National Czech Programme | eosc

Výstup KB_1

Technická zpráva: Sběr požadavků a návrh architektury systému bezpečnostního monitoringu

Výstup byl vytvořen za podpory Ministerstva školství, mládeže a tělovýchovy a Operačního programu Jan Amos Komenský v rámci projektu Open Science II (reg. č. CZ.02.01.01/00/24_030/0015041).

Spolufinancováno Evropskou unií

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Projekt Open Science II
CZ.02.01.01/00/24_030/0015041
Univerzita Karlova
Ovocný trh 560/5, 116 36 Praha 1
eosc2@ruk.cuni.cz; www.eosc.cz

Manažerské shrnutí

Dokument shrnuje analýzu požadavků bezpečnostního monitoringu vycházejících ze stávajícího stavu Národní repozitářové platformy (NRP) a identifikuje oblasti, ve kterých je vhodné posílit bezpečnostní dohled nad infrastrukturou. Navrhované rozšíření se zaměřuje především na schopnost detailní analýzy síťového provozu, která v současné architektuře chybí, a doplňuje ji o další detekční mechanismy, jako jsou například honeypoty určené k odhalování pokročilých či cílených útoků. Cílem je vytvořit ucelený systém, který umožní nejen sběr a vyhodnocování bezpečnostních událostí, ale také včasnou identifikaci anomálií a potenciálních hrozeb.

V rámci návrhu byla zvolena taková technická řešení, která nevyžadují nákup ani instalaci nového hardwaru a staví na již existujících prvcích infrastruktury. Díky tomu nevznikají nové náklady a návrh je možné realizovat postupně s minimálními zásahy do stávajícího prostředí. Celý koncept staví na open-source technologiích, které umožňují transparentní přizpůsobení potřebám infrastruktury a nezávislost na dodavateli. Tento přístup zároveň umožňuje flexibilní rozšiřování podle budoucích potřeb a kapacit.

Obsah dokumentu

Úvod

Během prvních měsíců řešení projektu OS II byla provedena analýza vznikajícího prostředí Národní repozitářové platformy (NRP), zejména infrastruktury, na níž jednotlivé repozitáře jsou či budou provozovány, a byla provedena analýza požadavků z hlediska kybernetické bezpečnosti a monitoringu.

Tento dokument popisuje výsledky této analýzy, shrnuje zjištěné požadavky, a navrhuje architekturu plánovaného systému pro bezpečnostní monitoring NRP, jehož implementace proběhne ve zbývajícím období řešení projektu.

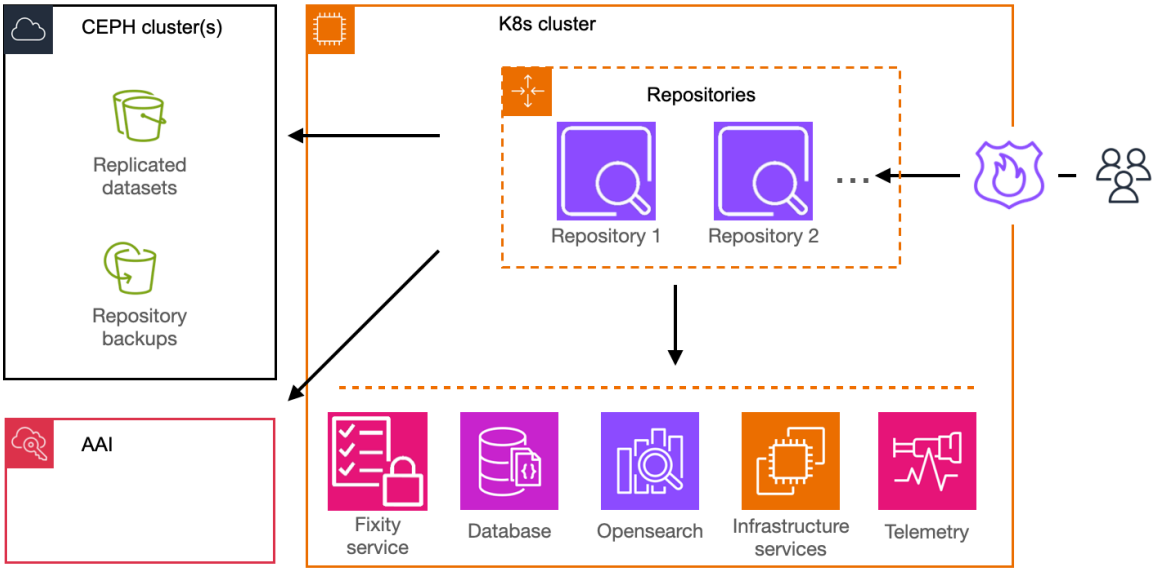
Analýza požadavků

Přehled architektury NRP

Repozitář obecně je technické, personální a procesní zajištění dlouhodobého úložiště pro ukládání a publikaci citovatelných digitálních objektů. Technicky lze repozitář chápat jako digitální službu, která je založená na nějaké *repozitářové platformě* (software). V rámci NRP se počítá s využitím zejména následujících tří základních repozitářových platforem (ačkoliv je možné vytvořit i repozitář založený na jiném systému):

- CESNET Invenio
- CLARIN DSpace
- ASEP/ARL

Jednotlivé repozitáře (tj. instance výše uvedených systémů) poběží v jednotném *prostředí pro běh aplikací* založeném na technologii *Kubernetes (K8s)*. Kromě aplikací repozitářů jsou v tomto prostředí připraveny i další podpůrné služby (např. databáze). Repozitáře dále využívají *úložiště dat*, jímž je v případě NRP objektové úložiště CEPH (kompatibilní s Amazon S3). V neposlední řadě je nezbytná *autentizační a autorizační infrastruktura (AAI)*. Repozitáře v NRP budou připojeny ke stávající AAI infrastruktuře v e-INFRA.CZ, která je založena na technologii Perun AAI. Tato architektura je znázorněna níže na obrázku 1.



Obrázek 1: Logická architektura NRP

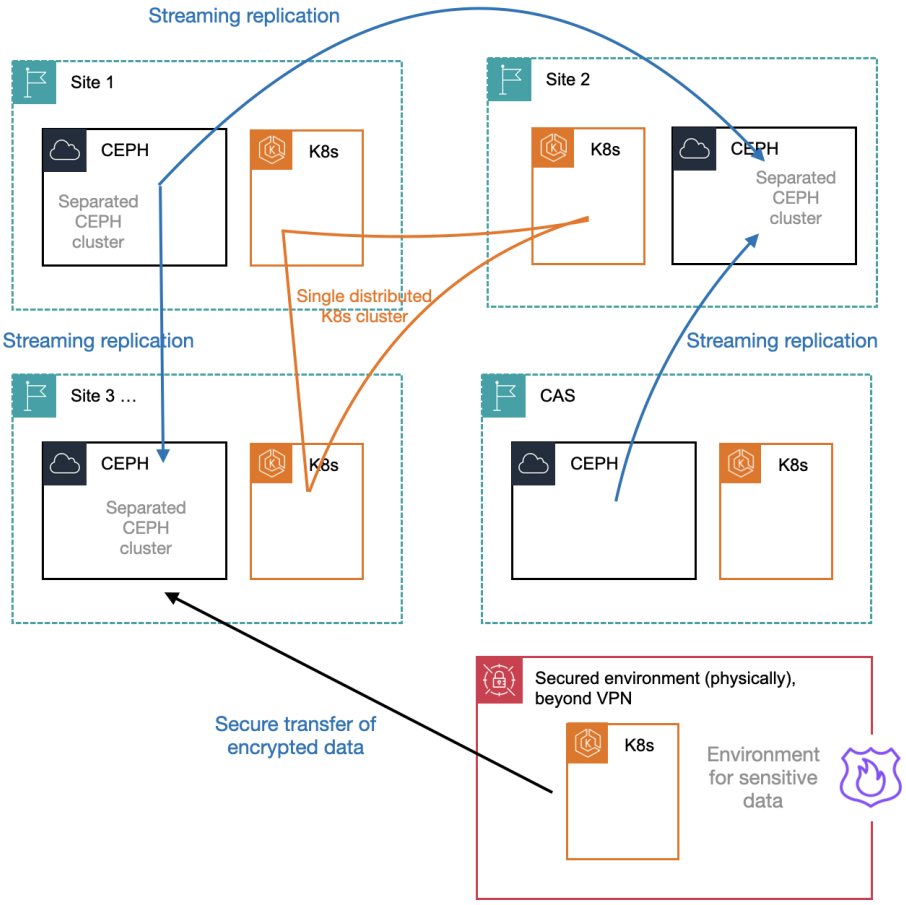
Přestože repozitářů je plánováno větší množství, všechny (v rámci NRP) poběží na společné infrastruktuře sestávající z prostředí pro běh aplikací (Kubernetes cluster) a datového úložiště (CEPH cluster), vždy v samostatných jmenných prostorech.

Systém pro bezpečnostní monitoring, tvořený v rámci PKA 10.2, by měl být zaměřen na monitoring této infrastruktury, tj. K8s a CEPH clusterů, a aplikací běžících na ní.

Fyzické umístění

Fyzicky je tato infrastruktura provozována v několika geografických lokalitách (aktuálně ve dvou, předpokládá se až pět), přičemž tyto uzly jsou provozovány sdružením CESNET v rámci e-INFRA CZ. Jedna lokalita bude provozována Akademií věd. Propojení těchto lokalit je znázorněno na obrázku 2.

Každá lokalita obsahuje nezávislý CEPH cluster, jehož data mohou být replikována do dalších míst prostřednictvím *streaming replication*. Dále jsou v každé lokalitě výpočetní zdroje, které jsou logicky propojeny do jednoho K8s clusteru. K8s cluster Akademie věd bude dedikován pro běh repozitářové platformy na bázi ARL. CEPH akademie věd bude mít možnost streamingu replik do infrastruktury e-INFRA.

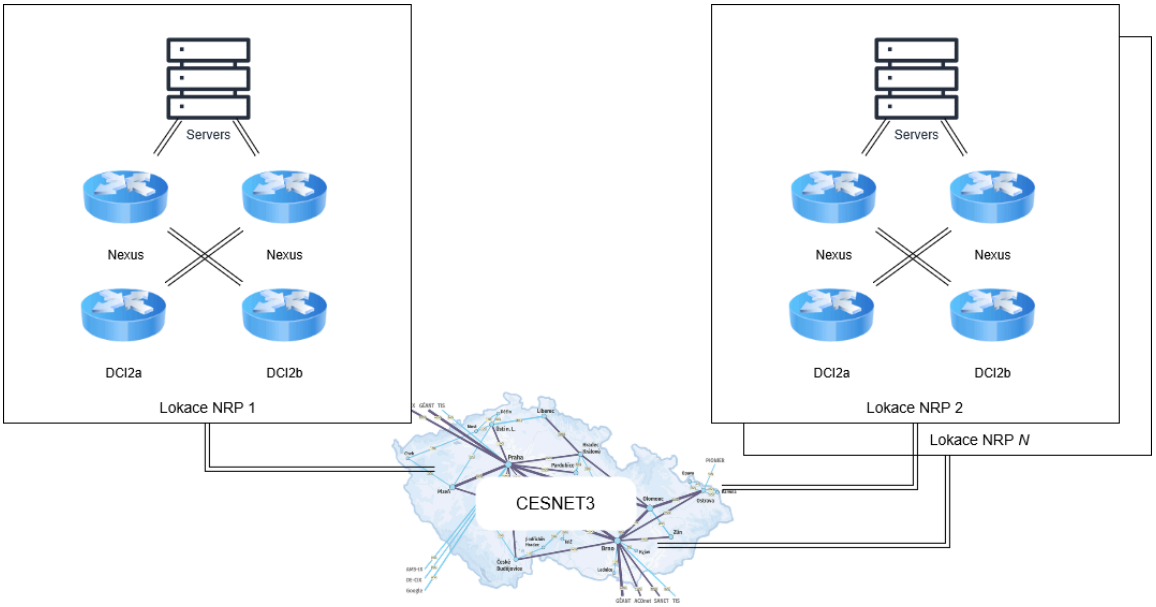


Obrázek 2: Fyzické rozdělení infrastruktury NRP do více lokalit

Infrastruktura NRP je oddělena od jiných služeb, a to jak fyzicky (tj. HW je dedikovaný pro NRP), tak i logicky — např. používá konkrétní rozsah IP adres. Je možné získat i seznam doménových jmen používaných jednotlivými repozitáři. Díky tomu je možné i na úrovni síťového provozu zachyceného mimo infrastrukturu snadno definovat, co je součástí monitorované infrastruktury.

Síťové připojení

Architektura z hlediska síťového připojení je znázorněna na obrázku 3. Jednotlivé lokality jsou vzájemně propojeny prostřednictvím páteřní sítě CESNET3, která zároveň zajišťuje komunikaci s okolním světem. Připojení je vždy realizováno nejméně dvěma nezávislými linkami o rychlostech 100 Gbps (v budoucnu až 400 Gbps), a to přes dva nezávislé routery, které zajišťují redundanci a funkčnost připojení i při výpadku kteréhokoliv prvku.



Obrázek 3: Síťové propojení jednotlivých lokalit

Neexistuje tedy žádné jedno místo, přes které by proudil veškerý síťový provoz do a z NRP. Pokud bychom chtěli všechen takový provoz monitorovat, znamenalo by to nutnost nasazení velkého počtu výkonných sond na různých místech. Podrobněji jsou možnosti umístění sond diskutovány dále v návrhu architektury.

Požadavky na detekci bezpečnostních hrozeb

V rámci diskusí se správci infrastruktury a repozitářů jsme identifikovali následující typy bezpečnostních hrozeb a jiných problémů, jejichž detekce v rámci bezpečnostního monitoringu by byla žádoucí:

- Obcházení autentizace ve webové aplikaci (uhodnutí hesla, zneužití SW zranitelnosti, ukradení session ID/cookies, apod.).
    - Autentizace uživatele je vždy prováděna skrze AAI infrastrukturu, tj. v samotných repozitářích žádné uživatelské účty ani hesla uložena nejsou. Případné odcizení účtu je záležitostí příslušného IdP a je mimo naši kontrolu.
    - Komunikace mezi systémy (např. autentizace do objektového úložiště) probíhá zpravidla pomocí tokenů přenášených přes zabezpečené kanály.
    - I přes nízkou pravděpodobnost úspěšného útoku na autentizační mechanismy je vhodné vše související s autentizací monitorovat a detekovat případné anomálie.
- Zneužití zranitelností webových aplikací (SQL injection a jiné)
    - Přestože aplikace procházejí penetračními testy (alespoň Invenio), je vhodné všechny takové pokusy o zneužití zranitelností detekovat.
    - Obecně vhodnější detekovat v aplikačním logu, ne v síťových datech.

- Útoky na systémy infrastruktury přes otevřené služby
    - Na systémech tvořících infrastrukturu pro běh repozitářů bývá SSH přístupné odkudkoliv, autentizace je ale možná jen klíčem (což je obecně považováno za velmi bezpečné).
    - Některé systémy (např. Ceph) mívají otevřené porty pro další služby, přístup k nim by měl být blokován firewallem.
    - Přesto je vhodné detekovat podezřelé pokusy o přihlášení zvenčí, případně kontrolovat, že nejsou veřejně dostupné služby, které by být neměly.
- Neoprávněný přístup k datům v S3 úložišti
    - Když chce uživatel přistoupit k uloženým datům, repozitářový systém si od S3 úložiště vyžádá “pre-signed” požadavek, speciální odkaz s časově omezenou platností umožňující stáhnout konkrétní datový objekt, předá ho uživateli a ten si pak data stáhne pomocí tohoto odkazu přímo z úložiště.
    - Mohlo by být užitečné detekovat pokusy o manipulaci s těmito odkazy.
- Traverzování jmenného prostoru objektového úložiště (hledání otevřených S3 bucketů)
- DDoS útoky
    - Jako každá jiná online služba, i repozitáře NRP mohou být terčem DDoS útoků. Předpokládá se zapojení stávajících detekčních a mitigačních mechanismů implementovaných v síti CESNET, žádné nové mechanismy specifické pro NRP pravděpodobně nebudou potřeba.
- Detekce již napadených stanic
    - Stanice napadené malware jsou často využívány k dalším útokům, což je v mnoha případech snadno detekovatelné na úrovní síťového provozu.
    - Podobné detekce se již provádí na úrovni celé sítě CESNET. Pro stroje infrastruktury NRP by se však dalo přesněji specifikovat, co je běžné a co nežádoucí chování.
- Nestandardní komunikace mezi stroji
    - Stroje v rámci infrastruktury mezi sebou komunikují určitými protokoly a způsoby, které se příliš nemění — jakákoliv odchylka (např. použití plain HTTP, SNMP komunikace mimo infrastrukturu) může znamenat bezpečnostní nebo provozní problém, který je vhodné detekovat.
- Dále je možné detekovat obecné anomálie na různých úrovních.
    - Příkladem může být sledování, z jakých sítí obvykle chodí data do kterých repozitářů, a následná detekce významných odchylek (např. požadavky na větší množství dat ze země, ze které dříve žádní uživatelé nepřicházeli). Ačkoliv takové případy nemusí znamenat útok, je vhodné je umět detekovat a upozornit na ně.

Tento výčet hrozeb rozhodně nelze považovat za úplný. Navíc oblast kybernetické bezpečnosti je velmi dynamická a kdykoliv se mohou objevit zcela nové hrozby. Bezpečnostní monitoring je proto potřeba budovat dostatečně obecný a detekční systémy musí být flexibilní, aby bylo možné je rychle upravovat a detekovat i nové hrozby.

Dále byly vyjádřeny požadavky i na provozní monitoring — např. detekce retransmisí TCP (které zpravidla značí problém s klientem nebo sítí), nebo sledování, přes které uzly sítí

chodí která data, za účelem výkonnostních optimalizací. Provozní monitoring sice není cílem navrhovaného systému (a není v plánu systém za tímto účelem speciálně přizpůsobovat), některé provozní informace je však obvykle možné snadno vyčíst i z dat sbíraných za účelem bezpečnostního monitoringu.

V neposlední řadě byla identifikována potřeba schopnosti detekce NAT u externích IP adres, tedy případů, kdy se za jednou adresou skrývá více zařízení, resp. uživatelů. V případě detekce příchozích útoků lze totiž další provoz z dané adresy blokovat, ale v případě, že jde o NAT, je zde riziko současného zablokování i velkého množství legitimních uživatelů a k blokování je tedy nutno přistupovat opatrněji.

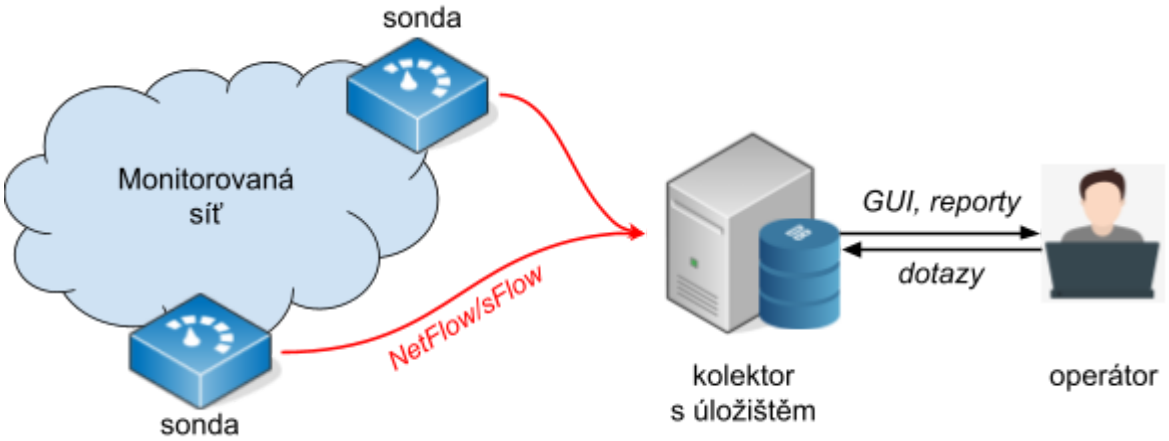
Návrh architektury

Z analýzy požadavků vyplývá potřeba detailního monitoringu infrastruktury NRP i samotných repozitářových systémů a detekce různých typů potenciálních bezpečnostních problémů. Monitoringem se zde rozumí jak sběr a zpracování aplikačních logů, tak analýza síťového provozu. Systém pro sběr aplikačních logů je však již řešen v rámci projektu NRP, proto se následující kapitoly zaměřují především na návrh systému pro monitoring síťového provozu.

Monitorování síťového provozu

Viditelnost, jak se zařízení a uživatelé v síti skutečně chovají, poskytuje monitorování síťového provozu. Umožňuje odhalit řadu anomálií, které jsou popsány v dříve uvedených požadavcích na detekci bezpečnostních hrozeb, a pomáhá zpětně analyzovat průběh bezpečnostních incidentů.

Monitorování provozu je typicky založeno na standardních technologiích NetFlow/IPFIX či sFlow. První zmiňovaná dvojice vytváří agregované záznamy o síťových tocích (tzv. flow záznamy), druhá technologie zachycuje vzorky paketů a statistiky síťových rozhraní. V těchto technologiích se vyskytují dva klíčové prvky, sonda a kolektor. Sonda (někdy označovaná také jako exportér) ve specifikovaném bodě sítě kontinuálně sleduje procházející provoz a periodicky exportuje agregované záznamy toků, resp. vzorky síťových paketů, na kolektor. Kolektor následně sbírá záznamy z jedné nebo více sond, ukládá je pro potřeby forenzní analýzy, provádí automatizované detekce bezpečnostních incidentů a reportuje je. Na 4. obrázku je vyobrazeno schéma typické monitorovací infrastruktury.



Obrázek 4: Monitorovací infrastruktura se sondami a kolektorem

Pro účely detekce bezpečnostních událostí v rámci NRP je vhodné pracovat s NetFlow/IPFIX záznamy toků, neboť ty poskytují snadno zpracovatelné a interpretovatelné informace o síťovém provozu. V případě, že budou dostupné sFlow záznamy, je možné v případě potřeby jednotlivé vzorky paketů konvertovat za pomocí specializované NetFlow/IPFIX sondy do podoby vzorkovaných toků.

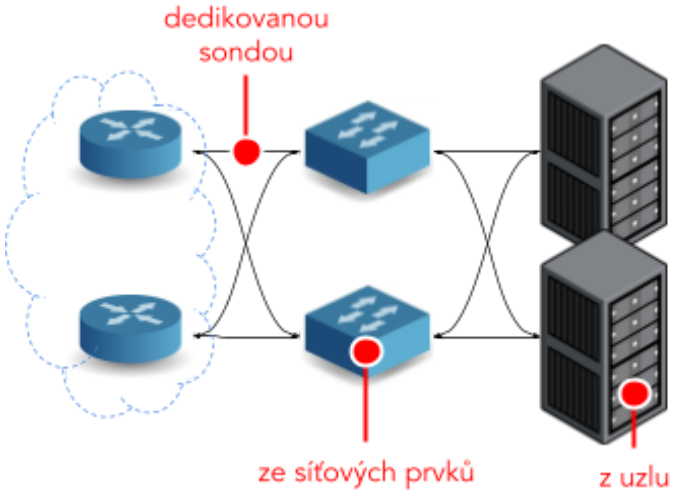
Sondy a jejich umístění

Z pohledu viditelnosti provozu je třeba rozlišovat i způsob sběru dat. Sběr záznamů o tocích je možné provádět z prvků síťové infrastruktury (např. routery s podporou exportu NetFlow/IPFIX) či za pomocí specializovaných dedikovaných síťových sond. Přičemž kvalita sbíraných dat a náklady na realizaci se u jednotlivých způsobů značně liší.

Použití již existujících prvků (např. router či switch) představuje nejjednodušší a nejméně nákladnou variantu. Tato metoda nevyžaduje žádné nové hardwarové investice a z hlediska provozu i údržby je prakticky beznákladová. Její nevýhodou je však nižší úroveň viditelnosti, neboť monitoring provozu je u těchto zařízení typicky pouze doplňkovou funkcionalitou a probíhá nad vzorkovaným provozem (např. je analyzován jen každý tisící paket). Přesto je tento způsob vhodný pro detekci nových či neobvyklých druhů provozu, neboť takové chování může signalizovat kompromitaci stroje nebo bezpečnostní incident.

Další možností je nasazení softwarových sond přímo na uzly v Kubernetes clusteru. Tímto způsobem je možné analyzovat kompletní nevzorkovaný síťový provoz daného uzlu a získat tak výrazně vyšší úroveň detailů. Výhodou tohoto řešení je, že nevyžaduje nový hardware a lze jej provozovat na stávajících systémech. Nicméně má omezenou viditelnost pouze na lokální provoz konkrétního uzlu a samotný monitoring odčerpá část systémových prostředků.

Opačný protipól oproti využití stávajícího hardwaru představuje možnost nasazení dedikovaných síťových monitorovacích sond. Obvykle se jedná o běžný serverový hardware vybavený jednou nebo více vysokorychlostními síťovými kartami a specializovaným softwarem. Významnou předností tohoto řešení je schopnost analyzovat veškerý síťový provoz ve zvoleném místě pozorování, kdy je provoz na sondu odkloněn skrze TAP či SPAN port. Dedikovaná sonda zvládne poskytnout nevzorkovaný pohled na síťový provoz i při velmi vysokých rychlostech v řádu stovek Gb/s. Za nevýhodu tohoto řešení lze ovšem považovat vysoké nároky na pořízení hardwaru, jeho údržbu a následnou obnovu. Samotná výrobní cena jedné sondy se pohybuje v řádu vyšších stovek tisíc korun.



Obrázek 5: Možnosti získávání dat pro monitorování síťového provozu

Monitorování jedné lokality NRP výše uvedenými možnostmi je vyobrazeno na 5. obrázku. Nejlepší řešení monitorování síťového provozu lze dosáhnout použitím specializovaných dedikovaných sond, neboť ty jsou schopny zajistit kompletní viditelnost veškerého síťového provozu do a z NRP.

Nasazení dedikovaných sond je nicméně velice nákladné. Každá lokalita NRP díky důrazu na vysokou dostupnost obsahuje řadu redundantních vysokorychlostních linek, které by bylo třeba monitorovat za použití více než jedné sondy. Jelikož NRP bude geograficky oddělená do až pěti lokalit, řešení by bylo třeba aplikovat na všech lokalitách. Náklady pouze na pořízení samotného dodatečného HW by dosahovaly vyšší jednotky milionů korun, což vzhledem k alternativám není ekonomicky výhodné. Zároveň je třeba vzít v potaz, že majoritu provozu, co se objemu týká, budou představovat synchronizace clusterů a přenosy datových sad k uživatelům. Ty z hlediska bezpečnostního monitoringu nenesou příliš užitečných informací. Mnohem větší hodnotu mají informace o provozu na repozitářové či podpůrné aplikace, řídící provoz do datového úložiště či provoz samotné podkladové infrastruktury (Kubernetes). Tento typ provozu je objemově menší.

Bylo tedy rozhodnuto, že pro monitorování síťového provozu budou použita data získatelná ze stávajících síťových prvků a ze softwarových sond na vybraných uzlech Kubernetes clusteru. Nebude tedy třeba pořizovat žádný dodatečný hardware. Realizace samotná bude rozdělena do několika fází. V první fázi budou využita NetFlow/IPFIX či sFlow data z routerů či switchů pro získání operačního přehledu jednotlivých lokalit NRP. Nad těmito daty vznikne první řešení realizující detekci anomálií a bezpečnostních incidentů. Další fáze se pak zaměří na identifikaci uzlů v Kubernetes clusteru, kde bude dávat smysl provozovat softwarové sondy[1] monitorující vybraná síťová rozhraní, tj. sondy poběží na stejných serverech, kde běží i ostatní komponenty NRP. Získaná data poslouží k rozšíření viditelnosti do síťového provozu a vylepšení či rozšíření analytických schopností monitorovacího systému.

Jako doplněk nad rámec monitorování jednotlivých lokalit lze uvažovat i o využití dat ze sítě CESNET3, která NRP poskytuje síťovou konektivitu. Tato síť je již nyní na perimetru monitorována za pomocí výkonných dedikovaných IPFIX sond, které jsou spravovány mimo projekt OS-II jako součást ochrany sítě samotné. Jejich využití tak nepřináší žádné dodatečné náklady a údržba je zajišťována sdružením CESNET. Uvedené sondy sledují veškerý příchozí a odchozí provoz ze zahraničních linek či z komerčního českého internetu (NIX) tak, jak je uvedeno na 6. obrázku. Z podstaty svého umístění neposkytují viditelnost do komunikace mezi lokalitami NRP či do komunikace mezi NRP a tuzemskými univerzitami, které jsou přímo připojeny do sítě CESNET3. Tento doplňkový monitoring lze ovšem zacílit na známé IP rozsahy NRP, kde může poskytovat komplexní přehled o komunikaci NRP s vnějším světem a lze jej použít pro detekci zahraničních útoků či anomálního typu provozu.

[1] Uvažuje se použití open-source sondy ipfixprobe (vyvíjené sdružením CESNET)

Obrázek 6: Znázornění sítě CESNET3 se sondami na jejím perimetru

Analýza a uchování síťových toků

Na sondy navazuje kolektor síťových toků představující centrální prvek navrhovaného monitorovacího řešení. Jeho úkolem je shromažďovat data z různých částí infrastruktury a poskytovat jednotný, korelovaný pohled na síťový provoz napříč lokalitami a technologickými doménami. Kolektor není pouhým úložištěm, ale je aktivním prvkem, který umožní průběžnou automatickou analýzu, detekci anomálií a dlouhodobé uchovávání dat pro forenzní účely. V rámci architektury bude provozován jako server ve virtualizační platformě a bude tvořit analytické jádro celého systému.

Data budou do kolektoru přicházet z heterogenních zdrojů, které se liší způsobem získávání i úrovní detailu. Zásadním požadavkem je identifikace zdroje dat a oddělené ukládání vzorkovaných a nevzorkovaných dat. Oba typy mají odlišnou vypovídací hodnotu a vyžadují rozdílné analytické postupy. Vzorkovaný provoz je vhodný pro identifikaci trendů, objemových anomálií nebo neobvyklých toků mezi segmenty, zatímco nevzorkovaný provoz umožňuje detailní forenzní analýzu, sledování laterálního pohybu útočníka či přesné mapování aplikační komunikace. Z toho vyplývá, že detekční mechanismy musí být specifické pro jednotlivé datové proudy. Oddělené databázové struktury umožní optimalizovat výkon, retenci i způsob zpracování podle charakteru dat.

Celé řešení bude postaveno výhradně na open-source technologiích, které umožňují transparentnost, auditovatelnost a možnost úprav podle potřeb prostředí NRP. Pro příjem NetFlow/IPFIX dat bude využit nástroj *ipfixcol2*, který poskytuje vysoký výkon a flexibilitu při zpracování toků. Dlouhodobé uchování toků pro potřeby analytiky a forenzní analýzy zajistí databáze *ClickHouse*, která je vhodná pro velké objemy dat a analytické dotazy. Vizualizační vrstva bude řešena pomocí platformy Grafana, která umožňuje vytvořit vhodné webové prostředí s přehlednými dashboardy a rozhraním pro dotazování. Nad daty na kolektoru

bude navíc implementována detekční vrstva, tvořená sadou nástrojů a skriptů přizpůsobených konkrétním typům dat a dříve uvedeným detekčním scénářům.

Obrázek 7: Ilustrace možného grafického rozhraní síťového kolektoru s přehledem trendů

Další součásti systému bezpečnostního monitoringu

Bezpečnostní analýza aplikačních logů
V rámci projektu NRP je budován systém pro centrální sběr a uložení aplikačních logů, kam by měly odesílat záznamy o svém provozu všechny komponenty infrastruktury NRP a pravděpodobně i všechny aplikace repozitářů. V rámci projektu NRP by měla být zavedena i základní bezpečnostní analýza těchto logů.

Předpokládáme však, že i v rámci projektu OS II může vyvstat potřeba analýzy aplikačních logů, např. za účelem detekce hrozeb s využitím korelace logů s daty o síťovém provozu, nebo jiné typy analýz, jejich potřeba se ukáže až v průběhu řešení projektu.

Hlášení bezpečnostních událostí
Hlášení událostí detekovaných systémem bezpečnostního monitoringu bude probíhat především skrze systémy Warden a Mentat, což jsou již zavedené nástroje, dlouhodobě provozované sdružením CESNET. Ve specifických případech mohou být zavedeny i jiné vhodné kanály pro konkrétní typy událostí. Incidenty budou řešeny standardními postupy týmu CESNET-CERTS, případně dále správci repozitářů či jinými příslušnými osobami. Tyto nástroje a procesy, stejně jako personální zajištění, jsou již podpořeny v rámci projektu NRP.

Honeypoty
V rámci bezpečnostního monitoringu budou na různá místa infrastruktury NRP nasazeny i tzv. honeypoty — dedikované systémy aktivní obrany simulující určitou službu (např. SSH či

HTTP server), jejichž cílem je nalákat případného útočníka, prezentovat mu data takovým způsobem, aby si myslel, že napadl skutečný systém, a podrobně sledovat jeho chování.

Budou využity některé z existujících open-source implementaci honeypotů. Těch existuje velké množství a zaměřují se na simulaci nejrůznějších aplikačních protokolů. V rámci projektu budou vybrány honeypoty, které simulují takové služby, které se i reálně vyskytují v infrastruktuře NRP.

U honeypotů velmi záleží i na jejich umístění v rámci sítě. Honeypot ve vnitřní síti, běžným způsobem nedostupný zvenčí, slouží zejména k včasnému a spolehlivému odhalení průniku do sítě. Jakékoliv připojení na takový honeypot je podezřelé a vyžaduje okamžité prošetření. Naopak honeypoty na perimetru sítě, dostupné z internetu, bývají cílem útoků neustále a používají se pro zjišťování informací o používaných technikách a infrastruktuře útočníků. Poskytují např. informace o používaných IP adresách či doménách, seznamy uživatelských jmen a hesel zkoušených v rámci pokusů o přihlášení, vykonávané požadavky či příkazy (z nichž lze odvodit, na jaké zranitelnosti útoky cílí), často se pomocí honeypotů podaří získávat konkrétní vzorky malware pro další analýzu. V rámci projektu je v plánu nasadit oba typy honeypotů, pravděpodně jako aplikace v rámci Kubernetes clusteru.

Získaná data budou analyzována a využívána v rámci kontinuálních snah o zlepšování zabezpečení a vylepšování detekčních metod.

Sdružení CESNET již řadu honeypotů provozuje a má zavedené mechanismy pro zpracování některých jimi sbíraných dat (např. tvorba seznamu škodlivých IP adres nebo extrakce URL, na nichž je malware, z SSH příkazů). Stávající mechanismy však zdaleka nevyužívají veškerý potenciál dat z honeypotů a budou tedy zkoumány i možnosti jejich rozšíření.