FR CESNET – Závěrečná zpráva

Název projektu: Vytvoření bezpečnostního týmu CSIRT (CSIRT-CUNI pracoviště), vybudování monitorovacích systémů pro podporu řešení bezpečnostních incidentů a detekci anomálií v datových sítích Univerzity Karlovy v Praze, zapojení Univerzity Karlovy do systému pro sdílení informací o detekovaných bezpečnostních událostech Warden (http://warden.cesnet.cz).

Číslo projektu, ročník: 549, 2014/2

Hlavní řešitel: Ing. Vladimír Horák

Postup při řešení, způsob řešení

Zřízení CSIRT týmu na Univerzitě Karlově

CSIRT tým Univerzity Karlovy (CSIRT-CUNI) začal pracovat v pilotním provozu v květnu 2015. Tvoří ho tým tří pracovníků Ústavu výpočetní techniky Univerzity Karlovy, kteří se střídají v řešení bezpečnostních incidentů v týdenních službách. Jde o tři z řešitelů tohoto projektu. Pro zpracování a archivaci informací o bezpečnostních incidentech máme k dispozici ticketovací systém s www rozhraním, interní dokumentací ve formě wiki a zajištěný privilegovaný přístup k potřebným informacím a nástrojům (rozdělení IP adres univerzitní sítě a kontakty správců, kontaktní údaje uživatelů, NetFlow logy a výstup ADS z rozhraní sítí PASNET/CESNET, klienta systému Warden a přístup do systému Mentat).

Pro zpracování a archivaci informací o bezpečnostních incidentech jsme zvolili ticketovací systém OTRS 4 („Free“ variantu), který jsme postupně upgradovali na současnou verzi OTRS 5s. Důvody výběru – schopnost dobře pracovat s e-maily a přílohami, otevřenost systému a možnost úprav, cena.

Hlavním vstupním kanálem informací o incidentech jsou e-maily na adresu abuse@cuni.cz. Aby se nestalo, že důležitý e-mail odfiltruje spamový filtr, má v něm adresa abuse@cuni.cz absolutní výjimku. Většinu došlých e-mailů musí proto probrat a zpracovat člověk. Proces jsme částečně zautomatizovali filtry, které přiřadí příchozí e-mail k již existujícímu ticketu nebo při založení nového ticketu doplní metadata podle obsahu e-mailu.

Formou e-mailů také přijímáme informace ze systému Warden. Kombinace přijímání reportů e-mailem a možnost dohledávání přes www rozhraní systému Mentat se nám osvědčila. Podařilo se nám přijít na několik systémových problémů (chyby v údaji časového pásma, false-positive detekce související s novými službami a protokoly apod.), které jsme zdokumentovali a nahlásili autorům. V systému Mentat využíváme také funkci „Reporting filters“, byť jen v nejnutnějších případech, hlavně pro filtrování nejasných reportů z provozu studentských kolejí, kde nejsme schopni řádně analyzovat podstatu problému a zajistit nápravu, protože nejde o zařízení pod správou univerzity.

Nainstalovali jsme systém DokuWiki, vytvořili v něm interní dokumentaci a průběžně ji aktualizujeme. Dokumentace obsahuje především přehled typů incidentů. Každému typu jsme přidělili prioritu a zdokumentovali způsob řešení. Tento seznam průběžně doplňujeme a upravujeme. V provozní dokumentaci je pak popsán obecný postup při řešení incidentu a časové údaje a limity v závislosti na jeho prioritě. Zvláštní postup jsme stanovili pro incident typu „žádost policie o informace“, kde všechny kroky musí nezávisle zkontrolovat dva členové týmu.

Členové týmu mají v rámci Informačního systému univerzity přístup k údajům o uživatelích, které potřebují pro zpracování incidentů (především zjištění vztahu k univerzitě a kontaktního e-mailu).

Z technických nástrojů jsou důležité především netflow logy. K dispozici máme dva nástroje: systém CESNETu FTAS a systém univerzity Invea FlowMon. Každý má jiné vlastnosti, ale navzájem se doplňují. Oba dva monitorují provoz na rozhraní sítí PASNET/CESNET. Systém FTAS sbírá netflow data z hraničních routerů se samplingem 20, zatímco FlowMon data sbírá sondou připojenou přes TAP přímo na optická vlákna a bez samplingu. FlowMon by teoreticky měl zachytit provoz na síti i při selhání (přetížení cpu) hraničních routerů. V praxi je

z uživatelského pohledu FTAS mnohem rychlejší a stabilnější a dobře poslouží pro přehled za delší časový úsek (např. zneužití určitého DNS serveru k DDoS útokům během dne). FlowMon používáme pro ověřování incidentů, u kterých šlo o jednotky spojení a které FTAS kvůli samplingu nemusel zachytit.

Netflow logy systému FlowMon jsme také zpřístupnili správcům univerzitních sítí. Pro každou síť jsme vytvořili samostatný profil jen pro IP rozsahy sítě. Práce s tímto omezeným profilem je výrazně rychlejší.

Informace záměru zřídit CSIRT-CUNI tým v rámci řešení projektu FR CESNET byla publikována na www stránkách Ústavu výpočetní techniky. Vznik CSIRT-CUNI týmu a přehled téměř ročního pilotního provozu jsme prezentovali v rámci univerzity na „Semináři správců sítí UK“ v dubnu 2016.

Základní informace o CSIRT týmu včetně pole působnosti, kontaktů, PGP klíče a způsobu hlášení incidentu jsme zveřejnili na www stránkách https://csirt.cuni.cz/.

Záměr zřídit CSIRT-CUNI tým vzalo na vědomí 23. zasedání kolegia rektora Univerzity Karlovy dne 20. dubna 2015 a o zahájení pilotního provozu pracoviště je informace ve Výroční zprávě o činnosti Univerzity Karlovy za rok 2015. Vlastní formální zřízení CSIRT týmu na Univerzitě Karlově, formální definice jeho role, oblasti působení, organizační struktury a personálního obsazení je zakotvené v připravovaném návrhu opatření rektora „Pravidla počítačové sítě Univerzity Karlovy“. Sestavení pravidel se ukázalo komplikovanější, než jsme čekali. Samotný návrh vznikl v Ústavu výpočetní techniky ve spolupráci se zástupci Oddělení podpůrných služeb a bezpečnosti sdružení CESNET a následně byl prodiskutován se správci fakultních sítí a upraven podle jejich připomínek. Dvakrát jsme proto požádali o prodloužení projektu. Finální návrh by měl být předložen na zasedání kolegia rektora v lednu 2017. Do vydání opatření bude CSIRT-CUNI tým pracovat v režimu „pilotního provozu“.

Nákup a nasazení ADS pluginu na FlowMon kolektor na rozhraní sítí PASNET/CESNET

Pro ověřování informací uvedených v reportech bezpečnostních incidentů a pro analýzu síťového provozu používáme netflow systém FlowMon firmy Invea, který je nasazený na 20Gb rozhraní sítí PASNET/CESNET. V rámci řešení projektu jsme zakoupili výkonnější verzi kolektoru a doplnili pluginem ADS (Anomaly Detection Systém) pro lepší analýzu přenášených dat a detekci bezpečnostních anomálií.

Původní FlowMon Collector R5-4000 Pro jsme nahradili nově zakoupeným výkonnějším typem FlowMon Collector R6-24000 Pro. Po otestování jsme přenesli data z původního kolektoru a nový systém je v provozu od 5. května 2015.

V dubnu 2015 proběhlo poptávkové řízení na FlowMon ADS ISP 10 včetně zákaznické podpory Gold Support. Poptali jsme firmy Invea-Tech a.s., AGORA plus a.s. a Veracomp s.r.o. V květnu 2015 jsme na základě nabídky s nejnižší cenou vybrali firmu AGORA plus, a.s. Uzavření smlouvy a dodání pluginu se ale nečekaně protáhlo kvůli problémům na straně dodavatele (především neschopností dodat návrh smlouvy kvůli letním dovoleným). Plugin byl proto formálně nainstalovaný až v září 2015. Firma Invea (autor pluginu) nám ale kvůli těmto problémům poskytla dočasnou licenci na plnohodnotně použitelnou demoverzi, takže jsme funkční ADS plugin měli k dispozici již od července.

16. prosince 2015 proběhlo školení řešitelů projektu pro práci s ADS pluginem, na kterém jsme se školitelem již mohli konzultovat praktické zkušenosti s používáním systému.

Na konci roku 2016 jsme zakoupili (už mimo rámec projektu) prodloužení licence ADS pluginu na rok 2017.

Využití systému Nessus sdružení CESNET pro pravidelné testování systémů kriticky důležitých pro provoz univerzity

Původním záměrem projektu bylo využít pro pravidelné testování interních systémů Univerzity Karlovy službu bezpečnostního scanneru Nessus poskytovanou sdružením CESNET připojeným institucím. Bohužel během řešení projektu přestalo sdružení tuto službu poskytovat, ale jako náhradu nám zapůjčilo licence scanneru Nessus pro vlastní instalaci.

Scanner Nessus jsme nainstalovali během podzimu 2015 a pilotně otestovali na síti Ústavu výpočetní techniky. Od července a srpna ho používáme pro pravidelné testování kritických systémů univerzity (lokální síť rektorátu, servery Informačního systému) a sítě 1. Lékařské fakulty.

Během pilotního i pravidelného provozu jsme zjistili, že scanner generuje značné množství upozornění na chyby různého stupně závažnosti (včetně kritických), které ale nejsou reálně přítomny. Detekce je mnohdy založena na inzerované verzi protokolu/služby a databázi známých zranitelností, aniž by bylo konkrétně ověřeno, že protokol či služba tuto zranitelnost skutečně obsahuje (např. upozornění na chyby v modulech php, které server nepodporuje apod.).

V některých sítích (např. Přírodovědecké fakulty) scanner nenalezl žádné servery, zřejmě vlivem fakultního firewallu.

Možnosti sdílení protokolů o jednotlivých testech různými uživateli Nessusu jsou výrazně omezené.

Z těchto důvodů jsme nezpřístupnili scanner Nessus přímo jednotlivým fakultním správcům a používáme ho jen jako dodatečný zdroj informací o bezpečnostních hrozbách, případně po ad-hoc domluvě s fakultními správci na jednorázové testy.

Zahájení pilotního provozu systému detekce anomálií pro správce fakultních síti UK a poskytnutí detekce jako služby správcům dalších organizací připojených k síti PASNET

Pro získání zkušeností s ADS pluginem a pro jeho vyladění jsme ho nasadili a testovali na rozsahu IP adres serverů ve správě Ústavu výpočetní techniky, kde jsme měli potřebnou zpětnou vazbu od kolegů z oddělení správy serverů. Při pokusu o rozšíření sledování anomálií na všechny rozsahy IP adres univerzity v Praze jsme ale narazili na výkonostní omezení kolektoru.

V další fázi jsme se zaměřili na automatizaci – export dat o anomáliích ze systému a reportování do systému Warden. Původně jsme plánovali použít pro export z ADS pluginu syslog nebo SNMP trapy. Obojí jsme vyzkoušeli, ale ani jedním formátem není možné z pluginu získat všechny potřebné údaje. Nakonec jsme pro exportování použili lehce upravený návodný skript z dokumentace FlowMon. Takto získaná data jsme pak transformovali skriptem poskytnutým CESNETem do formátu vhodného pro export do Wardenu. Reportování jsme omezili na anomálie, jejichž zdroj je podle IP adresy v autonomních systémech připojených k internetu přes CESNET, protože u nich je šance, že se reporty bude někdo zabývat.

Vytvořili jsme na kolektoru profily podle IP rozsahů jednotlivých sítí připojených do PASNETu a začali poskytovat správcům univerzitních sítí přístup k FlowMon kolektoru a k analýze

provozu jejich sítí na základě netflow. Od původního plánu zpřístupnit jim i ADS plugin a umožnit jim vlastní ladění alertů jsme ale museli ustoupit a to kvůli tomu, že ADS plugin je schopen pracovat pouze s jedním profilem současně.

Ukázalo se, že ladění systému je náročné a pro využití potenciálu ADS je nutné, aby se ladění a vyhodnocování výstupů někdo věnoval pravidelně.

Provázání a definování způsobu sdílení informací s CESNET-CERTS

Zapojení do systému Warden

Pro zapojení do systému Warden, provozovaném a dozorovaném CESNET-CERTS, jsme nainstalovali samotného klienta služby ve verzi warden_client_3.0-beta2 a pomocnou utilitu warden_filer z balíčku contrib_3.0-beta2. Jako distribuční server pro sdílení informací se systémem Warden, kde byl klient a pomocný sw nainstalován, byl použit virtuální server na platformě VMware s operačním systémem Debian 8.

V první fázi jsme zprovoznili a zaregistrovali klienta cz.cuni.warden.client pouze pro čtení informací ze systému Warden. Registrace proběhla v listopadu 2015 a od té doby je klient v provozu. Ve druhé fázi jsme zprovoznili zasílání bezpečnostních incidentů, generovaných ADS pluginem Invea NetFlow sondy, do systému Warden. Nejprve jsme v srpnu 2016 zaregistrovali klienta cz.cuni.warden.flowmon, který měl práva zasílat do systému Warden informace. ADS plugin v Invea NetFlow sondě jsme nakonfigurovali tak, že pro každý vygenerovaný bezpečnostní incident vytvoří a odešle e-mailovou zprávu, která obsahuje všechny informace o daném incidentu. Tato zpráva je pak doručena na výše zmiňovaný distribuční server warden.cuni.cz, kde se všechny doručené zprávy periodicky zpracovávají. Ze všech došlých zpráv jsou vybrány jen ty reporty, které mají jako zdroj incidentu IP adresu z rozsahu CESNETu. Tyto reporty jsou následně zpracovány skriptem, který nám poskytl CESNET a který vygeneruje pro každý incident zprávu ve formátu JSON. Tyto zprávy jsou pak periodicky odesílány utilitou warden_filer_sender do systému Warden.

Kromě incidentů generovaných ADS pluginem Invea NetFlow sondy jsme zprovoznili i zasílání incidentů detekovaných naším zdrojem „sshreport“. Jde o detekci slovníkových útoků na službu ssh na serverech univerzity. Mechanismus zasílání alertů do systému Warden je analogický tomu, jak se zpracovávají alerty z ADS pluginu. Náš zdroj detekuje incident, vytvoří e-mailovou zprávu s informacemi o incidentu a odešle na server warden.cuni.cz ke zpracování. Zde jsou pak všechny došlé e-maily zpracovány, vygenerovány zprávy ve formátu JSON a ty pak periodicky odesílány do Wardenu.

Zpřístupnění detailnějšího mapování adresového prostoru

Interní databázi přidělení IP adres univerzity koncovým sítím a lokalitám jsme doplnili REST API rozhraním „netinfo“, přes které může CESNET-CERTS získat aktuální seznam koncových sítí, e-mailových adres správců a atributů sítě (NAT, Eduroam). Ze strany CESNET-CERTS jsou přes API viditelné informace o sítích, jejichž správci si přejí dostávat e-mailem informace o incidentech také přímo. E-maily mohou omezit na incidenty určité priority (priorita je jedním z atributů sítě).

První verzi API jsme poskytli CESNETu a diskutujeme způsob využití, nastavení a význam priorit apod.

Dosažené cíle

Zřízení CSIRT týmu na Univerzitě Karlově

- personální a technické zajištění CSIRT-CUNI
- nasazení ticketovacího systému pro řešení a archivaci incidentů
- provozní interní dokumentace ve formě wiki
- prezentace CSIRT-CUNI správcům fakultních sítí
- prezentace CSIRT-CUNI navenek formou www stránky csirt.cuni.cz
- práce týmu v pilotním režimu od května 2015
- 2087 uzavřených incidentů, z toho 1739 vyřešených, 41 žádostí policie o informace

Nákup a nasazení ADS pluginu na FlowMon kolektor na rozhraní sítí PASNET/CESNET

- nákup a nasazení výkonnější verze FlowMon kolektoru R6-24000 Pro
- nákup a nasazení FlowMon ADS ISP 10
- zaškolení řešitelů pro práci s ADS
- odladění ADS systému

Využití systému Nessus sdružení CESNET pro pravidelné testování systémů kriticky důležitých pro provoz univerzity

- instalace systému Nessus lokálně
- pravidelné testování sítí rektorátu a serverů Informačního systému univerzity
- jednorázové testy sítí nebo serverů na žádost jejich správců

Zahájení pilotního provozu systému detekce anomálií pro správce fakultních síti UK a poskytnutí detekce jako služby správcům dalších organizací připojených k síti PASNET

- zprovoznění skriptů pro zpracování e-mailových zpráv o bezpečnostních incidentech, jejich transformaci do formátu JSON a odeslání do systému Warden
- vytvoření profilů na FlowMon kolektoru pro fakultní sítě a zpřístupnění netflow analýzy provozu správcům fakultních sítí

Provázání a definování způsobu sdílení informací s CESNET-CERTS

- instalace serveru pro zpracovávání zpráv systému Warden
- zprovoznění klienta cz.cuni.warden.client pro čtení zpráv ze systému Warden
- zprovoznění klienta cz.cuni.warden.flowmon pro odesílání zpráv do systému Warden
- odesílání relevantních alertů (tj. se zdrojem v AS CESNETu) o anomáliích detekovaných ADS pluginem Invea NetFlow do systému Warden
- zprovoznění vlastního zdroje zpráv o detekci slovníkových ssh útoků na servery univerzity a odesílání relevantních alertů (tj. se zdrojem v AS CESNETu) o útocích do systému Warden
- zpřístupnění detailnějšího mapování adresového prostoru univerzity CESNET-CERTS přes REST API „netinfo“

Zdůvodnění případných změn v projektu

Zřízení CSIRT týmu na Univerzitě Karlově

CSIRT-CUNI není ještě formálně ustanoven, protože nejsou schválena „Pravidla počítačové sítě Univerzity Karlovy“, která mají formálně definovat jeho roli a oblasti působení.

Ze stejného důvodu nemohla být vydána tisková zpráva o zřízení týmu CSIRT-CUNI.

Využití systému Nessus sdružení CESNET pro pravidelné testování systémů kriticky důležitých pro provoz univerzity

CESNET tuto službu již neprovozuje. Nahrazeno lokální instalací systému.

Zahájení pilotního provozu systému detekce anomálií pro správce fakultních síti UK a poskytnutí detekce jako služby správcům dalších organizací připojených k síti PASNET

Nebylo možné poskytnout správcům sítí přímý přístup k ladění ADS pluginu pro jejich rozsah IP adres, protože ADS plugin může pracovat jen s jedním profilem.

Konkrétní výstupy, další využitelnost

Zřízení CSIRT týmu na Univerzitě Karlově

Základní informace o CSIRT-CUNI týmu, poli působnosti a způsobu hlášení incidentů jsou na webu https://csirt.cuni.cz

Odkazy na informace o záměru zřídit CSIRT-CUNI tým a o pilotním provozu:

- Zápis z 23. zasedání kolegia rektora dne 20. dubna 2015, na kterém rektor univerzity prezentoval záměr zřídit CSIRT-CUNI tým: https://www.cuni.cz/UK-979-version1-kr_1423.pdf
- Harmonogram dlouhodobého – strategického záměru Univerzity Karlovy 2016-2020 zahrnující zřízení bezpečnostního týmu CSIRT-CUNI: https://www.cuni.cz/UK-7919-version1-adz_2017_uk.pdf
- Informace o zahájení pilotního provozu pracoviště CSIRT-CUNI ve Výroční zprávě o činnosti Univerzity Karlovy za rok 2015: http://www.cuni.cz/UK-4511-version1-vzc2015web.pdf
- Aktualita o Semináři pro správce univerzitních sítí v dubnu 2016 na webu Ústavu výpočetní techniky s prezentací o vzniku CSIRT-CUNI týmu a o zkušenostech z pilotního provozu: http://uvt.cuni.cz/UVT-514.html

Stránka na webu Ústavu výpočetní techniky s informacemi o řešených projektech: http://uvt.cuni.cz/UVT-865.html

Body z navržených „Pravidel počítačové sítě Univerzity Karlovy“ týkající se CSIRT týmu:

> Část A: Pravidla pro uživatele počítačové sítě Univerzity Karlovy
>
> I. Definice pojmů
>
> 9. CSIRT-CUNI je označení bezpečnostního týmu, jehož hlavním úkolem je příjem informací o zjištěných bezpečnostních incidentech týkajících se počítačové sítě UK, jejich řešení a koordinace řešení ve spolupráci s provozovateli částí počítačové sítě UK, správci a uživateli
>
> II. Základní zásady používání počítačové sítě UK

3. Uživatel nesmí:

i) pokoušet se získat přístupová práva, která mu nenáleží; pokud uživatel získá taková práva chybou programového či technického vybavení, je povinen na tuto skutečnost neprodleně upozornit správce nebo CSIRT-CUNI

III. Práva a povinnosti uživatele

3. Uživatel je povinen

g) bez zbytečného odkladu upozornit CSIRT-CUNI na porušování těchto pravidel, zejména pokud se domnívá, že došlo či dochází ke zneužívání některého z ICT prostředků či některé ze služeb počítačové sítě UK nebo k vyzrazení osobních přístupových údajů

Část B: Pravidla provozování počítačové sítě Univerzity Karlovy

I. Základní povinnosti a práva ÚVT

5. ÚVT je provozovatelem bezpečnostního týmu CSIRT-CUNI

II. Základní povinnosti a práva provozovatele částí počítačové sítě UK

6. Provozovatel je povinen zajistit uchovávání identity uživatelů užívajících zařízení v jeho síti, a to včetně informace umožňující prokázat využívání tohoto zařízení uživatelem v daném čase. Tyto údaje musí být uchovávány alespoň 6 měsíců. Na základě žádosti ÚVT nebo Policie ČR je povinen tyto informace bez prodlení zajistit a poskytnout pro účely zjištění odpovědnosti za způsobení bezpečnostního incidentu či k poskytnutí údajů vyžádaných Policií ČR. O bezpečnostních incidentech řešených na žádost nebo ve spolupráci s Policií ČR provozovatel vždy informuje tým CSIRT-CUNI. Povinnost zajištění uchovávání identity uživatelů se na provozovatele nevztahuje v případech, kdy se provoz části sítě řídí zvláštními dohodami, které UK uzavřela, pokud správce části sítě k požadovaným informacím nemá přístup.

9. V případě zjištění bezpečnostního incidentu je provozovatel povinen na vyžádání poskytnout příslušnou součinnost ÚVT, členům CSIRT-CUNI, případně orgánům činným v trestním řízení.

III. Základní povinnosti a práva správce počítačové sítě UK

10. Správce je povinen poskytnout nezbytnou součinnost ÚVT a jmenovaným členům CSIRT-CUNI týmu při řešení bezpečnostních incidentů. Správce je povinen v případě, že je informován o zablokování nebo odpojení zařízení dle čl. I., odst. 8. této části B připojeného v části sítě v jeho správě nebo v případě jiného opatření realizovaného ÚVT dle čl. I., odst. 9. této části B majícího povahu omezení či ukončení poskytování služeb či poskytování připojení k počítačové síti UK, neprodleně informovat správce zařízení (případně správce podřízené části sítě) a vedoucího dotčeného pracoviště nebo uživatele, prostřednictvím jehož identity bylo zařízení připojeno.

Zahájení pilotního provozu systému detekce anomálií pro správce fakultních síti UK a poskytnutí detekce jako služby správcům dalších organizací připojených k síti PASNET

Nabídka služby analýzy provozu a přímého přístupu k FlowMon analyzátoru pro správce sítí členů sdružení PASNET: http://www.pasnet.cz/sluzby-bezpecnost/

Provázání a definování způsobu sdílení informací s CESNET-CERTS

Zapojení do systému Warden

Konkrétním výstupem projektu jsou alerty ve formátu JSON o bezpečnostních incidentech, které posíláme do systému Warden. Zdrojem je jednak ADS plugin Invea NetFlow kolektoru, jednak náš systémem detekce slovníkových ssh útoků (sshreport).

Zpřístupnění detailnějšího mapování adresového prostoru

Výstupem projektu je REST API „netinfo“ poskytující CESNET-CERTS informace o konkrétní IP síti/adrese (jméno sítě, e-mailová adresa koncového správce, atributy „NAT“ a „Eduroam“).

Přínosy projektu, vlastní hodnocení

Zřízení CSIRT týmu na Univerzitě Karlově

I před zřízením CSIRT-CUNI týmu se na Univerzitě Karlově informace o bezpečnostních incidentech sbíhaly centrálně na adrese abuse@cuni.cz a byly řešeny a archivovány. Projekt byl ale rozhodujícím impulsem k formálnímu zřízení CSIRT týmu ve smyslu zabezpečení personálního obsazení, organizačního a technického zajištění. Jde zejména o vznik týmu, jehož členové se podle časového rozvrhu střídají ve sledování a řešení incidentů v souladu s interním provozním řádem. K tomu mají k dispozici ticketovací systém s možností lepšího dohledávání souvislostí mezi incidenty a který slouží také pro archivaci. Všichni z týmu mají přístup k potřebným informacím (interní provozní dokumentace) a nástrojům (statistiky síťových prvků, netflow analyzátory, Nessus, systém ADS, přístup do Informačního systému univerzity, přístup do systému Warden a Mentat). Provoz týmu zajišťuje Ústav výpočetní techniky Univerzity Karlovy a bude pochopitelně pokračovat i po skončení tohoto projektu.

Je možné konstatovat, že díky projektu se proces zpracování bezpečnostních incidentů na Univerzitě Karlově výrazně vylepšil.

Nasazení ADS pluginu na FlowMon kolektor na rozhraní sítí PASNET/CESNET

ADS plugin na FlowMon kolektor jsme zprovoznili, odladili a využíváme ho, ale nasazení technologie ADS na páteřní 20Gb spoj mezi sítěmi PASNET a CESNET je mírně problematické. Protože jde o provoz na páteřní lince nefiltrovaný žádným firewallem, systém detekuje velké množství anomálií a odladění systému pro získávání užitečných výstupů je obtížné kvůli velkému rozsahu IP adres připojených sítí a kvůli velkému datovému toku na lince. Celkově ale považujeme systém za přínosný a budeme ho využívat i po ukončení projektu. Prodloužení licence na ADS plugin (do konce roku 2017) jsme již zakoupili.

Využití systému Nessus sdružení CESNET pro pravidelné testování systémů kriticky důležitých pro provoz univerzity

Protože sdružení CESNET přestalo tuto službu poskytovat, provozujeme lokální instalaci Nessusu. Pravidelně testujeme síť rektorátu a Informačního systému univerzity. Další univerzitní sítě nebo servery testujeme na vyžádání správce. Výhledově chceme otestovat i jiné systémy tohoto druhu.

Zahájení pilotního provozu systému detekce anomálií pro správce fakultních síti UK a poskytnutí detekce jako služby správcům dalších organizací připojených k síti PASNET

Systém detekce anomálií běží. Pro distribuci z něj získávaných informací směrem ke správcům sítí používáme infrastrukturu systémů Warden/Mentat. Z technických důvodů bohužel není možné poskytnout správcům fakultních sítí a sítí dalších organizací připojených k síti PASNET přístup přímo k www rozhraní ADS a umožnit jim vlastní ladění systému „na míru“. Správcům sítí jsme alespoň poskytli možnost analýzy netflow záznamů z IP rozsahů jejich sítí.

Provázání a definování způsobu sdílení informací s CESNET-CERTS

Zapojení do systému Warden

Zapojili jsme se do systému sdílení informací o bezpečnostních incidentech Warden, který provozuje sdružení CESNET. Získáváme z něj informace vztahující se k univerzitním sítím (využíváme výstup ve formě e-mailů v kombinaci s výborným filtrováním a dohledáváním přes rozhraní Mentat), ale vstup do ticketovacího systému CSIRT-CUNI je automatizovaný jen pro reporty určitého typu/sítí.

Současně jsme do Wardenu začali automatizovaně poskytovat informace z dvou vlastních zdrojů: z ADS modulu na FlowMon kolektoru, který monitoruje data na páteřním spoji sítí PASNET a CESNET a z vlastního systému detekce slovníkových ssh útoků na univerzitní servery (sshreport).

Sdílení informací přes systém Warden/Mentat považujeme za užitečné a budeme ho dále rozvíjet.

Zpřístupnění detailnějšího mapování adresového prostoru

Týmu CESNET-CERTS jsme poskytli detailnější mapování adresového prostoru univerzity, především proto, aby v kritických situacích mohl co nejrychleji předat informace přímo koncovým správcům univerzitních sítí. Umožní to také přímé posílání reportů ze systému Warden těm fakultním správcům sítí, kteří o to projeví zájem.

Tisková zpráva

Na Univerzitě Karlově byl zřízen bezpečnostní tým CSIRT-CUNI (https://csirt.cuni.cz) pro řešení bezpečnostních incidentů v univerzitní počítačové síti a zprovozněna detekce anomálií síťového provozu. Tým se zapojil do systému sdílení informací o bezpečnostních událostech Warden sdružení CESNET. Uvedených skutečností bylo dosaženo za finančního přispění Fondu rozvoje CESNET z.s.p.o.

V Praze dne 30. prosince 2016 Ing. Vladimír Horák, řešitel grantu