MVCRP015VB4Z

Smlouva

o poskytnutí účelové podpory
na řešení projektu výzkumu, vývoje a inovací s názvem

„Predikce a ochrana před kybernetickými incidenty“

VI20152020026

uzavřená mezi smluvními stranami

Česká republika – Ministerstvo vnitra

a

CZ.NIC, z.s.p.o.

Č.j.MV-90617-3/OBVV-2015
Počet stran: 13
Přílohy: 2/19 18 ks.

Smluvní strany

Česká republika – Ministerstvo vnitra

se sídlem Nad Štolou 936/3, 170 34 Praha 7
IČ: 00007064
DIČ: CZ00007064
zastoupená ředitelem odboru bezpečnostního výzkumu a policejního vzdělávání
JUDr. Petrem Novákem, Ph.D.
číslo bankovního účtu: 3605881/0710
adresa pro doručování: Ministerstvo vnitra, odbor bezpečnostního výzkumu a policejního vzdělávání (gesční útvar MV ČR pro oblast bezpečnostního výzkumu), Nad Štolou 936/3, 170 34 Praha 7, tel.: 974 832 746, fax: 974 833 518, e-mail: obv@mvcr.cz

(dále jen „**poskytovatel**")

a

CZ.NIC, z.s.p.o.

se sídlem Milešovská 1136/5, 130 00 Praha 3
IČ: 67985726
DIČ: CZ67985726
statutární zástupce: Mgr. Ondřej Filip, MBA, výkonný ředitel
zapsaná ve spolkovém rejstříku vedeném Městským soudem v Praze, oddíl L, vložka 58624
[redacted]
adresa pro doručování: sídlo příjemce

kontaktní osoba: manažer projektu
[redacted]

(dále jen „**příjemce**")

uzavírají v rámci Programu bezpečnostního výzkumu České republiky v letech 2015 - 2020 (BV III/1 – VS), na základě § 9 zákona č. 130/2002 Sb., o podpoře výzkumu, experimentálního vývoje a inovací z veřejných prostředků a o změně některých souvisejících zákonů ve znění pozdějších předpisů (dále jen „zákon č. 130/2002 Sb.") a v souladu se zákonem č. 89/2012 Sb., občanský zákoník (dále jen „občanský zákoník") tuto

Smlouvu o poskytnutí účelové podpory
na řešení projektu výzkumu, vývoje a inovací
(dále jen „Smlouva")

[redacted]

Článek 1
Předmět Smlouvy

1) Předmětem této Smlouvy je závazek příjemce řešit projekt výzkumu, vývoje a inovací s názvem **„Predikce a ochrana před kybernetickými incidenty"** a identifikačním kódem **„VI20152020026"** a závazek poskytovatele poskytnout příjemci na tento projekt účelovou podporu z veřejných prostředků (dále jen "podpora") v rozsahu a za podmínek stanovených Smlouvou.

2) Předmětem řešení projektu je průmyslový výzkum, zaměřený na vybudování účinného systému detekce, identifikace a predikce kybernetických hrozeb a vyhodnocování kybernetických bezpečnostních incidentů (tzv. Cyber Threat Intelligence).

3) Cíle projektu, předpokládané výsledky, rozpočet a harmonogram projektu, včetně dalších údajů jsou uvedeny ve schváleném projektu, který je přílohou č. 1 Smlouvy (dále jen „Projekt").

Článek 2
Administrátor Projektu

1) Administrátor Projektu je zaměstnanec gesčního útvaru pro oblast bezpečnostního výzkumu určený poskytovatelem, který je odpovědný za spolupráci a komunikaci s příjemcem ve všech záležitostech věcného plnění Projektu a finančního využití poskytnuté podpory.

2) Jméno a kontaktní údaje administrátora projektu budou příjemci sděleny při předání Smlouvy.

Článek 3
Manažer Projektu

Manažer Projektu určený příjemcem je odpovědný za řízení Projektu, včetně finančního řízení, za spolupráci a komunikaci s poskytovatelem.

Článek 4
Hlavní řešitel Projektu

Za odbornou úroveň Projektu dle § 9 odst. 1 písm. e) zákona č. 130/2002 Sb. je příjemci odpovědný Pavel Bašta.

Článek 5
Doba řešení Projektu

1) Příjemce zahájí řešení Projektu dne 1. 9. 2015.

2) Příjemce je povinen ukončit řešení Projektu nejpozději ke dni 31.8.2020.

Článek 6
Uznané náklady, výše podpory a platební podmínky

1) Uznané náklady[1] na řešení Projektu se stanovují ve výši **13 592 900 Kč** (slovy: třináctmilionůpětsetdevadesátdvatisícdevětsetkorunčeských). Tato částka zahrnuje podporu ve výši **10 194 000 Kč** (slovy: desetmilionůjednostodevadesátčtyřitisíckorun českých), která je poskytovaná formou dotace z rozpočtové kapitoly Ministerstva vnitra a vlastní zdroje příjemce.

2) Členění uznaných nákladů na jednotlivé položky a pro jednotlivé roky řešení Projektu je uvedeno v rozpočtu Projektu.

[1] Uznané náklady jsou takové způsobilé náklady, které poskytovatel schválil a které jsou zdůvodněné.

3) Nedojde-li v důsledku rozpočtového provizoria podle zákona č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů (dále jen „zákon o rozpočtových pravidlech") k regulaci čerpání rozpočtu, poskytovatel poskytne podporu příjemci v prvním roce řešení Projektu ve lhůtě do 60 kalendářních dnů ode dne nabytí účinnosti Smlouvy. V dalších letech řešení poskytovatel poskytne podporu do 60 kalendářních dnů od začátku kalendářního roku za podmínky, že jsou splněny závazky příjemce vyplývající ze Smlouvy, zejména, že příjemce předložil roční zprávu včetně vyúčtování poskytnutých finančních prostředků, a tato zpráva byla schválena poskytovatelem, a že jsou zařazeny údaje do informačního systému výzkumu, vývoje a inovací v souladu se zákonem č. 130/2002 Sb., Nařízením vlády č. 397/2009 Sb., o informačním systému výzkumu, experimentálního vývoje a inovací (dále jen „NV č. 397/2009 Sb.") a se zvláštním právním předpisem (zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů).

4) Pokud v průběhu řešení Projektu dojde ke snížení plánovaných finančních prostředků na výzkum a vývoj poskytovatele v rámci státního rozpočtu, je poskytovatel oprávněn jednostranně snížit podporu uvedenou v odst. 1 tohoto Článku a bude uzavřen písemný dodatek ke Smlouvě, v němž se vymezí související úpravy Projektu.

5) Podpora bude poskytována v souladu s rozpočtem bezhotovostním převodem z bankovního účtu poskytovatele na běžný korunový bankovní účet příjemce.

6) Příjemce má povinnost provést audit celého Projektu. Auditorskou zprávu předloží příjemce poskytovateli spolu se závěrečným vyúčtováním Projektu. Audit se týká všech nákladů Projektu. Do uznaných nákladů lze zahrnout pouze náklady na provedení auditu v závislosti na době realizace a účetní náročnosti Projektu až do výše 100 000 Kč.

Článek 7
Změny Rozpočtu

1) Podstatnou změnou rozpočtu, pro jejíž provedení je nutný předchozí souhlas poskytovatele se rozumí:
   a) zdůvodněná změna celkové výše rozpočtu příjemce,
   b) zdůvodněný přesun uvnitř rozpočtové skupiny mezi položkami přesahující 10 % celkových nákladů této skupiny v rámci rozpočtu příjemce v daném kalendářním roce,
   c) zdůvodněný přesun mezi rozpočtovými skupinami přesahující 10 % celkového rozpočtu příjemce v daném kalendářním roce.

2) Ostatní změny rozpočtu musí být se zdůvodněním oznámeny poskytovateli do 7 pracovních dnů od jejich provedení. Dojde-li k ostatní změně rozpočtu v měsíci prosinci, oznámí ji příjemce v roční zprávě za příslušný rok.

3) V případě, že součet objemu jednotlivých změn rozpočtu dle odst. 2 tohoto Článku v daném kalendářním roce dosáhne hranice stanovené v odst. 1 písm. b) nebo c) tohoto Článku, podléhá každá další změna rozpočtu předchozímu souhlasu poskytovatele.

4) Přesun finančních prostředků z rozpočtových skupin do rozpočtové skupiny osobní náklady a přesun finančních prostředků mezi jednotlivými položkami v rámci rozpočtové skupiny osobní náklady lze provést pouze s předchozím souhlasem poskytovatele.

5) Pokud příjemce neobdrží stanovisko poskytovatele do 15 kalendářních dnů ode dne odeslání informace o podstatné změně rozpočtu dle odst. 1 tohoto Článku nebo o změně dle odst. 3 a 4 tohoto Článku, považuje se změna rozpočtu za schválenou poskytovatelem. Poskytovatel může lhůtu prodloužit o 15 kalendářních dnů; je však povinen o prodloužení lhůty příjemce písemně informovat.

6) Žádosti příjemce o předchozí souhlas poskytovatele podle odst. 1 a 3 tohoto Článku i oznámení změny rozpočtu podle odst. 2 tohoto Článku předává příjemce prostřednictvím formuláře zveřejněného na webových stránkách Ministerstva vnitra včetně nové verze rozpočtu a komentáře popisujícího jeho změny.

7) Při postupu příjemce v rozporu s tímto Článkem bude postupováno dle Článku 20 odst. 3 Smlouvy.

Článek 8
Míra podpory

1) Mírou podpory se rozumí v procentech vyjádřený podíl výše podpory k uznaným nákladům příjemce v daném roce řešení Projektu.

2) Maximální povolená výše míry podpory činí 75 %.

3) Maximální povolená výše míry podpory nesmí být v žádném roce řešení Projektu překročena.

Článek 9
Subdodávky

1) V rámci řešení Projektu nebudou realizovány subdodávky.

2) Pokud se v průběhu řešení Projektu vyskytne potřeba realizace subdodávky, postupuje příjemce podle zákona č. 137/2006 Sb., o veřejných zakázkách.

3) Subdodávky je příjemce povinen pořizovat za tržní ceny (tj. cena v místě a čase obvyklá). Toto je příjemce povinen poskytovateli doložit.

4) Subdodávky na výzkum nebo experimentální vývoj mohou být realizovány maximálně do výše 20 % celkových uznaných nákladů Projektu.

5) Nové subdodávky musí být předem odsouhlaseny poskytovatelem a upraveny písemným dodatkem ke Smlouvě.

6) Je-li subdodavatelem veřejně financovaná výzkumná organizace, mohou být předmětem subdodávek pouze výzkum nebo experimentální vývoj za těchto podmínek:

   a) výzkumná organizace poskytuje danou výzkumnou službu nebo provádí smluvní výzkum za tržní cenu nebo

   b) nelze-li určit tržní cenu, výzkumná organizace poskytne danou výzkumnou službu nebo provede smluvní výzkum za cenu, která zahrnuje plné náklady a přiměřený zisk.

7) Je-li příjemce výzkumnou organizací, může pořizovat subdodávky pouze od jiné výzkumné organizace.

8) Při pořízení subdodávek v rozporu s tímto Článkem bude postupováno dle Článku 20 Smlouvy.

Článek 10
Vedení účetnictví o uznaných nákladech Projektu

1) O vynaložených nákladech Projektu je příjemce povinen po celou dobu řešení Projektu vést v účetnictví oddělenou evidenci podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů v souladu s § 8 odst. 1 zákona č. 130/2002 Sb.

2) Nezpůsobilými náklady projektu jsou zejména:
   - zisk,
   - daň z přidané hodnoty (u příjemců, kteří jsou plátci této daně a kteří uplatňují její odpočet nebo odpočet její poměrné části)[2],

[2] Zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů

- jiné daně (silniční daň, daň z nemovitosti, daň darovací, dědická, apod.),
- náklady na marketing, prodej a distribuci výrobků,
- úroky z dluhů,
- náklady na finanční pronájem a pronájem s následnou koupí (např. leasing, aj.),
- manka a škody,
- náklady na pohoštění, dary a reprezentaci,
- náklady na vydání periodických publikací, učebnic a skript,
- náklady/výdaje na pořízení budov a pozemků,
- opravy nebo údržba místností, stavby, rekonstrukce budov nebo místností, nábytek či zařízení, která nejsou pevnou součástí místností, a další náklady, které bezprostředně nesouvisejí s předmětem řešení projektu,
- správní poplatky,
- výdaje související s likvidací příjemce, nedobytné pohledávky,
- platby příspěvků do soukromých penzijních fondů,
- peněžitá pomoc v mateřství,
- ostatní sociální výdaje na zaměstnance, které nejsou zaměstnavatelé povinni odvádět dle zvláštních předpisů (např. dary k životním jubileím, příspěvky na rekreaci, příspěvky na penzijní připojištění, životní pojištění apod.),
- odstupné,
- nájemné, kdy příjemce je vlastníkem nemovitosti nebo ji užívá zdarma,
- výdaje na školení a vzdělávání personálu (pokud se nejedná o odborné akce přímo související s řešením projektu).

3) Do uznaných nákladů na pořízení hmotného a nehmotného majetku lze zahrnout pouze část ceny majetku, která odpovídá podílu užití majetku na řešení Projektu.

4) Příjemce účtuje doplňkové náklady související s Projektem **metodou doplňkových nákladů (AC – Additional Costs)**.

5) Výše celkových doplňkových nákladů, účtovaných metodou kalkulace doplňkových nákladů (AC – Additional Costs) nesmí po celou dobu řešení Projektu překročit 10 % celkových uznaných přímých nákladů.

6) Příjemce může finanční prostředky daného kalendářního roku, u kterých předpokládá jejich nevyčerpání, převést nejpozději do konce listopadu daného kalendářního roku na bankovní účet poskytovatele číslo [redacted] při převodu finančních prostředků příjemce uvede do Zprávy pro příjemce: VRATKA, kód projektu, název příjemce). Poskytovatel převede nevyčerpané finanční prostředky do nespotřebovaných nároků rozpočtu, aby mohly být použity ke stejnému účelu v dalším kalendářním roce. V případě, že v dalším kalendářním roce dojde ke snížení nároků z nespotřebovaných výdajů na základě rozhodnutí vlády dle § 47 odst. 6 písm. c) zákona o rozpočtových pravidlech, bude částka převedených finančních prostředků odpovídajícím způsobem snížena, případně nebude poskytnuta.

7) Je-li příjemce veřejnou výzkumnou institucí nebo veřejnou vysokou školou, může finanční prostředky, které nemohly být efektivně použity v roce, ve kterém byly poskytnuty, převést do fondu účelově určených prostředků, a to do výše 5% objemu těchto prostředků poskytnutých na Projekt v daném kalendářním roce. Takto převedené prostředky mohou být použity pouze k účelu, ke kterému byly poskytnuty[3]. Převod musí příjemce písemně oznámit poskytovateli a odůvodnit.

8) Jestliže příjemce převede finanční prostředky z Rozpočtu daného kalendářního roku do dalšího kalendářního roku ve svém účetnictví, s výjimkou odst. 7 tohoto Článku, je povinen tyto prostředky poskytovateli vrátit do 10. ledna následujícího roku převedením

[3] § 18 odst. 10 a 11 zákona č. 111/1998 Sb., o vysokých školách; § 26 odst. 2 zákona č. 341/2005 Sb., o veřejných výzkumných institucích

na bankovní účet poskytovatele číslo [redacted] (při převodu finančních prostředků příjemce uvede do Zprávy pro příjemce: VRÁTKA, kód projektu, název příjemce). Tyto prostředky budou poskytovatelem odvedeny do státního rozpočtu.

9) Pokud příjemce uplatňuje rozdílný hospodářský rok, provádí vyúčtování nákladů na Projekt a poskytnuté podpory k 31. 12. daného kalendářního roku a při uzávěrce hospodářského roku provede kontrolu tohoto vyúčtování a o výsledku písemně informuje poskytovatele.

Článek 11
Povinnosti příjemce

1) Příjemce je povinen postupovat při řešení Projektu v souladu s Projektem a dalšími podmínkami uvedenými ve Smlouvě.

2) Příjemce je povinen použít podporu v souladu s podmínkami, účelem a způsobem stanovenými Smlouvou. Použije-li příjemce podporu v rozporu s podmínkami stanovenými Smlouvou na jiný účel nebo jiným způsobem, závažným způsobem poruší povinnosti stanovené Smlouvou. V takovém případě bude postupováno dle Článku 20 odst. 4 Smlouvy.

3) Příjemce je povinen dodržovat podmínky uvedené v Projektu, na jejichž základě byla stanovena maximální povolená výše míry podpory. Porušení této povinnosti se pokládá za závažné porušení povinnosti a bude postupováno dle Článku 20 odst. 4 Smlouvy.

4) Příjemce je povinen předložit poskytovateli v každém příslušném roce řešení Projektu podklady pro účely vypořádání podpory se státním rozpočtem v souladu s § 14 odst. 10 a § 75 zákona o rozpočtových pravidlech a příslušnými předpisy pro zúčtování se státním rozpočtem platnými pro daný rok. O způsobu a termínech předložení podkladů bude příjemce ze strany poskytovatele každoročně písemně informován.

5) Příjemce je povinen písemně informovat poskytovatele o veškerých podstatných skutečnostech, které by mohly mít vliv na průběh a výsledek řešení Projektu a které nastaly v době ode dne nabytí platnosti a účinnosti Smlouvy, a to ve lhůtě do 15 kalendářních dnů ode dne, kdy se o takové skutečnosti dozvěděl.

6) Podstatnou změnou, pro jejíž provedení je nutný předchozí souhlas poskytovatele je změna harmonogramu projektu, změna výsledků projektu, změna data ukončení řešení projektu, změna manažera Projektu, změna hlavního řešitele Projektu a změna řešitelů Projektu. Pokud příjemce neobdrží stanovisko poskytovatele do 15 kalendářních dnů ode dne odeslání informace o podstatné změně, považuje se podstatná změna za schválenou poskytovatelem. Poskytovatel může lhůtu prodloužit o 15 kalendářních dnů; je však povinen o prodloužení lhůty příjemce písemně informovat. Formulář pro informování poskytovatele příjemcem dle tohoto ustanovení je zveřejněn na webových stránkách Ministerstva vnitra. Při postupu příjemce v rozporu s tímto ustanovením, bude postupováno dle ustanovení Článku 20 odst. 3 Smlouvy.

7) O ostatních změnách informuje příjemce poskytovatele průběžně, nejpozději v roční zprávě dle Článku 12 odst. 2 Smlouvy.

8) Příjemce je povinen každou zahraniční pracovní cestu, jejíž náklady přesáhnou 60 000 Kč, předložit s předstihem nejméně 30 kalendářních dní před zahájením zahraniční pracovní cesty se zdůvodněním poskytovateli ke schválení. Nejpozději do 30 kalendářních dní po ukončení cesty je příjemce povinen předložit poskytovateli podrobnou zprávu o jejím průběhu a výsledcích ve vztahu k řešení Projektu.

9) Veškerá oznámení dle tohoto Článku předává příjemce formou a ve lhůtách, které jsou uvedeny ve Smlouvě.

10) Příjemce je povinen poskytnout i další údaje požadované poskytovatelem pro věcné a finanční řízení Projektu, a to v termínech stanovených poskytovatelem.

Článek 12
Zprávy

1) Příjemce předkládá poskytovateli ke schválení v průběhu řešení Projektu zprávy o průběhu řešení Projektu (roční zprávy, mimořádné zprávy). Po ukončení řešení Projektu příjemce předloží poskytovateli závěrečnou zprávu.

2) Roční zprávu je příjemce povinen předložit poskytovateli za každý rok řešení Projektu vždy ve lhůtě do 20. ledna následujícího kalendářního roku, nestanoví-li poskytovatel písemně jinak. Roční zpráva obsahuje zejména informace o postupu řešení Projektu, o dosažených výsledcích a způsobu jejich využití v uplynulém roce. V roční zprávě zároveň příjemce upřesní postup řešení Projektu na další rok a předloží aktuální verzi harmonogramu. Samostatnou částí roční zprávy je vyúčtování nákladů na Projekt a poskytnuté podpory za uplynulý rok ve struktuře Rozpočtu a aktuální verze rozpočtu.

3) Mimořádnou zprávu předkládá příjemce poskytovateli v průběhu řešení Projektu na vyžádání poskytovatele, který zároveň stanoví předmět zprávy a termín jejího předložení.

4) Závěrečnou zprávu z řešení Projektu předloží příjemce do 30 kalendářních dnů ode dne ukončení řešení Projektu uvedeného v Článku 5 Smlouvy. Závěrečná zpráva z řešení Projektu zahrnuje zejména informaci o dosažených cílech, výsledcích, způsobu jejich využití a výstupech Projektu. Součástí závěrečné zprávy je vyúčtování nákladů na Projekt a poskytnuté podpory za celé období řešení Projektu ve struktuře Rozpočtu.

5) Příjemce je povinen předkládat poskytovateli zprávu o využití výsledků Projektu v souladu s Popisem výsledků projektu a plánem jejich využití, který je přílohou č. 2 Smlouvy a smlouvou o využití výsledků podle § 11 zákona č. 130/2002 Sb., a to každoročně po dobu 5 let ode dne ukončení Smlouvy, vždy ve lhůtě do 20. ledna následujícího kalendářního roku.

6) U Projektů obsahujících utajované informace budou zprávy uvedené v tomto Článku zpracovávány v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon č. 412/2005 Sb.").

7) Poskytovatel stanoví rozsah, strukturu a formu zpráv uvedených v tomto Článku.

8) Poskytovatel schvaluje roční a mimořádné zprávy nejpozději do 30 kalendářních dnů ode dne jejich doručení nebo v této lhůtě uplatní písemné připomínky a stanoví lhůtu pro jejich vypořádání příjemcem.

9) Pokud příjemce nepředloží zprávy uvedené v odst. 1 až 4 tohoto Článku, bude postupováno dle Článku 20 odst. 3 Smlouvy.

Článek 13
Kontroly

1) Poskytovatel je oprávněn ve smyslu § 13 zákona č. 130/2002 Sb. provádět u příjemce kontrolu plnění cílů Projektu, včetně kontroly čerpání a využívání podpory a účelnosti vynaložených prostředků podle této Smlouvy.

2) Poskytovatel je oprávněn provádět finanční kontrolu v souladu se zákonem č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů a provádět kontrolu podle zákona č. 255/2012 Sb., o kontrole (kontrolní řád).

3) Příjemce je povinen umožnit poskytovateli provedení všech kontrol uvedených v odstavci 1 a 2 tohoto Článku a poskytnout mu při nich potřebnou součinnost, zejména poskytnout na pracovištích příjemce volný přístup k osobám podílejícím se na řešení Projektu, ke všem dokumentům, počítačovým záznamům a zařízením, která přísluší k řešení Projektu.

4) Příjemce je povinen předložit na žádost poskytovatele pro potřeby kontroly Projektu originály veškerých účetních dokladů vztahujících se k Projektu.

5) Příjemce je povinen předkládat poskytovateli na vyžádání přehledy jakýchkoliv účetních záznamů vztahujících se k Projektu.

6) Osoby provádějící kontrolu jsou povinny předložit příjemci písemné pověření ředitele věcně příslušného odboru poskytovatele k provedení kontroly.

7) Kontrolu je poskytovatel oprávněn provést kdykoliv v době řešení Projektu a následně ve lhůtě do 5 let ode dne ukončení Smlouvy. Příjemce je povinen po celou tuto dobu uchovávat veškeré doklady týkající se Projektu.

Článek 14
Nákup a vlastnictví majetku pořízeného pro řešení Projektu

1) V rámci řešení Projektu příjemce nebude pořizovat hmotný a nehmotný majetek.

2) Hmotný a nehmotný majetek nespecifikovaný řádně podle § 8 odst. 5 zákona č. 130/2002 Sb. je příjemce povinen pořizovat postupem podle zákona č. 137/2006 Sb., o veřejných zakázkách.

3) Pokud se v průběhu řešení Projektu vyskytne potřeba pořídit hmotný a nehmotný majetek, postupuje se podle zákona č. 137/2006 Sb., o veřejných zakázkách.

4) Hmotný a nehmotný majetek je příjemce povinen pořizovat za tržní ceny (tj. cena v místě a čase obvyklá). Toto je příjemce povinen poskytovateli doložit.

5) Vlastníkem majetku, pořízeného z poskytnuté podpory je ve smyslu ustanovení § 15 odst. 1 zákona č. 130/2002 Sb. příjemce.

6) Při pořízení majetku v rozporu s tímto Článkem bude postupováno dle Článku 20 Smlouvy.

Článek 15
Práva k výsledkům Projektu a jejich využití

1) Práva k výsledkům Projektu patří příjemci.

2) Při využití výsledků Projektu je příjemce povinen postupovat v souladu s ustanovením § 16 odst. 4 zákona č. 130/2002 Sb., Popisem výsledků projektu a plánem jejich využití a smlouvou o využití výsledků podle § 11 zákona č. 130/2002 Sb.

Článek 16
Poskytování informací

1) Příjemce je povinen předávat poskytovateli veškeré informace o Projektu pro účely jejich předání do informačního systému výzkumu, experimentálního vývoje a inovací ve formě a termínech stanovených poskytovatelem v souladu se zákonem č. 130/2002 Sb. a NV č. 397/2009 Sb., a další informace stanovené poskytovatelem.

2) Při jakémkoliv předávání nebo zveřejňování informací týkajících se Projektu a výsledků Projektu, včetně konferencí, je příjemce povinen zveřejnit informaci o poskytnuté podpoře poskytovatelem na základě Smlouvy a o příslušnosti k programu výzkumu a vývoje poskytovatele.

3) Pokud je předmět řešení Projektu utajovanou informací podle zákona č. 412/2005 Sb., je příjemce povinen uvést stupeň důvěrnosti těchto údajů podle zákona č. 412/2005 Sb., a poskytnout poskytovateli konkrétní informace o Projektu a jeho výsledcích postupem podle zákona č. 130/2002 Sb.

4) Příjemce je povinen při změně Smlouvy předat poskytovateli informace o změně údajů zveřejňovaných v informačním systému výzkumu, experimentálního vývoje a inovací, pokud k takovéto změně v důsledku změny Smlouvy dojde.

Článek 17
Povinnost mlčenlivosti

1) Poskytovatel a příjemce jsou povinni zajistit mlčenlivost o všech informacích, které jim jako důvěrné byly poskytnuty a jejichž předání dalším subjektům by mohlo poškodit práva toho, kdo je poskytl.

2) V případě, že jsou poskytovatel a příjemce na základě Smlouvy oprávněni poskytovat informace třetím stranám, jsou povinni zajistit, aby tyto třetí strany zachovávaly mlčenlivost o těchto informacích, které jim byly poskytnuty jako důvěrné, a používaly je jen k účelům, k nimž jim byly předány.

3) Poskytovatel a příjemce jsou zproštěni povinnosti zachovávat mlčenlivost v případě:

   a) že se obsah informací, které jim byly poskytnuty jako důvěrné, stane veřejně přístupným, a to na základě jiných činností prováděných mimo rámec Smlouvy nebo na základě opatření, která nesouvisí s řešením Projektu;

   b) že byl požadavek zachovávat mlčenlivost odvolán těmi, v jejichž prospěch byla tato povinnost stanovena.

Článek 18
Odpovědnost za škodu

1) Odpovědnost za škodu se řídí ustanoveními občanského zákoníku.

2) Poskytovatel neodpovídá za jednání nebo za nečinnost příjemce. Poskytovatel neodpovídá za nedostatky výrobků vytvořených nebo služeb poskytnutých na základě výsledků Projektu.

3) Příjemce se zavazuje, že odškodní třetí strany v případě uplatnění požadavku na náhradu škody, která vznikla jednáním nebo nečinností příjemce nebo která souvisí s nedostatky výrobků vytvořených nebo služeb poskytnutých na základě výsledků Projektu, pokud neprokáže, že za tyto neodpovídá.

4) Prokáže-li třetí strana své nároky spojené s prováděním Smlouvy vůči poskytovateli, je příjemce povinen poskytovateli poskytnout pomoc.

Článek 19
Odstoupení od Smlouvy

1) Poskytovatel je oprávněn od Smlouvy odstoupit v případě, že:

   a) příjemce uvedl neúplné, nesprávné nebo nepravdivé údaje a skutečnosti ve veřejné soutěži nebo při uzavření Smlouvy;

   b) příjemce nesplnil povinnosti nebo jiné podmínky stanovené Smlouvou ani poté, co jej poskytovatel k tomu písemně vyzval a stanovil mu náhradní dobu k jejich splnění; náhradní doba k plnění nesmí být kratší než 30 kalendářních dnů;

   c) příjemce vstoupil do likvidace nebo na něho byla vyhlášena nucená správa, vůči majetku příjemce probíhá insolvenční řízení, v němž bylo vydáno rozhodnutí o úpadku nebo insolvenční návrh nebyl zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení, nebo nebyl konkurs zrušen proto, že majetek byl zcela nepostačující, byla povolena reorganizace nebo byl nařízen výkon rozhodnutí prodejem podniku, pokud by tato skutečnost mohla dle názoru poskytovatele ovlivnit řešení Projektu nebo zájmy poskytovatele;

d) dojde ke vzniku závažných ekonomických nebo technických důvodů, které podstatně ovlivní řešení Projektu, nebo se výrazně sníží možnost využití poznatků Projektu;

e) z důvodu podstatného porušení Smlouvy podle § 2002 odst. 1 občanského zákoníku.

2) Odstoupení od Smlouvy musí být odůvodněno a nabývá účinnosti dnem jeho doručení příjemci.

Článek 20
Vrácení podpory a sankce

1) V případě odstoupení od Smlouvy podle ustanovení Článku 19 odst. 1 písm. a), b) a e) Smlouvy je příjemce povinen vrátit poskytnutou podporu poskytovateli v plné výši. K vrácené podpoře je příjemce povinen zaplatit smluvní pokutu ve výši 0,1 % z částky podpory uvedené v Projektu pro rok, v němž vznikl důvod k odstoupení od Smlouvy, a to za každý den za dobu ode dne připsání poskytnuté podpory, která má být vrácena, na bankovní účet příjemce do dne jejího připsání na účet poskytovatele.

2) V případě odstoupení od Smlouvy podle ustanovení Článku 19 odst. 1 písm. c) a d) Smlouvy a v případě uzavření dohody o ukončení Smlouvy je příjemce povinen vrátit poskytnutou podporu v poměrné výši, stanovené poskytovatelem, a to ve lhůtě do 30 kalendářních dnů ode dne doručení sdělení o odstoupení od Smlouvy nebo ode dne nabytí účinnosti dohody o ukončení Smlouvy. Z poskytnuté podpory mohou být uhrazeny jen uznané náklady Projektu použité příjemcem na poskytovatelem schválené výstupy z Projektu, kterých bylo dosaženo do okamžiku odstoupení od Smlouvy, případně ukončení Smlouvy dohodou.

3) V případě, že příjemce neinformuje poskytovatele dle Článku 7 odst. 1 až 3, Článku 11 odst. 6, Článku 12 odst. 1 až 4 této Smlouvy, poskytovatel uloží příjemci smluvní pokutu ve výši 2 % z částky podpory uvedené v Projektu pro rok, v němž vznikl důvod k uložení smluvní pokuty. Podpora pro následující kalendářní rok bude příjemci poskytnuta ve výši, snížené o uplatněnou smluvní pokutu.

4) V případě, že příjemce použije poskytnutou podporu nebo část poskytnuté podpory v rozporu s podmínkami, účelem nebo způsobem stanovenými touto Smlouvou, je poskytovatel oprávněn požadovat od příjemce vrácení takto použitých prostředků. Příjemce je povinen tyto prostředky převést na účet poskytovatele, a to ve lhůtě do 30 kalendářních dnů ode dne, kdy byl tento požadavek poskytovatele písemně doručen příjemci.

5) V případě, že příjemce nevyužije výsledky Projektu nebo neumožní jejich využití dle § 16 odst. 4 zákona č. 130/2002 Sb. a v souladu se smlouvou o využití výsledků dle § 11 zákona č. 130/2002 Sb., vrátí poskytovateli poskytnutou podporu v plné výši.

6) V případě, že u příjemce byly po ukončení Smlouvy zjištěny na základě provedené kontroly závažné finanční nesrovnalosti nebo podvod, může poskytovatel od příjemce písemně požadovat vrácení poskytnuté podpory v celé výši. K vrácené podpoře je příjemce povinen zaplatit smluvní pokutu ve výši 0,1 % z poskytnuté podpory za každý den, a to za dobu ode dne připsání poskytnuté podpory, která má být vrácena, na bankovní účet příjemce do dne jejího připsání na účet poskytovatele.

7) Poskytnutá podpora nebo její poměrná část se vrací a smluvní pokuta se platí připsáním na bankovní účet poskytovatele, který bude příjemci poskytovatelem sdělen.

8) Neoprávněné použití nebo zadržení podpory se posuzuje jako porušení rozpočtové kázně podle zákona o rozpočtových pravidlech.

9) Poskytovatel je oprávněn přerušit nebo zastavit poskytování podpory příjemci, pokud jsou naplněny skutkové podstaty, pro které může být Smlouva ukončena v souladu s ustanovením Článku 19 odst. 1 Smlouvy. Ustanovením tohoto odstavce nejsou dotčena

práva poskytovatele stanovená Smlouvou. Příjemci nenáleží náhrada škody, která mu vznikne v důsledku přerušení nebo zastavení poskytování podpory.

10) Tímto Článkem není dotčen nárok poskytovatele na náhradu škody, která mu vznikne v důsledku neplnění Smlouvy příjemcem.

Článek 21
Ukončení řešení Projektu a ukončení Smlouvy

1) Příjemce je povinen řešení Projektu ukončit nejpozději ke dni uvedenému v Článku 5 Smlouvy. Řešení Projektu se považuje za ukončené rovněž v případě předčasného zastavení řešení Projektu v souvislosti s ukončením Smlouvy v souladu s ustanovením tohoto Článku odst. 4 písm. b) a c) Smlouvy.

2) Po ukončení řešení Projektu poskytovatel provede závěrečné hodnocení Projektu, zejména zhodnocení plnění cílů Projektu, včetně kontroly čerpání a využívání podpory, účelnosti vynaložených prostředků Projektu podle Smlouvy a dále provede závěrečné zhodnocení dosažených výsledků Projektu a jejich vztah k cílům Projektu.

3) Smlouva je splněna dnem schválení závěrečné zprávy poskytovatelem a úspěšným závěrečným hodnocením Projektu poskytovatelem v souladu s § 13 odst. 4 zákona č. 130/2002 Sb.

4) Smlouva je ukončena:

   a) dnem ukončení Smlouvy stanoveným ve Smlouvě v Článku 25 odst. 2,

   b) dnem doručení písemného odstoupení od Smlouvy poskytovatelem,

   c) dnem nabytí účinnosti dohody smluvních stran o ukončení Smlouvy.

5) Po ukončení Smlouvy je poskytovatel oprávněn podle § 9 odst. 1 písm. k) zákona č. 130/2002 Sb. provádět u příjemce kontrolu využití výsledků Projektu v souladu s § 16 zákona č. 130/2002 Sb., Popisem výsledků projektu a plánem jejich využití a smlouvou o využití výsledků podle § 11 zákona č. 130/2002 Sb., a to ve lhůtě do 5 let ode dne ukončení Smlouvy.

Článek 22
Doručování písemností

1) Písemnosti dle Smlouvy se doručují na adresu poskytovatele nebo příjemce uvedenou v této Smlouvě. V případě doručování prostřednictvím provozovatele poštovní služby je náhradní doručení uložením zásilky možné. V takovém případě se považuje písemnost za doručenou 10. kalendářní den ode dne oznámení o uložení zásilky na poště.

2) Písemnosti v elektronické formě lze doručovat do datové schránky poskytovatele nebo příjemce podle zvláštního zákona[4], s výjimkou ustanovení Článku 12 odst. 6 Smlouvy. Písemnost se považuje za doručenou nejpozději 10. kalendářní den ode dne, kdy byl dokument dodán do datové schránky.

Článek 23
Spory smluvních stran

Spory smluvních stran vznikající ze Smlouvy nebo v souvislosti s ní, budou řešeny příslušným soudem.

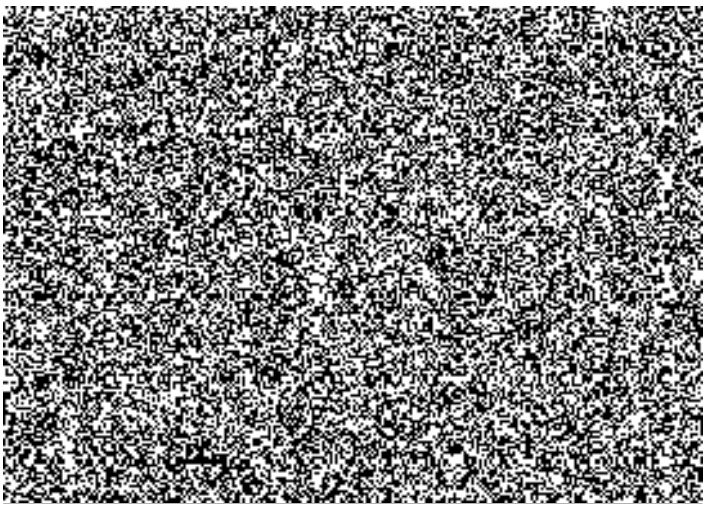
[4] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.

Článek 24
Závěrečná ustanovení

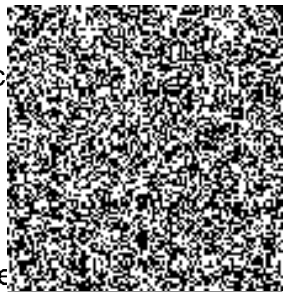
1) Smlouva, včetně příloh, může být doplňována, upravována a měněna pouze písemnými, po sobě číslovanými dodatky ke Smlouvě, podepsanými smluvními stranami.
2) Nestanoví-li Smlouva jinak, návrh posledního dodatku ke Smlouvě lze doručit druhé smluvní straně nejpozději 60 kalendářních dnů přede dnem ukončení řešení Projektu uvedeným v Článku 5 Smlouvy.
3) Smlouva se řídí právním řádem České republiky.
4) Vztahy neupravené Smlouvou se řídí především zákonem č. 130/2002 Sb. a občanským zákoníkem.
5) Základní ustanovení Smlouvy (Články 1 až 25 Smlouvy) mají v případě rozporu přednost před ustanoveními Projektu.
6) Nedílnou součástí Smlouvy jsou:
   a) Příloha č. 1 - Projekt,
   b) Příloha č. 2 - Popis výsledků projektu a plán jejich využití.
7) Smlouva se vyhotovuje ve dvou stejnopisech, z nichž poskytovatel i příjemce obdrží po jejich podpisu jedno vyhotovení.
8) Smluvní strany prohlašují a podpisem Smlouvy stvrzují, že jimi uvedené údaje, na jejichž základě je uzavřena Smlouva a poskytnuta podpora poskytovatelem, jsou správné, úplné a pravdivé.
9) Smluvní strany prohlašují, že si tuto Smlouvu přečetly, s jejím obsahem souhlasí a že byla sepsána na základě jejich pravé a svobodné vůle, a na důkaz toho připojují své podpisy.

Článek 25
Platnost a účinnost Smlouvy

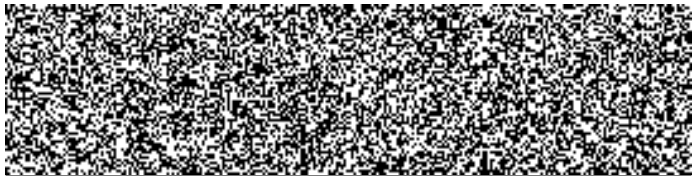
1) Smlouva se uzavírá na dobu určitou a nabývá platnosti dnem podpisu smluvních stran a účinnosti dnem 1. 9. 2015.
2) Smlouva je ukončena dnem 27.2.2021.
3) Ukončení Smlouvy před datem uvedeným v odst. 2 tohoto Článku je upraveno v ustanovení Článku 21 odst. 4 písm. b) a c) Smlouvy.



Za příjemc



Mgr. Ondře



CZ.NIC, z. s. p. o.
Milešovská 5
130 00 Praha 3
IČ 67985726
DIČ CZ67985726

Predikce a ochrana před kybernetickými incidenty

Program: **BV III/1-VS**

Uchazeč: **CZ.NIC, z. s. p. o.**

Další účastníci: **0**

Hlavní obor: **IN - Informatika**

Vedlejší obor: **JC - Počítačový hardware a software**

Stupeň důvěrnosti údajů: **S - údaje jsou zveřejnitelné a odpovídají skutečnosti**

1. Identifikační údaje Programu a vyhlášení veřejné soutěže

1.1 Kód Programu

Kód Programu
VI

1.2 Název Programu

Název Programu
Program bezpečnostního výzkumu České republiky 2015-2020

1.3 Dílčí cíl, který nejvíce odpovídá zamýšlené oblasti uplatnění výsledků

Název tematické oblasti v rámci daného dílčího cíle Programu, která bude projektem řešena
2d) Účinná detekce a identifikace hrozeb kritické infrastruktury

1.4 Číslo a datum vyhlášení

Číslo a datum vyhlášení
Vyhlášení první VS z 26.11.2014.

2. Identifikace projektu

2.1 Název projektu

Název projektu

Predikce a ochrana před kybernetickými incidenty

2.2 Název projektu anglicky

Název projektu anglicky

Prediction and Protection against Cyber Incidents

2.3 Anotace projektu

Anotace projektu

Cílem projektu je vybudování účinného systému detekce, identifikace a predikce kybernetických hrozeb a vyhodnocování kybernetických bezpečnostních incidentů (tzv. Cyber Threat Intelligence). Ve svém řešení projekt vychází ze zákona č. 181/2014 Sb. a cílí na další využití informací o kybernetických incidentech a podporu spolupráci a sdílení informací mezi klíčovými hráči – národním a vládním CERT/CSIRT, provozovateli kritické informační infrastruktury, významných informačních systémů a sítí.

2.4 Anotace projektu anglicky

Anotace projektu anglicky

The project aims to establish an efficient system of detection, identification and prediction of cyber threats and evaluation of cyber security incidents (Cyber Threat Intelligence). Its solution is based on the Cybersecurity Act and aims to further use the information about cyber incidents and to promote cooperation and information sharing among the key players–the national and governmental CERT/CSIRT, operators of critical information infrastructure, major information systems and network.

2.5 Kategorie činnosti

Kategorie činnosti

průmyslový výzkum

2.6 Předpokládané datum zahájení projektu

Předpokládané datum zahájení projektu

01.09.2015

2.7 Datum ukončení projektu

Datum ukončení projektu

31.08.2020

2.8 Projekt má více uchazečů

Projekt má více uchazečů

NE

2.9 Klíčová slova

Klíčová slova

Bezpečnost; kybernetická bezpečnost; CERT; CSIRT; kritická infrastruktura; sítě; elektronické komunikace; incident; útok;

2.10 Klíčová slova anglicky

Klíčová slova anglicky

Security; cybersecurity; CERT; CSIRT; critical infrastructure; network; electronic communication; incident; attack;

3. Identifikace uchazeče

3.1 Název uchazeče

Název uchazeče
CZ.NIC, z. s. p. o.

3.2 Právní forma

Právní forma
ZSP - zájmové sdružení právnických osob (§ 20f až 21 občanského zákoníku), občanské sdružení, ...

3.3 IČ

IČ
67985726

3.4 DIČ

DIČ
CZ67985726

3.5 Sídlo uchazeče

Státní příslušnost			
CZ - Česká republika			
Kraj	Obec		
Praha	Praha 3		
Ulice	Č. popisné	Č. orientační	PSČ
Milešovská	1136	5	130 00
Telefon	E-mail		
+420 222 745 111	kontakt@nic.cz		
Web stránka			
nic.cz			

3.7 Statutární zástupce/zástupci uchazeče

Titul před jménem	Jméno	Příjmení	Titul za jménem
JUDr., PhDr.	Marek	Antoš	
Pracovní pozice osoby na pracovišti			
místopředseda představenstva			
Telefon	Fax	E-mail	
+420 222 745 111	+420 222 745 112	kontakt@nic.cz	

Titul před jménem	Jméno	Příjmení	Titul za jménem
Mgr.	Ondřej	Filip	MBA
Pracovní pozice osoby na pracovišti			
výkonný ředitel; pověřený plnou mocí			
Telefon	Fax	E-mail	
+420 222 745 111	+420 222 745 112	ondrej.filip@nic.cz	

Titul před jménem	Jméno	Příjmení	Titul za jménem
Ing.	Jiří	Kysela	
Pracovní pozice osoby na pracovišti			
člen představenstva			
Telefon	Fax	E-mail	
+420 222 745 111	+420 222 745 112	kontakt@nic.cz	

3.8 Kategorie uchazeče

Kategorie uchazeče
SP - střední podnik

3.9 Popis předchozích zkušeností uchazeče v oblasti výzkumu a vývoje za posledních 5 let

Popis předchozích zkušeností uchazeče v oblasti výzkumu a vývoje za posledních 5 let

Sdružení CZ.NIC a jeho výzkumné a vývojové oddělení Laboratoře CZ.NIC má za sebou celou řadu výzkumných projektů v oblasti Internetu, internetových protokolů, analýz síťových provozů, pasivního i aktivního monitoringu a návrhů prototypů.

Mezi hlavní výzkumné projekty patří zejména:

• TURRIS – bezpečnostní projekt, který pomáhá uživatelům s ochranou domácí sítě pomocí speciálního routeru. Součástí výzkumného projektu byl jak návrh hardwaru, tak softwaru.

• BIRD (Internet Routing Daemon) - speciální software (tzv. routovací démon) určený pro významné propojovací uzly (peeringová centra).

• Knot DNS - výkonný ryze autoritativní DNS server podporující všechny hlavní protokoly DNS včetně transferů zón, dynamických updatů a DNS-SEC rozšíření.

Sdružení CZ.NIC se rovněž podílí na řešení např. následujících mezinárodních projektů v oblasti výzkumu a vývoje podpořených Evropskou komisí:

• STORK 2.0 (Secure idenTity acrOss boRders linKed 2.0; Project Reference: 297263) – projekt se zaměřuje na otázky přeshraničního uznávání nástrojů elektronické identifikace. V rámci projektu sdružení CZ.NIC zajišťuje především lokalizaci a implementaci národní brány PEPS a podílí se ve spolupráci s Ministerstvem vnitra rovněž na analýzách v oblasti bezpečnosti a důvěryhodnosti elektronických nástrojů používaných v ČR.

• GEN6 (Government ENabled with IPv6; Project Reference: 297239) - cílem projektu je především podpora veřejné správy při přechodu na novou verzi internetového protokolu - IPv6. Sdružení CZ.NIC v rámci projektu vede výzkumné aktivity (včetně tvorby metodiky a vývoje softwaru) zaměřené na monitoring a srovnání připravenosti veřejné správy v České republice i Evropě.

3.10 Úspěšně vyřešené projekty uchazeče v oblasti výzkumu a vývoje v posledních třech letech

3.11 Výsledky projektů výzkumu a vývoje uchazeče, které byly nebo jsou prokazatelně úspěšně využívány komerčně

Identifikátor	Název
VD2007010B01	Kybernetické hrozby z hlediska bezpečnostních zájmů České republiky

Kým a po jakou dobu komerčně využíván, případně číslo patentu nebo jiného typu právní ochrany

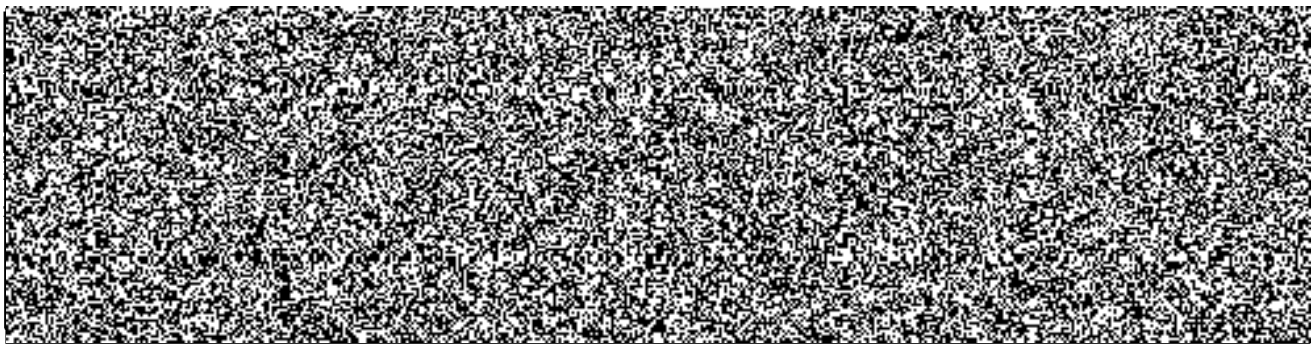
Na základě memoranda s Ministerstvem vnitra (později s Národním bezpečnostním úřadem) sdružení CZ.NIC od prosince 2010 zabezpečuje provoz a rozvoj národního bezpečnostního týmu CSIRT.CZ, jehož základ byl vytvořen v rámci bezpečnostního výzkumu v letech 2007 až 2010. Od 1. Ledna 2015 tento tým funguje v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, jako národní CSIRT pro Českou republiku. Na základě memoranda s NBÚ a v souladu se zákonem o kybernetické bezpečnosti má tým nekomerční charakter. Udržitelnost projektu však pomáhá zmírňovat ztráty způsobené ČR kybernetickým zločinem, které dle odborných odhadů dosahují v zemích EU až 0,41% HDP, tj. v České republice 18 - 19 mld. Kč ročně.

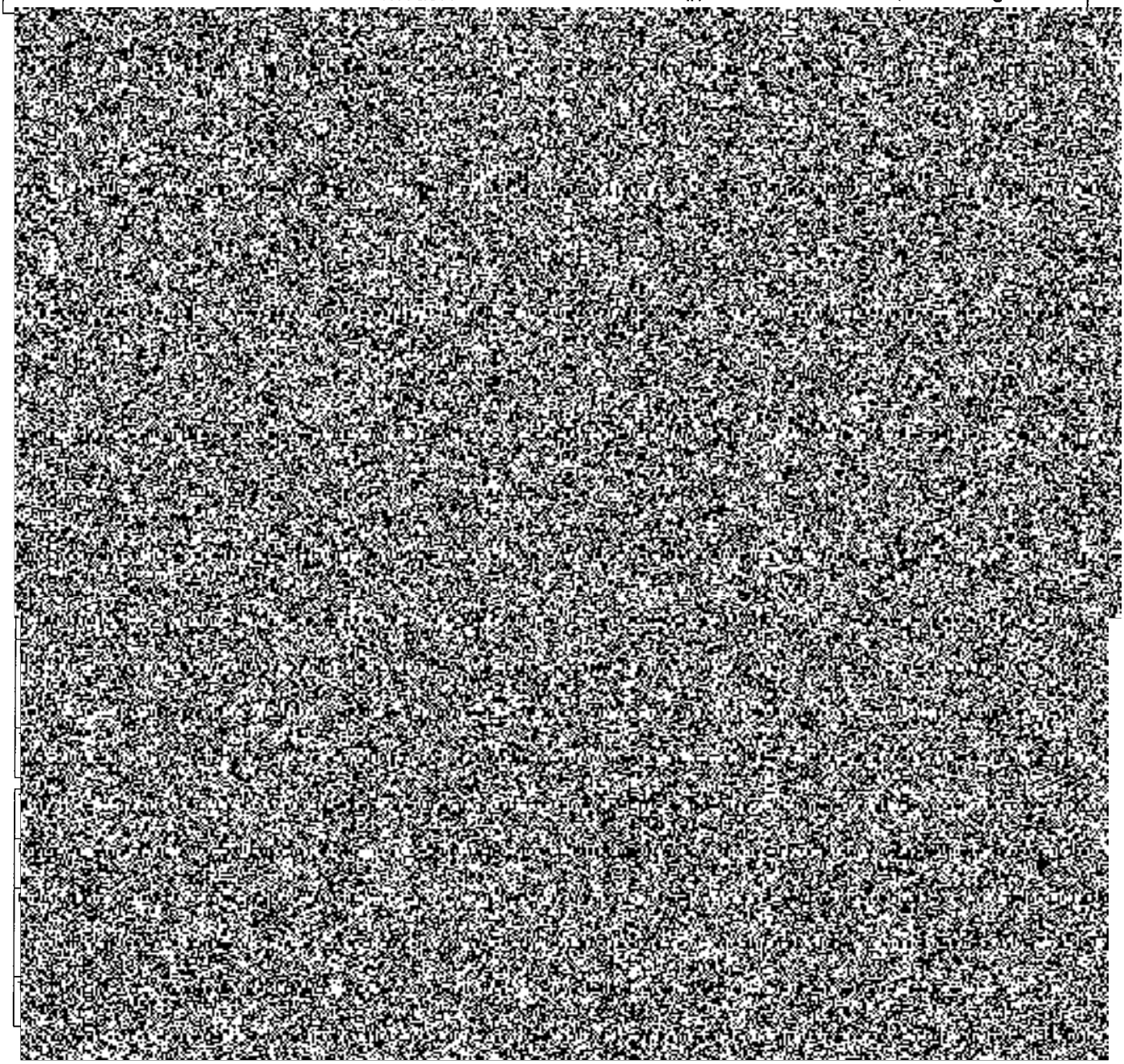
Identifikátor	Název
BIRD	The BIRD Internet Routing Daemon

Kým a po jakou dobu komerčně využíván, případně číslo patentu nebo jiného typu právní ochrany

Podle průzkumu asociace EURO-IX je BIRD nejvíce používaný (přes 50%) směrovací server na světě, který je nasazen na klíčových uzlech světového Internetu (tzv. Internet Exchange Points, IXP), jako jsou IXP v Amsterdamu (od srpna 2012), Frankfurtu (od února 2010) či Londýně (od ledna 2010) a samozřejmě v Praze (NIX.CZ). BIRD je poskytován bezplatně v podobě open-source, úspěšná komercionalizace projektu je zajišťována prostřednictvím programu podpory (support program), která se pohybuje od 10 000 – 50 000 €/ročně.

3.12 Řešitelský tým projektu

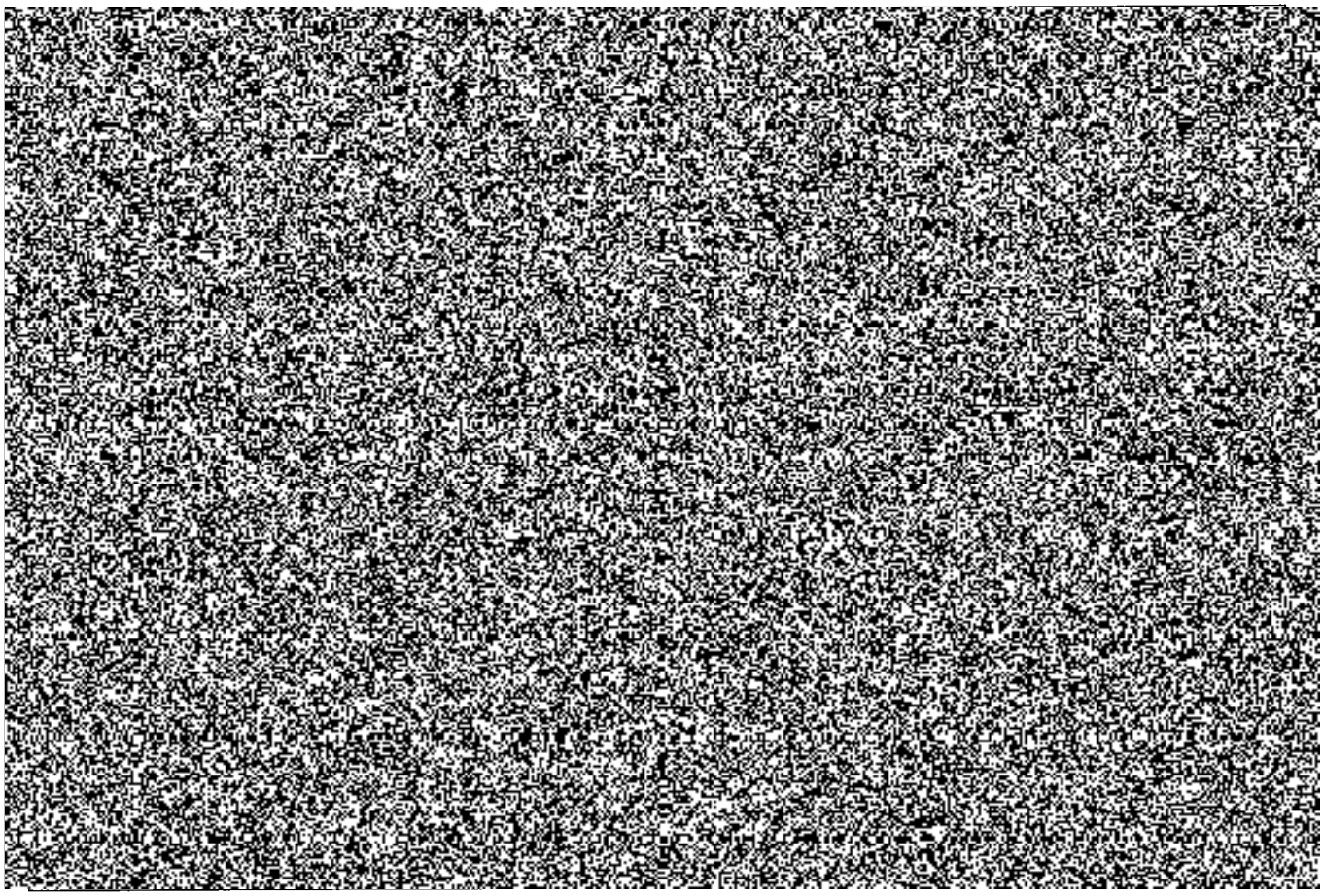




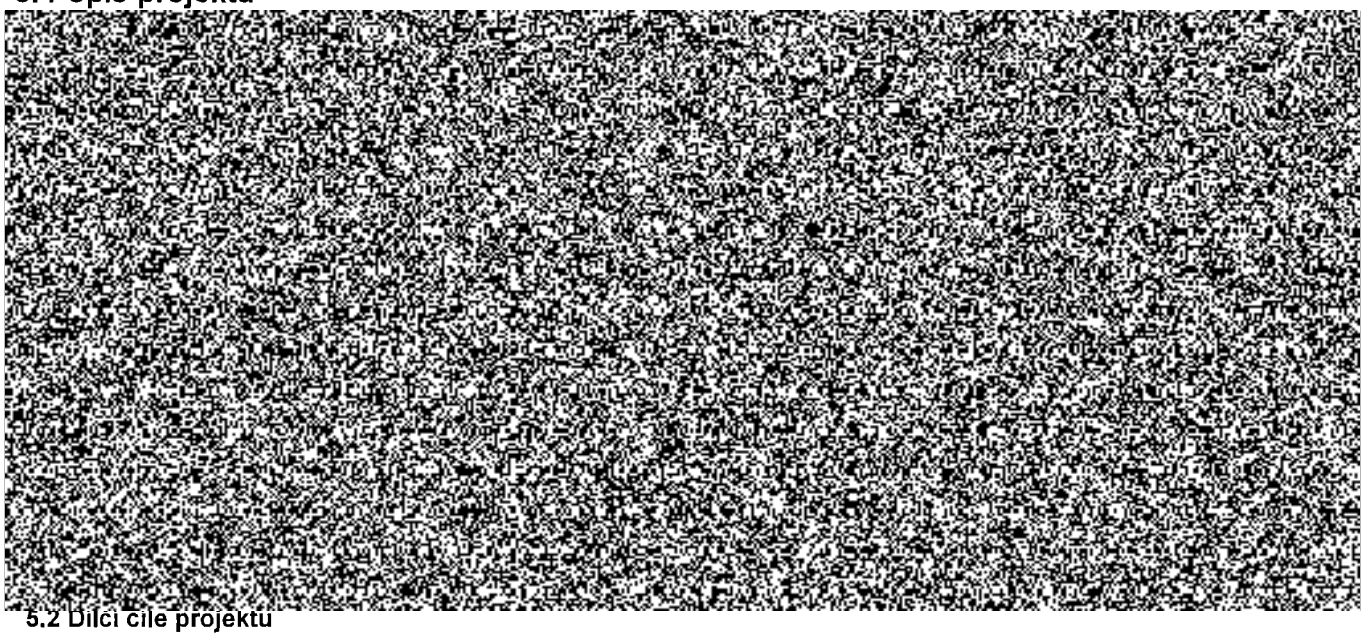
Popis činností, za které bude odpovídat v projektu

Řízení projektu, včetně finančního řízení, spolupráce a komunikace s poskytovatelem dotace (Ministerstvem vnitra ČR) a dalšími zapojenými subjekty. Manažer projektu je rovněž odpovědný za komunikaci projektu a jeho integraci v rámci CZ.NIC a zajišťuje úzkou spolupráci s hlavním řešitelem projektu.

3.14 Další pracovníci projektového týmu



5. Popis projektu



5.2 Dílčí cíle projektu

Dílčí cíle projektu

Mezi dílčí cíle projektu patří:

- Ve spolupráci s dalšími subjekty, vládním pracovištěm CERT (NCKB/NBÚ) a provozovateli kritické infrastruktury (provozovatelé významných sítí elektronických komunikací, datacentra...) vytvořit efektivní model spolupráce v oblasti kybernetické bezpečnosti.

- Vytvořit komunikační model (matici) mezi vrcholovými aktéry (především národním a vládním CERT) kybernetické bezpečnosti.

- Vydat monografii s názvem „Kybernetická bezpečnost", která se bude věnovat zejména jednotlivým typům útoků (kybernetických bezpečnostních incidentů) a osvědčeným postupům, jak jim čelit, kdy monografie bude poskytovat přímou vazbu a konkrétní případy opatření dle vyhlášky č. 316/2014 Sb. o kybernetické bezpečnosti, stejně jako evropskou legislativu (především Směrnice NIS)

- Vytvořit jednotnou metodologii pro zvládání kybernetických bezpečnostních incidentů na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti a souvisejících právních předpisů.

- Provádět pravidelné roční hodnocení hrozeb a rizik pro oblast kybernetické bezpečnosti na národní úrovni, a to jak na základě informací a dat zjištěných v rámci systému (poloprovozu) Cyber Threat Intelligence, tak aktuálních poznatků ze zahraničí. Tato hodnocení budou obsažena v závěrečné výzkumné zprávě hodnotící hrozby a rizika kybernetické bezpečnosti v České republice.

- Propagovat důležitost vysoké míry zabezpečení kritické informační infrastruktury, nejnovější bezpečnostní mechanismy a doporučení, stejně jako aktuální kybernetické hrozby.

- Podpořit mezinárodní spolupráci a oblasti výzkumu kybernetické bezpečnosti a propagaci a otevřené šíření výsledků bezpečnostního výzkumu na mezinárodní scéně (APWG, FIRST, Trusted Introducer, TF-CSIRT, TERENA, CENTR, ICANN...).

5.3 Hlavní výsledky projektu

Kód	Druh výsledku	Počet
Z	poloprovoz, ověřená technologie	1

5.4 Vedlejší výsledky projektu

Kód	Druh výsledku	Počet
B	odborná kniha	1

5.5 Popis současného stavu problematiky řešené oblasti

Popis současného stavu problematiky řešené oblasti

Internet se dnes stal neodmyslitelnou součástí a nezbytným komunikačním nástrojem nejen našich každodenních životů, ale též prakticky všech podnikatelských i nepodnikatelských činností. Spolu s jeho rostoucím významem roste rovněž důležitost ochrany této sítě a informací přenášených nebo uchovávaných jak v datacentrech, tak v koncových zařízeních uživatelů.

Podle poslední studie bezpečnostní divize Intelu McAfee se škoda způsobená kybernetickou kriminalitou na celém světě pohybuje ročně kolem 500 miliard dolarů a jak uvedla Evropská komise již v roce 2012 ve svém sdělení (COM(2012)140), je škoda způsobená kybernetickou kriminali-

Popis současného stavu problematiky řešené oblasti

tou výnosnější než celosvětový obchod s marihuanou, kokainem a heroinem dohromady. Zmiňovaná studie McAffee vyčíslila, že kybernetická kriminalita způsobuje v zemích EU průměrné ztráty ve výši 0,41% HDP. V případě České republiky se tak jedná o přibližně 18 - 19 mld. Kč ročně.

Za účelem společně čelit kybernetickým hrozbám a minimalizovat ztráty způsobené tímto typem kriminality jsou zřizovány bezpečnostní týmy CERT (Computer Emergency Response Team), resp. CSIRT (Computer Security Incident Response Team), jejichž hlavním cílem je koordinace a řešení bezpečnostních incidentů v rámci počítačových sítí. Na základě výsledků bezpečnostního výzkumu „Kybernetické hrozby z hlediska bezpečnostních zájmů České republiky (VD2007010B01)" v letech 2007 až 2010 bylo vytvořeno modelové pracoviště národního CSIRT, jehož provoz na základě Memoranda s Ministerstvem vnitra a následně Národním bezpečnostním úřadem zabezpečuje od prosince 2010 pod názvem „CSIRT.CZ" sdružení CZ.NIC, které tento tým dále rozvíjí.

Dne 1. ledna 2015 nabyl účinnosti zákon č. 181/2014 Sb., o kybernetické bezpečnosti, jehož cílem je především minimalizovat škody způsobené kybernetickou kriminalitou v České republice a zajistit na národní úrovni koordinaci bezpečnostních incidentů mezi jednotlivými subjekty. V souladu s tímto zákonem (zejm. § 18 a § 32) plní funkci národního týmu CERT bezpečnostní tým CSIRT.CZ, provozovaný sdružením CZ.NIC.

Implementace zákona a promítnutí a dosažení jeho cíle – minimalizace ztrát způsobených kybernetickými útoky a jejich efektivní řešení – přináší nové výzvy pro národní CERT(CSIRT.CZ). Jednou z hlavních výzev je predikce a ochrana před kybernetickými incidenty.

K realizaci tohoto cíle řešitelský tým považuje po vzoru jiných zemí (Hong-Kong, Rakousko, Portugalsko, Polsko...) za nezbytné vybudování účinného systému detekce, identifikace a predikce kybernetických hrozeb a vyhodnocování kybernetických bezpečnostních incidentů (tzv. Cyber Threat Intelligence). V současné době jsou jednotlivé informace evidovány odděleně v různých zdrojích a nejsou vzájemně porovnávány a korelovány. Korelace dat a schopnost dávat je do souvislostí přitom představuje klíčový aspekt pro identifikaci a řešení rozsáhlých incidentů, APT (Advanced Persistent Threat) hrozeb, případně sledování činností kriminálních skupin operujících ve virtuálním prostoru. Z tohoto důvodu projekt počítá s využitím níže uvedeného spektra zdrojů jak z provozů velkých sítí a center, tak od koncových uživatelů. Rozsah těchto dat a možnost jejich následné analýzy činí projekt unikáním nejen v podmínkách ČR, ale i jiných zemí.

- OTRS - systém pro zpracování incidentů hlášených národnímu bezpečnostnímu týmu CERT (CSIRT.CZ), a to jak na principu vzájemné důvěry, tak předávaných na základě odst. 2, § 8 zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Cílem projektu bude tento proces co nejvíce zefektivnit a optimalizovat s cílem maximálního vytěžení předávaných informací.

- Malicious Domain Manager - systém vyvinutý sdružením CZ.NIC, který slouží ke sběru informací o incidentech na stránkách provozovaných v rámci domény .CZ a k jejich následnému řešení.

- TURRIS - unikátní výzkumný projekt vytvořený sdružením CZ.NIC, který umožňuje detekování anomálního síťového provozu u koncových uživatelů.

- Honeypoty - sdružení CZ.NIC již nyní provozuje vlastní síť honeypotů, které slouží k podrobnému zkoumání chování útočníků.

- CleanMX a Shadow Server - služby poskytující informace o IP adresách, které mohou v rámci ČR představovat bezpečnostní riziko.

- Spamhause - databáze poskytující informace o IP adresách, které byly zneužity pro odesílání nevyžádané pošty.

- PassiveDNS - databáze uchovávající kompletní historická DNS data pro IP adresy a doménová jména. Tato databáze umožňuje dohledávat například nová umístění C&C serverů, či třeba aktuální propojen doménových jmen a IP adres sloužících k distribuci malware.

- Kontaktní údaje hlášené národnímu CERT– v současné době jsou kontaktní údaje od orgánů uvedených v §3, písm. a) a b) (zejm. poskytovatelé služeb a sítí a osoby zajišťující významnou síť el. komunikací) předávány národnímu CERT v prostém elektronickém formuláři. Cílem projektu je tento proces zefektivnit a vytvořit efektivní jejich správu s možností předání údajů vládnímu CERT v zákonem stanovených případech.

V rámci projektu budou analyzovány další vhodné zdroje a doplňovány jako další vstup systému.

Na základě analýzy a korelace výše uvedených dat poté bude moci být vybudován systém distribuce informací o bezpečnostních incidentech a jejich efektivní sdílení se zapojenými subjekty, zejm. dalšími týmy CERT/CSIRT a provozovateli významných informačních systémů (viz uživatelé výsledků projektu).

5.6 Přínosy a dopady projektu v oblasti bezpečnosti a cílů stanovených Programem

Přínosy a dopady projektu v oblasti bezpečnosti a cílů stanovených Programem

Hlavním přínosem projektu bude posílení kybernetické bezpečnosti České republiky a eliminace ztrát způsobenými kybernetickým zločinem. Dle odborných odhadů bezpečnostní divize McAffee tyto ztráty představují v zemích EU ztrátu ve výši 0,41% ve HDP. V případě České republiky se tak jedná o přibližně 18 - 19 mld. Kč ročně.
Za účelem dosažení tohoto cíle bude v rámci projektu v České republice vybudován po vzoru jiných států systém detekce, identifikace a predikce kybernetických hrozeb a vyhodnocování kybernetických bezpečnostních incidentů (tzv. Cyber Threat Intelligence). Takovýto systém umožňující čelit kybernetickým hrozbám a efektivně sdílet informace o kybernetických útocích dosud v České republice chybí. Jak potvrdily zkušenosti národního bezpečnostního týmu CSIRT.CZ např. z útoků na významné české servery v březnu 2013, absence takového systému ztěžuje koordinaci řešení bezpečnostních incidentů a snižuje reakční schopnosti jednotlivých hráčů. I to je jedním z důvodů, proč se celá řada provozovatelů kritické informační infrastruktury, resp. významných informačních systémů rozhodla vybudování tohoto systému podpořit formou prohlášení o podpoře, ve kterých se rovněž zavázala využívat jeho výsledky. Spolupráce s těmito subjekty a především jejich bezpečnostními týmy CSIRT pak přispěje k realizaci preventivních opatření před kybernetickými útoky a zajistí tak předcházení případným škodám hned na jejich počátku.

Mezi další významné uživatele výsledků projektu bude patřit Národní centrum kybernetické bezpečnosti (resp. Národní bezpečnostní úřad), který systému i dalších výstupů projektu využije při provozu vládního bezpečnostního týmu CERT. Projekt tak pomůže naplnit cíle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a přispěje k vyšší odolnosti ČR před stále častějšími a závažnějšími kybernetickými útoky. V so-

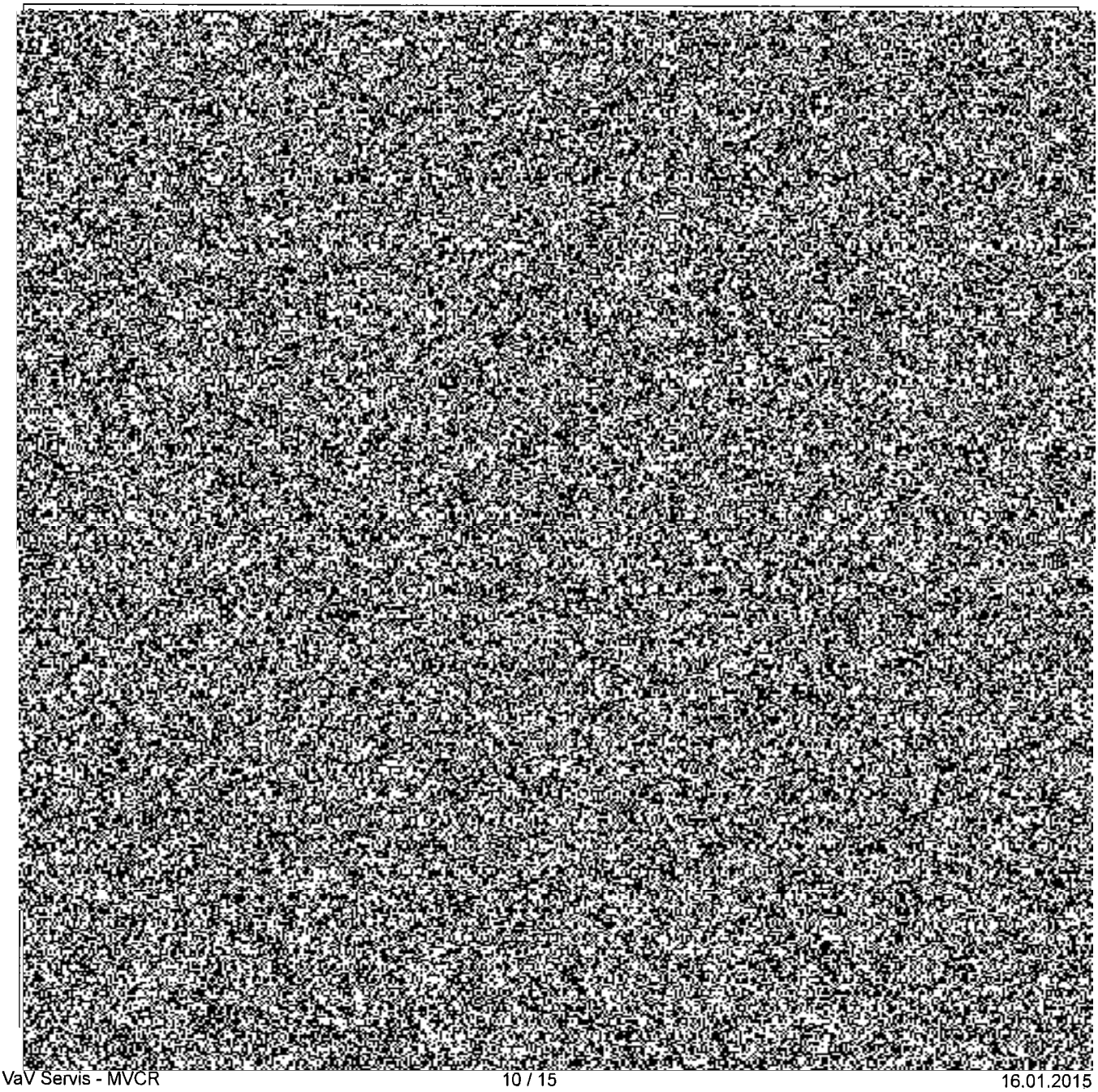
Přínosy a dopady projektu v oblasti bezpečnosti a cílů stanovených Programem

uvislosti se zákonem č. 181/2014 Sb., projekt rovněž nastaví komunikační matici mezi vrcholovými aktéry kybernetické bezpečnosti, zejm. vládním a národním CSIRT. K implementaci zákona č. 181/2014 Sb., jistě přispěje též definice jednotné metodologie pro zvládání kybernetických bezpečnostních incidentů. S ohledem na výše zmíněný zákon projekt v neposlední řadě přispěje k efektivnímu využití informací předávaných národnímu CERT a jejich případnému využití při vyhlášení stavu kybernetického nebezpečí.

To, co tento systém činí unikátním nejen v měřítkách České republiky, ale rovněž evropském i celosvětovém je šíře zdrojů, které budou v rámci systému analyzovány a které budou následně sloužit k predikci kybernetických útoků. Tento seznam zdrojů již nyní zahrnuje jak data od významných velkých provozovatelů, tak ze zařízení koncových uživatelů, která jsou pro komplexní analýzu a predikci bezpečnostních incidentů nezbytná. Výstupy založené na analýze těchto zdrojů poskytnou státním autoritám – Národnímu bezpečnostnímu úřadu, resp. vládě, potřebná data k objektivnímu zhodnocení závažnosti situace při případných masivních kybernetických útocích a následném vyhlášení stavu kybernetického nebezpečí.

Nedílnou součástí projektu pak bude mj. publikace „Kybernetická bezpečnost", která se bude věnovat praktickým aspektům kybernetické bezpečnosti a vazbě na příslušná legislativní opatření – zejm. zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ale též připravované evropské legislativy (Směrnice NIS). V publikaci pak budou využity rovněž výstupy Výzkumné zprávy v podobě analýzy bezpečnostních hrozeb a rizik v České republice a návrhy ochranných opatření. Vzhledem k účinnosti zákona o kybernetické bezpečnosti od 1. ledna 2015, resp. 1. ledna 2016 podobná publikace v ČR dosud chybí.

5.7 Popis realizace projektu (zvolená metodologie, použité metody, technologie a postupy)



Popis realizace projektu (zvolená metodologie, použité metody, technologie a postupy)

indikace možného útoku. Obsluha pak bude o této události informována a bude tuto informaci korelovat například s daty z honeypotů, které pomohou identifikovat konkrétní hrozbu, kterou zaznamenaný incident představuje. Po jejím vyhodnocení analytiky pak budou přijata další potřebná opatření, například vydání varování pro subjekty KII a VIS prostřednictvím vládního CERT (Národního centra kybernetické bezpečnosti). Dalším kritériem bude historie dané IP adresy či domény, kde opakující se incidenty mohou ukazovat na problém se zabezpečením zařízení provozovaného na dané adrese, nebo dokonce na záměrné zneužívání daného zařízení pro páchání kybernetických útoků. Pokud systém na takovouto adresu upozorní, analytici opět provedou hlubší zkoumání incidentu s využitím dalších dostupných zdrojů.

3.2. Hlubší analýza vybraných incidentů

Systém umožní provádění dalších hlubších analýz incidentů, které budou na základě výše naznačených indikátorů označeny jako vhodné pro posouzení lidskou obsluhou. Ta následně porovná všechna data relevantní danému incidentu a posoudí je v širším kontextu.

5.8 Způsob a podíl zapojení jednotlivých účastníků do realizace projektu

Způsob a podíl zapojení jednotlivých účastníků do realizace projektu

Projekt je předkládán sdružením CZ.NIC jako jediným účastníkem. V průběhu své realizace však předpokládá zapojení širokého množství subjektů a to jak soukromých (především provozovatelé kritické informační infrastruktury a významných informačních systémů), tak institucí veřejné správy, především Národního bezpečnostního úřadu (NBÚ), resp. Národního centra kybernetické bezpečnosti.

V rámci soukromých subjektů, z nichž mnozí klíčoví hráči formou „Prohlášení o podpoře" již potvrdili účast na projektu i využití jeho výsledků, projekt cílí především na ty subjekty, které mají vlastní bezpečnostní tým CERT/CSIRT, nebo jej teprve plánují založit. Tyto subjekty představují z pohledu kybernetické bezpečnosti klíčové hráče, kdy masivní výpadky jejich sítí či datacenter budou mít významný vliv na fungování českého Internetu a tím zajištění elektronické komunikace. Tyto subjekty budou jednak poskytovat informace o provozu v počítačových sítích (zejm. CESNET, CASABLANCA, národní peeringový uzel NIX.CZ...) a jednak budou mít přímý přístup do systému detekce, identifikace a predikce kybernetických hrozeb a vyhodnocování kybernetických bezpečnostních incidentů (tzv. Cyber Threat Intelligence). Přístup do tohoto systému jim umožní získávat varování o aktuálních bezpečnostních hrozbách a předcházet tak vzniku kybernetických bezpečnostních incidentů, např. prostřednictvím blokování komunikace závadné IP adresy. Cílem výše uvedené spolupráce pak bude zajistit efektivní komunikaci mezi národním CERT/CSIRT a soukromoprávními subjekty spadajícími do gesce zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

Stejný typ spolupráce, avšak v mnohem intenzivnější míře bude nastaven mezi provozovatelem národního CERT (CSIRT.CZ) a vládním pracovištěm CERT provozovaným Národním centrem kybernetické bezpečnosti (NCKB), resp. Národním bezpečnostním úřadem (NBÚ). Intenzivní spolupráce s NBÚ jako gestorem kybernetické bezpečnosti pak bude v rámci projektu nastavena především při vytváření komunikačního modelu (matice) mezi vrcholovými aktéry kybernetické bezpečnosti a vytvoření jednotné metodologie pro zvládání kybernetických bezpečnostních incidentů na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti a souvisejících právních předpisů. Sdružení CZ.NIC jako předkladatel projektu bude v tomto ohledu plnit především roli technického a odborného garanta a předního poskytovatele know-how v oblasti kybernetické bezpečnosti.

Vedle subjektů na národní úrovni budou do projektu zapojeny též subjekty na mezinárodní úrovni a to především bezpečnostní týmy již provozující pokročilý systém Cyber Threat Intelligence (zejm. Hong-Kong), tak další subjekty organizujících kybernetická cvičení (především Evropská komise, resp. agentura ENISA), na kterých, stejně jako na konferencích a setkání bezpečnostních odborníků budou moci členové řešitelského týmu získat nejnovější světové poznatky uplatnitelné v projektu.

5.9 Intenzita podpory

Intenzita podpory - CZ.NIC, z. s. p. o.

5.10 Předpokládaní uživatelé výsledků

Předpokládaní uživatelé výsledků

Mezi hlavní uživatele výsledků projektu bezpečnostního výzkumu bude patřit především Národní bezpečnostní úřad (NBÚ), resp. Národní centrum kybernetické bezpečnosti (NCKB), které je na národní úrovni garantem kybernetické bezpečnosti a významní provozovatelé kritické informační infrastruktury, zejm. data centra či poskytovatelé připojení k Internetu, kteří např. na základě seznamů závadných IP adres (tzv. graylistů) budou moci zablokovat komunikaci dané IP adresy nebo na základě nových informací o aktuálních zranitelnostech nastavit zabezpečení svých systémů (zejm. routerů, firewallů či load-balancerů).

Předkládaný projekt v současné době disponuje prohlášeními o podpoře (Letter of Intent) a potvrzeném zájmu využití výsledků výzkumu od následujících významných hráčů na poli kybernetické bezpečnosti:

- Národní bezpečnostní úřad (NBÚ)/Národní centrum kybernetické bezpečnosti (NCKB), které bude moci na základě výzkumu získávat pokročilé analýzy a hodnocení bezpečnostních incidentů. Tato varování upravené v §12 zákona č. 181/2014 Sb. pak budou moci sloužit k objektivnímu zhodnocení situace a v případě nutnosti vyhlášení stavu kybernetického nebezpečí. Cílem projektu je též vytvořit a nastavit efektivní model spolupráce a komunikační model (matici) mezi národním a vládním pracovištěm CERT a mezi národním CERT (CSIRT.CZ) a významnými provozovateli kritické informační infrastruktury.

- Provozovatelé kritické informační infrastruktury v podobě sítí elektronických komunikací – v současné době projekt disponuje prohlášeními o podpoře nejvýznamnějších provozovatelů sítí elektronických komunikací zajišťující připojení k Internetu v České republice. Mezi tyto subjekty patří: NIX.CZ – národní peeringový uzel zajišťující vzájemné propojení 118 sítí generující datový tok až v objemu 352.1 Gbps. Výsledky projektu bude NIX využívat zejména v rámci projektu FENIX, jehož cílem je umožnit v případě masivního DoS útoku zajistit dostupnost klíčových internetových služeb; O2 – poskytovatel hlasových (pevná i mobilní síť) služeb a nejvýznamnější poskytovatel internetového připojení (ISP) koncovým uživatelům. Bezpečnostní tým O2 potvrdil svým dopisem využívání výsledků projektu. CESNET – provozovatel komplexní národní IT infrastruktury pro potřeby české vědy, výzkumu, vývoje a vzdělávání. ČD Telematika – klíčový poskytovatel kritické informační infrastruktury zejm.

Předpokládaní uživatelé výsledků

v podobě rozsáhlé optické sítě s kapacitou až 80 x 10 Gbps. ČD Telematika disponuje též vlastním CSIRT týmem, který bude na projektu spolupracovat a dopisem potvrdil využití výsledků projektu.

- Provozovatelé významných informačních systémů v podobě sítí datacenter - v současné době projekt disponuje prohlášeními o podpoře od nejvýznamnějších provozovatelů datacenter v České republice. Mezi tyto subjekty patří Active 24 – významný provozovatel datových center a poskytovatel webhostingových služeb, který má více než 320 000 zákazníků. Casablanca – provozovatel datacenter s celkovou plochou více než 1 600 m2 připojených na páteřní síť. Casablanca však výstupy projektu využije nejen ve svých datacentrech, ale též v rámci dalších služeb jako je poskytování konektivity lokálním ISP (poskytovatelům připojení k Internetu) a též v rámci vlastního týmu CSIRT a posílení jeho kapacit.

- Seznam.cz – nejvýznamnější český vyhledávač a poskytovatel služeb (především e-mailu) nejširší veřejnosti. Výstupy projektu bude využívat především interní bezpečnostní tým CSIRT.

Seznam všech prohlášení o podpoře projektu včetně potvrzení o využití výsledků je v příloze projektu. Řešitelský tým dále předpokládá, že okruh uživatelů výsledků projektu bude průběžně rozšiřován, a to nejen o poskytovatele připojení k Internetu a datacentra a jejich bezpečnostní týmy, ale též bezpečnostními firmami, ať již se jedná o antivirové systémy či pokročilá řešení.

5.11 Projekt počítá se subdodávkami

Projekt počítá se subdodávkami

NE

5.12 Harmonogram projektu

Název činnosti	Uchazeč	Období, kdy je činnost uskutečňována											
		1	2	3	4	5	6	7	8	9	10	11	12
Rok 2015													
1.1 Přípravná fáze (2015) Analýza existujících systémů Cyber Threat Intelligence, zkušenost s jejich nasazením u bezpečnostních týmů CERT/CSIRT v zahraničí; Analýza dostupných zdrojů využitelných pro potřeby systému.	CZ.NIC, z. s. p. o.									X	X	X	X
Rok 2016													
2.1 Přípravná fáze (pokračování ve 2016) Dokončení analýzy existujících systémů Cyber Threat Intelligence; Výběr vhodného nástroje pro potřeby ČR; Dokončení analýzy dostupných zdrojů využitelných pro potřeby systému a případné smluvní ošetření poskytovaných zdrojů.	CZ.NIC, z. s. p. o.	X	X	X									
2.2 Implementační fáze Úprava a lokalizace systému pro potřeby národního bezpečnostního týmu (úprava komunikačních rozhraní datových zdrojů, nastavení automatizovaného zpracování určitých typů událostí, sdružování bezpečnostních událostí...). Nastavení komunikačních kanálů.	CZ.NIC, z. s. p. o.				X	X	X	X	X	X	X	X	X
2.3 Metodika predikce, detekce a analýzy incidentů (2016) Výběr incidentů indikujících nové útoky či přípravu na útoky; Tvorba postupů pro vyhodnocení incidentů a jejich závažnosti; Vyhodnocení incidentů.	CZ.NIC, z. s. p. o.				X	X	X	X	X	X	X	X	X
2.4 Publikace "Kybernetická bezpečnost" - přípravná fáze Identifikace a výběr zdrojů, stanovení obsahové struktury a přibližného rozsahu i zaměření kapitol, konzultace s odbornou veřejností.	CZ.NIC, z. s. p. o.				X	X	X	X	X	X	X	X	X
2.5 Tvorba jednotné metodologie pro zvládání incidentů Vytvoření jednotné metodologie pro zvládání kybernetických bezpečnostních incidentů na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti a souvisejících právních předpisů.	CZ.NIC, z. s. p. o.				X	X	X	X	X	X	X	X	X
Rok 2017													
3.1 Metodika predikce, detekce a analýzy incidentů (2017) Výběr incidentů indikujících nové útoky či přípravu na útoky; Tvorba postupů pro vyhodnocení incidentů a jejich závažnosti; Vyhodnocení incidentů.	CZ.NIC, z. s. p. o.	X	X	X	X	X	X	X	X	X	X	X	X
3.2 Ověřovací fáze provozu systému Cyber Threat Intelligence Ověření poloprovozu – systému Cyber Threat Intelligence a vyzkoušení této technologie pro boj s kybernetickou kriminalitou v ČR. Případná úprava komunikačních kanálů.	CZ.NIC, z. s. p. o.	X	X	X	X	X	X	X	X	X	X	X	X
3.3 Publikace "Kybernetická bezpečnost" - vydání Autorská tvorba publikace "Kybernetická bezpečnost", konzultace s odbornou veřejností včetně NBÚ, zajištění oponentur, korektur a vydání.	CZ.NIC, z. s. p. o.	X	X	X	X	X	X	X	X	X	X	X	
Rok 2018													
4.1 Hlubší analýza vybraných incidentů a jejich predikce (2018) Na základě získaných dat a již existujících postupů pro detekci, analýzu a predikci kybernetických incidentů bude možné provádět pokročilejší analýzy. Zároveň poroste schopnost predikce kybernetických bezpečnostních incidentů.	CZ.NIC, z. s. p. o.	X	X	X	X	X	X	X	X	X	X	X	X
4.2 Ověření a provoz systému Cyber Threat Intelligence Ověření poloprovozu – systému Cyber Threat Intelligence a vyzkoušení této technologie pro boj s kybernetickou kriminalitou v ČR. Průběžná úprava systému na základě zpětné vazby jak od uživatelů, tak vývoje nových incidentů.	CZ.NIC, z. s. p. o.	X	X	X	X	X	X	X	X	X	X	X	X
Rok 2019													
5.1 Hlubší analýza vybraných incidentů a jejich predikce (2019) Na základě získaných dat a již existujících postupů pro detekci, analýzu a predikci kybernetických incidentů bude možné provádět pokročilejší analýzy. Zároveň poroste schopnost predikce kybernetických bezpečnostních incidentů.	CZ.NIC, z. s. p. o.	X	X	X	X	X	X	X	X	X	X	X	X

Název činnosti	Uchazeč	Období, kdy je činnost uskutečňována											
		1	2	3	4	5	6	7	8	9	10	11	12
5.2 Ověření a provoz systému Cyber Threat Intelligence Ověření poloprovozu – systému Cyber Threat Intelligence a vyzkoušení této technologie pro boj s kybernetickou kriminalitou v ČR. Průběžná úprava systému na základě zpětné vazby jak od uživatelů, tak vývoje nových incidentů.	CZ.NIC, z. s. p. o.	X	X	X	X	X	X	X	X	X	X	X	X
Rok 2020													
6.1 Hlubší analýza vybraných incidentů a jejich predikce (2020) Na základě získaných dat a již existujících postupů pro detekci, analýzu a predikci kybernetických incidentů bude možné provádět pokročilejší analýzy. Zároveň poroste schopnost predikce kybernetických bezpečnostních incidentů.	CZ.NIC, z. s. p. o.	X	X	X	X	X	X	X	X				
6.2 Ověření a provoz systému Cyber Threat Intelligence Ověření poloprovozu – systému Cyber Threat Intelligence a vyzkoušení této technologie pro boj s kybernetickou kriminalitou v ČR. Průběžná úprava systému na základě zpětné vazby jak od uživatelů, tak vývoje nových incidentů.	CZ.NIC, z. s. p. o.	X	X	X	X	X	X	X	X				

5.13 Popis rizik projektu a jejich řízení

Popis rizik projektu a jejich řízení

Níže uvedená analýza rizik pro projekt „Predikce a ochrana před kybernetickými incidenty (PROKI) byla zpracována metodou FMEA, kdy jsou každému potenciálnímu riziku přiřazeny údaje o pravděpodobnosti výskytu P (1-5) a závažnosti Z (1-5). Jejich vynásobením je určena Míra rizika FMEA MR/FMEA (1-25). Riziko s vyšší než 6 je v rámci této analýzy považováno za závažné; riziko ohodnocené menší mírou než 3 je považováno za nevýznamné. Vzhledem k maximálnímu rozsahu obsahuje níže uvedená analýza pouze vybraná klíčová rizika v oblastech výzkumu a vývoje; regulační a právní rizika a projektová rizika.

1. Projektová rizika

R1.1. Neudělení projektu – projektu nemusí být na základě žádosti vybrán k podpoře. V takovém případě bude analýza bezpečnostních incidentů probíhat v omezenější míře, technologické zaostávání ČR v této oblasti vůči ostatním státům se bude prohlubovat a ČR nebude připravena detekovat, identifikovat a predikovat kybernetické hrozby a vyhodnocovat bezpečnostní incidenty a to zejm. na základě korelace dat z širokého množství zdrojů. P: 3; Z: 4; MR/FMEA: 12 (závažné riziko)

R1.2. Zvýšená finanční náročnost projektu - v průběhu řešení projektu se může ukázat, že ke splnění stanovených cílů nestačí alokované finanční prostředky. V tomto případě projekt bude dofinancován z vlastních zdrojů sdružení, resp. příjmů z jiných činností (zejm. provozu národní domény .cz), které jsou schopny toto riziko dostatečně pokrýt. P: 2; Z: 6; MR/FMEA: 6 (závažné riziko)

R1.3. Neplnění stanovených cílů projektu - náročnost a nepředvídatelnost bezpečnostního výzkumu může vést ke zpoždění dosahování cílů projektu. V projektu se jedná o výzkum aplikovaný, jehož cíle jsou lépe předpověditelné než cíle výzkumu základního. Preventivní opatření představuje zvýšení prostředků vynakládaných na projekt včetně posílení kapacit (personálních i odborných) řešitelského týmu. P: 1; Z: 5; MR/FMEA: 5 (méně závažné riziko)

R1.4. Riziko odchodu nedostatečně motivovaných lidských zdrojů – po dobu 5 let realizace projektu mohou odejít někteří členové týmu. Přesto, že v oblasti IT patří obecně migrace pracovních sil mezi jednu z nejvyšších, sdružení CZ.NIC disponuje dlouhodobou stabilitou personálního týmu. Případný odchod člena týmu, který nelze nikdy vyloučit by byl řešen hledáním odpovídající náhrady a to jak z interních (více než 70 zaměstnanců), tak externích zdrojů. Preventivním opatření je též nastavení odpovídající finanční i nefinanční motivace projektového týmu. P: 3; Z: 3; MR/FMEA: 9 (závažné riziko).

2. Rizika výzkumu a vývoje

R2.1. Neadekvátní postupy při výzkumu a vývoji - volba neodpovídajících nebo neaktuálních postupů, která ve svých důsledcích může vést k omezené schopnosti predikce bezpečnostních incidentů. Toto riziko neodmyslitelně spojené s každým výzkumem je eliminováno jednak dostatečným know-how řešitelského týmu včetně již úspěšně predikovaných incidentů a jednak bude eliminováno porovnáváním použitých metod s metodami používanými jinými bezpečnostními týmy v zahraničí. Míra rizika tak spíš reflektuje množství predikovaných incidentů, kdy v případě výskytu adekvátních incidentů lze nyní již oprávněně tvrdit, že je tým dokáže předpovědět. P: 3; Z: 4; MR/FMEA: 12 (závažné riziko)

3. Regulační a právní rizika

R3.1. Změna provozovatele národního CERT – v současné době je provoz národního CERT zajišťován v souladu s §32 zákona č. 181/2014 Sb. sdružením CZ.NIC s tím, že nejpozději 31. 12. 2016 by mělo proběhnou výběrové řízení na nového poskytovatele. Vzhledem k nekomerčnímu charakteru provozu sdružení CZ.NIC nepředpokládá zájem ze strany soukromých firem a s ohledem na personální i odborné požadavky, stejně jako své zkušenosti v oboru nepředpokládá, že by mu mohl významně konkurovat jiný subjekt, který by splnil rovněž požadavky § 18 zákona č. 181/2014 Sb.. V případě této hypotetické situace však může být projekt i nadále realizován a to především na principu důvěry mezi CERT/CSIRT týmy. P: 1; Z: 5; MR/FMEA: 5 (méně závažné riziko).

6. Financování a náklady projektu

6.1 Výše státní podpory projektu podle jednotlivých uchazečů

Uchazeč	Rok	Způsobilé náklady projektu (tis. Kč)	Z toho vlastní zdroje (tis. Kč)	Požadovaná státní podpora (tis. Kč)	Intenzita podpory (%)
CZ.NIC, z. s. p. o.	**Celkem**	**13592.90**	**3398.90**	**10194.00**	**75.00**
	2015	889.46	222.46	667.00	74.99
	2016	2668.10	667.10	2001.00	75.00
	2017	2668.10	667.10	2001.00	75.00
	2018	2668.10	667.10	2001.00	75.00
	2019	2668.10	667.10	2001.00	75.00
	2020	2031.04	508.04	1523.00	74.99
PROJEKT	**Celkem**	**13592.90**	**3398.90**	**10194.00**	**75.00**

6.2 Rozpočet projektu

6.2.1 Výpočet maximální míry podpory uchazeče CZ.NIC, z. s. p. o.

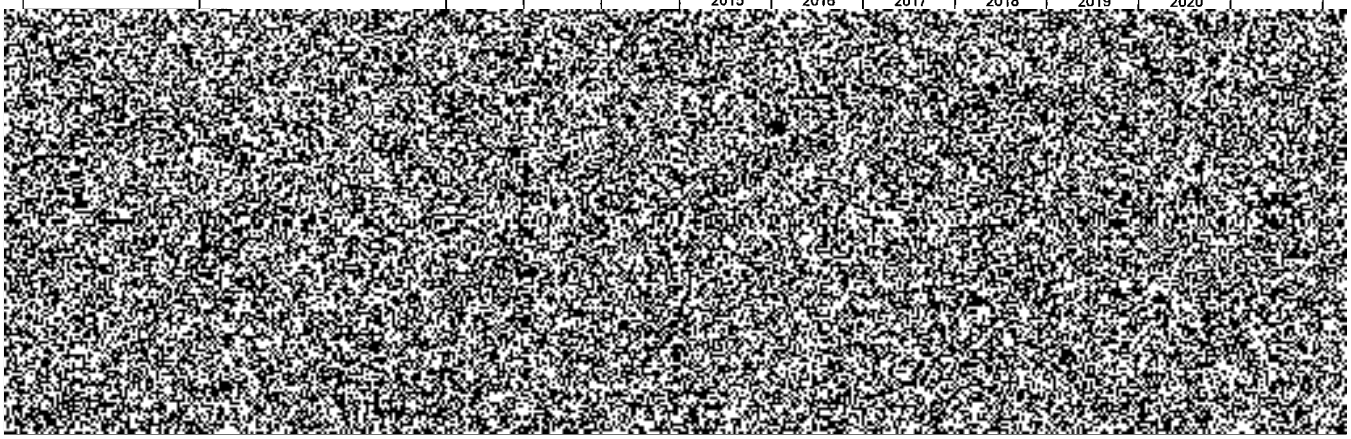
Kategorie uchazeče	střední podnik
Kategorie výzkumu	průmyslový výzkum
Způsobilé náklady uchazeče (tis. Kč)	**13592.90**

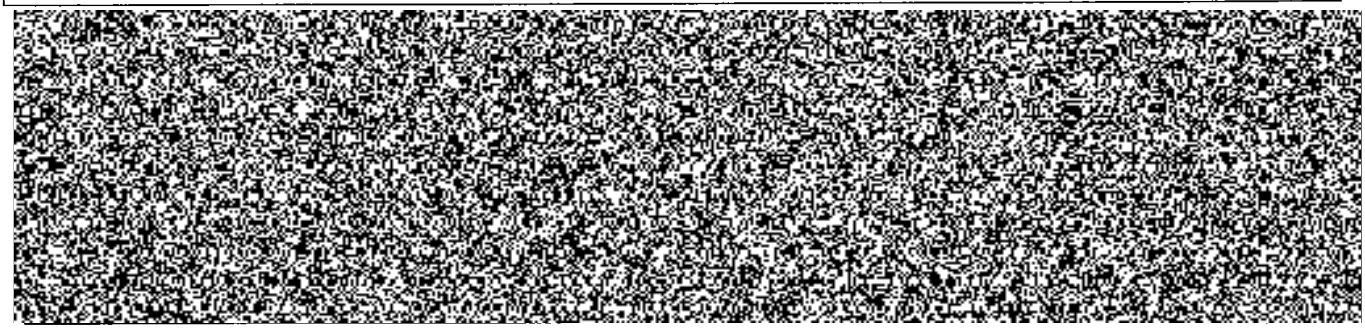
Účastní se projektu alespoň dva nezávislé podniky?	NE
Hradí každý podnik maximálně 70% nákladů projektu?	NE
Účastní se projektu malý nebo střední nebo zahraniční podnik?	NE
Účastní se projektu výzkumná organizace?	NE
Nese výzkumná organizace minimálně 10 % nákladů projektu?	NE
Může výzkumná organizace zveřejnit své výsledky?	NE
Budou výsledky projektu obecně šířeny?	ANO

Základní intenzita podpory (%)	50.00
Bonus (%)	25.00
Maximální intenzita podpory (%)	**75.00**
Maximální výše podpory (tis. Kč)	**10194.67**

6.2.2 Náklady na mzdy/platy uchazeče CZ.NIC, z. s. p. o.

Jméno	Pozice v projektu	Druh pracovní smlouvy	Hodinová mzdová sazba (Kč)	Průměrný počet odprac. hodin měsíčně	Náklady na mzdy/platy v jednotlivých letech trvání projektu (tis. Kč)						Náklady celkem (tis. Kč)
					2015	2016	2017	2018	2019	2020	





6.2.3 Náklady uchazeče CZ.NIC, z. s. p. o. na pořízení majetku

6.2.4 Rozpočet nákladů uchazeče CZ.NIC, z. s. p. o.

Náklady/výdaje uchazeče (tis. Kč)	2015	2016	2017	2018	2019	2020	Celkem
Osobní náklady/výdaje - mezisoučet	**808.60**	**2425.55**	**2425.55**	**2425.55**	**2425.55**	**1846.42**	**12357.22**
a) mzdy/platy na základě pracovního poměru	528.81	1586.23	1586.23	1586.23	1586.23	1057.10	7930.83
b) osobní náklady/výdaje na základě dohody o pracovní činnosti	0.00	0.00	0.00	0.00	0.00	0.00	0.00
c) osobní náklady/výdaje na základě dohody o provedení práce	0.00	0.00	0.00	0.00	0.00	0.00	0.00
d) povinné pojistné na sociální zabezpečení	132.20	396.56	396.56	396.56	396.56	396.56	2115.00
e) povinné pojistné na zdravotní pojištění	47.59	142.76	142.76	142.76	142.76	142.76	761.39
f) odvody do FKSP nebo sociálního fondu	0.00	0.00	0.00	0.00	0.00	0.00	0.00
g) cestovné	100.00	300.00	300.00	300.00	300.00	250.00	1550.00
Náklady/výdaje na pořízení hmotného a nehmotného majetku - mezisoučet	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
a) dlouhodobý hmotný majetek	0.00	0.00	0.00	0.00	0.00	0.00	0.00
b) dlouhodobý nehmotný majetek	0.00	0.00	0.00	0.00	0.00	0.00	0.00
c) drobný hmotný majetek	0.00	0.00	0.00	0.00	0.00	0.00	0.00
d) drobný nehmotný majetek	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Další provozní náklady/výdaje - mezisoučet	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
Náklady/výdaje na služby - mezisoučet	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
a) subdodávky	0.00	0.00	0.00	0.00	0.00	0.00	0.00
b) ostatní služby	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Doplňkové náklady/výdaje - mezisoučet	**80.86**	**242.55**	**242.55**	**242.55**	**242.55**	**184.62**	**1235.68**
Doplňkové náklady účtované metodou AC (10%)	80.86	242.55	242.55	242.55	242.55	184.62	1235.68
Celkové způsobilé náklady - mezisoučet	**889.46**	**2668.10**	**2668.10**	**2668.10**	**2668.10**	**2031.04**	**13592.90**
Celková státní podpora - mezisoučet	**667.00**	**2001.00**	**2001.00**	**2001.00**	**2001.00**	**1523.00**	**10194.00**

6.2.5 Rozpočet nákladů za celý projekt

Náklady/výdaje za celý projekt (tis. Kč)	2015	2016	2017	2018	2019	2020	Celkem
Osobní náklady/výdaje	**808.60**	**2425.55**	**2425.55**	**2425.55**	**2425.55**	**1846.42**	**12357.22**
Náklady/výdaje na pořízení hmotného a nehmotného majetku	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
Další provozní náklady/výdaje	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
Náklady/výdaje na služby	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
Doplňkové náklady/výdaje	**80.86**	**242.55**	**242.55**	**242.55**	**242.55**	**184.62**	**1235.68**
Celkové způsobilé náklady	**889.46**	**2668.10**	**2668.10**	**2668.10**	**2668.10**	**2031.04**	**13592.90**
Celková státní podpora	**667.00**	**2001.00**	**2001.00**	**2001.00**	**2001.00**	**1523.00**	**10194.00**

Žádost o poskytnutí účelové podpory			
Program: BV III/1-VS	PID: VI1VS/314	Hlavní obor: IN	Stupeň důvěrnosti: S

Souhlas statutárního zástupce uchazeče CZ.NIC, z. s. p. o. s návrhem projektu, se zveřejněním údajů v rozsahu požadovaném CEP a potvrzení správnosti údajů předkládaných k žádosti a souhlas s postupem stanoveným v zadávací dokumentaci.

Datum podpisu	Místo podpisu	Otisk razítka uchazeče projektu

Titul před jménem	Jméno	Příjmení	Titul za jménem	Podpis
JUDr., PhDr.	Marek	Antoš		

Titul před jménem	Jméno	Příjmení	Titul za jménem	Podpis
Mgr.	Ondřej	Filip	MBA	

Titul před jménem	Jméno	Příjmení	Titul za jménem	Podpis
Ing.	Jiří	Kysela		