POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE
Fakulta bezpečnostního managementu
Katedra managementu a informatiky

Automatizace procesů řízení systému a organizace pomocí nástrojů pro extrakci, transformaci a čtení dat

Diplomová práce

Automation of system and organization control processes using tools for data extraction, transformation and reading

Master thesis

VEDOUCÍ PRÁCE
RNDr. Václav HNÍK, CSc.

AUTOR PRÁCE
Bc. Tomáš HOLÝ

MILOVICE
2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Milovicích, dne 4. 3. 2022

Bc. Tomáš HOLÝ

Poděkování

Na tomto místě bych rád poděkoval RNDr. Václavu Hníkovi, CSc. za cenné připomínky a odborné rady, kterými přispěl k vypracování této diplomové práce.

ANOTACE
V diplomové práci budou představeny procesy řízení systému organizace, funkce a role uvnitř vybraného organizačního celku a jím využívaný nástroj určený k automatizaci procesů a činností organizace. Konkrétně se bude jednat o nástroj pro extrakci, transformaci a nahrání dat, Pentaho. Organizačním celkem využívajícím tento nástroj je bezpečnostní operační centrum neboli SOC, jenž se podílí na zajišťování bezpečnosti v kyberprostoru. Budu se zabývat procesy, funkcemi, rolemi a jejich vlivy a vztahy uvnitř bezpečnostního operačního centra a možnostmi využití nástroje Pentaho pro účely SOC, které budou představeny v praktické části práce.

KLÍČOVÁ SLOVA
Procesy řízení systému * procesy organizace * bezpečnostní operační centrum * automatizace * nástroje ETL * Pentaho * transformace * SOC * kybernetická bezpečnost

ANNOTATION
The diploma thesis will introduce the management systems of the organization, functions and roles within the selected organizational unit and the tool used by it to automate the processes and activities of the organization. Specifically, it will be a tool for data Extraction, Transformation and Load, Pentaho. The organizational unit using this tool is the Security Operations Center, or SOC, which is involved in ensuring security in cyberspace. I will deal with the processes, functions, roles and their influences and relationships within the Security Operations Center and the possibilities of using the Pentaho tool for SOC purposes, which will be presented in the practical part of the thesis.

KEYWORDS
System Management Processes * Organization Processes * Security Operations Center * Automation * ETL Tools * Pentaho * Transformation * SOC * Cyber Security

Obsah

ÚVOD

Organizace mohou ke stanovení a dosažení svých cílů strukturovat a využívat své vedení, zdroje a procesy různými způsoby. Pomocí organizačního řízení neboli managementu řízení, mohou udávat svým zaměstnancům směr a povzbuzovat je k tomu, aby pracovali na společném cíli. Pokud management organizace pochopí, jak taková strategie funguje, snadněji dosáhne své vize a to s vynaložením minimálních nákladů.

Problémy však nelze řešit pouze plošnými škrty v rozpočtu, zvláště proto, že různé organizace ve stále se zvyšující míře vytvářejí, shromažďují a ukládají obrovské množství dat a informací ve formě osobních údajů, informací o zdravotním stavu pacientů nebo údajů o platbách svých klientů a další. To jsou hlavní důvody toho, proč je na tyto organizace vyvíjen nátlak na zajištění správy a zabezpečení těchto dat před kybernetickými hrozbami. Řešením jsou právě strategické investice do technologií zvyšujících efektivitu práce a především bezpečnost dat. Organizace sice disponují základními druhy zabezpečení, jako jsou například brány firewall a antivirový a antispamový software, avšak tento druh ochrany se v současné době stává nedostatečným. Proto byl vyvinut a aplikován soubor organizačních a technických opatření, jejichž cílem je zajištění bezproblémového chodu organizace a jejích činností, úkolů a povinností vyplývajících z požadavků na zajišťování kybernetické bezpečnosti.

Z důvodu úspory času a financí, nedostatku personálu a neustálého vývoje v oblasti kybernetické bezpečnosti je snahou organizací většinu svých procesů a činností automatizovat. K tomu mohou využít nepřeberné množství nástrojů pro extrakci, transformaci a nahrání dat (ETL)[1]. Jedná se o proces extrahování dat z výchozího zdroje, jejich převedení do jiné podoby a nahrání do cílového zdroje.

Na trhu existuje nespočet nástrojů ETL. Liší se od sebe funkcemi, vlastnostmi, uživatelským prostředím nebo cenou, a je na každé organizaci, který si zvolí. Nástroje ETL se primárně používají pro nakládání s velkými objemy dat v databázích nebo datových skladech, ovšem v případě použití v prostředí SOC[2] je možné s jejich pomocí automatizovat například generování varování o událostech, procesy e-mailové korespondence, manipulaci se soubory, úpravu

[1] Z anglického Extract, Transform and Load
[2] Z anglického Security Operation Center

dokumentů a mnoho dalších procesů a úkonů. Jde o efektivní řešení vyžadující ke svému fungování minimálního lidského zásahu.

Bezpečnostní operační centrum neboli SOC lze popsat jako jednotný organizační celek, jemuž je svěřena správa a odpovědnost za zabezpečení informací, informačních technologií a dalších aktiv před kybernetickými hrozbami a jenž je za tímto účelem tvořen odpovídajícím prostředím, technologiemi, procesy, zásadami a zejména personálem. Primárním úkolem SOC je průběžné zkoumání internetového provozu, sítí, aplikací, koncových zařízení a dalších systémů na přítomnost bezpečnostních hrozeb. Ve většině případů je SOC samostatnou součástí organizace s přítomností nepřetržité směny v případě, že je požadována okamžitá reakce na nastalou událost. Členové týmu SOC jsou obvykle ve své působnosti a činnostech soběstační, ovšem není vyloučena spolupráce s jinými zaměstnanci či odděleními v rámci organizace. Jejich znalosti v oblasti kybernetické bezpečnosti by měly být na takové úrovni, aby byli schopni zmírnit hrozby pro chráněné zájmy. Za tímto účelem SOC provozuje nástroje, jež monitorují síť 24 hodin denně, 7 dní v týdnu. S jejich pomocí je schopen detekovat hrozby a reagovat na bezpečnostní incidenty téměř okamžitě.

Problematice uvedené ve výše zmíněných odstavcích se budu podrobněji věnovat v teoretické části práce, která bude předcházet části praktické. V té představím reálné příklady využití ETL nástroje Pentaho v prostředí SOC.

Budou představeny reálné příklady využití nástroje ETL, s jejichž pomocí lze automatizovat procesy a činnosti vyskytující se v prostředí SOC a zefektivnit výkon jeho pracovníků. Tyto činnosti jsou většinou manuální a monotónní, jejich vykonání trvá dlouho a neexistuje spolehlivý způsob, jak ověřit výsledky. To jsou jedny z hlavních důvodů, proč použít nástroj ETL. U všech mnou zvolených příkladů budou představeny a popsány jejich nejdůležitější fáze (kroky) a v případě relevantních situací budou jednotlivé příklady vyhodnoceny z pohledu náročnosti zadání, výkonové náročnosti nebo spolehlivosti běhu.

1. ŘÍZENÍ SYSTÉMU A ORGANIZACE

Základem každé organizace je stanovit si cíle, kterých chce dosáhnout a především způsoby vedoucí k dosažení těchto cílů. Předpokladem splnění těchto podmínek je efektivním a účinným způsobem využívat procesů řízení, plánování, organizování, vedení anebo kontroly organizačních zdrojů. Je ale potřeba začít od začátku, tedy vytvořením dobře strukturovaného a funkčního plánu, sledovat průběh jeho plnění a případně provádět změny na základě analýz dosažených výsledků a zpětných vazeb. K účinným metodám vedoucích k efektivnímu řízení organizace patří například školení a vzdělávání zaměstnanců, formy hodnocení a odměňování, způsoby pověřování úkoly nebo systém kariérního růstu.

Systém řízení organizace, která primárně zajišťuje bezpečnost v kyberprostoru nebo je součástí některého z odvětví kritické infrastruktury, obsahuje další specifické činnosti, které jsou svázány s úzce vymezeným polem působnosti. Takto vymezené procesy systému řízení, kterým se budu věnovat v následujících odstavcích a podkapitolách, vychází ze zákona č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Ten stanovuje bezpečnostní opatření, jež jsou klíčová pro zajišťování bezpečnosti v kyberprostoru.

1.1 Systém řízení bezpečnosti

Obecně si můžeme pod systémem řízení bezpečnosti představit zajišťování ochrany před hrozbami a z nich plynoucích rizik. V tomto případě se hrozbami rozumí ty, které se nachází v kyberprostoru, a které mohou nějakým způsobem ohrozit nebo narušit bezpečnost aktiv. V první řadě je ale zapotřebí zabezpečit slabá místa nacházející se ve vlastním kyberprostoru a poté identifikovat hrozby, které by je mohly zneužít. Cílem pak je zajistit bezpečnost aktiv před narušením jejich důvěrnosti, integrity a dostupnosti.[3] V neposlední řadě je také důležitá ochrana aktiv subjektů třetích stran a dalších bráněných subjektů. Aktiva přitom dělíme na aktivní, primární a podpůrná a zahrnují například zaměstnance,

[3] *Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [online]. [cit. 4.1.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

informace nebo komunikační prostředky, jejichž selhání může mít dopad na informační a komunikační systémy.[4]

Jednotlivé hrozby a rizika jsou posuzovány z pohledu závažnosti dopadu na bezpečnost a také se vyhodnocuje pravděpodobnost, s jakou mohou nastat. Dle závažnosti dopadu na bezpečnost jsou následně vyvíjeny adekvátní reakce na incidenty. Touto prioritizací v rozhodovacím procesu můžeme události buďto vyšetřit, ignorovat nebo přesunout na zkušenějšího člena týmu.

Specifickou úlohu mají SOC působící v odvětví kritické infrastruktury. V případě pozitivní identifikace kybernetické hrozby může bezpečnostní tým jejím šetřením dojít k závěru, že událost je natolik závažná, že je zapotřebí přijmout opatření, která zabrání jejímu dalšímu šíření a napáchání větších škod. Takové situace mohou eskalovat až k vyhlášení stavu kybernetického nebezpečí. *„Jedná se o stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v IS, nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací.“* Případně může vláda na žádost ředitele Národního úřadu pro kybernetickou a informační bezpečnost vyhlásit nouzový stav.

Aby bylo možné lépe předcházet kybernetickým hrozbám a následkům z nich plynoucím, je nezbytnou součástí řízení organizace spolupráce s dalšími aktéry, kteří se na zajištění kybernetické bezpečnosti podílejí. To vyžaduje účinné propojení státních a nestátních organizací kooperujících jak na národní, tak i mezinárodní úrovni.

Systém řízení bezpečnosti je tvořen organizačními a technickými opatřeními, která by se dala charakterizovat jako soubor procesů, činností, řízení a zásad zajišťujících adekvátní úroveň poskytovaných služeb a to s využitím nejmodernějších technologií a kvalifikovaného personálu.

[4] *Vyhláška č. 82/2018 Sb., Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)* [online]. [cit. 11.1.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82?text=Vymezen%C3%AD%20pojm%C5%AF

1.1.1 Organizační opatření

Organizačními opatřeními se rozumí soubor převážně řídících činností celé organizace. Ta zde nevystupuje pouze jako zprostředkovatel služeb zajišťujících bezpečnost v kyberprostoru, ale disponuje i určitými pravidly a procesy týkající se řízení lidí, řízení spolupráce nebo krizového řízení. Provozním cílem je proces neustálého zlepšování, jenž je navržen tak, aby organizace udržovala krok s vývojovými trendy v oblasti kybernetické bezpečnosti.

1.1.1.1 Řízení lidí

Klíčem k úspěšnému kybernetickému útoku je nalezení nejslabšího článku v zabezpečení organizace. Typickým příkladem je zaměstnanec, který bez sebemenšího váhání otevřel přílohu e-mailu od původce, za kterým se skrývá neznámý útočník.

Z výše uvedeného odstavce je zřejmé, že klíčovou roli v zajišťování obrany proti kybernetickým hrozbám hrají samotní zaměstnanci. Z toho důvodu se provádí pravidelná školení v oblasti kybernetické bezpečnosti, protože zejména zodpovědný zaměstnanec v kombinaci s pokročilými technologiemi jsou nejlepší variantou, jak předcházet kybernetickým hrozbám. Důležitou součástí odborného vývoje zaměstnanců je neustálé nabývání nových vědomostí v kombinaci se samostudiem. Z úkolů Akčního plánu k národní strategii kybernetické bezpečnosti ČR na období let 2021 až 2025 vyplývá mimo jiné vypracovat Národní plán vzdělání v oblasti kybernetické bezpečnosti. Dosažení vyšší úrovně vzdělání tedy není cílem pouze jednotlivce, ale veškerých subjektů působících v dané oblasti. Zvyšování úrovně vědomostí zaměstnance může probíhat například ve formě odborných kurzů, cvičení, přednášek a školení nebo v různých podobách jako studijní obor kybernetické bezpečnosti na středních a vysokých školách. Podpora vzdělávacích aktivit může probíhat pomocí e-learningových kurzů a školení, které se v hojné míře začaly využívat zejména během pandemie Covid-19.[5] Důležitou a mnohdy vyžadovanou dovedností jedince je také znalost cizích jazyků, především angličtiny. Ta se používá jak pro potřeby komunikace, například

[5] *AKČNÍ PLÁN K NÁRODNÍ STRATEGII KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY NA OBDOBÍ LET 2021 AŽ 2025* [online]. [cit. 22.1.2022]. Dostupné z: https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/akcni_plan_2021-2025.pdf

s podporou produktu nebo se zahraničními subjekty, tak z důvodu používání aplikace, jež není lokalizována do českého jazyka. Určitou překážkou pro vzdělávání zaměstnanců může být omezený rozpočet organizace, jelikož náklady na účast v některých kurzech se mohou pohybovat v řádu tisíců dolarů.

Řízení lidských zdrojů zahrnuje další procesy, kterým se budu podrobněji věnovat v kapitole č. 4. Ta bude pojednávat například o složení, výzvách, druzích anebo úkolech SOC.

1.1.1.2 Řízení incidentů

Zjednodušeně řečeno, řízení incidentu počíná ohlášením problému a končí jeho vyřešením. Incidentem je jakékoliv narušení aktiv informačního a komunikačního systému, které může nepříznivě ovlivnit uživatele nebo celou organizaci. Aktivy mohou být *„technické vybavení, komunikační prostředky a programové vybavení informačního a komunikačního systému a objekty, ve kterých jsou tyto systémy umístěny, dále informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém a v neposlední řadě zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému“*[6]. Většinou se incidenty ohlašují na SOC, nebo jsou jím přímo detekovány. Události související převážně s provozem systémů se ohlašují na specializovaných odděleních známých jako „Help Desk“ nebo „Service Desk.

Primárně se řízení incidentů skládá z kroků, jimiž jsou identifikace události, její záznam a zařazení do příslušné kategorie, přiřazení preferencí, prvotní reakce na událost, prvotní diagnóza, vyšetření incidentu, následná reakce na incident a uzavření incidentu.

Až na proces vyšetření incidentu, který do značné míry závisí na zkušenostech personálu, je možné výše zmíněné kroky v určité míře automatizovat.

[6] *Vyhláška č. 82/2018 Sb., Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)* [online]. [cit. 15.1.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82?text=kybernetick%C3%BD+bezpe%C4%8Dnostn%C3%AD+incident

Například nástroje SIEM[7] jsou schopny na základě úrovně relevance, závažnosti a důvěryhodnosti vyhodnotit povahu události a přiřadit jí celkovou důležitost nebo význam.

1.1.1.3 Krizové řízení

„Jde o souhrn řídících činností orgánů krizového řízení zaměřených na analýzu a vyhodnocení bezpečnostních rizik a plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s přípravou na krizové situace a jejich řešením, nebo ochranou kritické infrastruktury.“ V případě identifikace kybernetického bezpečnostního incidentu, zejména pak po vyhlášení stavu kybernetického nebezpečí, nebo nouzového stavu budou muset být přijata opatření na ochranu informačních systémů nebo služeb a sítí elektronických komunikací v oblasti kybernetické bezpečnosti. *„Opatřeními jsou:*

- *varování,*
- *reaktivní opatření a*
- *ochranné opatření.“*[8]

Reaktivní opatření nejsou striktně stanovena, jelikož vždy záleží na povaze hrozby a možných následcích. V zásadě se ale bude jednat o snahu zabránit dalšímu šíření hrozby, zamezit nebo zmírnit škody, přijmout nápravná opatření a informovat dotčené subjekty. K přijetí reaktivních opatření je zavázána povinná osoba. Té je kromě toho dále uložena povinnost zpracovat a doručit Úřadu Oznámení o provedení reaktivního opatření a jeho výsledku.

Povinnou osobou se dle Vyhlášky č. 82/2018 rozumí orgán nebo osoba, které se ukládají povinnosti v oblasti kybernetické bezpečnosti a jsou jimi:

„a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b),

b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d),

[7] Z anglického Security Information and Event Management. SIEM řešení umožňují v reálném čase analyzovat a zpracovávat bezpečnostní události generované síťovými prvky nebo aplikacemi.

[8] *Zákon č. 181/2014 Sb., zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [online]. [cit. 24.1.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#f5279196

c) správce a provozovatel informačního systému kritické informační infrastruktury,

d) správce a provozovatel komunikačního systému kritické informační infrastruktury,

e) správce a provozovatel významného informačního systému,

f) správce a provozovatel informačního systému základní služby, pokud nejsou správcem nebo provozovatelem podle písmene c) nebo d).“[9]

V případě, že stav kybernetického nebezpečí přeroste ve vážnější situaci vyžadující více prostředků na její řešení, může vláda za podmínek stanovených zákonem vyhlásit nouzový stav. *„Pokud nebude možné odvrátit ohrožení bezpečnosti informací v informačních systémech nebo bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v rámci stavu kybernetického nebezpečí, ředitel Úřadu neprodleně požádá vládu o vyhlášení nouzového stavu.“*[10]

Primárním cílem přijatých reaktivních a proaktivních opatření je zamezit dalšímu šíření hrozby. V případě, že se jedná o hrozící nebo trvající útok nebo hrozbu ohrožující ve značném rozsahu důležité zájmy ČR a nelze je odvrátit v součinnosti s ozbrojenými silami ČR a neexistuje jiného účinného způsobu jejich odvrácení, je Vojenské zpravodajství oprávněno provést aktivní zásah, a to pouze po předchozím souhlasu ministra obrany.[11]

K minimalizaci dopadů krizové situace přispívá důsledná a pravidelná příprava všech zainteresovaných součástí organizace a to zejména formou cvičení. Příprava na možné bezpečnostní incidenty může pomoci identifikovat stávající slabá místa či nedostatky v oblasti kybernetické bezpečnosti.[12] V případě kybernetických útoků totiž není otázkou, jestli nastanou, ale kdy nastanou. V prostředí SOC může jít například o generování vyrozumívacích zpráv o probíhajících událostech nebo vzniklých incidentech.

[9] Tamtéž
[10] Tamtéž
[11] *Zákon č. 289/2005 Sb. Zákon o Vojenském zpravodajství* [online]. [cit. 27.1.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-289#cast4
[12] *Kybernetická bezpečnost: Přínosy cvičení* [online]. [cit. 15.1.2022]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/cviceni/prinosy-cviceni/

Bezpečnostní týmy musí mít také k dispozici funkční plány či směrnice, podle kterých mohou přijímat opatření ke zmírňování nebo zabránění vzniku hrozeb. Jedná se například o typový plán Narušení bezpečnosti informací kritické informační infrastruktury nebo Plán kontinuity činností, které stanovují zejména opatření a činnosti přijímané subjekty v oblasti kybernetické bezpečnosti pro případ vzniku hrozby a k řešení následků krizové situace. Součástí typového plánu je také „Karta opatření pro řešení krizové situace“.[13]

1.1.1.4 Řízení spolupráce

Dalším klíčem k úspěšnému boji proti kybernetickým zločincům a jejich útokům je vzájemná spolupráce bránících se subjektů. Tuto spolupráci je potřeba aplikovat jak na národní, tak především na mezinárodní úrovni, a to z toho důvodu, že kybernetické útoky již nejsou záležitostí pouze jednoho státu.

Oblast spolupráce se prolíná i s dalšími oblastmi řízení bezpečnosti. Jde například o řízení lidských zdrojů a to ve formě společných školení nebo cvičení. Jedním z největších je například cvičení Cyber Coalition, které se koná každoročně od roku 2008 prostřednictvím estonského Centra pro cvičení a výcvik kybernetické bezpečnosti. Jednotlivé scénáře pro cvičení se odvíjí od aktuálních trendů a situací v oblasti kybernetické bezpečnosti.[14] *„Scénáře pro rok 2021 zahrnovaly kybernetický útok na plynovody; kybernetický útok narušující rozmístění jednotek a logistiku; útok ransomwaru související s pandemií, kdy jsou odcizena data o vakcínách a kompromitovány očkovací programy.“*[15] Významná je také spolupráce na poli vědy a výzkumu a dalších vzdělávacích aktivit.

Jednotlivé úseky, oddělení, odbory nebo týmy organizace musí fungovat jako celek spolupracující na koordinovaném úsilí o zajišťování obrany před kybernetickými útoky. Výchozím bodem spolupráce přitom může být právě SOC, ve kterém je integrována většinová podpora služeb, schopností a technologií pro boj proti kybernetickým útokům.

---

[13] *ROZPRACOVÁNÍ TYPOVÉHO PLÁNU NA POSTUPY PRO ŘEŠENÍ krizové situace NARUŠENÍ BEZPEČNOSTI INFORMACÍ KRITICKÉ INFORMAČNÍ INFRASTRUKTURY: Přínosy cvičení* [online]. [cit. 18.1.2022]. Dostupné z: https://krizoverizeni.plzensky-kraj.cz/Framework/Document.ashx?ID=171617

[14] Více informací na: https://ccdcoe.org/

[15] *NATO’s flagship cyber defence exercise kicks off in Estonia* [online]. 29.11.2021 [cit. 6.2.2022]. Dostupné z: https://www.nato.int/cps/en/natohq/news_189156.htm?selectedLocale=en

Na mezinárodní úrovni zajišťuje spolupráci v oblasti kybernetické bezpečnosti Úřad, konkrétně Národní centrum kybernetické bezpečnosti (NCKB), který je také jednotným kontaktním místem pro zajištění přeshraniční spolupráce v rámci Evropské unie.[16] Riziko eskalace hrozby na mezinárodní úrovni je o to větší, jelikož stále nejsou implementována jednotná pravidla a opatření ke zmírnění kybernetických hrozeb. Situace se však v průběhu posledních let výrazně zlepšuje, a to zejména díky aktivnímu zapojování ČR do mezinárodních diskuzí nebo cvičení. ČR se dále podílí na tvorbě mezinárodních standardů a právních norem a ochotně spolupracuje s ostatními partnery v oblasti kybernetické bezpečnosti.

1.1.2 Technická opatření

Kybernetická bezpečnost je dynamickým a rychle se rozvíjejícím odvětvím. Není neobvyklé, že opatření, která platila včera, jsou dnes již zastaralá. Útočníci mění a zejména zdokonalují své taktiky, takže je nutné na ně reagovat co nejrychleji. V první řadě je potřeba implementovat vlastní technologie a systémy a následně podniknout kroky k jejich zabezpečení. Až poté se mohou bezpečnostní týmy věnovat vlastnímu šetření bezpečnostních událostí. Technickými opatřeními se rozumí zejména:

- Nástroje pro detekci kybernetických bezpečnostních událostí – ty jsou schopné provádět monitoring a analýzy síťového provozu v reálném čase a v mnoha případech disponují funkcemi pro vyhodnocování bezpečnostních událostí.
- Nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí – slouží primárně k auditování událostí, jejich vyhodnocování a včasnému varování nebo vyrozumívání. Tyto funkce často bývají součástí nástrojů pro detekci kybernetických bezpečnostních událostí.
- Prostředky pro šifrování dat a kryptografické nástroje – jedná se o účinné prostředky a nástroje, pomocí nichž lze vybudovat a posílit

[16] *Zákon č. 181/2014 Sb., zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [online]. [cit. 24.1.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#f5279196

obranu a ochranu aktiv. Existují například ve formě bezpečnostních tokenů[17], šifrovacích PGP klíčů[18] nebo čipových karet.

- Nástroje pro zajišťování fyzické bezpečnosti – jedná se o systém opatření zajišťujících ochranu aktiv před fyzickým působením událostí, sil anebo jevů, které by mohly způsobit narušení těchto aktiv. Patří sem například mechanické zábranné prostředky, elektronické zabezpečovací signalizace (EZS), zařízení elektronické požární signalizace (EPS) nebo bezpečnostní kamerové systémy (CCTV) chránící aktiva před neoprávněným vniknutím pachatele nebo jinými nežádoucími událostmi.
- Bezpečnost průmyslových a řídících systémů – jde o systém zabezpečující řízení provozu pomocí procesů automatizace. Využíván je zejména v odvětvích kritické infrastruktury, například v energetice, dopravě nebo komunikačních a informačních systémech. Typickým příkladem je systém SCADA[19], který se používá pro řízení, monitorování a analýzu průmyslových zařízení a procesů.

[17] Bezpečnostní token je fyzické zařízení nebo softwarový nástroj poskytující dvoufaktorové ověření.
[18] PGP je zkratkou pro termín Pretty Good Privacy a jde o šifrovací metodu, kterou vyvinul v roce 1991 Phil Zimmermann. Umožňuje zajistit, aby zprávu mohl dešifrovat a přečíst pouze příjemce, pro kterého je určena.
[19] Z anglického Supervisory Control And Data Acquisition. Do češtiny lze přeložit jako Systémy dohledového řízení a sběru dat.

2. AUTOMATIZACE PROCESŮ

Automatizaci procesů lze stručně popsat jako dosažení funkcí nebo postupů za pomoci technologií, tedy s minimálním zásahem člověka. Toho je potřeba především při tvorbě procesu automatizace v některém z dostupných softwarových nástrojů. Těm se budu věnovat podrobněji v kapitole č. 3 této práce. Pomocí automatizace procesů v organizaci je možné docílit snížení nákladů a chybovosti, zvýšení rychlosti, efektivnosti, přesnosti a mnoha dalších výhod. Automatizace tak usnadňuje život nejen zaměstnancům organizace, ale také jejím zákazníkům, dodavatelům a dalším partnerům.

V dnešní době není neobvyklé, že většina organizací přesouvá své procesy na informační systémy. Nejprve však musí existovat postup, který přenese fyzické informace do počítače nebo data z jednoho zdroje do druhého, jak tomu bude v mnou uvedených příkladech. Nesporná výhoda automatizace procesů spočívá v tom, že jde o levné řešení.

Základem je nashromáždit vhodné procesy pro automatizaci. Obecně platí, že jsou jimi procesy, které jsou založeny na pravidlech. Jedná se o lepší řešení, nežli automatizovat ty procesy, které vyžadují rozhodování na základě úsudku analytika. V některých případech také stačí komplikovaný proces rozdělit na dílčí části a pokusit se o automatizaci jednotlivě. Tímto postupem je možné docílit odstranění lidské chybovosti a využít výpočetní technologie ke zpracování složitých matematických úloh.

Důležité také je automatizovat pouze ty procesy, u kterých se neliší kroky vedoucí k cíli. Jakákoliv změna v jednotlivých krocích totiž může zapříčinit nefunkčnost nebo nedokončení procesu automatizace. Procesy vhodné pro automatizaci by měly být rutinní, správně definované, pokud možno neměnné a jednotlivé kroky nebo úlohy by měly být zpracovávány v neměnném pořadí.

Výčet případů, ve kterých je možné využít schopností nástrojů pro automatizaci, je téměř neomezený. Tento fakt byl ještě více umocněn s příchodem pandemie COVID-19, během které se sice rozšířilo pole působnosti kybernetických hrozeb, ale především došlo k nárůstu využití automatizovaných vzdálených služeb, cloudových aplikací nebo distribuovaných systémů.

Součástí většiny procesů jsou vstupní a výstupní data. Ta by měla být dobře strukturovaná a čitelná pro některý z nástrojů ETL. Vstupními, ale i výstupními

daty mohou být například tabulky a dokumenty sady Office, soubory CSV nebo JSON[20] a další. Vždy ale záleží na zvoleném ETL nástroji, jaké formáty zdrojů dat podporuje.

2.1 Automatizace procesů SOC

Pro členy týmu SOC jsou opakující se činnosti prakticky na denním pořádku. Následkem toho se může stát, že budou analytici inklinovat ke stereotypu, čímž se může zvýšit jejich chybovost.

Ačkoliv jsou pomocí automatizace procesů usnadňovány činnosti analytiků SOC, jsem přesvědčený, že nejlepších výsledků je dosaženo jejich vzájemnou kombinací. Příkladem může být událost, jenž je nástrojem pro automatizaci posouzena jako bezpečnostní incident. Dokud však nedojde k prošetření události bezpečnostním analytikem, nepředstavuje 100procentní hrozbu. Bezpečnostní analytici mohou vycházet ze svých zkušeností nebo jazykové citlivosti. V případě pozitivní identifikace musí dále ověřit například autenticitu hrozby, odhalit jejího původce, podniknout kroky nezbytné k zabránění vzniku dominového efektu a případně informovat dotčené subjekty.

Základem efektivního řízení organizace jsou také procesy a způsoby spolupráce a komunikace vně i uvnitř organizace. Členové týmu SOC využívají řadu komunikačních kanálů, pomocí kterých mohou informovat nebo varovat spolupracující subjekty o zjištěných bezpečnostních hrozbách nebo předávat interní informace v rámci vlastní organizace. K tomu lze využít automatizovaného šifrování anebo dešifrování datových toků pomocí generovaných PGP klíčů.

Automatizovat lze i další činnosti vykonávané členy týmu SOC. Může jít například o práci s e-maily, porovnávání dat, procesy plánování nebo přidělování událostí k prošetření analytikům. Není ale nutností automatizovat veškeré procesy. Zejména v dnešní době technologického pokroku, kdy jsme na informačních a komunikačních systémech stále více závislí, je potřeba přistupovat k možnostem využití automatizace s rozvahou, neboť nám mohou přinést více škody než užitku.

Před samotným nasazením automatizovaných procesů do reálného provozu je nutné vyhodnotit množství práce vynaložené na jejich sestavení, náročnost

[20] Z anglického JavaScript Object Notation

na výpočetní výkon anebo ověřit jejich funkčnost, spolehlivost a bezchybnost. Je otázkou, jak výše uvedené události ověřit, pokud se budou nacházet mimo prostředí nástroje Pentaho. Příkladem může být zpracování dat mimo nástroj, kdy může být obtížné získat měřitelné výsledky. Další výzkumnou otázkou je popis a vyhodnocení náročnosti práce autora, kterou vynaložil při sestavování jednotlivých úloh. Kombinací těchto výzkumných otázek si práce klade za cíl vyhodnotit význam a efektivnost aplikovaných automatizovaných úloh v prostředí SOC.

3. NÁSTROJE PRO AUTOMATIZACI

Zřejmě nikoho nepřekvapí, že jsou dnes ETL nástroje pro organizace nutností. Manuální správa dat již dávno přerostla v infrastrukturu založenou na výpočetních technologiích, jako jediného způsobu, jak udržet krok v neustále se měnícím prostředí. Počátky využití ETL nástrojů spadají již do minulého století. *„Nástroje ETL se začaly objevovat v 70. letech 20. století, kdy došlo k hojnému využívání centralizovaných datových úložišť. Ale teprve koncem 80. a začátkem 90. let, kdy se datové sklady dostaly do centra pozornosti, jsme byli svědky vytvoření účelových nástrojů, které pomáhaly načítat data do těchto nových skladů. První uživatelé potřebovali způsob, jak „extrahovat" data ze silových systémů, „transformovat" je do cílového formátu a „nahrávat" je. První nástroje ETL byly primitivní, ale svou práci zvládly. Je pravda, že množství dat, které zpracovávaly, bylo na dnešní standardy skromné."*[21]

Množství zpracovávaných dat není jedinou výzvou, které musí jejich zpracovatelé čelit. Kromě objemu a množství jsou často data ve své původní podobě prakticky nepoužitelná a to nejméně do té doby, dokud nejsou podrobena efektivní analýze, zpracování a převodu do užitečné podoby. Hlavní úlohou ETL nástrojů tedy je zpracovat co největší množství dat v co nejkratším čase a pokud možno bez zásahu uživatele. Toho je potřeba především pro modelování procesů v ETL nástroji a v případech, kdy dojde k problémům v průběhu zpracování dat. Procesy ETL se skládají z kroků, které jsou poměrně křehké. V okamžiku, kdy se například změní skladba dat u zdroje, musí být ve většině případů stávající model upraven nebo vytvořen nový.

Pod nástrojem ETL si lze představit aplikaci běžící na grafickém uživatelském rozhraní nebo webovém rozhraní, s jejíž pomocí mohou organizace provádět analýzy většiny svých dat a díky výstupům si usnadnit nebo zefektivnit některé procesy a činnosti.

3.1 Výběr ETL nástroje

Jedním z prvních úkolů organizace, rozhodne-li se pro využití nástrojů ETL, je vyhodnotit, který pro ni bude nejvhodnější. Současný trh jich nabízí nepřeberné

[21] *WHAT IS ETL?: The Ultimate Guide* [online]. [cit. 9.2.2022]. Dostupné z: https://www.matillion.com/what-is-etl-the-ultimate-guide/

množství, proto jsem v následujících podkapitolách vyhodnotil klíčové vlastnosti nástrojů ETL, na základě kterých se organizace mohou rozhodovat.

3.1.1 Podporované zdroje dat a cíle

Díky různorodosti zdrojů dat je téměř jisté, že nenajdeme jednu ETL platformu, která by podporovala veškeré existující nástroje, databáze a další zdroje dat, které organizace využívá. Ta by proto měla zvolit ten nástroj, který svými funkcemi pokryje co největší množství pro organizaci důležitých zdrojů.

Kompromisem může být volba nejúčinnějšího nástroje jako primárního, který bude umět zpracovat pro organizaci nejdůležitější data a pro ostatní buď použije nástroj s omezenějšími funkcemi, nebo využije vlastních zdrojů. Nevýhodami tohoto přístupu mohou být zvýšené nároky na správu více nástrojů či nekompatibilita výstupů.

3.1.2 Rozšiřitelnost a budoucnost

Rozšiřitelností můžeme rozumět tu součást podpory ze strany poskytovatele nástroje, která mu zajistí pokud možno co nejdelší životnost a funkčnost. Typickými rozšířeními bývají například integrace dalších zdrojů dat, podpora nových platforem, případně optimalizační záplaty apod.

3.1.3 Rozšiřitelnost

Nástroj by měl splňovat nároky organizace a poskytovat úměrnou kvalitu služeb po celou dobu používání. S rostoucím množstvím a variabilitou dat by měl být schopen tyto data i nadále zpracovávat. Proto je důležité, aby bylo možné nástroj rozšířit o nové funkce, nejčastěji pomocí pluginů nebo zásuvných modulů.

3.1.4 Použitelnost

Použitelnost nástroje ETL se odvíjí například od toho, jak snadná je práce s jeho rozhraním, jak v něm lze vytvářet úlohy nebo do jaké míry je přizpůsobitelný určitým požadavkům. Kritériem pro výběr může být také vyhodnocení produktivity jeho používání. Jde například o systém vytváření a zaznamenávání událostí ve formě logů nebo způsob řešení problémů, tedy zda je obsluha vyřeší sama nebo se bude muset spolehnout na podporu produktu.

3.1.5 Podpora a dokumentace

Podpora produktu ze strany tvůrců jednotlivých nástrojů se vztahuje na používání ETL nástroje v budoucnosti. Nikdo přece nestojí o produkt, který přestane plnit svou funkci po kratší době, než organizace zamýšlela. Podpora produktu zahrnuje mnoho proměnných, jako jsou například sídlo podpory, rychlost s jakou je schopna řešit problémy či forma komunikačních kanálů. Při rozhodování mohou pomoci také zkušenosti jiných uživatelů a jejich recenze. Součástí každého ETL nástroje jsou smluvní podmínky, na základě kterých bývá veškerá podpora sjednána. Většinou se odvíjí od ceny za předplatné daného nástroje a od jeho verze (například Open Source[22] nebo Enterprise vs Community Edition u nástroje Pentaho[23]). Nárokům organizace by také měla odpovídat úroveň poskytované dokumentace k nástroji. Podrobný a zároveň přehledný popis funkcí a schopností nástroje může ušetřit drahocenný čas při sestavování ETL požadavků.

3.1.6 Cena

Při výběru ETL nástroje téměř jistě narazíme na dva nebo více ETL nástrojů poskytujících podobné nebo dokonce shodné funkce, což může komplikovat rozhodování. Pokud jsou veškeré výše zmíněné funkce u vybraných nástrojů totožné, může být rozhodujícím faktorem cena. Poplatky spojené s využíváním nebo pořízením ETL nástrojů se mohou lišit i v řádu tisíce dolarů. Potom je na organizaci, kolik finančních prostředků bude chtít do nástroje investovat.

Kromě výše uvedených rozhodovacích faktorů existují ještě další, kterými se od sebe ETL nástroje liší. Pro mnoho organizací bude zásadní otázkou způsob a úroveň zabezpečení ETL relací. Pro některé budou klíčové spolehlivost a stabilita nástroje, což se týká především relací s nepřetržitým provozem. Je pravděpodobné, že než organizace nalezne ideální nástroj, bude jich muset ve svém prostředí a s vlastními daty použít a vyzkoušet několik. Jedině tak ale bude mít zaručeno, že v konečné fázi rozhodnutí bude mít k dispozici

[22] Open Source se používá pro označení programu nebo systému s volně přístupným zdrojovým kódem
[23] Verze nástroje Pentaho Community Edition je dostupná zdarma.

veškeré informace, a především praktické zkušenosti s produktem, který může mít zásadní vliv na vývoj organizace.

3.2 ETL nástroj Pentaho

Z dostupných nástrojů jsem si pro svou práci zvolil Pentaho od Hitachi Vantara, který poskytuje optimální funkce pro získávání dat z různých zdrojů s následnou transformací a výstupem do mnou požadované podoby. Tato práce si klade za cíl představit software Pentaho v kontextu s jeho využitím v procesech subjektu SOC. Za tímto účelem jsem v Pentaho vytvořil vlastní úlohy o různorodých činnostech, s rozdílnými zdroji dat a s rozdílnou obtížností, na kterých budou demonstrovány schopnosti nástroje Pentaho a jednotlivé kroky úloh.

Pentaho Data Integration, jak zní úplný název nástroje, je volně dostupný ETL nástroj umožňující vytvářet projekty, které využívají Business Intelligence. *„Business Intelligence (BI) je soubor nástrojů a strategií, které analyzují a převádějí nezpracovaná data na použitelné a koherentní informace pro použití v obchodních analýzách, které pomáhají při rozhodování.“*[24] Nástroj Pentaho jsem si zvolil z důvodu pozitivních recenzí a zkušeností uživatelů a poskytovaných funkcí potřebných pro mé příklady.

3.2.1 ETL procesy v Pentaho

Úlohy v praktické části této práce byly provedeny v jednom z nástrojů sady Pentaho, a to v Pentaho Data Integration. *„Nástroj Pentaho Data Integration (PDI) poskytuje funkce ETL, které usnadňují proces zachycování, čištění a ukládání dat pomocí jednotného a konzistentního formátu, který je dostupný a relevantní pro koncové uživatele a technologie internetu věcí.“*

V této práci budu převážně používat výrazy tak, jak jsou v Pentaho pojmenovány. Překlad do českého jazyka by mohl působit matoucím dojmem a některá slovní spojení by nevystihovala podstatu věci nebo pro ně neexistuje český ekvivalent. To však nebude mít pro pochopení souvislostí vliv.

Tvorba procesů v PDI je rozdělena do dvou úloh a to: „transformace“ a „joby“. Liší se především v tom, že v jobech se zpracovává jedna transformace

[24] *What is Business Intelligence? Definition, Techniques, Tools and Tips from Experts* [online]. 5.9.2019 [cit. 28.1.2022]. Dostupné z: https://callminer.com/blog/what-is-business-intelligence-definition-techniques-tools-and-tips-from-experts

za druhou, kdežto transformace se skládají z „kroků“ a ty se provádějí paralelně. Pomocí kroků v transformacích můžeme například převádět řádky na sloupce (a opačně), třídit data dle zvolených kritérií nebo slučovat více buněk do jedné. Kroky v jobech potom slouží především ke spojování transformací a jejich provádění, k práci se soubory, odesílání e-mailů či přenosu souborů přes FTP.

Pentaho dovoluje svým uživatelům vybrat si ze široké škály předdefinovaných kroků (pod položkou Design), které plní funkce, požadavky či úlohy, které mají být s daty učiněny. Názvy jednotlivých kroků nám také napovídají, jakým způsobem bude se zdroji dat zacházeno.

Obsluha nástroje je založena na principu Drag and Drop. Tedy jednotlivé kroky, ať už v jobech nebo transformacích, jsou skládány v jednotný celek pomocí přetahování. Práce s aplikací je tedy velmi snadná a intuitivní. Pro ještě jednodušší užívání je možné mezi kroky vyhledávat. Uživatelé mají k dispozici také „tržiště“, ve kterém je možné dohledat a nainstalovat chybějící kroky ve formě pluginů.

Pentaho, jako i jiné nástroje, umožňuje zpracovávat velké objemy dat. Jednou z hlavních výzev SOC je především jejich analýza. Proto je nutná selekce dat, která jsou pro SOC klíčová, jejich co nejrychlejší a nejpřesnější zpracování a nakonec získání výstupů, které umožní účelné rozhodování.

Data je Pentaho schopno zpracovávat téměř z jakéhokoliv zdroje. V mé práci budou zdroji dat např. SIEM QRadar, MISP a další databáze nebo soubory ve formátech Excel či Word. Důležitým požadavkem na získávání dat nejen z těchto zdrojů je alespoň částečná znalost programování v rozhraní API[25] či tvorby dotazů pomocí SQL[26], díky čemuž je v maximální možné míře využito možností Pentaho.

Předtím, než se uživatel pustí do samotné práci s jakýmkoliv ETL nástrojem, měl by si položit otázku, zda neexistuje alternativní způsob, jakým provést zamýšlený úkol. Například většinu práce s tabulkami zvládne bez problémů sada MS Office. Samozřejmě i zde hrají úlohu zkušenosti obsluhy, ale pro běžného

[25] Z anglického Application Programming Interface a označuje v informatice rozhraní pro programování aplikací

[26] Z anglického Structured Query Language. Jedná se o zkratku pro standardizovaný strukturovaný dotazovací jazyk, který je používán pro práci s daty v relačních databázích

uživatele jde o dostačující řešení. Problémem může být až větší množství údajů obsažených v dokumentu nebo zpracování více souborů zároveň.[27]

Dalším důležitým krokem je vytvořit si plán. Než začneme se samotným sestavováním jednotlivých kroků v transformacích a jobech, měl by si uživatel ETL nástroje jednotlivé úlohy promyslet. Je potřeba si stanovit, čeho a jakým způsobem chceme dosáhnout a v jakém formátu a podobě budou naše výstupy.

Jednotlivým úlohám a jejich krokům se budu podrobněji věnovat v praktické části práce, protože v souvislosti s konkrétními příklady budou lépe pochopitelné.

[27] Například v Excelu 2010 je maximální velikost jednoho listu 1 048 576 řádků a 16 384 sloupců. Databáze s IP adresami mohou však obsahovat například desítky milionů záznamů.

4. SOC

V dnešní době, kdy jsou informační systémy nedílnou součástí fungování a existence většiny organizací, potřebují mít ve svých řadách zaměstnance specializující se na oblast kybernetické bezpečnosti. Aby mohli optimálně vykonávat své činnosti, musí být sjednoceni ve svém účelu, v rámci jasných zásad a musí mít k dispozici aktuální zdroje vhodné pro odhalování digitálních hrozeb v kybernetickém prostoru. Jinak řečeno, jedná se o profesionály v oblasti kybernetické bezpečnosti soustředěné do jednotného souboru osob tvořící personál bezpečnostního operačního centra.

Proces vytváření SOC, stejně jako další činnosti v oblasti kybernetické bezpečnosti, by neměly být unáhlené. Zkratkovitá jednání a rozhodování mohou vést k ještě vážnějším hrozbám, než před kterými se máme v kybernetickém světě bránit. Organizace musí předem vyhodnotit své potřeby a své zdroje, aby mohla učinit nejvhodnější postupy a řešení.

Průběhu vytváření SOC v organizaci předchází několik zásadních otázek, na které je nutné znát odpovědi, případně mít vypracovány postupy vedoucí k nalezení těchto odpovědí.

4.1 Hlavní přínosy SOC v organizaci

Jednou z prvotních otázek při rozhodování týkající se problematiky kybernetické bezpečnosti jsou očekávání organizace. Ta mohou mít mnoho podob. Může se jednat například o to, jaký přínos bude mít nasazení řešení SIEM, jaké množství finančních prostředků investovat do kybernetické bezpečnosti nebo na jaké úrovni bude řešena spolupráce s dalšími subjekty. Stěžejní je porozumět řešenému problému. Následně je důležité vědět, zda nasazením těchto řešení problém vyřešíme.

Kybernetická bezpečnost je různorodá oblast s mnoha proměnlivými částmi a prioritami. Pro organizace je například často složité posoudit, které kroky vůči kybernetickým hrozbám vyžadují individuální řešení nebo zda vůbec disponují schopnostmi dané nebezpečí odvrátit. V těchto a mnoha dalších případech může SOC poskytnout téměř okamžitou reakci na události odehrávající se uvnitř nebo vně počítačových sítí. SOC plní především následující funkce:

- Zajištění dozoru nad provozovanými sítěmi – jednou z nekalých taktik útočníků v kyberprostoru je pohyb v takových místech v síti, kde nebudou zpozorováni a kde budou moci plánovat svou další činnost. Tato místa je obtížné monitorovat a mít pod kontrolou a řešením tohoto problému může být zajištění dozoru pomocí SOC.
- Správa alertů – lze konstatovat, že i přes implementovaná bezpečnostní opatření a řešení (SIEM, koncové body) budou nadále generována upozornění na nežádoucí bezpečnostní události. Ne všechny ale mohou vykazovat znaky ohrožení sítě. Může se jednat o události „false positive“ či povolené výjimky. V dalších případech upozornění nevykresluje přesně události, které se v síti skutečně odehrávají. Kromě toho může nadbytečné množství výstrah zapříčinit zatížení systému. Alarmy, které vypovídají o skutečné nežádoucí události, je potřeba v adekvátním čase analyzovat a především vyloučit možné napadení sítě pod správou organizace. Úkolem SOC je třídit tato varování, rozlišovat události typu „false positive“ od těch legitimních a dále podnikat kroky spojené s nálezem pozitivní hrozby.
- Řešení incidentů – v případě zjištění výskytu reálné bezpečnostní hrozby je zapotřebí mít k dispozici funkční plán reakce na incidenty. Především díky jasně definovaným postupům se lze vypořádat s potenciálními hrozbami v okamžiku, kdy jsou objeveny. SOC dále slouží jako hlavní kontaktní místo pro příslušníky organizace v případech podezření na narušení bezpečnosti či jiné události, které nejsou v souladu se standardním chováním. Tým SOC by měl mít schopnost zmírňovat bezpečnostní rizika a v případě nutnosti poskytovat informace a součinnost s jinými odděleními, např. s oddělením forenzní analýzy, právním oddělením či oddělením pro styky s veřejností. Plán reakce na incidenty by měl dále obsahovat takové činnosti a úkony, kterými by se měli řídit i ostatní členové organizace.

4.2 Úkoly SOC

Primárním úkolem SOC a jeho týmu je nepřetržitě monitorovat, odhalovat, analyzovat a reagovat na kybernetické hrozby. *„SOC zajišťuje komplexní centralizaci řízení bezpečnostních událostí a incidentů v jednom bodě s cílem*

minimalizovat reakční doby na incident a škody z něj plynoucí."[28] Hlavními přednostmi SOC jsou tedy všestrannost, organizovanost, rychlost, centralizovanost, bezpečnost a automatizace.

Tým SOC zodpovídá především za aktiva, jimiž jsou zařízení, procesy, aplikace a nástroje, s jejichž pomocí je zabezpečována kybernetická bezpečnost. K tomu musí mít úplný přehled o hrozbách, koncových bodech, serverech, ale i o službách třetích stran a síťovém provozu mezi nimi. Aby byl tým SOC schopen detekovat a odvrátit hrozící útok, musí mít povědomí o nejnovějších bezpečnostních technologiích, trendech v oblasti počítačové bezpečnosti a o vývoji nejnovějších hrozeb.

Odpovědností týmu SOC v případě výskytu alertu je, aby provedl jeho analýzu, vyloučil možnost toho, že je daná událost „false positive" a následně určil, o jak závažnou hrozbu se jedná a co nebo kdo je jejím cílem. Jedná-li se o pozitivní případ narušení bezpečnosti nebo o jeho pokus, je primární reakcí SOC varovat přímo dotčené subjekty, přijmout opatření vedoucí k odpojení nebo izolaci koncových bodů, podniknout kroky k nalezení a ukončení běhu škodlivých procesů (nebo zabránění jejich spuštění), předat informace o průběhu události zainteresovaným stranám a další. SOC se spolupodílí na vyšetřování hlavní příčiny. K tomu využívá dat z logů o síťových tocích a další informace vypovídající například o povaze útoku nebo jeho původcích.

Ačkoliv se většina procesů SOC řídí zavedenými osvědčenými postupy, je také potřeba dbát pokynů nařízení nebo jiných předpisů vydaných organizací nebo jinými odpovědnými orgány. Jednání v souladu s těmito předpisy nejenže pomáhají chránit citlivá data, ale také mohou ochránit organizaci před poškozením pověsti, případně před právními následky vyplývajícími z jejich porušení.

Běžně jsou SOC zřizována v různých odvětvích, především tam, kde je provoz subjektu z velké části závislý na komunikačních a informačních technologiích. Se SOC se tak můžeme setkat u subjektů působících v odvětví KI, například v energetice nebo dopravě. Většina velkých organizací, zejména ty, jež zajišťují bezpečnost kritické informační infrastruktury, má vlastní SOC. Tam, kde jsou

[28] *Security Operations Center: Centrální bod bezpečnosti* [online]. [cit. 29.1.2022]. Dostupné z: https://www.aec.cz/cz/produkty-a-sluzby/Stranky/soc.aspx

omezené zdroje, mohou být funkce SOC buďto svěřeny poskytovatelům těchto služeb, umístěny na cloud nebo mohou být hostovány ve virtuálních SOC.

4.3 Druhy SOC

Kromě rozhodování o pracovních rolích, které mohou být zahrnuty v týmu SOC, vyvstává také otázka, který z existujících modelů SOC v organizaci implementovat. Ve většině případů se budou organizace rozhodovat dle svých finančních možností. Přece jen, výstavba SOC závisí na využívaných technologiích, na zaměstnancích, umístění, spolupráci a dalších faktorech, jejichž kvalita se odvíjí od množství finančních prostředků do nich investovaných.

Pokud nemá organizace vybudováno zázemí a vlastní technické prostředky k tomu, aby provozovala vlastní SOC, může využít služeb virtuálního SOC. Jako jiné virtuální služby je i tato založena na decentralizovaných bezpečnostních technologiích, které jsou schopny monitorovat události a reagovat na hrozby, aniž by se nacházely fyzicky v místě organizace. Tímto řešením mohou organizace ušetřit na nákladech za hardware nebo jinou infrastrukturu a přitom mít možnost kdykoliv přistupovat k virtuálnímu SOC z jakéhokoliv místa. V případě využití této varianty se většinou neuvažuje o 24/7 směně a tak může docházet k případům, kdy nebudou hrozby zachyceny včas.

Další variantou je multifunkční SOC. Jedná se o SOC, který nejen že zabezpečuje bezpečnostní operace, ale je navíc rozšířen o personál a služby zajišťující dohled a správu nad síťovou infrastrukturou. V případě využití této varianty jsou veškeré služby, jak bezpečnostní, tak provozní, soustředěny na jednom místě a díky tomu je zajištěna okamžitá reakce na nenadálé události. Naproti tomu může být kooperativní činnost uvnitř takto tvořeného útvaru snadno narušena rozdílnými preferencemi jednotlivých týmů (bezpečnost vs. zajištění provozu).

Organizace, jež mají omezené množství technických, personálních a rozpočtových zdrojů, nejspíše zvolí formu sdíleného řízení SOC. Na základě svých priorit mohou organizace svěřit některé činnosti externím subjektům a stěžejní prvky ponechat pod svou správou. Nevýhody spočívají v tom, že se časem mohou zvýšit náklady na provozování interních a externích služeb

současně. Pozornost je také potřeba věnovat vhodnému výběru zprostředkovatele, který bude tuto službu zajišťovat.

V případě, že jsou jiné SOC podřízeny dalšímu „centrálnímu“ SOC, hovoříme o tzv. velitelském SOC. *„V mnoha případech se jedná o propojené, globální bezpečnostní operační centrum, které se skládá z několika vyhrazených SOC pracujících ve vzájemném tandemu.“*[29] Bývá tvořeno specifickými pracovišti zaměřenými na provádění forenzní analýzy či procesy obnovy. Slučuje prostředky k tomu, aby mohl čelit nejnebezpečnějším hrozbám v oblasti kybernetické bezpečnosti.[30] [31] Většinou je budováno ve velkých korporacích nebo vládních agenturách (ministerstva apod.).

Ve většině případů se můžeme setkat se samostatným SOC. *„Jedná se o centralizovaný SOC s vlastní infrastrukturou, týmem a procesy zaměřenými výhradně na bezpečnost.“*[32] Velikost SOC se liší v závislosti na velikosti organizace, rizicích a bezpečnostních potřebách. Tým SOC je složen z dostatečného počtu bezpečnostních expertů s různými dovednostními úrovněmi pro nepřetržité monitorování provozu. Nevýhodou jsou vysoké počáteční investice, což si mohou dovolit pouze větší organizace, podniky či vládní organizace.

Provozování účinného a efektivního SOC je nezbytnou součástí strategie organizace ke zmírňování nežádoucích dopadů na aktiva a zamezování hrozeb v kyberprostoru.

4.4 Náklady na vybudování SOC

Náklady na vybudování SOC lze v zásadě rozdělit do dvou samostatných kategorií a to na náklady na technologie a lidské zdroje. První se týká pořízení a údržby hardwaru a softwaru, zatímco druhá vyjadřuje náklady spojené s platy specializovaných analytiků nebo jejich vyškolováním. Výše těchto nákladů

[29] SAMSON JR., Ron. *Five Security Operations Center Models Compared: Find The Right SOC Model* [online]. 2021 [cit. 11.1.2022]. Dostupné z: https://www.clearnetwork.com/types-of-security-operations-centers-soc/
[30] *The Five Types of Security Operations Center Models* [online]. [cit. 11.1.2022]. Dostupné z: https://arcticwolf.com/resources/briefs-2/security-operations-center-models-2
[31] SAMSON JR., Ron. *Five Security Operations Center Models Compared: Find The Right SOC Model* [online]. 2021 [cit. 11.1.2022]. Dostupné z: https://www.clearnetwork.com/types-of-security-operations-centers-soc/
[32] Tamtéž

se do značné míry odvíjí od velikosti a rozsahu zájmů organizace. Tedy kolik koncových bodů je třeba sledovat, odvětví, ve kterém se organizace nachází, fyzická umístění atd.

4.5 Složení týmu SOC

Ve většině případů má tým SOC svého vedoucího. Tato role je kriticky důležitá, protože vedoucí SOC je zodpovědný za vedení svého týmu, včetně technického dohledu nebo povinností v oblasti řízení lidí, jako je personální obsazení, zajištění školení, plánování anebo koučování.

Ideálním kandidátem na pozici vedoucího je lídr, který dokáže přesně a účelně stanovit priority, efektivně komunikovat a za krizových situací podávat výkony na takové úrovni, že bude neustále působit jako stabilizační síla jak týmu SOC, tak i organizace. Vedoucí SOC plánuje, spravuje a řídí funkce a operace SOC. Dále se podílí na monitorování a analýze incidentů, předcházení bezpečnostních hrozeb a na zabezpečení technologií a procesů používaných k zajištění včasné reakce na bezpečnostní incidenty a jejich řešení. Vedoucí SOC se podílí na vývoji a podpoře svých podřízených analytiků a bývá styčným pracovníkem pro spolupráci s dalšími týmy nebo organizacemi. Manažeři SOC by také měli mít dovednosti nad rámec výkonu SOC, jako je například schopnost analýzy vývoje bezpečnostních situací. Dále by měli mít přehled o nových technologiích anebo se aktivně podílet na přípravě a implementaci krizových plánů.

Členy týmu SOC jsou kromě jeho vedoucího pracovníci na pozicích analytiků v úrovních L1, L2 a L3[33] a další členové, jež se mohou lišit v závislosti na druhu a potřebách SOC nebo organizace.

Nepopiratelnou výhodou pro manažera působícího v oblasti kybernetické bezpečnosti je absolvování manažerských a „leadership“ školení. Kladem může být získání vysokoškolského titulu, protože u většiny vysokoškolských technologicky zaměřených oborů se tyto typy dovedností vyučují jako součást osnov. Studiem takových oborů však ještě není zaručeno, že osoba automaticky získá vůdčí schopnosti.[34]

[33] Jedná se o úrovně bezpečnostních analytiků s rozdílnými zkušenostmi a znalostmi. Ty nejnižší mají L1 analytici a L3 analytici by měli být nejzkušenější.
[34] *8 Skills All Leadership Trainings Should Teach Managers* [online]. 2019 [cit. 3.11.2021]. Dostupné z: https://www.scienceofpeople.com/leadership-training/

Kromě vůdčích dovedností v oblasti kybernetické bezpečnosti se studenti na specializovaných vysokých školách učí teorii kybernetické bezpečnosti a následně její užití v praxi, přičemž získávají další individuální znalosti a dovednosti v oblastech technologie, práva, politiky, státní správy, krizového řízení a reakce na incidenty.

Výše zmíněné požadavky jsou však natolik specifické, že většina institucí provozujících SOC trpí nedostatkem personálu. *„45 procent zaměstnanců SOC se domnívá, že jejich SOC je nedostatečně personálně zabezpečen, a z nich si téměř dvě třetiny (63 procent) myslí, že by mohly využít dalších 2–10 zaměstnanců.“*[35]

Detekční nástroje v oblasti kybernetické bezpečnosti se pyšní okázalým označením „detekování v reálném čase“. Avšak zatímco systémy a nástroje jsou takových výkonů schopny, lidská reakce bývá zpravidla pomalejší. Většina vedoucích SOC je přesvědčena, že jeho analytici jsou schopni se rychle rozhodovat, což na ně vytváří obrovský tlak. Na základě toho mohou být jejich rozhodnutí založena spíše na nereálných očekáváních než na potřebách dané situace. Existuje celá řada neznámých, které není ani zkušený analytik schopen zaručeně a rychle určit. Například jak dlouho se útočníci pohybovali uvnitř sítě nebo kdo jsou původci útoku. A proto je na vedoucích, aby pro svůj tým zajistili klidné prostředí, jež má pozitivní vliv na provádění kvalitní a efektivní analýzy v co nejširším rozsahu.[36]

4.6 Výzvy SOC

Jako jiné součásti organizace, může být i tým SOC ovlivňován mnoha faktory snižujících efektivitu práce. Nejběžnějšími překážkami, se kterými se můžeme v provozu SOC setkat, jsou především personálního, procesního a technologického charakteru. S přijetím zákona o kybernetické bezpečnosti vyvstávají také otázky, jakým způsobem účelně nastavit spolupráci v oblasti kybernetické bezpečnosti se třetími stranami. V případě řešení bezpečnostních událostí dnes již není problémem zpracovat velké objemy dat, ale do popředí

[35] *Key challenges and frustrations of SOC workers* [online]. [cit. 8.11.2021]. Dostupné z: https://www.helpnetsecurity.com/2018/06/06/challenges-soc-workers/
[36] *Understanding the SOC Team Roles And Responsibilities* [online]. 2021 [cit. 11.11.2021]. Dostupné z: https://www.siemplify.co/blog/understanding-the-soc-team-roles-and-responsibilities/

důležitosti se dostává proces analýzy dat a k tomu je zapotřebí dostatek adekvátního personálu.

Personální problémy úzce souvisí s výstavbou SOC, konkrétně při obsazování volných pracovních pozic. S nedostatkem pracovních sil se dnes na trhu práce potýkají téměř všechny obory, oblast kybernetické bezpečnosti nevyjímaje.

4.6.1 Nedostatek personálu

Nalezení vyškoleného a zkušeného personálu je v oblasti bezpečnosti dlouhodobým problémem. Tento fakt také umocňují rychle se vyvíjející technologie v kyberprostoru a zvyšující se nároky na dovednosti pracovníků SOC. Není také výjimkou, že o konečné pozici rozhoduje sám uchazeč, jelikož má zpravidla více pracovních nabídek.

Nalezení vhodného pracovníka v oblasti kybernetické bezpečnosti je o to složitější, že k tomu, aby mohl obsluhovat nástroje SOC, musí disponovat odpovídající odborností v oblasti správy, monitorování a vyhodnocování událostí vedoucích k účinnému zásahu proti hrozbám. Je v režii organizace, jaké zvolí podmínky a požadavky na své zaměstnance při výstavbě SOC. Mohou vyžadovat například víceleté zkušenosti v oblasti kybernetické bezpečnosti, případně zkušenosti s prací v SOC nebo týmu jemu podobnému. Důležitým požadavkem je znalost standardů a norem souvisejících s kybernetickou bezpečností a osvědčených postupů spojených s operacemi SOC. Výhodou uchazeče o místo v týmu SOC je, pokud je schopen práce pod minimálním dohledem a s velkou mírou autonomie. S tím souvisí schopnost správně se rozhodovat, umět řešit problémy a mít analytické dovednosti s důrazem na detail a přesnost.[37]

4.6.2 Procesní problémy

Bezpečnostní operační centrum disponuje adekvátními schopnostmi a prostředky poskytující možnost odhalení nežádoucích aktivit uvnitř sítí a následné adekvátní reakce. To vyžaduje schopnost týmu SOC učit se dovednosti a procesy za chodu, aby byla zajištěna kontinuita poskytovaných služeb. Pro většinu SOC je i v dnešní době stále obtížné ospravedlnit svou

[37] *The SOC hiring handbook: Your guide to building and retaining a strong security team* [online]. [cit. 9.11.2021]. Dostupné z: https://logrhythm.com/uk-soc-hiring-handbook/

hodnotu. Zajištění kybernetické bezpečnosti pomocí SOC představuje neurčitou a nehmotnou oblast práce, kterou lze jen stěží kvantifikovat prostřednictvím zisku, jenž je cílem převážné většiny jiných organizací.

Největší riziko představují skryté neboli latentní procesy. Ty se nejčastěji vyskytují ve dvou formách a to systém/člověk. V případě systémových procesů může být problémem to, že se nedokáží přizpůsobit změnám nebo potřebám prostředí, které SOC monitoruje. Problémy procesů, v nichž hlavní úlohu hraje lidský faktor, bývají zapříčiněny tím, že se procesy vyvíjejí rychleji, než jim člověk stihne porozumět. Lidé pak zaostávají za procesy a navíc procesy zaostávají za prostředím organizace. Může se tak stát, že dříve, než stihne tým SOC porozumět nasazeným zdrojům a z nich plynoucím datům, rozhodne organizace o jejich náhradě. Tomu odpovídají údaje ze studie „2020 CISO Benchmark Study" provedené firmou CISCO, která uvádí, že organizace jsou schopny v témže dni vyšetřit pouze 48 % vygenerovaných bezpečnostních událostí a z nich pouhých 26 % je považováno za legitimní.[38]

4.6.3 Technologické problémy

Technologie tvoří podpůrnou infrastrukturu týmu SOC a mohou zahrnovat nesčetné množství komponent, jejichž narušení může mít katastrofální následky. Příkladem může být situace, kdy z nedostatku finančních prostředků nebude mít tým SOC adekvátní nástroje či aplikace, pomocí kterých by byl schopen zasáhnout proti aktuální hrozbě.

Tím, že se činnosti zaměstnanců SOC ve velké míře skládají z opakujících se úkonů, zvyšuje se možnost vyčerpání a vyhoření personálu, což může mít za následek snížení rychlosti detekce a reakce na události. Aby se předešlo těmto problémům, je nezbytná automatizace a integrace procesů jak týmu SOC, tak i dalších součástí organizace.

Mobilní zařízení a jejich zabezpečení jsou dalším aspektem, který nelze při navrhování a budování SOC opomíjet. Zvláštní důraz je pak třeba klást

[38] *The Security Intelligence Handbook: How to Disrupt Adversaries and Reduce Risk With Security Intelligence.* 3rd ed. Annapolis: CyberEdge Group, 2020. [cit. 23.1.2022]. ISBN 978-1-948939-15-7.

na opatření zamezující ztrátu nebo odcizení dat, například pomocí oddělených úložišť nebo šifrování.

4.6.4 Komunikace a spolupráce

V prostředích, jako je SOC, kde je vyvíjen zvýšený tlak na zaměstnance, je zcela zásadní funkční a bezproblémová spolupráce mezi všemi členy týmu. Kromě spolupráce na určitých analytických procesech se může dále jednat o sdílení výsledků s ostatními, efektivní rozdělování úkolů či neméně důležitá zpětná vazba. Kromě toho musí být práce mezi analytiky rozdělena rovnoměrně v závislosti na jejich dovednostech. Nadcházejícím trendem je operativní využívání platforem s funkcemi pro sdílení informací, plánování apod.

Úspěch týmu SOC je založen také na nezbytné a neustálé interakci a komunikaci s ostatními odděleními či složkami organizace. Tým SOC úzce spolupracuje například se správci sítě, technickou podporou, s oddělením pro informační bezpečnost nebo s právním oddělením. To vyžaduje od všech těchto součástí být týmu SOC nápomocny a mít také dostatečný přehled o jeho činnostech, úlohách, funkcích a provozu.

Ke zmírnění dopadů nebo zamezení dalšího šíření bezpečnostní hrozby je zapotřebí rychlé, koordinované a organizované reakce. To platí jak na národní, tak i na mezinárodní úrovni. Proto je důležitá funkční spolupráce všech zainteresovaných stran, která v sobě integruje jak komunikační prostředí, tak širokou škálu funkcí pro spolupráci. Díky tomu může být například všem zúčastněným stranám nabídnuto jednotné řešení bezpečnostní události.

„Dále je nutné rozvíjet spolupráci i se soukromým sektorem, především v oblasti vědy a výzkumu.“[39] Přínosem může být například spolupráce s vysokými školami a to nejen na vývoji produktů, ale také při výměně informací či účasti na školeních nebo stážích.

Především v posledních dvou letech, kdy se svět snaží vypořádat s pandemií COVID-19, se ve velkém rozšířilo používání aplikací umožňujících vzdálenou komunikaci, jako je například MS Teams.

[39] *Strategie kybernetické obrany ČR 2018 – 2022* [online]. [cit. 25.11.2021]. Dostupné z: https://vzcr.cz/uploads/46-Strategie-kyberneticke-obrany-CR.pdf

4.6.5 Automatizace

Zvýšení provozní výkonnosti může být docíleno pomocí automatizace konkrétních úkolů. Může se jednat například o zefektivnění složitých procesů, usnadnění přístupu analytiků k datům nebo vytvoření dalších forem týmové komunikace a spolupráce. Pomocí automatizace procesů můžeme například optimalizovat závažnost výstrah, takže se analytici mohou zaměřit nejprve na nejkritičtější události a až poté se zaobírat těmi méně závažnými.

Automatizací opakujících se činností a úkolů lze zmírnit nebo zabránit vyhoření či vyčerpání zaměstnanců SOC.

4.7 SOC a kybernetická bezpečnost v ČR

V posledních letech dochází k exponenciálnímu nárůstu kybernetických útoků jak ve světě, tak v České republice nevyjímaje. Příkladem může být kybernetický útok na nemocnici v Benešově v roce 2019, jejíž zaměstnanci byli dokonce nuceni zrušit plánované zákroky nebo využít služeb jiných zařízení. Obavy z této formy zločinu také sílí s tím, jak se stále více zařízení připojuje do internetu. Situaci ještě více umocnila pandemie COVID-19, v jejímž průběhu vzrostl skokově počet uživatelů využívajících služeb celosvětové sítě.

Možným řešením vedoucím k úspěšnému boji proti kyberkriminalitě jsou například investice ve výši 7,5 miliard z Integrovaného regionálního operačního programu (IROP)[40] na podporu kybernetické bezpečnosti informačních systémů veřejné správy, nemocnic, škol či oblasti eGovernmentu.[41]

České společnosti berou problematiku ochrany před kybernetickými útoky vážně. Vlastní kybernetické bezpečnostní operační centrum má například Jihomoravský kraj. Tento SOC má na starost ochranu dat krajského úřadu a jeho příspěvkových organizací[42]. Letiště Praha provozuje SOC, jenž monitoruje své IT systémy a další operace 24/7, a v roce 2021 zahájila společnost ČEZ

[40] Jedná se o jeden z programů, přes které se rozdělují peníze poskytnuté z Evropského fondu pro regionální rozvoj (EFRR).

[41] *Do kybernetické bezpečnosti nemocnic a zabezpečení systémů veřejné správy půjde v příštích šesti letech jen z IROP 7,5 miliardy korun* [online]. [cit. 26.11.2021]. Dostupné z: https://irop.mmr.cz/cs/ostatni/web/novinky/do-kyberneticke-bezpecnosti-nemocnic-a-zabezpeceni?feed=Novinky

[42] *KYBERNETICKÉ OPERAČNÍ CENTRUM BUDE SLOUŽIT I KRAJSKÝM PŘÍSPĚVKOVÝM ORGANIZACÍM* [online]. 30.9.2016 [cit. 26.11.2021]. Dostupné z: https://www.kr-jihomoravsky.cz/Default.aspx?ID=320058&TypeID=2

provoz integrovaného bezpečnostního dohledového centra (iSOC). Nejen výše zmíněné organizace, ale i mnohé další, které zpracovávají důležité personální údaje, zabezpečují chod kritických informačních infrastruktur, řídí letový provoz nebo provoz nemocnice, investují do zabezpečení svých informačních technologií desítky milionů korun. Je tedy zřejmé, že další organizace budou tento trend následovat.

5. PRAKTICKÁ ČÁST

Dříve, než přejdu k samotným příkladům, považuji za důležité zmínit fakt, že pro plnohodnotné využití možností jakéhokoliv ETL nástroje, Pentaho nevyjímaje, je nutné strávit s prací v nástroji desítky, možná i stovky hodin. Uživatel si musí osvojit grafické prostředí, pochopit tvorbu transformací a jobů nebo jejich jednotlivých kroků.

V praktické části práce představím možné využití nástroje Pentaho pro automatizaci reálných procesů probíhajících v prostředí SOC.

Prvním příkladem je proces informování vedoucího směny SOC o nepřiděleném tiketu[43] v tiketovacím systému Jira a to prostřednictvím komunikačního nástroje Rocket.Chat[44]. Díky tomu vedoucí směny nebudou muset fyzicky kontrolovat stav o tiketech a navíc budou informováni o jakékoliv změně téměř okamžitě. V nástroji Pentaho bude vytvořena transformace obsahující kroky extrakce dat ze dvou rozdílných zdrojů (Jira a databáze plánu směn), jejich transformace do požadovaných forem dat a nakonec nahrání do nástroje Rocket.Chat, jenž zajistí odeslání zprávy vedoucímu směny.

Ve druhém příkladu bude vytvořen job, jehož hlavním cílem je porovnat data nacházející se ve dvou rozdílných zdrojích (QRadar[45] a MISP[46]). Pro tento typ operace je nástroj Pentaho ideálním řešením, jelikož běžné tabulkové procesory nejsou schopny zpracovat tak velké množství dat.[47]

Z důvodu bezpečnostních zásad nejsou v příkladu zobrazeny některé údaje (především URL, přihlašovací údaje atd.), nebo jsou nahrazeny smyšlenými. Z důvodu lepší přehlednosti jsou defaultní názvy kroků (v závorkách) přejmenovány na mnou zvolená názvy (ve dvojitých uvozovkách).

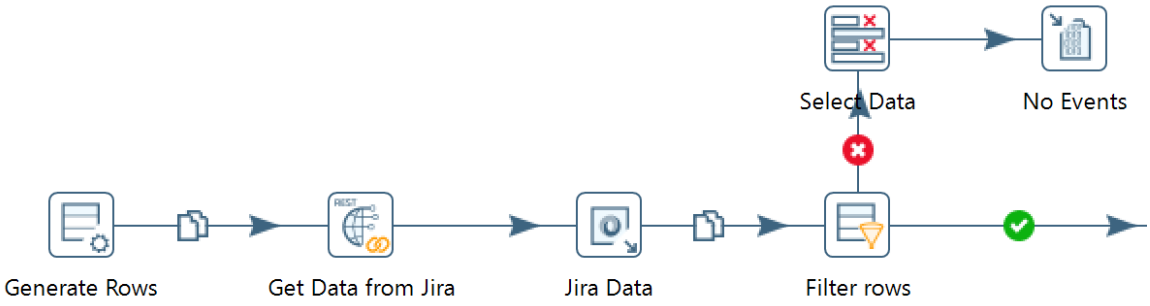
---

[43] Tiketem může být například vygenerovaná bezpečnostní událost vyžadující okamžité řešení pracovníkem SOC.
[44] Rocket.Chat je open-source plně přizpůsobitelná komunikační platforma vyvinutá v JavaScriptu pro organizace s vysokými standardy ochrany dat.
[45] Nástroj QRadar primárně shromažďuje data z protokolů (logů) organizace, jejích síťových zařízení, hostitelských aktiv, operačních systémů, aplikací, zranitelností a aktivit a chování uživatelů.
[46] MISP je softwarové řešení s otevřeným zdrojovým kódem pro shromažďování, ukládání, distribuci a sdílení indikátorů kybernetické bezpečnosti a hrozeb souvisejících s kybernetickou bezpečností.
[47] Jak jsem již dříve zmínil, maximální množství řádků jednoho listu MS Excel je 1 048 576. V tomto příkladu však budou zpracovávány i desítky milionů řádků.

5.1 Příklad č. 1: Zaslání zprávy vedoucímu směny SOC

První transformace je tou nejobsáhlejší a nejobtížnější ze všech zmíněných příkladů. Proto bude její popis rozdělen do několika na sebe navazujících částí, jež dohromady tvoří jednotný celek. Jeho finální podoba bude zobrazena v závěru tohoto příkladu. Transformace začíná procesem extrakce dat z tiketovacího systému Jira (viz obrázek č. 1). V drtivé většině případů je při tvorbě transformací počátečním bodem krok Generate Rows. V tomto kroku uživatel definuje veškeré vstupní informace, které jsou následně použity v dalších krocích transformace. Jedná se například údaje typu „Headers“ či cesty k souborům či adresářům.

Pro získání dat z prostředí Jira jsem použil krok „Get Data from Jira“ (Rest Client) a to pomocí URL požadavku a HTTP metody GET[48]: „https://*jira.xy*/rest/api/latest/search?jql=(project=POC+or+project=SIM)+AND+assignee+IS+EMPTY+AND+created+%3E=-7m“. Zkratka „jql“ v URL značí Jira Query Language a jde o jeden ze způsobů, kterým se lze dotazovat na data v Jira. Dotaz zní zjednodušeně následovně: V databázi Jira hledej tikety (POC nebo SIM), které nemají přiděleny řešitele (Assignee is Empty) a jsou vytvořeny v posledních 7 minutách. Výstupy jsou údaje definované v kroku „JSON input“ (Jira Data). V tomto případě nás zajímá, zda existuje nepřiřazený tiket a pokud ano, tak číslo tohoto nepřiděleného tiketu.

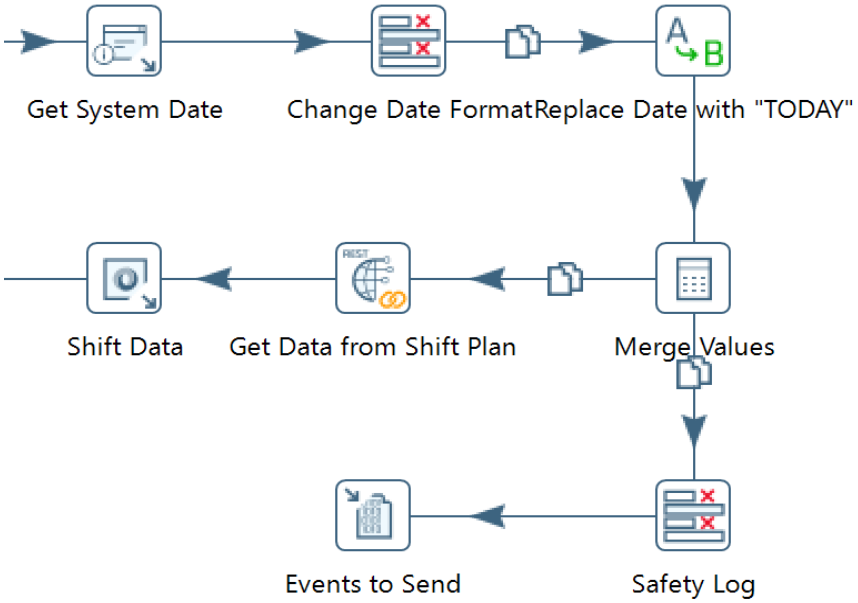


Obrázek č. 1: Kroky extrakce dat z Jira (zdroj: nástroj Pentaho)

Pokud by neexistoval nepřiřazený tiket, byla by celá úloha v tuto chvíli ukončena a událost zaznamenána v kroku „No Events“ (Write to log).

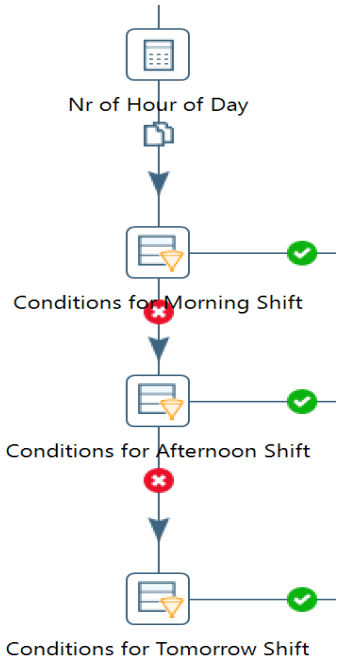
[48] Pomocí HTTP metody GET jsou vyžadována data ze zadaného zdroje.

V našem případě ale proces pokračuje dále (viz obrázek č. 2), jelikož byl nalezen nepřiřazený tiket (evidovaný např. pod ID „SIM-111“ a nacházející se např. na URL „https://jira.xy/project/SIM-111“), o kterém potřebujeme informovat vedoucího směny. Z důvodu rozložení směn v organizaci na ranní a odpolední je nutné vyhledat příslušného pracovníka v databázi plánu směn. Za tímto účelem musíme nejprve definovat datum hledání pro aktuální den a tento importovat do URL, čímž získáme požadavek: https://*domena.xy*/smeny?datum=**yyyy-mm-dd**. Výstupem budou údaje obsahující typ směny (ranní, odpolední) a jmenný seznam pracovníků těchto směn (viz krok „Shift Data“ na obrázku č. 2).



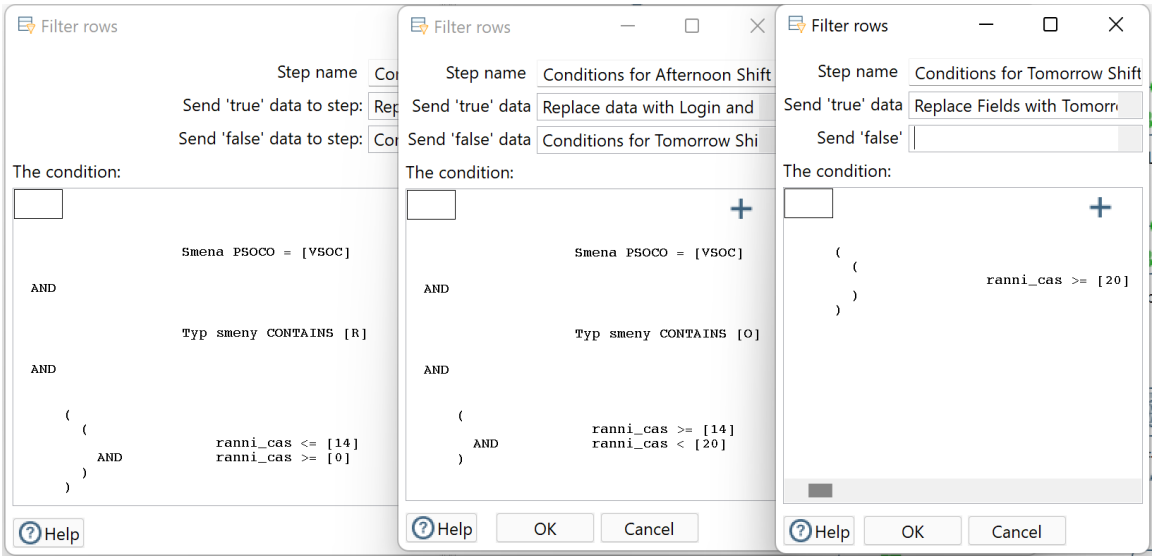
Obrázek č. 2: Kroky pro extrakci dat z databáze plánu směn (zdroj: nástroj Pentaho)

Jelikož jsou směny příslušníků SOC rozděleny do rozdílných časových úseků (ranní směna – 7:00 až 14:00 hod., odpolední směna – 14:00 až 20:00 hod.), je nutné specifikovat tyto podmínky, na základě kterých bude informován konkrétní pracovník směny. Pro výpočet hodin je použit krok „Nr of Hour of Day“ (Calculator), díky kterému získáme hodnoty 1 až 24, jež budou použity pro stanovení podmínek (viz kroky na obrázku č. 3 začínající slovem „Conditions“).



Obrázek č. 3: Stanovení podmínek pro určení konkrétního pracovníka směny v krocích (zdroj: nástroj Pentaho)

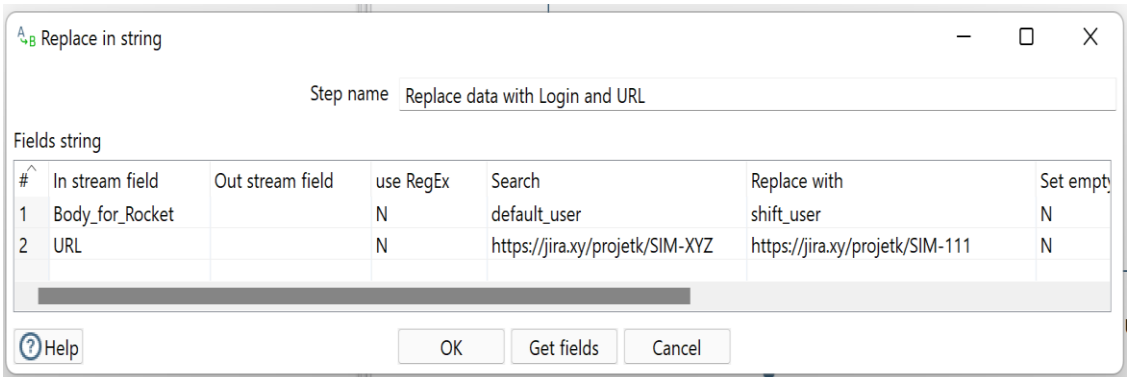
Jednotlivé podmínky jsou podrobně znázorněny na obrázku č. 4. Vyjadřují typ směny (VSOC) a zda se jedná o ranní (R) nebo odpolední (O) směnu. Podmínka v kroku „Conditions for Tomorrow Shift“ (okno v pravé části obrázku) se aplikuje v případě, že nepřiřazený tiket bude generován po 20. hodině, a o jeho vytvoření bude vyrozuměn pracovník směny ranní dne následujícího, aby byla zaručena kontinuita procesu předávání informací.



Obrázek č. 4: Stanovení podmínek pro určení konkrétní směny – nastavení (zdroj: nástroj Pentaho)

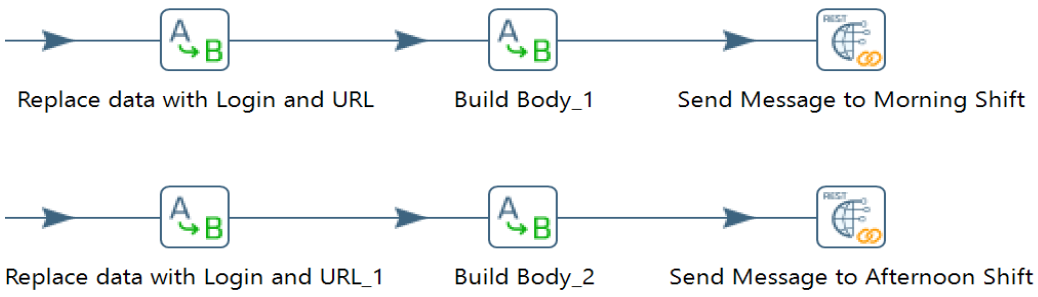
V předchozích krocích jsme získali data a informace ze zdrojů o existujícím tiketu, který má nepřiřazeného řešitele a o konkrétních příslušnících jednotlivých směn. Díky tomu máme k dispozici číslo tiketu (SIM-111) a uživatelské jméno (shift_user), které poslouží v kroku „Replace data with Login and URL“ (Replace in string) jako proměnné hodnoty, jimiž nahradíme údaje obsažené v počátečním kroku celé transformace, v kroku „Generate Rows“. Jak tato náhrada probíhá, je znázorněno na obrázku č. 5.

V tomto kroku stanovujeme, které defaultní položky (na obrázku ve sloupci „In stream field“ a „Search“) mají být nahrazeny daty získanými v předešlých krocích (sloupec „Replace with“). Nastavení polí lze vyložit jako: v poli „Body_for_Rocket“ vyhledej údaj „default_user“ a tento nahraď údajem „shift_user“ definovaným v poli „Replace with“. Stejný proces se provede s údaji uvedenými ve druhém řádku obrázku.



Obrázek č. 5: Nastavení kroku „Replace data with Login and URL“. Záměna proměnných: "user" a "URL" (zdroj: nástroj Pentaho)

Finální fáze procesu odeslání zprávy vedoucímu směny je znázorněna na obrázku č. 6.



Obrázek č. 6: Proces odeslání zprávy o nepřiřazeném tiketu pracovníku ranní/odpolední směny (zdroj: nástroj Pentaho)

V komplikovanějších procesech je možno pro zpracování dat v jednotlivých krocích transformace využít regulárních výrazů. S jejich pomocí lze buďto vyhledávat data ve složitějších řetězcích nebo provádět manipulaci s textem jeho záměnou nebo přeměnou v jiný. V některých případech je použití regulárních výrazů tou jedinou cestou, jak dosáhnout kýženého výsledku.

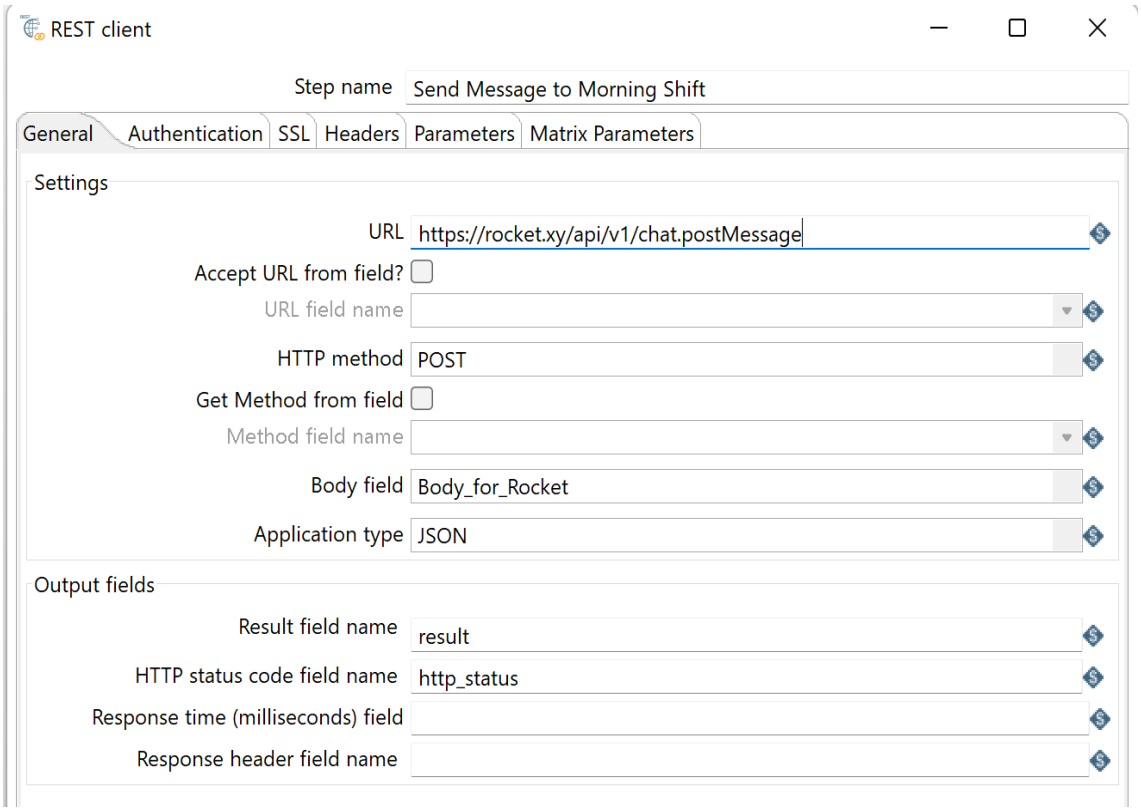
Důležitým krokem je vytvoření těla HTTP zprávy (z anglického HTTP message body), které se v mém příkladu nachází na obrázku č. 5 v prvním řádku pod položkou „Body_for_Rocket“ a dále například v krocích „Send Message to Morning Shift“ nebo „Send Message to Afternoon Shift“ (REST client) v řádku „Body field“ na obrázku č. 7. Ten zobrazuje další položky pro nastavení HTTP požadavku využívajícího pro dorozumívání mezi klientem a serverem protokol API[49]. Jedná se o smluvený způsob zasílání dat s jasně danou strukturou.

Požadavek v nastavení „Rest client“ je tvořen:

- URL, kterou je „https://rocket.xy/api/v1/chat.postMessage“,
- HTTP metodou POST[50],
- polem „Body field“, kterým je v mém příkladu formát: { "channel": "@shift_user", "text": "Neprirazena udalost v Jira: https://jira.xy/browse/SIM-111"} a
- polem „Application type“, kterým je formát JSON[51].

Ve většině případů je ještě potřeba doplnit další údaje v kartách Authentication, SSL a především Headers, kterými mohou být například přihlašovací údaje ke klientskému serveru nebo dodatečné informace týkající HTTP požadavku.

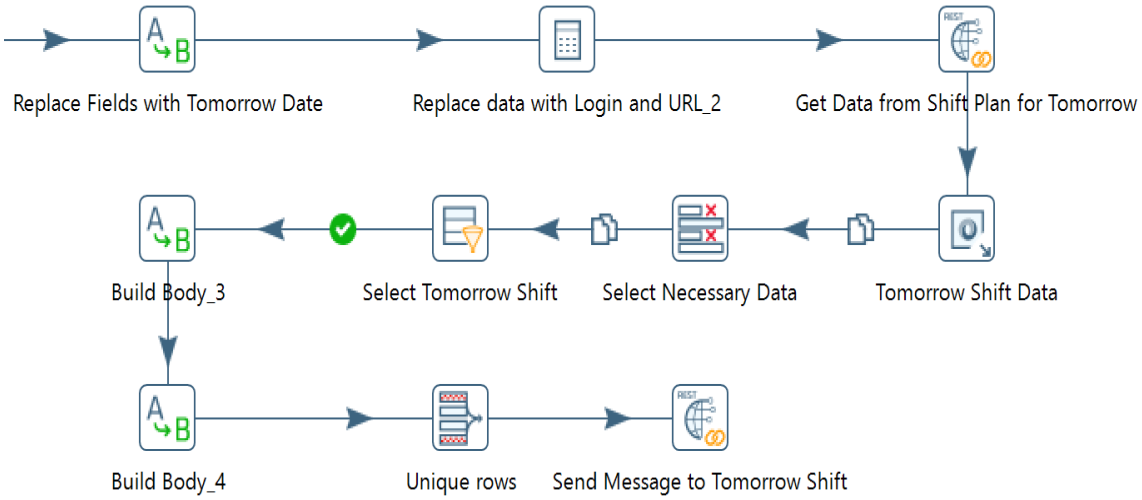
[49] API je soubor procedur, funkcí, protokolů a knihoven, který je využíván programátory v rámci tvorby aplikací a softwaru.
[50] Kromě HTTP metody POST existují další, například PUT, DELETE, TRACE nebo GET. Kupříkladu rozdíl mezi metodou POST a GET je v tom, že pomocí GET většinou data vyžadujeme, kdežto příkaz POST data v cíli mění nebo do cíle zasílá.
[51] JSON je způsob zápisu dat nezávislý na počítačové platformě, určený pro přenos dat, která mohou být organizována v polích nebo agregována v objektech. Objekty jsou tvořeny páry ve formátu index:hodnota, přičemž index je konstantní a hodnota je proměnná. V mém příkladu jsou párovými objekty channel:@shift_user a text:Neprirazena udalost v Jira: https://jira.xy/browse/SIM-111.



Obrázek č. 7: Zobrazení jednotlivých položek nastavení kroku Rest client (zdroj: nástroj Pentaho)

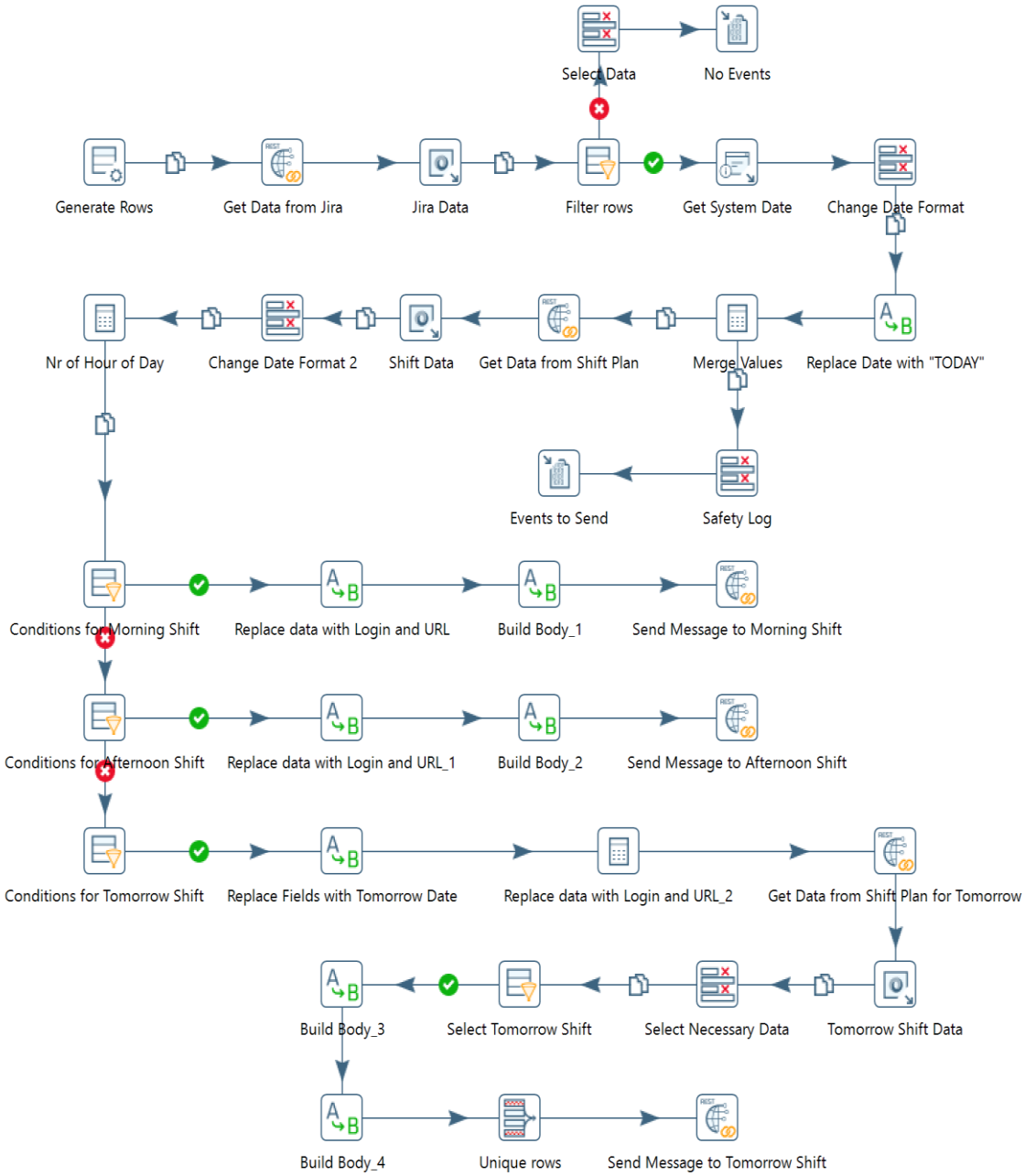
V případě, že jsou veškerá nastavení správná, vyšle krok Rest client požadavek na odeslání zprávy příjemci, tedy příslušníkovi směny. Ten následně provede přiřazení tiketu odpovědné osobě.

Vzhledem ke způsobu rozložení směn, tedy nepřítomnosti směny na pracovišti po 20. hodině, bylo nutné počítat i s podmínku pro tuto variantu. Řešením jsou jednotlivé kroky transformace následující po kroku „Conditions for Tomorrow Shift“ (Filter rows). Opět je potřeba získat data o pracovnících z plánu směn, tentokrát však o těch z ranní směny dne následujícího a sestavit zbývající kroky transformace. Jejich popisu není potřeba, protože se liší jen vstupními daty, jež jsou popsány v předešlých odstavcích. Pro úplnost jsou znázorněny na obrázku č. 8.



Obrázek č. 8: Proces odeslání zprávy o nepřiřazeném tiketu pracovníku směny následujícího dne (zdroj: nástroj Pentaho)

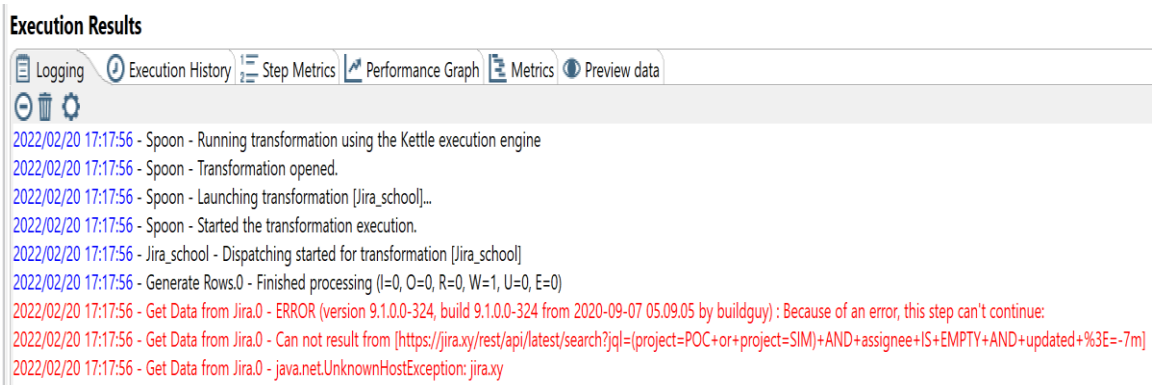
V tento okamžik je transformace kompletní a její podoba je znázorněna na obrázku č. 9. Před samotným nasazením transformace do „ostrého“ provozu je zapotřebí otestovat její funkčnost a bezchybnost. Faktem je, že testovací fází prochází transformační proces od samého počátku. Jednotlivé kroky jsou sestavovány a především testovány v pořadí znázorněném na obrázcích. Jak jsem již zmínil, je důležité si každý krok nejprve důkladně promyslet. Musíme si stanovit cíl a způsob, jakým jej chceme dosáhnout a především vyčlenit čas potřebný na sestavení úloh. V tomto případě se jedná o nejnáročnější příklad této práce, jelikož k jejímu sestavení je vyžadováno znalostí tří odlišných zdrojů dat, postupů převodu dat do rozličných formátů a důkladného stanovení podmínek. Čas potřebný k sestavení kompletního příkladu je obtížné konkrétně definovat, ale odvíjí se od znalostí tvůrce. Může se jednat o dobu v rozmezí několika hodin až dní. Naopak, z důvodu zpracování minimálního množství dat je čas běhu úlohy měřitelný v řádu jednotek sekund. To, že jsou členové týmu SOC o hrozící události informováni téměř okamžitě, je pro zajištění kybernetické bezpečnosti klíčové.



Obrázek č. 9: Zobrazení finální podoby transformace (zdroj: nástroj Pentaho)

Za účelem podávání zpráv o chybovosti či funkčnosti jednotlivých kroků transformace disponuje nástroj Pentaho vlastním logovacím mechanismem. Logy jsou zobrazovány v textové podobě a poskytují užitečné informace o problému (viz obrázek č. 10). To značně usnadňuje tvorbu, nastavení a sestavení jednotlivých kroků. V příkladu můžeme vidět, že v kroku nelze pokračovat z důvodu chyby, kterou je neznámá doména „jira.xy“ (řádky s červeným písmem začínající „ERROR“. Díky této informaci můžeme chybu snadno napravit zadáním správné

domény. Tímto způsobem pokračujeme s každým krokem transformace, dokud nejsou vyloučeny všechny možné problémy a chyby.



Obrázek č. 10: Příklad LOGu s informací o chybné úloze (zdroj: nástroj Pentaho)

5.2 Příklad č. 2: Porovnání dat ze dvou zdrojů (QRadar a MISP)

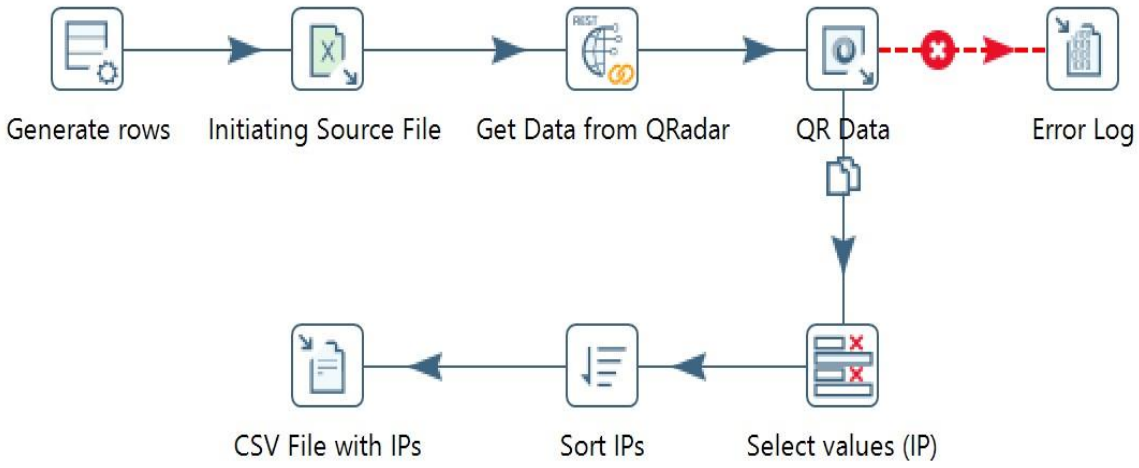
Předpokládejme, že máme sadu dat, v našem případě v podobě desítek milionů IP adres, které se nachází ve dvou rozdílných zdrojích, tedy v QRadaru a MISPech. Cílem úlohy je extrahovat definované množství IP adres z databáze QRadaru a ověřit, zda se vyskytují v MISP databázích, v jakém množství a zda jde o jedinečné výskyty či nikoliv.

Příklad se skládá z jednoho Jobu, který je tvořen čtyřmi transformacemi (obrázek č. 11). V první transformaci jsou nejprve data extrahována z QRadaru, poté jsou transformována do souborů, jež slouží jako vstupní data pro porovnání v MISPech (třetí transformace) a v poslední transformaci jsou získaná data seskupena a setříděna dle stanovených kritérií. Kromě IP adres se v databázích nachází i další údaje související se síťovým provozem, například URL adresy nebo domény.

Obrázek č. 11: Job tvořený čtyřmi transformacemi (Start je pouze iniciační bod) (zdroj: nástroj Pentaho)

První transformace (obrázek č. 12 na další stránce), pod názvem „Search for IP in QR“, je primárně tvořena procesem sestávajícím z extrakce dat (IP adres)

z databáze QRadaru, konkrétně z referenčních dat pomocí API. Referenční data jsou v tomto případě tvořena daty z interních nebo externích zdrojů, která je možné použít ve vyhledávání, filtrech, podmínkách pro testování pravidel a odpovědích na pravidla QRadar.[52] Výsledkem této transformace je seznam se zdrojovými IP adresami uložený ve formátu CSV („CSV File with IPs“). IP adresy mohou být předem seřazeny nebo roztříděny dle zdrojů (krok „Sort IPs“). CSV soubor jako výstupní formát tohoto procesu jsem zvolil z toho důvodu, že existuje možnost využití dat i k jinému účelu. V případě většího množství dat je vhodnější využít funkce „kopírování“ výstupů jedné transformace do vstupů transformace druhé. V neposlední řadě spočívá výhoda v tom, že je možné spouštět jednotlivé transformace samostatně, zejména v případech, kdy víme, že se nezměnily vstupní data v jednotlivých transformacích. Lze tak přeskočit úvodní procesy extrakce dat ze zdrojů a místo toho přejít rovnou k úloze jejich vyhledání („Search for IP in MISP“).

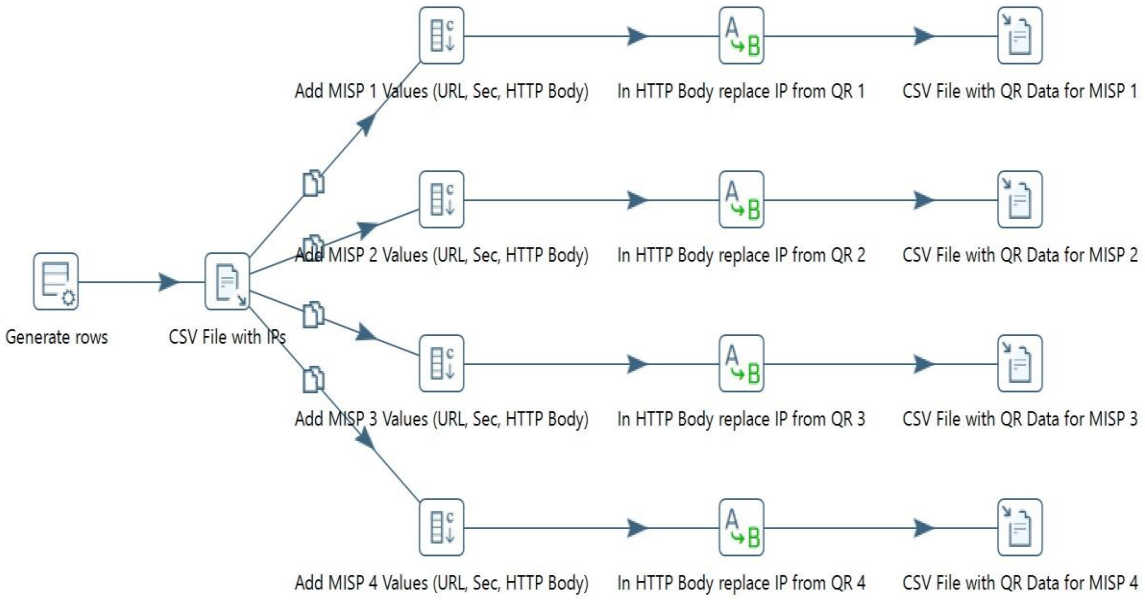


Obrázek č. 12: Kroky transformace „Search for IP in QR“. Vyhledání dat v QRadaru, jejich roztřídění a vytvoření CSV souboru s IP adresami (zdroj: nástroj Pentaho)

V transformaci „Build Source Files“ zobrazené na obrázku č. 13 jsou transformovány potřebné údaje nutné ke kompilaci těla HTTP zprávy pro hledání IP adres v jednotlivých databázích MISP (v mém příkladu 1 až 4). Výstupy jsou

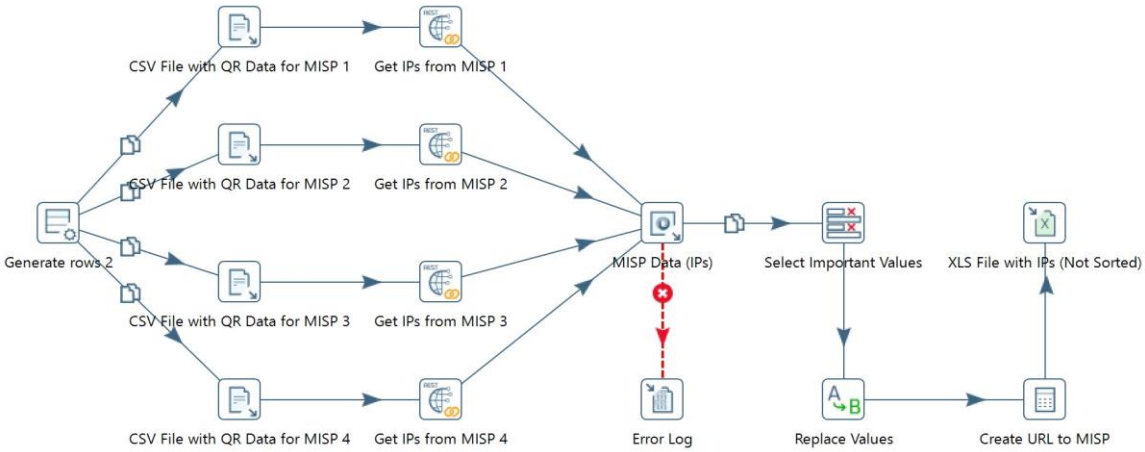
[52] *Using reference data in QRadar* [online]. [cit. 24.2.2022]. Dostupné z: https://www.ibm.com/docs/en/qsip/7.3.2?topic=administration-using-reference-data-in-qradar

poté další CSV soubory („CSV File with QR Data for MISP 1 až 4“). Ty obsahují mimo jiné bezpečnostní tokeny, které slouží jako jedinečné identifikátory uživatele nutné pro jeho přihlášení do databáze.



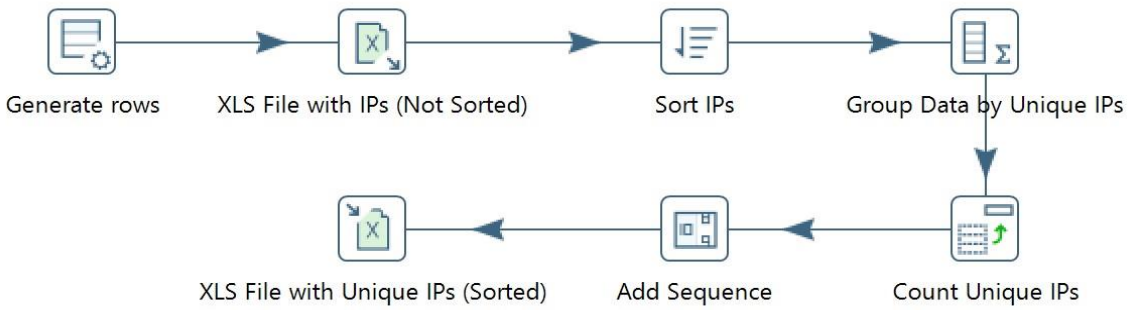
Obrázek č. 53: Kroky transformace „Build Source Files“. Proces kompilace dat potřebných pro vyhledání IP adres v MISP databázích (zdroj: nástroj Pentaho)

Na obrázku č. 14, který je možné nalézt na následující stránce, je zobrazena grafická podoba transformace „Search for IP in MISP“ složená z kroků, jejichž úlohou je prohledat databáze MISPů 1 až 4, zda se v nich nachází IP adresy získané v první transformaci. V kroku „Create URL to MISP“ jsou vytvořeny URL odkazy vedoucí k událostem v MISPech, jež souvisí s nalezenými IP adresami. Tyto informace jsou nahrány do tabulkového dokumentu v posledním kroku transformace, „XLS File with IPs (Not Sorted)“.



Obrázek č. 64: Transformace „Search for IP in MISP“. Proces vyhledání IP adres v databázích MISPů a vytvoření XLS souboru s jejich výsledky (zdroj: nástroj Pentaho)

Jedna IP adresa se může v jednotlivých MISP databázích vyskytovat několikrát. Protože je cílem příkladu nalézt pouze jedinečné IP adresy vyskytující se jak v databázích MISPů, tak QRadaru, je finálním krokem příkladu čtvrtá transformace. Ta seskupí shodující se IP adresy do jedné. Výsledkem je XLS tabulka s jedinečnými IP adresami a počtem jejich výskytů v MISP databázích seřazenými dle zadaných kritérií. Jednotlivé kroky transformace „Group by Unique IP“ jsou zobrazeny na obrázku č. 15.

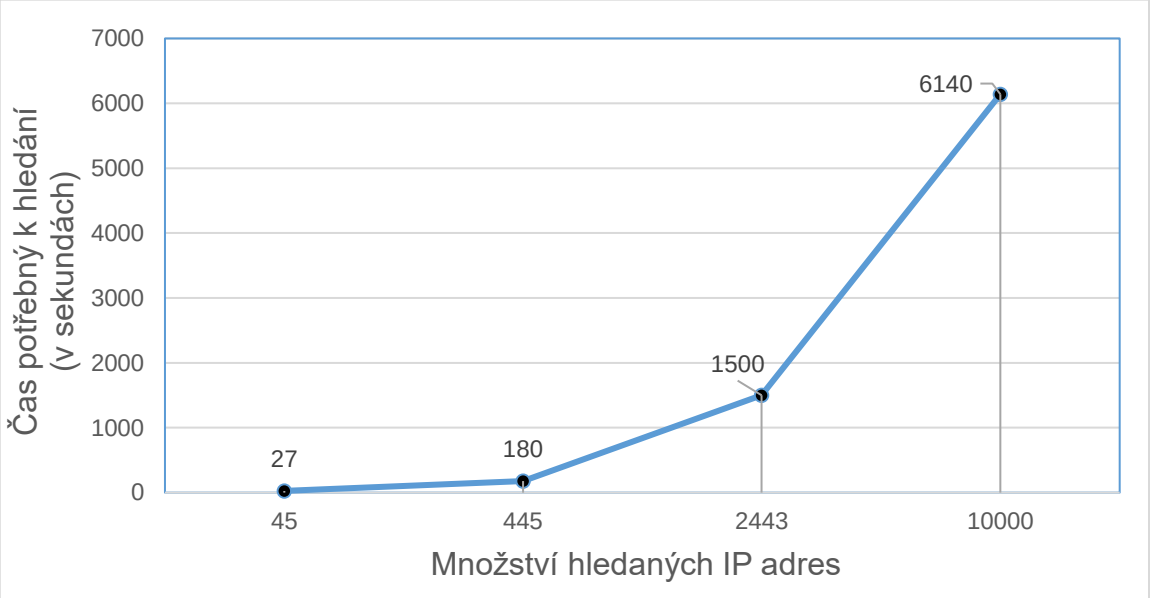


Obrázek č. 75: Transformace „Group by Unique IP“. Seskupení nalezených IP adres v MISP databázích do jedinečného údaje (zdroj: nástroj Pentaho)

Procesy plynoucí z tohoto jobu může SOC využít například k vyhodnocování relevantnosti svých zdrojů, tedy aby bylo možné lépe určit, které zdroje poskytují relevantnější informace o nebezpečích v kybernetickém prostoru.

Jde také o časově náročnou úlohu. Celý proces je závislý na tom, s jakou rychlostí jsou jednotlivé zdroje schopny vyhledávat data. Celý proces tak může trvat i několik hodin (viz graf č. 1).

Zatímco hledání 45 IP adres probíhalo přibližně po dobu 27 sekund, hledání 2 443 IP adres pak trvá přibližně 1 500 sekund, tedy 25 minut. Z výsledků lze jednoduše spočítat, že hledání například 10 000 IP adres by trvalo přibližně 6140 sekund, tedy 1 hodinu a 42 minut.

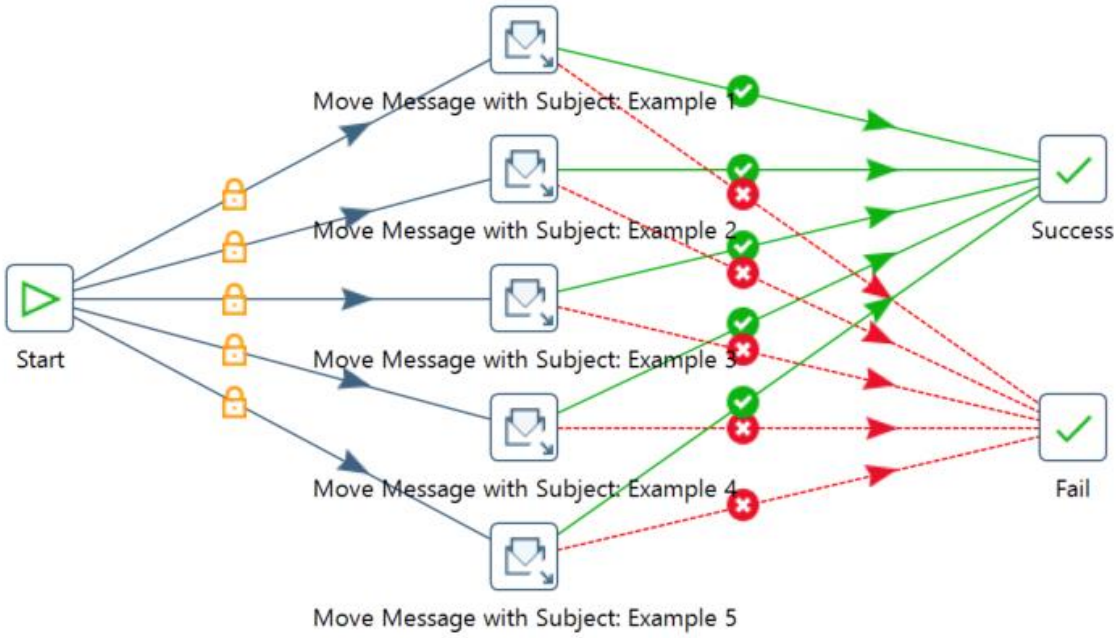


Graf č. 1: Závislost množství IP adres na čase potřebného k jejich vyhledávání

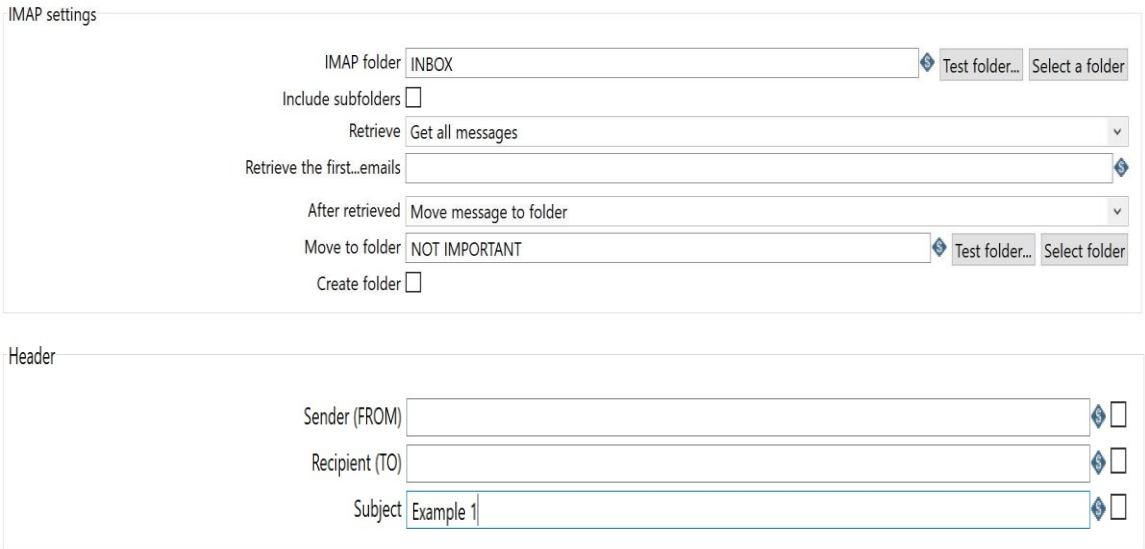
5.3 Příklad č. 3: Přesun e-mailových zpráv

Třetím příkladem je job skládající se z kroků, s jejichž pomocí jsou e-mailové zprávy obsahující předmět (Subject) „Example 1 až 4“ přesunuty ze složky INBOX do složky NOT IMPORTANT (viz obrázky č. 16 a 17). Toho je samozřejmě možné dosáhnout i pomocí nastavení e-mailových účtů, například v nastavení poštovních klientů (např. MS Outlook) nebo skrze webová rozhraní. Automatizovanou úlohu tak lze uplatnit v případě, pokud výše uvedená nastavení nejsou přístupná a to zejména z důvodu používání nekompatibilních platforem či bezpečnostních zásad. Díky této úloze lze také nakládat s e-mailovými zprávami způsobem, kterého jinak není možné dosáhnout. Příkladem může být automatizace přesouvání příloh zpráv na pevné úložiště. Výhodou použití ETL nástroje

PENTAHO je, že poskytuje detailní informace o manipulaci s e-maily nebo o případných chybách či neúspěších (viz kroky „Success“ a „Fail“).



Obrázek č. 16: Příklad kroků přesunutí e-mailových zpráv do jiné složky na základě předmětu zprávy (zdroj: nástroj Pentaho)



Obrázek č. 17: Podrobné nastavení kroku „Move Message with Subject: Example 1“ (zdroj: nástroj Pentaho)

5.4 Vyhodnocení procesů automatizace

Jak bylo již zmíněno v předchozích odstavcích, před samotnou tvorbou transformací nebo jobů je důležité stanovit si cíle a způsoby jejich dosažení.

Na základě vlastní zkušenosti mohu konstatovat, že tato podmínka se však týká celého průběhu tvorby automatizované úlohy. Téměř pro každý krok transformace nebo jobu lze najít alternativní řešení, s jejichž pomocí je možné dosáhnout efektivnějších výsledků. Především v průběhu fáze testování není neobvyklé, že se jednotlivé kroky procesu automatizace musí upravovat nebo měnit za jiné a to zejména v případě, že dojde ke změně u některých vstupních dat. Potom uživateli nezbývá nic jiného, než upravit i většinu následujících kroků, což prodlužuje dobu tvorby celého procesu automatizace.

Pohledem na obrázky uvedené v příkladech výše lze odvodit, že se liší zejména počtem kroků. To, co již není na první pohled zřejmé, je jejich náročnost na sestavení. Jako každý uživatel, i já musel začít s tvorbou jednodušších úloh a navíc se naučit základy programování v rozhraní API nebo porozumět zápisu dat ve formátu JSON. Po získání dostatečných zkušeností a vědomostí lze přejít k tvorbě úloh složitějších. Čas potřebný k sestavení automatizované úlohy v Pentaho nelze přesně stanovit, ale v zásadě se odvíjí především od náročnosti zadané úlohy a zkušeností obsluhy nástroje. Zatímco úlohu ve třetím příkladu je možné sestavit během několika minut, sestavení úloh v prvním a druhém příkladu se může protáhnout i na několik hodin. Navíc je potřeba přičíst čas potřebný k jejich testování.

Důležitou fází „života“ automatizované úlohy je proces testování a to nejlépe ještě před tím, než dojde k jejímu nasazení do reálného provozu. V rámci testování je nutné ověřit data, která jsou extrahována, tj. zda jsou správně zkopírována, poté transformační logiku, tj. zda je správně aplikována filtrace dat nebo jejich čištění a nakonec nahrání dat do cíle. Tato problematika byla také řešena v konkrétní situaci v příkladu č. 1.

Jednotlivé automatizované úlohy v příkladech lze v jejich konečné fázi spouštět bez lidského zásahu a až na 2. příklad jsou za tímto účelem vytvořeny. V tomto příkladu se jedná o jednorázový proces vytvořený za účelem získání statistických údajů.

Vyzdvihnout musím podporu nástroje Pentaho ze strany Hitachi. U většiny kroků v transformacích a jobech je možné zobrazit podrobnou nápovědu k jejich účelu nebo funkcím. Navíc je součástí instalačního balíčku nástroje Pentaho poměrně velké množství příkladů transformací a jobů, které může uživatel využít

jako výchozí bod pro vlastní úlohy a ty dále rozšiřovat dle svých představ a potřeb. V případě, že ani s touto nápovědou není obsluha nástroje schopna sestavit funkční úlohu, může využít rad ostatních uživatelů, kteří sdílí své zkušenosti na různých internetových stránkách nebo přímo na oficiálním „komunitním fóru“ Hitachi Vantara[53].

[53] Dostupné na: https://forums.pentaho.com/

ZÁVĚR

V úvodu práce jsem představil jedny ze základních procesů a činností, které jsou nedílnou součástí efektivního fungování organizace, jejíž primárním cílem a úkolem je zajišťování bezpečnosti v kyberprostoru. Za tímto účelem je potřeba vytvořit funkční a spolehlivý systém řízení bezpečnosti a to nejlépe tím způsobem, že organizace ve svém prostředí aplikuje organizační a technická opatření. Ta jsou tvořena především personálem včetně procesů souvisejících s řízením lidí, incidentů nebo spolupráce, ale také technologiemi, jež poskytují bezproblémový provoz. Jde o výčet procesů, které, pokud jsou správně nastaveny, zvyšují a upevňují bezpečnostní statut organizace. V oblasti kybernetické bezpečnosti jde o prvořadou vlastnost.

Kybernetické útoky již dávno nejsou pouhými náhodnými událostmi. Naopak, vyskytují se v čím dál větší míře a s různě závažnými následky. Není proto překvapením, že je snahou organizací těmto událostem v kyberprostoru předcházet. Jedním z možných řešení může být například vybudování a provozování bezpečnostních operačních center. Jejich týmy složené z bezpečnostních analytiků dohlíží na veškerou aktivitu v provozovaných komunikačních a informačních systémech za účelem odhalování a identifikace potenciálních bezpečnostních hrozeb a zabránění jejich dalšímu šíření. Konkrétně jsou úkoly SOC, jeho složení nebo hlavní výzvy, jimž musí čelit, popsány v teoretické části práce. Díky tomu je možné získat alespoň základní představu o fungování a úloze SOC.

K tomu, aby mohl tým SOC hrozby nejen identifikovat, ale také analyzovat anebo hlásit případné zjištěné zranitelnosti, potřebuje kromě adekvátních zkušeností a znalostí především účinné nástroje, které nejen že budou schopny řešit bezpečnostní události v reálném čase, ale také zlepší bezpečnostní pozici celé organizace.

Cílem této práce bylo představit možnosti využití ETL nástrojů pro automatizaci procesů v prostředí SOC. Konkrétně byly v její praktické části uvedeny příklady úloh, jež byly vytvořeny pomocí nástroje Pentaho a které může tým SOC využít k zefektivnění svých činností a úkolů. Přínosem práce může být také to, že zmíněné příklady byly vytvořeny na základě faktických požadavků a preferencí a lze je tedy použít v reálném provozu.

Využití automatizovaných úloh vytvořených nástroji ETL je čím dál častějším jevem. Jsou běžnou a nedílnou součástí každé vyspělé organizace působící v oblasti kybernetické bezpečnosti a jak je možné vidět na mnou zvolených příkladech, nemusí být vždy použity ke zpracování velkého objemu dat. Naopak, nástroje ETL jsou dnes již schopné automatizovat činnosti, úlohy nebo procesy, které jsou závislé spíše na rychlosti zpracování a dále na přesnosti nebo bezpečnosti. Díky tomu, že automatizované úlohy ve většině případů fungují nezávisle a samostatně, bez jakéhokoliv lidského zásahu, se mohou týmy SOC věnovat činnostem vyžadujících lidský úsudek, například analýze bezpečnostních událostí.

Vytvořením automatizované úlohy však práce na ní nekončí. I nadále je potřeba jejího testování a údržby. Jedná se o nutné kroky, které pomáhají udržet tyto úlohy funkční po celou dobu jejich používání. Ve většině případů se totiž jedná o softwarové nástroje, které je přinejmenším z bezpečnostních důvodů nutné pravidelně aktualizovat či záplatovat. Stejně tak se musí vyvíjet a vzdělávat odborníci, kteří tyto úlohy vytváří, jelikož je téměř jisté, že se budou objevovat další procesy, činnosti nebo úkony vhodné pro automatizaci.

Kombinací informací z teoretické i praktické části práce lze snadno usoudit, čeho lze pomocí ETL nástrojů dosáhnout a jak významným způsobem mohou pomoci rozvoji organizace. Vždy však záleží na výběru vhodného procesu určeného k automatizaci a správného nástroje ETL. V teoretické části práce jsem provedl analýzu funkcí, požadavků a hodnot, na jejichž základě se lze při výběru ETL nástroje rozhodovat, ale i na základě vlastních zkušeností si dovolím tvrdit, že bude organizace využívat více ETL nástrojů současně.

Pomocí správného uvažování a modelování úloh může organizace dosáhnout lepších výkonů, vyšší bezpečnosti anebo také minimalizace nákladů. ETL nástroje jsou schopny změnit způsob, jakým procesy proudí uvnitř organizace.

SEZNAM POUŽITÝCH ZKRATEK

BI – Business Intelligence
CCTV – Supervisory Control and Data Acquisition (bezpečnostní kamerové systémy)
CSV – Comma-separated values (hodnoty oddělené čárkami)
EPS – Elektronická požární signalizace
EZS – Elektronická zabezpečovací signalizace
FTP – File Transfer Protocol (protokol pro přenos souborů)
HTTP – Hypertext Transfer Protocol (internetový protokol pro komunikaci WWW servery)
IROP – Integrovaný regionální operační program
iSOC – Integrované bezpečnostní dohledové centrum
JQL – Jira Query Language (programovací jazyk Jira)
JSON – JavaScript Object Notation (JavaScriptový objektový zápis)
MISP – Malware Information Sharing Platform (platforma pro sdílení informací o hrozbách)
NATO – North Atlantic Treaty Organization (Severoatlantická aliance)
PDI – Pentaho Data Integration
PGP – Pretty Good Privacy (dost dobré soukromí)
POC – Proof of Concept (důkaz konceptu)
SCADA – Supervisory Control and Data Acquisition (dispečerské řízení a sběr dat)
SIEM – Security Information and Event Management (Management bezpečnostních informací a událostí)
SIM – Security Information Management (Řízení bezpečnosti informací)
SOC – Security Operation Center (Bezpečnostní operační centrum)
URL – Uniform Resource Locator (jednotný lokátor zdroje)

SEZNAM POUŽITÉ LITERATURY

MONOGRAFIE

[1] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. [cit. 13.2.2022]. ISBN 978-80-88168-15-7.

[2] MUNIZ, Joseph, Gary MCINTYRE a Nadhem ALFARDAN. *Security Operations Center: Building, Operating and Maintaining your SOC*. Indianapolis, USA: Cisco Press, 2015. ISBN 978-0-13-405201-4.

[3] *The Security Intelligence Handbook: How to Disrupt Adversaries and Reduce Risk With Security Intelligence.* 3rd ed. Annapolis: CyberEdge Group, 2020. [cit. 23.1.2022]. ISBN 978-1-948939-15-7.

ZÁKONNÁ ÚPRAVA A IAŘ (INTERNÍ AKTY ŘÍZENÍ)

[4] *AKČNÍ PLÁN K NÁRODNÍ STRATEGII KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY NA OBDOBÍ LET 2021 AŽ 2025* [online]. [cit. 22.1.2022]. Dostupné z: https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/akcni_plan_2021-2025.pdf

[5] *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025* [online]. [cit. 25.1.2022]. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

[6] *Vyhláška č. 432/2011 Sb. Vyhláška o zajištění kryptografické ochrany utajovaných informací* [online]. [cit. 27.1.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2011-432?text=vyhl%C3%A1%C5%A1ky+%C4%8D.+432%2F2011+Sb

[7] *Vyhláška č. 82/2018 Sb., Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)* [online]. [cit. 15.1.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82?text=kybernetick%C3%BD+bezpe%C4%8Dnostn%C3%AD+incident

[8] *Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [online]. [cit. 4.1.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[9] *Zákon č. 289/2005 Sb. Zákon o Vojenském zpravodajství* [online]. [cit. 27.1.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-289#cast4

[10] *Zákon č. 412/2005 Sb., Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti* [online]. [cit. 18.1.2022]. Dostupné z: zakonyprolidi.cz/cs/2005-412

WEBOVÉ STRÁNKY A ELEKTRONICKÉ ZDROJE

[11] *8 Skills All Leadership Trainings Should Teach Managers* [online]. 2019 [cit. 3.11.2021]. Dostupné z: https://www.scienceofpeople.com/leadership-training/

[12] *Do kybernetické bezpečnosti nemocnic a zabezpečení systémů veřejné správy půjde v příštích šesti letech jen z IROP 7,5 miliardy korun* [online]. [cit. 26.11.2021]. Dostupné z: https://irop.mmr.cz/cs/ostatni/web/novinky/do-kyberneticke-bezpecnosti-nemocnic-a-zabezpeceni?feed=Novinky

[13] *Fyzická bezpečnost (technické prostředky a další prvky fyzické bezpečnosti a jejich certifikace): Informace k fyzické bezpečnosti* [online]. [cit. 25.1.2022]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost-technicke-prostredky-a-dalsi-prvky-fyzicke-bezpecnosti-a-jejich-certifikace/1014-informace/

[14] *Key challenges and frustrations of SOC workers* [online]. [cit. 8.11.2021]. Dostupné z: https://www.helpnetsecurity.com/2018/06/06/challenges-soc-workers/

[15] *Kybernetická bezpečnost: Přínosy cvičení* [online]. [cit. 15.1.2022]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/cviceni/prinosy-cviceni/

[16] *KYBERNETICKÁ OBRANA: VOJENSKÉ ZPRAVODAJSTVÍ SE PODÍLÍ NA ZAJIŠŤOVÁNÍ KYBERNETICKÉ OBRANY ČESKÉ REPUBLIKY* [online]. [cit. 26.11.2021]. Dostupné z: https://vzcr.cz/kyberneticka-obrana-46

[17] *KYBERNETICKÉ OPERAČNÍ CENTRUM BUDE SLOUŽIT I KRAJSKÝM PŘÍSPĚVKOVÝM ORGANIZACÍM* [online]. 30.9.2016 [cit. 26.11.2021]. Dostupné z: https://www.kr-jihomoravsky.cz/Default.aspx?ID=320058&TypeID=2

[18] *NATO's flagship cyber defence exercise kicks off in Estonia* [online]. 29.11.2021 [cit. 6.2.2022]. Dostupné z: https://www.nato.int/cps/en/natohq/news_189156.htm?selectedLocale=en

[19] *ORGANIZATIONAL MANAGEMENT* [online]. [cit. 3.1.2022]. Dostupné z: https://www.toolshero.com/tag/organizational-management/

[20] *ROZPRACOVÁNÍ TYPOVÉHO PLÁNU NA POSTUPY PRO ŘEŠENÍ krizové situace NARUŠENÍ BEZPEČNOSTI INFORMACÍ KRITICKÉ INFORMAČNÍ INFRASTRUKTURY: Přínosy cvičení* [online]. [cit. 18.1.2022]. Dostupné z: https://krizoverizeni.plzensky-kraj.cz/Framework/Document.ashx?ID=171617

[21] SAMSON JR., Ron. *Five Security Operations Center Models Compared: Find The Right SOC Model* [online]. 2021 [cit. 11.1.2022]. Dostupné z: https://www.clearnetwork.com/types-of-security-operations-centers-soc/

[22] *Security Operations Center: Centrální bod bezpečnosti* [online]. [cit. 29.1.2022]. Dostupné z: https://www.aec.cz/cz/produkty-a-sluzby/Stranky/soc.aspx

[23] *Strategie kybernetické obrany ČR 2018 – 2022* [online]. [cit. 25.11.2021]. Dostupné z: https://vzcr.cz/uploads/46-Strategie-kyberneticke-obrany-CR.pdf

[24] *The Five Types of Security Operations Center Models* [online]. [cit. 11.1.2022]. Dostupné z: https://arcticwolf.com/resources/briefs-2/security-operations-center-models-2

[25] *The secret of success is to do the common thing uncommonly well!* [online]. 8. 2. 2018 [cit. 28.1.2022]. Dostupné z: https://www.academyofhappylife.com/secret-o-success-common-thing-uncommonly-well/

[26] *The Security Intelligence Handbook: How to Disrupt Adversaries and Reduce Risk With Security Intelligence.* 3rd ed. Annapolis: CyberEdge Group, 2020. [cit. 23.1.2022]. ISBN 978-1-948939-15-7.

[27] *The SOC hiring handbook: Your guide to building and retaining a strong security team* [online]. [cit. 9.11.2021]. Dostupné z: https://logrhythm.com/uk-soc-hiring-handbook/

[28] *Understanding the SOC Team Roles And Responsibilities* [online]. 2021 [cit. 11.11.2021]. Dostupné z: https://www.siemplify.co/blog/understanding-the-soc-team-roles-and-responsibilities/

[29] *Using reference data in QRadar* [online]. [cit. 24.2.2022]. Dostupné z: https://www.ibm.com/docs/en/qsip/7.3.2?topic=administration-using-reference-data-in-qradar

[30] *What is Business Intelligence? Definition, Techniques, Tools and Tips from Experts* [online]. 5.9.2019 [cit. 28.1.2022]. Dostupné z: https://callminer.com/blog/what-is-business-intelligence-definition-techniques-tools-and-tips-from-experts

[31] *WHAT IS ETL?: The Ultimate Guide* [online]. [cit. 9.2.2022]. Dostupné z: https://www.matillion.com/what-is-etl-the-ultimate-guide/