# Smlouva o spolupráci
# při řešení výzkumného projektu č. 678/2021

uzavřená podle ustanovení § 1746 odst. 2 a souv. zákona č. 89/2012 Sb.,
občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník")

CESNET, zájmové sdružení právnických osob
se sídlem: Zikova 1903/4, 160 00 Praha 6
zapsáno: ve spolkovém rejstříku vedeném Městským soudem v Praze pod spis. značkou L 58848
IČO: 63839172
DIČ: CZ63839172
bankovní spojení: Komerční banka Praha 6, č. účtu: 19-8482200297/0100
zastoupený: [redacted]., ředitelem
ID datové schránky: gn35eaq
(dále jen „CESNET")

na straně jedné

a

Vysoká škola báňská – Technická univerzita Ostrava
Centrum informačních technologií
se sídlem: 17. listopadu 2172/15, 708 00 Ostrava-Poruba
IČO: 61989100
DIČ: CZ61989100
bankovní spojení: ČSOB, č.ú.: 100954151/0300
zastoupená: prof. RNDr. Václavem Snášelem, CSc., rektorem
ID datové schránky: d3kj88v
(dále jen „Organizace")

na straně druhé

(dále jen společně „smluvní strany")
uzavírají níže uvedeného dne, měsíce a roku tuto smlouvu o spolupráci (dále jen „smlouva):

1. Cílem spolupráce smluvních stran je návrh a realizace koncepce praktického řešení bezpečnostních incidentů s ohledem na automatizaci procesů.

2. Tato spolupráce vychází z právního vztahu mezi CESNETem, jako sdružením a Organizací, jako řádným členem tohoto sdružení a je uzavřena jako tzv. „účinná spolupráce“ ve smyslu čl. 2.2.2: bodu 28. Sdělení Komise – Rámce pro státní podporu výzkumu, vývoje a inovací (2014/C 198/01 – dále jen „Rámec“).

1. Předmětem této smlouvy je spolupráce smluvních stran při řešení projektu č. 678/2021, jehož cílem je navržení i realizace koncepce praktického řešení bezpečnostních incidentů v prostředí VŠB-TU Ostrava s ohledem na automatizaci procesů a při zohlednění politiky zvládání incidentů v kontextu systému řízení informační bezpečnosti (ISMS).
2. Výsledky realizace Projektu a praktické poznatky budou prezentovány formou technické zprávy umístěné na webových stránkách Fondu rozvoje CESNET, z.s.p.o. Dalším výstupem bude plně funkční a zdokumentované technické řešení v prostředí poměrně velké univerzitní sítě (cca 20 tis. uživatelů) a dále zdrojové kódy, které budou volně přístupné na některém ze serverů určených k publikování zdrojových kódů (např. Github, Gitlab)

1. Hlavním řešitelem Projektu za Organizaci je [redacted], který je ve vztahu k Organizaci v pracovním poměru (dále jen „Hlavní řešitel“).
2. Organizace zajistí pro řešení Projektu institucionální zabezpečení a finanční prostředky ve výši 103.000,- Kč (slovy stotřitisíce korun českých).
3. CESNET poskytne na řešení Projektu finanční prostředky v celkové výši 200.000,-- Kč (slovy dvěstětisíc korun českých).
4. Výše finančních prostředků stanovených v odstavci 3 nesmí být překročena.
5. Organizace je povinna v přiměřeném rozsahu pravidelně informovat CESNET o průběhu realizace Projektu a doložit výši a účel čerpání poskytnutých finančních prostředků.
6. Organizace prohlašuje, že je samostatným správcem osobních údajů, a že v souladu s platnou právní úpravou se zavazuje zajistit, aby osobní údaje, které potřebuje CESNET využívat za účelem plnění této smlouvy, resp. plnění Projektu, mohl CESNET zpracovat v potřebném rozsahu. Organizace se zejména zavazuje, že bude plnit informační povinnosti vůči subjektům údajů (fyzickým osobám) v rozsahu stanoveném právními předpisy. CESNET prohlašuje, že je v rámci řešení projektů FR samostatným správcem osobních údajů, a to v souladu s platnou právní úpravou.
7. Smluvní strany prohlašují, že byly seznámeny s obsahem dokumentace Projektu, a že obdržely kopii této dokumentace.

1. CESNET poskytne Organizaci finanční prostředky na krytí nákladů dle čl. IV. odst. 3., spojených s řešením Projektu v celkové výši 200.000,- Kč na základě této smlouvy a na účet uvedený v této smlouvě.
2. CESNET převede Organizaci finanční prostředky ve výši 200.000,- Kč. do 3 měsíců po úspěšném ukončení projektu.
3. Pokud nebude naplněn cíl projektu, zavazuje se Organizace vrátit zpět na účet CESNETu finanční prostředky poskytnuté dle čl. V. odst. 1. Tyto prostředky se vrací na základě vyhodnocení projektu částečně popřípadě celé podle rozhodnutí Rady Fondu rozvoje.
4. Pokud nebudou výše uvedené finanční prostředky Organizací vyčerpány v plné výši, budou nevyčerpané finanční prostředky vráceny CESNETu po ukončení projektu.
5. Vratku finančních prostředků dle odst. 3 a 4 provede Organizace převodem na účet CESNETu uvedený v této smlouvě.

1. V případě, že při plnění této smlouvy vznikne jakýkoliv předmět práv duševního vlastnictví na základě společné činnosti smluvních stran v rámci Projektu, náleží vlastnická /majetková a jiná práva k takovému předmětu smluvním stranám ve spoluvlastnických podílech odpovídajících míře přispění k dosažení takového výsledku té které strany s přihlédnutím také k finančním příspěvkům smluvních stran a k duševnímu vlastnictví vkládanému do projektu. Smluvní strany, na základě dohody, písemně potvrdí své podíly na výsledku Projektu bez zbytečného odkladu po určení těchto podílů.
2. Smluvní strany se zavazují po skončení projektu umožnit bezplatný přístup k výsledkům Projektu pro členy sdružení CESNET a jimi zřízené výzkumné organizace.
3. Jde-li o výsledky spolupráce mající povahu autorského díla nebo počítačového programu, pak takové výsledky, včetně jejich publikace a prezentace, mají právo užívat obě smluvní strany při dodržení ustanovení zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění, zejména § 58 cit zákona o zaměstnaneckém díle.

1. Tato smlouva se uzavírá na dobu určitou, a to od nabytí účinnosti této smlouvy do ukončení řešení Projektu. Navrhovaná doba trvání Projektu je maximálně 12 měsíců. V případě uzavření dohody o prodloužení doby trvání Projektu se automaticky prodlužuje o stejnou dobu i platnost a účinnost této smlouvy. Platnost této smlouvy je dána dnem podpisu obou smluvních stran a účinnost dnem zveřejnění v registru smluv.
2. Smluvní strany souhlasí s uveřejněním této smlouvy v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, v platném znění. Organizace se zavazuje zajistit uveřejnění smlouvy

prostřednictvím registru smluv v souladu s výše uvedeným zákonem a CESNET o uveřejnění smlouvy informovat prostřednictvím datové schránky.

3. Smluvní strany souhlasí se zveřejněním plného znění této smlouvy tak, aby tato smlouva mohla být předmětem poskytnuté informace ve smyslu zákona č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění.
4. Tato smlouva může být ukončena vzájemnou dohodou smluvních stran nebo odstoupením od smlouvy v případě závažného porušení povinností stanovených touto smlouvou, nebo z důvodů uvedených v občanském zákoníku. Odstoupení od smlouvy nabývá účinnosti dnem doručení písemného oznámení o odstoupení druhé smluvní strany. Smluvní strany jsou v takovém případě povinny vyrovnat vzájemné závazky nejpozději do 30 dnů ode dne odstoupení od smlouvy.
5. Vztahy neupravené touto smlouvou se řídí příslušnými ustanoveními občanského zákoníku.
6. Vztahuje-li se důvod neplatnosti jen na některé ustanovení smlouvy, je neplatným pouze toto ustanovení, pokud z jeho povahy, obsahu anebo z okolností, za nichž bylo sjednáno, nevyplývá, že jej nelze oddělit od ostatního obsahu smlouvy.
7. Změny a doplňky této smlouvy mohou být prováděny pouze formou písemných číslovaných dodatků, odsouhlasených oběma smluvními stranami. Toto ustanovení je možné změnit pouze postupem dle tohoto odstavce.
8. Smluvní strany se zavazují řešit případné spory vzájemnou dohodou.
9. Výsledky Projektu posoudí hodnotící komise a smluvní strany se zavazují její rozhodnutí respektovat.
10. Tato smlouva je vyhotovena ve dvou stejnopisech s platností originálu, každá strana obdrží jedno paré.
11. Smluvní strany prohlašují, že si text smlouvy přečetly, s jejím obsahem bezvýhradně souhlasí a na důkaz toho připojují podpisy svých oprávněných zástupců.

V Praze dne.....

.....
[redacted]
ředitel
CESNET, z.s.p.o.

V Ostravě dne.....

.....
prof. RNDr. Václav Snášel, CSc.
rektor
VŠB – Technická univerzita Ostrava

**FOND ROZVOJE CESNET, z.s.p.o.** **LIST A**

Agentura Rady Fondu rozvoje CESNET, z.s.p.o., Zikova 1903/4, 166 35 Praha 6
tel. 234 680 236, e-mail: agentura-fr@cesnet.cz

## PODACÍ LIST PROJEKTU

Název projektu: Č. j. fondu 57 /2021

Koncepce řešení bezpečnostních incidentů v prostředí VŠB-TU Ostrava.

Oblast: I.

Tematický okruh: A.

Celkový počet řešitelů: 4 Navrhovaná délka trvání projektu (počet měsíců) : 12

Finanční prostředky požadované z FR CESNET (v tis. Kč včetně DPH):

| IV: | NIV: 200 | Celkem: 200 |
|---|---|---|

Hlavní řešitel:

Příjmení, jméno, titul: [redacted]

Název člena sdružení: Vysoká škola Báňská - Technická univerzita Ostrava

Ústav AV / org. součást VŠ: Centrum informačních technologií

Sídlo: 17.listopadu 15, Ostrava-Poruba, 708 33

Telefon: [redacted]

E-mail:

Anotace projektu (česky i anglicky):

Hlavním cílem projektu je navržení i realizace koncepce praktického řešení bezpečnostních incidentů v prostředí VŠB-TU Ostrava s ohledem na automatizaci procesů.

The main goal of the project is to design and implement the concept and solution of security incidents in the VŠB-TU Ostrava environment and automation of these processes.

**FOND ROZVOJE CESNET, z.s.p.o.** LIST B

Agentura Rady Fondu rozvoje CESNET, z.s.p.o., Zikova 1903/4, 166 35 Praha 6

**PROHLÁŠENÍ STATUTÁRNÍHO ZÁSTUPCE AV ČR NEBO VŠ - ČLENA SDRUŽENÍ CESNET**

Název projektu
Koncepce řešení bezpečnostních incidentů v prostředí VŠB-TU Ostrava.

Č. j. fondu 698 /2021

Hlavní řešitel: [redacted]

Název člena: Vysoká škola Báňská - Technická univerzita Ostrava

Ústav AV / org.součást VŠ: Centrum informačních technologií

Finanční prostředky požadované z FR CESNET (v tis. Kč. včetně DPH):

| IV: | NIV: | 200 | Celkem: | 200 |
|---|---|---|---|---|

**Vyjádření statutárního zástupce VŠ nebo AV ČR - člena sdružení CESNET :**

Prohlašuji, že řešitel je v hlavním pracovním poměru v naší organizaci a že pro řešení projektu

poskytne (název organizace) Vysoká škola Báňská - Technická univerzita Ostrava

institucionální zabezpečení a finanční příspěvek ve výši 103 000 Kč.

[redacted]

10. 02. 2021

Datum

prof. RNDr. Václav Snášel, CSc.
rektor VŠB-TUO

[redacted]

**FOND ROZVOJE CESNET, z.s.p.o.** LIST C

Agentura Rady Fondu rozvoje CESNET, z.s.p.o., Zikova 1903/4, 166 35 Praha 6

## IDENTIFIKAČNÍ LIST SPOLUŘEŠITELE - ČLENA SDRUŽENÍ

Název projektu: Č. j. fondu 679 /2021

Koncepce řešení bezpečnostních incidentů v prostředí VŠB-TU Ostrava.

Hlavní řešitel: [redacted]

Spoluřešitel:

Příjmení, jméno, titul: [redacted]

Název člena sdružení: Vysoká škola Báňská - Technická univerzita Ostrava

Ústav AV / org. součást VŠ: Centrum informačních technologií

Sídlo: 17. listopadu 2172/15, 708 00 Ostrava – Poruba

### PROHLÁŠENÍ SPOLUŘEŠITELE:

Souhlasím, aby uvedený hlavní řešitel řídil práce na projektu a disponoval přidělenými finančními prostředky.

Prohlašuji, že jsem uvedl úplné a pravdivé údaje a beru na vědomí, že v opačném případě nebo při porušení obecně uznávaných zásad vědeckopedagogické etiky nebo pro hrubé závady při řešení projektu a hospodaření s přidělenými finančními prostředky a při kontrole výsledků podle čl.15 e) Konkurzního řádu Rady Fondu rozvoje CESNET, z.s.p.o. mohu být vyloučen z účasti na výběrovém řízení.

Souhlasím s tím, aby Rada fondu rozvoje CESNET používala osobní údaje uvedené v této žádosti při zpracování a evidenci mého projektu ve výběrovém řízení vypsaném pro rok 2021.

[redacted]

Datum Podpis spoluřešitele

### VYJÁDŘENÍ VEDOUCÍHO PRACOVNÍKA SPOLUŘEŠITELE:

Souhlasím s účastí spoluřešitele na projektu a poskytnu mu institucionální zabezpečení.

9. 2. 2021 [redacted]

Datum Podpis vedoucího pracovníka

**FOND ROZVOJE CESNET, z.s.p.o.** LIST C

Agentura Rady Fondu rozvoje CESNET, z.s.p.o., Zikova 1903/4, 166 35 Praha 6

## IDENTIFIKAČNÍ LIST SPOLUŘEŠITELE - ČLENA SDRUŽENÍ

Č. j. fondu 671 /2021

Název projektu:
Koncepce řešení bezpečnostních incidentů v prostředí VŠB-TU Ostrava.

Hlavní řešitel: [redacted]

Spoluřešitel:

Příjmení, jméno, titul: [redacted]

Název člena sdružení: Vysoká škola Báňská - Technická univerzita Ostrava

Ústav AV / org. součást VŠ: Centrum informačních technologií

Sídlo: 17. listopadu 2172/15, 708 00 Ostrava – Poruba

**PROHLÁŠENÍ SPOLUŘEŠITELE:**

Souhlasím, aby uvedený hlavní řešitel řídil práce na projektu a disponoval přidělenými finančními prostředky.

Prohlašuji, že jsem uvedl úplné a pravdivé údaje a beru na vědomí, že v opačném případě nebo při porušení obecně uznávaných zásad vědeckopedagogické etiky nebo pro hrubé závady při řešení projektu a hospodaření s přidělenými finančními prostředky a při kontrole výsledků podle čl.15 e) Konkurzního řádu Rady Fondu rozvoje CESNET, z.s.p.o. mohu být vyloučen z účasti na výběrovém řízení.

Souhlasím s tím, aby Rada fondu rozvoje CESNET používala osobní údaje uvedené v této žádosti při zpracování a evidenci mého projektu ve výběrovém řízení vypsaném pro rok 2021.

9. 2. 2021
Datum

[redacted]
Podpis spoluřešitele

**VYJÁDŘENÍ VEDOUCÍHO PRACOVNÍKA SPOLUŘEŠITELE:**

Souhlasím s účastí spoluřešitele na projektu a poskytnu mu institucionální zabezpečení.

9. 2. 2021
Datum

[redacted]
Podpis vedoucího pracovníka

**FOND ROZVOJE CESNET, z.s.p.o.** LIST C

Agentura Rady Fondu rozvoje CESNET, z.s.p.o., Zikova 1903/4, 166 35 Praha 6

## IDENTIFIKAČNÍ LIST SPOLUŘEŠITELE - ČLENA SDRUŽENÍ

Název projektu: Č. j. fondu 678 /2021

Koncepce řešení bezpečnostních incidentů v prostředí VŠB-TU Ostrava.

Hlavní řešitel: [redacted]

Spoluřešitel:

Příjmení, jméno, titul: [redacted]

Název člena sdružení: Vysoká škola Báňská - Technická univerzita Ostrava

Ústav AV / org. součást VŠ: Centrum informačních technologií

Sídlo: 17. listopadu 2172/15, 708 00 Ostrava – Poruba

### PROHLÁŠENÍ SPOLUŘEŠITELE:

Souhlasím, aby uvedený hlavní řešitel řídil práce na projektu a disponoval přidělenými finančními prostředky.

Prohlašuji, že jsem uvedl úplné a pravdivé údaje a beru na vědomí, že v opačném případě nebo při porušení obecně uznávaných zásad vědeckopedagogické etiky nebo pro hrubé závady při řešení projektu a hospodaření s přidělenými finančními prostředky a při kontrole výsledků podle čl.15 e) Konkurzního řádu Rady Fondu rozvoje CESNET, z.s.p.o. mohu být vyloučen z účasti na výběrovém řízení.

Souhlasím s tím, aby Rada fondu rozvoje CESNET používala osobní údaje uvedené v této žádosti při zpracování a evidenci mého projektu ve výběrovém řízení vypsaném pro rok 2021.

9.2.2021
Datum

[redacted]
Podpis spoluřešitele

### VYJÁDŘENÍ VEDOUCÍHO PRACOVNÍKA SPOLUŘEŠITELE:

Souhlasím s účastí spoluřešitele na projektu a poskytnu mu institucionální zabezpečení.

9.2.2021
Datum

[redacted]
Podpis vedoucího pracovníka

**FOND ROZVOJE CESNET, z.s.p.o.** **LIST D**

Agentura Rady Fondu rozvoje CESNET, z.s.p.o., Zikova 1903/4, 166 35 Praha 6

## 2. CHARAKTERISTIKA CÍLE PROJEKTU A JEHO PŘEDPOKLÁDANÉHO PŘÍNOSU

Název projektu: Č. j. fondu 677 /2021

Koncepce řešení bezpečnostních incidentů v prostředí VŠB-TU Ostrava.

Hlavní řešitel: [redacted]

KONKRÉTNÍ VÝSTUPY

Výstupem bude funkční systém vč. procesního zajištění a provozních doporučení, která budou replikovatelná i v jiných sítích a institucích.

V ČEM SPOČÍVÁ PŘÍNOS PROJEKTU

Hlavní přínos spočívá v automatizaci mnoha procesů, které v současnosti realizujeme víceméně ručně, jejich přehled a možnost delegace některých činností na bezpečnost nespecializované pracovníky.

Uveďte, zda předpokládáte, že výsledkem projektu/jedním z výsledků projektu může být předmět způsobilý ochrany právem duševního vlastnictví ( např. vynález, užitný vzor, autorské dílo, počítačový program). Pokud ano, uveďte v návrhu projektu předpokládaný způsob ochrany takového výsledku a zda bude nutné omezení závěrečné zprávy projektu.

VLASTNÍ ROZVOJOVÝ PROJEKT JE PŘIPOJEN (min. 3 strany)

Osnova:
a) Současný stav řešeného problému
b) Cíle řešení
c) Způsob řešení
d) Prezentace výsledků
e) Charakteristika řešitelského kolektivu,
odborný životopis řešitele a spoluřešitelů
f) Navrhovaná doba trvání projektu (počet měsíců) - navrhovaná délka trvání
g) Konkretizace a zdůvodnění jednotlivých požadavků řešitele - položky dlouhodobého majetku (investiční) doložte nabídkou, ostatní položky (neinvestiční) rozepište po jednotlivých položkách v souladu se strukturou na listu E, není třeba dokládat nabídkou

PROHLÁŠENÍ

Uveďte, zda se na financování podaného projektu podílejí další subjekty.

| | Zdroj financování | Výše fin. prostředků |
|---|---|---|
| | | |

**FOND ROZVOJE CESNET, z.s.p.o.** **LIST E**

Agentura Rady Fondu rozvoje CESNET, z.s.p.o., Zikova 1903/4, 166 35 Praha 6

**ROZPOČET NÁKLADŮ S PŘIPOJENOU DOKUMENTACÍ**

Název projektu: Č. j. fondu 678 /2021

Koncepce řešení bezpečnostních incidentů v prostředí VŠB-TU Ostrava.

Hlavní řešitel: [redacted]

| | Spoluúčast nositele | Požadováno z Fondu rozvoje | Náklady celkem (**) |
|---|---|---|---|
| (*) Dlouhodobý hmotný a nehmotný majetek - položka nad 60 tis. Kč | | | |
| Náklady na dlouhodobý hm.a nehm.majetek celkem: | 103 | | 103 |
| (*) Ostatní náklady | | | |
| Mzdy | | | |
| Odměny řešitelům a spoluřešitelům | | 117 | 117 |
| Ostatní osobní výdaje (Ostatní mzdové náklady) | | | |
| Sociální a zdravotní pojištění | | 63 | 63 |
| Knihy, učební pomůcky, odborná dokumentace | | | |
| Drobný hmotný majetek | | | |
| Drobný nehmotný majetek | | | |
| Materiál | | | |
| Pronájem zařízení | | | |
| Cestovné tuzemské | | | |
| Cestovné zahraniční | | | |
| Školení | | | |
| Ostatní služby | | | |
| Režie | | 20 | 20 |
| Ostatní (neinvestiční) náklady celkem | | | |
| Náklady celkem | | | |
| **Náklady celkem** | 103 | 200 | 303 |

***Veškeré finanční údaje uvádějte v tis. Kč, včetně DPH***

**PROHLÁŠENÍ ŘEŠITELE**

Prohlašuji, že jsem uvedl úplné a pravdivé údaje a beru na vědomí, že v opačném případě nebo při porušení obecně uznávaných zásad vědeckopedagogické etiky nebo pro hrubé závady při řešení projektu a hospodaření s přidělenými finančními prostředky a při kontrole výsledků podle čl.15 e) Konkurzního řádu Rady Fondu rozvoje CESNET, z.s.p.o. mohu být vyloučen z účasti na výběrovém řízení.

Souhlasím s tím, aby Rada fondu rozvoje CESNET používala osobní údaje uvedené v této žádosti při zpracování a evidenci mého projektu ve výběrovém řízení vypsaném pro rok 2021.

7.2.2021 [redacted]

Datum Podpis

(*) Přesně rozepište v návrhu projektu podle jednotlivých položek v částkách bez DPH a včetně DPH

(**)Včetně příspěvku VŠ či fakulty nebo ústavu AV ČR, ale bez případných příspěvků z jiných zdrojů

# Koncepce řešení bezpečnostních incidentů v prostředí VŠB-TU Ostrava

## Současný stav řešeného problému

V současné je Bezpečnostní IT tým Centra informačních technologií VŠB-TU Ostrava dennodenně konfrontován s mnoha opakujícími se bezpečnostními incidenty. Ty můžeme rozdělit pro účely tohoto projektu na tyto základní druhy:

- hlášení externích organizací a bezpečnostních týmů o podezřelém provozu zařízení v síti univerzity,
- interně zjištěné nezabezpečené nebo napadené systémy,
- systémy útočící na naši síť,
- systémy, jejichž provoz chceme blokovat (např. phishingové weby).

Úkolem bezpečnostního týmu univerzity je vyhodnotit tyto informace, kategorizovat a potvrdit je. Často je výstupem tohoto postupu blokace systému nebo další komunikace s uživateli.

Bezpečnostní tým Centra informačních technologií rovněž periodicky provádí kontrolu zranitelností zařízení v síti a při nalezení závažnějších problémů aktivně a opakovaně oslovuje zodpovědné osoby s žádostí o nápravu a eventuálně přistupuje k blokaci zařízení.

Za poslední rok Bezpečnostní tým řešil více než 1000 těchto incidentů a v posledních letech je viditelný nárůst počtu incidentů v řádech desítek procent. Zejména administrativa spojená s řešením každého incidentu nadměrně a neúměrně vytěžuje zaměstnance poštovního i bezpečnostního týmu. Často je nutná osobní komunikace, resp. upomínání provozovatelů zavirovaných systémů a hlídání dohodnutých termínů. Je smutnou skutečností, že některé incidenty související s nezabezpečenými systémy řešíme i více než půl roku.

Veškerou evidenci incidentu vedeme v Helpdeskovém systému. Ale i přesto, že se této oblasti věnuje více specialistů, tak je prakticky velmi problematické zajistit koordinaci a řešení mnoha paralelně řešených incidentů.

Aktuální mechanismy pro blokaci jsou nasazeny částečně a nejsou unifikovány, případné zpětné dohledávání informací je tedy zdlouhavé.

# Cíle řešení

Cílem řešení je doplnění portálu pro technickou IT podporu o část, ve kterém budou moci pověřené osoby realizovat úkony spojené s procesem řešení bezpečnostního incidentu.

Plánujeme část komunikace přenést na IT Helpdesk. Proto budou stávající procesy zjednodušeny, což zároveň umožní řešit alespoň méně technické úkony pracovníkům IT Helpdesku.

Vytvořené rozhraní bude sloužit jako centrální bod pro blokace a podstatnou část práce zautomatizuje. Automatizace procesu bude spočívat v automatizovaném hlídání časů a automatickém odesílání informačních e-mailů uživatelům. Proces a chování aplikace při blokaci zařízení ve vnitřní síti univerzity jsme znázornili na vývojovém diagramu níže. V případě blokování phishingových domén bude automaticky staré blokace odstraňovat.

1. Bezpečnostní incident vyhodnocuje bezpečnostní specialista, který také zhodnotí nutnost okamžité blokace, popř. nastavení časech vyřešení (T1, T2).
2. Email s informací o nutnosti řešit problém jeho systému bude automatizovaně odeslán zodpovědné osobě systému (ZO).
3. Pokud ZO nevyřeší opravu do definovaného času T1, bude koncovému zařízení automatizovaně zablokován provoz v síti (DHCP, BHR). Zároveň bude ZO informována emailem o proběhlé blokaci.
4. Pokud ZO nevyřeší opravu do definovaného času T2, tak bude systém ze sítě úplně odpojen (zrušená registrace v DHCP/DNS). Zároveň bude ZO informována e-mailem o zrušené registraci.

Nasazením tohoto procesu odpadá neustálá komunikace se zodpovědnými osobami, hlídání termínů i ruční blokace. Zároveň lze dohledat historii jednotlivých kroků vč. dokumentovaných výzev.

# Způsob řešení

Technické řešení chceme postavit pomocí open-source prostředků. Šablony zpráv a způsoby blokace budou řešeny modulárně a budou tak snadno upravitelné podle potřeb organizace, která se naše řešení rozhodne využít. Pro naše potřeby konkrétně implementujeme moduly:

- blokace uživatelů pevné sítě prostřednictvím registračního systému IP adres SIPAM,
- blokování IP adres technikou BHR (tzv. Black Hole Routing),
- blokování doménových jmen v DNS (RPZ zóna),
- blokace uživatelů nebo mobilních zařízení na RADIUS serverech,
- blokace v centrálním antivirovém řešení.

Dále prozkoumáme možnost integrace systému s antivirovým řešením společnosti ESET Security+, jež na univerzitě aktuálně využíváme a které má prostřednictvím API možnost vkládat další pravidla. Tím bychom docílili uplatnění bezpečnostních opatření i na zařízeních, která jsou zapojena mimo síť univerzity, což je v současné době důležité.

Při zadání nového záznamu k blokaci bude do zvolených systémů předán požadavek k blokaci, dojde k provázání odkazů na jednotlivé systémy (RequestTracker, BHR, DNS, SIPAM, Radius) a uživateli bude zaslána zpráva o naplánované nebo aktivované blokaci.

Blokování uživatelských účtů máme již centrálně řešeno a v tomto projektu se této oblasti věnovat nebudeme.

Servery, resp. aplikace vyvinuté a nasazené pro účely tohoto projektu budeme realizovat ve virtualizačním prostředí. Pro tyto potřeby plánujeme pořízení fyzického serveru, který bude redundantně 2x10GE porty zapojen do počítačové sítě datového centra. Pro realizaci jsme zvolili kapacitně odpovídající server, na kterém budeme provozovat virtualizační systém VMWARE a rámci něj budeme realizovat všechny potřebné servery (BHR, DNS, databázový apod.).

## Blokace registrací s využitím DAI

V síti máme nasazeny technologie DAI (Dynamic ARP Inspection), které zajišťují, že v síti nemůže být provozováno zařízení bez platné registrace v DHCP. Počítače ve vnitřní síti univerzity tedy můžeme také blokovat zrušením jejich registrace v DHCP.

Životní cyklus registrací koncových zařízení řešíme v aplikaci SIPAM, ve které jsou ošetřeny stavy registrované / registrované do / expirované zařízení. Aplikace SIPAM generuje podle pravidel konfigurace pro DNS a DHCP servery. Při blokaci zařízení bude na API systému SIPAM odeslán požadavek pro pozastavení registrace.

## BHR - Black Hole Routing

Implementaci BHR budeme řešit na virtualizovaném systému provozovaném v rámci univerzitního datového centra. Z něj budou navázány BGP spojení na BGP route-reflectory univerzitní sítě, které budou šířit informace o blokacích na všechny směrovače univerzity.

Pro technickou realizaci počítáme s nasazením OS Debian GNU/Linux, produktu ExaBGP a databáze PostgreSQL.

Tím lze dosáhnout téměř okamžité blokace jakékoliv IPv4/v6 adresy z adresního prostoru univerzity nebo i Internetu. S dalším budoucím rozvojem možností prvků páteřní počítačové sítě počítáme s využitím tohoto mechanismu pro filtraci nejen IP adres, ale případně i protokolů a portů.

Tento způsob blokace je vhodný pro konkrétní blokace IP adres, ve vnitřní síti univerzity i z Internetu.

## Blokování v DNS - RPZ

Implementaci RPZ budeme řešit na virtualizovaném systému provozovaném v rámci univerzitního datového centra. V rámci tohoto systému budou vedeny interní zóny (např. rpz.vsb.cz), které budou automaticky šířeny na všechny kešující DNS servery.

V současné době jsou v síti VŠB-TU Ostrava provozovány tři nezávislé kešující DNS servery, které současně obsluhují jednu IPv4/v6 adresu. Pro tyto účely využíváme techniky tzv. *anycastu*. Tímto způsobem řešíme vysokou dostupnost DNS služby a také rozkládání zátěže.

Tyto DNS systémy jsou využívány všemi koncovými systémy v síti univerzity a je technicky znemožněna dostupnost DNS služby mimo tyto univerzitu jiným způsobem.

Doménová jména, která budou blokována, budou směrována na dedikovaný server. Tento server zaznamená přístupy, tedy potenciálně kompromitované koncové systémy, popř. vypíše uživatelům prostřednictvím webového prohlížeče bližší informace o blokaci. Zvážíme potřebu nasadit pro tuto činnost více serverů pro případy většího množství přístupů.

Tento způsob blokace se nejčastěji uplatní např. při blokaci botnet nebo phishingových serverů, jejichž IP adresa v DNS se často mění. Je celkem běžné, že FQDN botnet serverů mají životnost v řádech jednotek minut a využití tohoto způsobu blokace je v podstatě nejrychlejší účinná metoda.

1. Realizuje řešitel incidentu, specifikuje dobu platnosti záznamu.
2. Systém vloží záznam do DB.
3. Automaticky se aktualizuje zóna RPZ.VSB.CZ.
4. Automaticky se distribuuje zóna na všechny kešující DNS servery univerzity.

## ESET Security+

Námi provozovaný systém ESET Security+ provozujeme s centralizovanou správou a umožňuje nám vkládat pravidla pro blokace ip adres a FQDN, která se aplikují na všech systémech, které mají instalovaného agenta tohoto bezpečnostního systému. To má zásadní výhodu, že můžeme některé bezpečnostní opatření aplikovat i na systémech, které jsou mimo síť univerzity a nemusí být připojeny do sítě ani prostřednictvím VPN klienta. V rámci projektu prozkoumáme možnost řešit tuto činnost přes API z centrální aplikace, kterou vytvoříme.

## Aplikace pro bezpečnostní incidenty a IT helpdesk

Rozhraní pro blokace bude provozováno jako webová aplikace. V rozhraní bude mít správce k dispozici formulář, ve kterém si bude moci zvolit co blokovat a přes jaké mechanismy blokace proběhne. Kromě zadávání nových blokací zde bude uveden přehled plánovaných/probíhajících blokací s možností úprav časů T1 a T2. O probíhajících blokačních procesech bude portál zodpovědnou osobu informovat prostřednictvím elektronicky podepsaných e-mailových zpráv.

Události budou zaznamenávány a zobrazovány jak v portálu, tak v univerzitním SIEM řešení.

Případné platné nebo blížící se blokace budou uživateli zobrazeny v přehledu registrovaných zařízení v uživatelském portálu univerzity.

Portál bude vyvíjen maximálně modulárně a bude tedy snadno upravitelný a doplnitelný o další požadovanou funkcionalitu.

# Fáze projektu

### 1.-2. měsíc od započetí projektu

V tomto prvním období budou započaty práce na realizaci projektu, proběhne nákup HW vybavení, instalace SW částí, testování výkonu a dostupnosti řešení.

Odhadovaná časová náročnost je 20 člověkodní.

### 3.-9. měsíc od započetí projektu

V této fázi projektu budou realizovány práce v následujících oblastech:

- vývoj centrálního blokačního portálu pro obsluhu a pracovníky IT Helpdesku,
- implementace, konfigurace a testování jednotlivých blokačních mechanismů a komunikace s jednotlivými systémy (Radius servery, BGP route reflectory, ESET management, DNS servery),
- provázání všech systémů,
- provozní testování.

Odhadovaná časová náročnost je 32 člověkodní.

### 10.-12. měsíc od započetí projektu

V této fázi projektu budou probíhat finální práce, rutinní provoz a také tvorba dokumentace a závěrečné zprávy.

Odhadovaná časová náročnost je 20 člověkodní.

# Prezentace výsledků

Výsledky a výstupy projektu budeme prezentovat v závěrečné zprávě řešení projektu, která bude veřejně dostupná na WWW stránkách fondu i na našich webových stránkách, kde bude umístěna i technická zpráva.

Po ukončení projektu předpokládáme využití našich poznatků i dalšími organizacemi zapojenými do sdružení CESNET.

Zdrojové kódy dáme k dispozici komunitě a budou publikovány na některém ze serverů určeným k publikování zdrojových kódů (např. Github, Gitlab).

Výstupy projektu plánujeme prezentovat i na některých odborných seminářích (např. Europen, EUNIS apod.).

Krom toho bude hlavním výstupem plně funkční a zdokumentované technické řešení v prostředí poměrně velké univerzitní sítě, která má 20 tis. uživatelů.

# Charakteristika řešitelského kolektivu

[redacted]

Zaměstnanec Centra informačních technologií VŠB-TUO, kde působí jako vedoucí oddělení IT infrastruktury. Profesně se zabývá správou počítačové sítě TUONET a správou unixových systémů a technických prostředků datového centra.

[redacted]

Zaměstnanec Centra informačních technologií VŠB-TU Ostrava, kde působí od roku 2016 jako administrátor linuxových systémů, počítačové sítě a virtualizační infrastruktury. Je členem bezpečnostního týmu VŠB-TUO. Podílel se na řešení několika projektů Fondu rozvoje CESNET.

[redacted]

Zaměstnanec Centra informačních technologií VŠB-TU Ostrava, kde působí od roku 2013 jako administrátor linuxových systémů poskytujících celouniverzitní služby. Je členem bezpečnostního týmu VŠB-TUO.

[redacted]

Zaměstnanec Centra informačních technologií VŠB-TU Ostrava, kde působí od roku 2016 jako administrátor linuxových systémů. Je členem bezpečnostního týmu VŠB-TUO. Podílel se na řešení několika projektů Fondu rozvoje CESNET.

# Navrhovaná doba řešení projektu

Navrhovaná doba trvání projektu je 12 měsíců.

# Konkretizace a zdůvodnění požadavků řešitele

Veškeré technické práce budou realizovány v prostředí virtualizační infrastruktury a na prvcích počítačové sítě VŠB-TU Ostrava, tedy v již pořízené a provozované infrastruktuře, která bude doplněna a z prostředků VŠB-TU Ostrava budou hrazeny náklady na:

- Server pro provoz serverů projektu (BHR, DNS, PostgreSQL, portálová aplikace) v celkové ceně 103 tis. Kč vč. DPH.

Z prostředků FR CESNETu budou hrazeny náklady na:

- Odměny řešitelům v celkové výši 120 tis. Kč a odvody na zdravotní a sociální pojištění ve výši 60 tis. Kč. Tyto částky budou vyplaceny po úspěšné obhajobě projektu.

- Režijní náklady v celkových nákladech 20 tis. Kč. Budou použity zejména na administrativu projektu, účast na odborných seminářích apod.

Při kalkulaci jsme vycházeli z nákladů 2500 Kč / člověkoden včetně odvodů. Podrobný rozpis prací a jejich časové náročnosti je uveden v kapitole "Fáze projektu".

# Vypořádání majetku pořízeného v rámci projektu

Investiční náklady budou plně hrazeny z prostředků VŠB-TU Ostrava.

# Prodejní nabídka

## Položky nabídky

| Název | Prodejní cena po započtení slev | Počet | Celková cena s DPH |
|---|---|---|---|
| HPE DL360 Gen10 4210 1P 16G NC 8SFF Svr | [redacted] | ks | 53 084,27 |
| HPE 500W FS Plat Ht Plg LH Pwr Sply Kit | | ks | 3 686,27 |
| HPE 16GB 1Rx4 PC4-2933Y-R Smart Kit | | ks | 14 590,79 |
| HPE 240GB SATA RI SFF RW DS SSD | | ks | 8 514,77 |

**Celková cena:** 66 013,30 Kč

**Celková cena s DPH:** 79 876,09 Kč

Upozornění: Celkové ceny zahrnují poplatky (recyklační, autorské).