráči hráli. Velmi

krátké časy u zbylých úloh jsou zapříčiněny využitím nápověd, které hráčům řeknou flag k dané úloze. Minimální doba strávená hraním není v grafu uvedena. Jednalo se o výjimky, které měly znalost flagu k úloze od jiného hráče a nebo využily nápověd pro rychlé dokončení.



Obr. 4.3: Žebříček jednotlivých úkolů druhého testování

V grafu lze vidět, že většina hráčů dosáhla úkolu tři, přičemž část hráčů dosáhla nejvýše úkolu pět. Z grafu také vyplývá, že jeden z hráčů dosáhl vysokého bodového hodnocení. To je ale zavádějící, tento hráč v realitě dopadl podobně jako většina, pouze nevyužil nápověd na dokončení úkolů, ale jednotlivé flagy mu byly řečeny některým z hráčů.

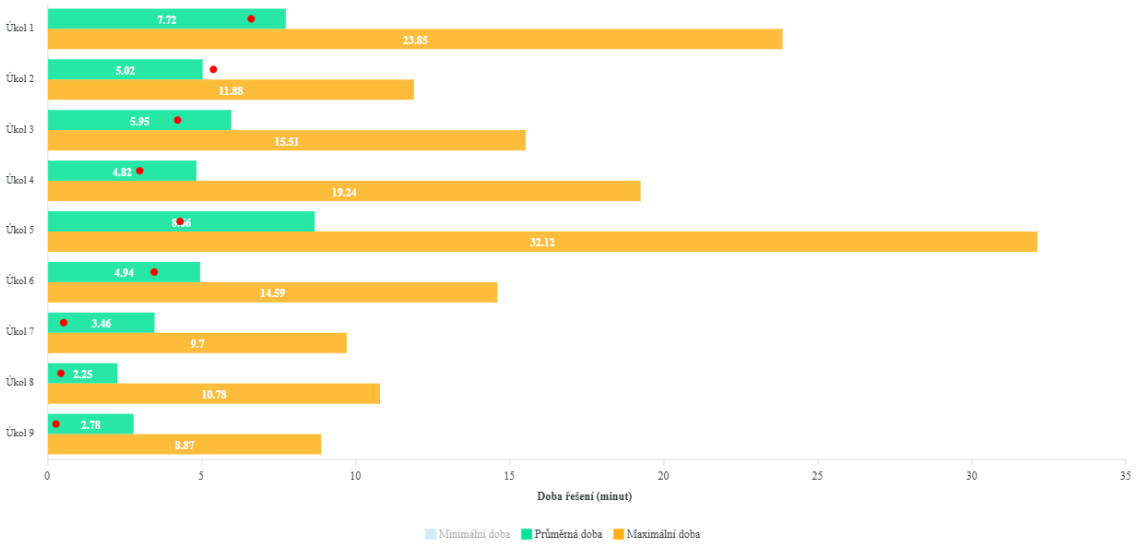
Z pozorování testování vyplynulo, že scénář není vhodný pro střední školy. Pokud by měl být na středních školách využit, tak by žáci měli vědět, jak pracovat v prostředí operačního systému Linux, jak využívat příkazovou řádku a měli by mít znalosti z oblasti komunikačních technologií. Dále bylo zjištěno, že první úloha scénáře je až moc obtížná a zmatečná, a proto by měla být do další verze hry rozdělena na alespoň dvě úlohy. Také bylo nalezeno pár chyb v systému virtualizace mikrogridu, včetně špatně nastavené vlajky k jednomu z úkolů.

Studenti sami měli pár návrhů na zlepšení. Jednalo se o návrh na změnu první úlohy. Úloha byla až moc náročná na to, že se jednalo o první. Změna by měla být taková, že se úloha rozdělí na více dílčích úloh, aby byla obtížnost více vzestupná. Další návrh na zlepšení byl u úkolu číslo šest. V této úloze má hráč za jeden z úkolů spustit skript, pomocí kterého se mu budou zobrazovat jednotlivé vlajky pro úkoly, které ho potřebují. V zadání nebylo vysvětleno, kde se tento skript nachází, a z tohoto důvodu nalezení daného skriptu zabralo čas. Poznatky z tohoto testování byly využity pro zlepšení scénáře.

4.5.3 Zpětná vazba ze třetího testování

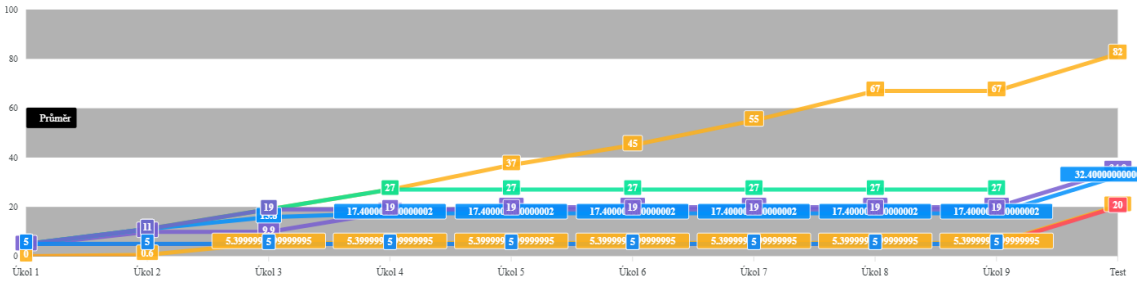
Výsledky dotazníku pro třetí testování, ve kterém byli hráči tázaní na hodnocení příběhu, obtížnosti, nápovědy, herní dobu a srozumitelnost, jsou následující. Příběh byl hodnocen průměrnou známkou 2,83. Z toho plyne, že zábavnost příběhu je

průměrná, ale jednalo se o očekávaný výsledek. Příběh jako takový upravován nebyl. Obtížnost úkolů byla hodnocena následovně: 50 % pokročilá obtížnost, 33,3 % střední obtížnost a 16,7 % těžká obtížnost. Z výsledků lze usuzovat, že scénář není vhodný pro všeobecné publikum, ale spíše pro specifická zaměření. Užitečnost nápověd byla hodnocena známkou 2, nápovědy využili všichni hráči. Dle tohoto výsledku lze usuzovat, že v ohledu nápověd došlo ke zlepšení. Herní doba byla průměrně 64 minut. Tento krátký čas je zapříčiněn tím, že hráči, kteří věděli, co mají dělat, se scénářem neměli větší potíže. Naopak hráči bez předchozích zkušeností často hru nedokončili. Doba řešení jednotlivých úkolů je v grafu 4.4. Srozumitelnost zadání 50 % hráčů ohodnotilo tak, že chápali, co je požadováno, 33,3 % ohodnotilo tak, že u pár úkolů si nebyli jisti, a zbylých 16,7 % si u více než poloviny nebyli jisti. Celkově pak za použití nápověd nebo bez scénář dokončilo 66,7 % hráčů.



Obr. 4.4: Doba řešení jednotlivých úkolů třetího testování

Z grafu je patrné, že nejvíce času strávili hráči u prvního a pátého úkolu. Při prvním úkolu byl tento čas zapříčiněn tím, že se někteří hráči seznamovali s platformou BUTCA a operačním systémem Linux. U pátého úkolu měli hráči obecně problém s příkazem na zápis hodnot nástroje mbpoll. Naopak nejméně času strávili hráči u posledních tří úloh. To je zapříčiněné tím, že k těmto úkolům se již dostali pouze ti hráči, kteří s předchozími úkoly neměli velké obtíže. Opět je vynechána minimální doba hraní. Někteří hráči od šestého úkolu využívali stoprocentních nápověd, aby hru dohráli.



Obr. 4.5: Žebříček jednotlivých úkolů třetího testování

Z grafu se dá vyčíst, že více jak polovina hráčů scénář dokončila, ale za využití nápověd. Jeden z hráčů získal téměř stoprocentní bodové ohodnocení. Tento hráč byl studentem oboru Informační bezpečnost z Fakulty informačních technologií VUT.

4.5.4 Finální úpravy vytvořeného scénáře

Na základě testování a dotazníků byl mírně upraven příběh. Do příběhu byly lépe zakomponovány požadavky, které hráč musí splnit pro získání flagu. Dále byly upraveny vybrané nápovědy. Přesněji pouze ta část, která hráči řekne, co se v nápovědě nachází. Celkově z testování vyplynulo, že scénář není vhodný pro široké publikum. Minimální požadavky jsou znalost práce v příkazové řádce operačního systému Linux a také práce v programu Wireshark. Důvod k této domněnce je takový, že hráči, kteří tyto znalosti neměli, měli problém s orientací v systému Linux. Program Wireshark není ve scénáři vysvětlen a očekává se, že hráč ho umí používat. Ideální hráč by měl mít znalosti v oblasti penetračního testování, komunikačních technologií a výše zmíněné. Bylo patrné, že hráči bez těchto znalostí nebyli schopni dokončit více než polovinu scénáře.

Závěr

Cílem bakalářské práce bylo nastudovat problematiku mikrogridu a kybernetické bezpečnosti. Na základě těchto poznatků poté vytvořit vzdělávací hru v rámci platformy BUTCA, která zábavnou formou edukuje studenty. Hra se zaměřuje na protokol Modbus a mikrogrid.

V úvodní části práce byl popsán mikrogrid jak z pohledu struktury, tak i fungování, včetně jeho role v moderní energetice. Dále byly popsány kybernetické útoky, které mohou být použity k útoku na mikrogrid. V druhé části práce byly popsány Cyber range platformy a koncept CTF her. A ve třetí části byly popsány dva energetické komunikační protokoly, jmenovitě Modbus a IEC 60870-5-104.

Na základě této práce byl vytvořen prvotní návrh herního scénáře, který kombinuje technické prvky mikrogridu s herními mechanismy. Scénář zahrnoval návrh virtuální infrastruktury, specifikaci úkolů a útoků, které mají hráči řešit, a také implementaci potřebných softwarových nástrojů. Převážně se scénář zaměřuje na tři oblasti, a to síťovou analýzu, FDI útoky a MitM útoky.

Tento návrh byl následně implementován a testován reálnými hráči. Testování poskytlo cennou zpětnou vazbu od hráčů. Poznatky z testování byly využity k úpravám scénáře, který byl poté implementován do platformy BUTCA. Dohromady testování proběhlo třikrát, což umožnilo odhalit silné stránky, ale také ukázalo oblasti pro zlepšení, například zvýšení srozumitelnosti zadání nebo lepší integraci nápovědy.

Literatura

[1] MARTÍN-MARTÍNEZ, F.; SÁNCHEZ-MIRALLES, A.; RIVIER, M. a CALVILLO, C.F. *Centralized vs distributed generation. A model to assess the relevance of some thermal and electric factors. Application to the Spanish case study.* Online. Energy. 2017, roč. 134, s. 850-863. ISSN 03605442. Dostupné z: https://doi.org/10.1016/j.energy.2017.06.055. [cit. 2024-11-26].

[2] SABRI, Yassine; EL KAMOUN, Najib a LAKRAMI, Fatima. *A Survey: Centralized, Decentralized, and Distributed Control Scheme in Smart Grid Systems.* Online. 2019 7th Mediterranean Congress of Telecommunications (CMT). 2019, s. 1-11. ISBN 978-1-7281-4420-7. Dostupné z: https://doi.org/10.1109/CMT.2019.8931370. [cit. 2024-11-26].

[3] HOOSHYAR, Ali a IRAVANI, Reza. *Microgrid Protection.* Online. Proceedings of the IEEE. 2017, roč. 105, č. 7, s. 1332-1353. ISSN 0018-9219. Dostupné z: https://doi.org/10.1109/JPROC.2017.2669342.[cit. 2024-10-20]

[4] HUBBLE, Andrew Harrison a USTUN, Taha Selim. *Composition, placement, and economics of rural microgrids for ensuring sustainable development.* Online. Sustainable Energy, Grids and Networks. 2018, roč. 13, s. 1-18. ISSN 23524677. Dostupné z: https://doi.org/10.1016/j.segan.2017.10.001. [cit. 2025-05-23].

[5] JIANG, Quanyuan; XUE, Meidong a GENG, Guangchao. E*nergy Management of Microgrid in Grid-Connected and Stand-Alone Modes.* Online. IEEE Transactions on Power Systems. 2013, roč. 28, č. 3, s. 3380-3389. ISSN 0885-8950. Dostupné z: https://doi.org/10.1109/TPWRS.2013.2244104. [cit. 2025-05-23].

[6] VANDOORN, Tine L.; MEERSMAN, Bart; DEGROOTE, Lieven; RENDERS, Bert a VANDEVELDE, Lieven. *A Control Strategy for Islanded Microgrids With DC-Link Voltage Control.* Online. IEEE Transactions on Power Delivery. 2011, roč. 26, č. 2, s. 703-713. ISSN 0885-8977. Dostupné z: https://doi.org/10.1109/TPWRD.2010.2095044. [cit. 2025-05-23].

[7] FAULKNER, Roger; WENZEL, Richard J a TAYLOR, Clay. *Mesogrids for Regional Power Delivery and Reliability.* Online. 2020 Clemson University Power Systems Conference (PSC). 2020, s. 1-6. ISBN 978-1-7281-9384-7. Dostupné z: https://doi.org/10.1109/PSC50246.2020.9131240. [cit. 2025-05-23].

[8] LEE, Dasheng a CHENG, Chin-Chi. *Energy savings by energy management systems: A review.* Online. Renewable and Sustainable Energy Reviews. 2016, roč. 56, s. 760-777. ISSN 13640321. Dostupné z: https://doi.org/10.1016/j.rser.2015.11.067. [cit. 2024-11-26].

[9] BARAI, Gouri R.; KRISHNAN, Sridhar a VENKATESH, Bala. *Smart metering and functionalities of smart meters in smart grid - a review*. Online. 2015 IEEE Electrical Power and Energy Conference (EPEC). 2015, roč. 57, s. 138-145. ISBN 978-1-4799-7662-1. ISSN 13640321. Dostupné z: https://doi.org/10.1109/EPEC.2015.7379940. [cit. 2024-11-27].

[10] NEJABATKHAH, Farzam; LI, Yun Wei; LIANG, Hao a REZA AHRABI, Rouzbeh. *Cyber-Security of Smart Microgrids: A Survey*. Online. Energies. 2021, roč. 14, č. 1. ISSN 1996-1073. Dostupné z: https://doi.org/10.3390/en14010027. [cit. 2024-10-24].

[11] GIANI, Annarita; BITAR, Eilyan; GARCIA, Manuel; MCQUEEN, Miles; KHARGONEKAR, Pramod et al. *Smart Grid Data Integrity Attacks*. Online. IEEE Transactions on Smart Grid. 2013, roč. 4, č. 3, s. 1244-1253. ISSN 1949-3053. Dostupné z: https://doi.org/10.1109/TSG.2013.2245155. [cit. 2024-11-27].

[12] ZHANG, Xiaoyu; XU, Maochao; DA, Gaofeng a ZHAO, Peng. *Ensuring confidentiality and availability of sensitive data over a network system under cyber threats*. Online. 2021, roč. 214. ISSN 09518320. Dostupné z: https://doi.org/10.1016/j.ress.2021.107697. [cit. 2024-11-28].

[13] JESUDOSS, A a SUBRAMANIAM, N. *A SURVEY ON AUTHENTICATION ATTACKS AND COUNTERMEASURES IN A DISTRIBUTED ENVIRONMENT*. Indian Journal of Computer Science and Engineering (IJCSE). 2014, roč. 5, č. 2, s. 71-77. ISSN 0976-5166. [cit. 2024-11-28].

[14] SUN, Yan; HAN, Zhu; YU, Wei a RAY LIU, K. *Attacks on Trust Evaluation in Distributed Networks*. Online. 2006 40th Annual Conference on Information Sciences and Systems. 2006, s. 1461-1466. ISBN 1-4244-0350-2. Dostupné z: https://doi.org/10.1109/CISS.2006.286695. [cit. 2024-11-28].

[15] GUNDUZ, M. Zekeriya a DAS, Resul. *Analysis of cyber-attacks on smart grid applications*. Online. 2018 International Conference on Artificial Intelligence and Data Processing (IDAP). 2018, s. 1-5. ISBN 978-1-5386-6878-8. Dostupné z: https://doi.org/10.1109/IDAP.2018.8620728. [cit. 2024-10-25].

[16] TAHERDOOST, Hamed. *Insights into Cybercrime Detection and Response: A Review of Time Factor*. Online. Information. 2024, roč. 15, č. 5. ISSN 2078-2489. Dostupné z: https://doi.org/10.3390/info15050273. [cit. 2024-11-28].

[17] SÜZEN, Ahmet Ali. *A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem*. Online. International Journal of Computer Network and Information Security. 2020, roč. 12, č. 1, s. 1-12. ISSN 20749090. Dostupné z: https://doi.org/10.5815/ijcnis.2020.01.01. [cit. 2025-05-28].

[18] MUHAMMAD, Adabi Raihan; SUKARNO, Parman a WARDANA, Aulia Arif. *Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning*. Online. Procedia Computer Science. 2023, roč. 217, s. 1406-1415. ISSN 18770509. Dostupné z: https://doi.org/10.1016/j.procs.2022.12.339. [cit. 2025-05-28].

[19] CANAAN, Bushra; COLICCHIO, Bruno; OULD ABDESLAM, Djaffar a REZA AHRABI, Rouzbeh. *Microgrid Cyber-Security: Review and Challenges toward Resilience*. Online. Applied Sciences. 2020, roč. 10, č. 16. ISSN 2076-3417. Dostupné z: https://doi.org/10.3390/app10165649. [cit. 2024-10-25].

[20] KARJALAINEN, Mika a KOKKONEN, Tero. *Comprehensive Cyber Arena; The Next Generation Cyber Range*. Online. 2020, s. 11-16. ISBN 978-1-7281-8597-2. Dostupné z: https://doi.org/10.1109/EuroSPW51379.2020.00011. [cit. 2025-05-28].

[21] KATSANTONIS, M. N.; MANIKAS, A.; MAVRIDIS, I. a GRITZALIS, D. *Cyber range design framework for cyber security education and training*. Online. International Journal of Information Security. 2023, roč. 22, č. 4, s. 1005-1027. ISSN 1615-5262. Dostupné z: https://doi.org/10.1007/s10207-023-00680-4. [cit. 2024-10-26].

[22] YAMIN, Muhammad Mudassar; KATT, Basel a GKIOULOS, Vasileios. *Cyber ranges and security testbeds: Scenarios, functions, tools and architecture*. Online. 2020, roč. 88. ISSN 01674048. Dostupné z: https://doi.org/10.1016/j.cose.2019.101636. [cit. 2024-11-28].

[23] LAZAROV, Willi. *Zpětnovazební profilační model pro výuku a trénink kybernetické bezpečnosti*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2024. Diplomová práce. Vedoucí práce: doc. Ing. Zdeněk Martinásek, Ph.D. Dostupné z: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=268192. [cit. 2025-05-16].

[24] KUCEK, Stela a LEITNER, Maria. *An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments*. Online. Journal of Network and Computer Applications. 2020, roč. 151. ISSN 10848045. Dostupné z: https://doi.org/10.1016/j.jnca.2019.102470. [cit. 2024-11-02].

[25] BEURAN, Razvan. Capture the Flag Platforms. Online. Cybersecurity Education and Training. 2025, s. 193-219. ISBN 978-981-96-0554-5. Dostupné z: https://doi.org/10.1007/978-981-96-0555-2_10. [cit. 2025-05-28].

[26] MOHAGHEGHI, S.; STOUPIS, J. a WANG, Z. *Communication protocols and networks for power systems-current status and future trends*. Online. 2009 IEEE/PES Power Systems Conference and Exposition. 2009, s. 1-9. ISBN 978-1-4244-3810-5. Dostupné z: https://doi.org/10.1109/PSCE.2009.4840174. [cit. 2025-05-22].

[27] TAWDE, Reshma; NIVANGUNE, Ashwin a SANKHE, Manoj. *Cyber security in smart grid SCADA automation systems*. Online. 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS). 2015, s. 1-5. ISBN 978-1-4799-6817-6. Dostupné z: https://doi.org/10.1109/ICIIECS.2015.7192918. [cit. 2025-05-22].

[28] FOVINO, Igor Nai; CARCANO, Andrea; MASERA, Marcelo a TROMBETTA, Alberto. *Design and Implementation of a Secure Modbus Protocol*. Online. Critical Infrastructure Protection III. IFIP Advances in Information and Communication Technology. 2009, s. 83-96. ISBN 978-3-642-04797-8. Dostupné z: https://doi.org/10.1007/978-3-642-04798-5_6. [cit. 2025-05-16].

[29] MAI, Kelvin; QIN, Xi; ORTIZ SILVA, Neil a CARDENAS, Alvaro A. *IEC 60870-5-104 Network Characterization of a Large-Scale Operational Power Grid*. Online. 2019 IEEE Security and Privacy Workshops (SPW). 2019, s. 236-241. ISBN 978-1-7281-3508-3. Dostupné z: https://doi.org/10.1109/SPW.2019.00051. [cit. 2025-05-22].

[30] MATOUŠEK, Petr. *Description and analysis of IEC 104 Protocol*. Faculty of Information Technology, Brno University o Technology, Tech. Rep, 2017. Dostupné z: https://www.fit.vut.cz/research/publication-file/c168651/279814/TR-IEC104v2.pdf. [cit. 2025-05-16].

Seznam symbolů a zkratek

DER	Distribuované energetické zdroje – Distributed Energy Resources
EMS	Systém energetického managementu – Energy Management System
IoT	Internet věcí – Internet of Things
PCC	Bod společného spojení – Point of Common Coupling
LC	Místní ovladač – Local Controller
SC-EMS	Dohledový kontrolér a systém energetického managementu – Supervisory Controller and Energy Management System
FDI	Injekce falešných dat – False Data Injection
DDoS	Distribuované odmítnutí služby – Distributed Denial of Service
MitM	Útok muže uprostřed – Man-in-the-Middle
IDS	Systém detekce narušení – Intrusion Detection System
SIEM	Bezpečnostní informace a správa událostí – Security Information and Event Management
CTF	Hra o vlajku – Capture the Flag
CR	Cyber Tange platforma – Cyber Range

Seznam příloh

A Návody ke scénáři

A.1 Scénář v textové podobě

Přílohou práce je i samotný scénář v textové podobě, který je dostupný na `https://drive.google.com/file/d/1g8IZXAAnYyE18KIF5Rf3tNctwiJCTrom/view?usp=sharing`, po předchozí domluvě s vedoucím bakalářské práce. Pro přístup k tomuto dokumentu kontaktujte Ing. Antonína Bohačíka pomocí e-mailu `antonin.bohacik@vut.cz`.

A.2 Návod ke scénáři a zdrojové soubory

Přílohou práce je i návod ke scénáři a také zdrojové soubory. Návod je dostupný na `https://drive.google.com/file/d/1z2Yj_Nlk7P8VVqY58LcYxA_O-iYiO3x1/view?usp=sharing` a zdrojové soubory jsou dostupné na `https://drive.google.com/file/d/1o9Lt5X4C56qxFJjKNKeyVUx13hFbA0k9/view?usp=sharing` po předchozí domluvě s vedoucím bakalářské práce. Pro přístup k těmto dokumentům kontaktujte Ing. Antonína Bohačíka pomocí e-mailu `antonin.bohacik@vut.cz`.

B Dotazníky

Přílohou práce je dokument obsahující odpovědi všech respondentů. Dokument je dostupný na `https://drive.google.com/file/d/1vRMZdMMnWvEVk8-9HrjMUXA75IfSk_Rl/view?usp=sharing`.