Veřejnoprávní smlouva o zajištění činnosti Národního CERT a o spolupráci v oblasti kybernetické bezpečnosti

podle § 19 zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a § 159 a násl. zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů (dále jen „správní řád")
(dále jen „**Smlouva**")

Česká republika – Národní bezpečnostní úřad
sídlo: Na Popelce 2/16, 150 06 Praha 5
IČ: 68403569
ID datové schránky: h93aayw
č.j: 9625/2015-NBÚ/41
zastoupený Ing. Dušanem Navrátilem, ředitelem Národního bezpečnostního úřadu
(dále jen „**NBÚ**")

a

CZ.NIC, z.s.p.o.
sídlo: Milešovská 1136/5, 130 00 Praha 3 - Vinohrady
IČ: 67985726
ID datové schránky: h4axdn8
zastoupené Mgr. Ondřejem Filipem, MBA, na základě plné moci ze dne 22. května 2015
(dále jen „**CZ.NIC**")

(NBÚ a CZ.NIC dále společně také jako „**Smluvní strany**")

VZHLEDEM K TOMU, ŽE

A. NBÚ vykonává na základě § 22 zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „ZKB") státní správu v oblasti kybernetické bezpečnosti, přičemž ZKB zakotvuje fungování dvou základních dohledových pracovišť, kterým dává kompetence v oblasti kybernetické bezpečnosti v České republice, z nichž jedním je Národní CERT;

B. NBÚ v souladu s § 19 odst. 1 ZKB vyhlásil dne 15. dubna 2015 řízení o výběru žádosti o uzavření veřejnoprávní smlouvy za účelem spolupráce v oblasti kybernetické bezpečnosti a zajištění činností Národního CERT podle § 17 odst. 2 ZKB, přičemž dne 17. srpna 2015 NBÚ vybral pro další postup žádost CZ.NIC, z.s.p.o.;

C. CZ.NIC je zájmovým sdružením právnických osob sdružujícím významné právnické osoby působící v České republice v oblasti doménových jmen a na trhu služeb elektronických komunikací, které je správcem národní domény nejvyšší úrovně .cz (ccTLD .cz), zabývá se mimo jiné bezpečností internetu, počítačovou a kybernetickou bezpečností a provozuje bezpečnostní tým CSIRT.CZ;

D. Do dne uzavření této Smlouvy vykonával roli Národního CERT bezpečnostní tým CSIRT.CZ provozovaný CZ.NIC na základě Memoranda o CERT/CSIRT České republiky ze dne 19. prosince 2012;

UZAVÍRAJÍ SMLUVNÍ STRANY NÍŽE UVEDENÉHO DNE, MĚSÍCE A ROKU TUTO SMLOUVU:

Část I.
Základní ustanovení

Čl. I.
Předmět Smlouvy

1. Na základě této Smlouvy se CZ.NIC zavazuje provozovat Národní CERT za podmínek stanovených v ZKB a dále v této Smlouvě.
2. CZ.NIC a NBÚ se dále zavazují rozvíjet spolupráci v oblasti kybernetické bezpečnosti k dosažení maximální možné míry zajištění kybernetické bezpečnosti České republiky (dále jen „**Spolupráce**").
3. CZ.NIC se zavazuje za účelem zajištění řádného plnění předmětu Smlouvy po dobu jejího trvání dosahovat organizační a institucionální kapacity, finanční stability a technického a technologického zajištění činnosti minimálně na úrovni uvedené v „Žádosti o uzavření veřejnosprávní smlouvy za účelem spolupráce v oblasti kybernetické bezpečnosti a zajištění provozu národního bezpečnostního týmu" (dále jen „**Žádost**"), kterou se účastnil řízení o výběru žádosti o uzavření veřejnoprávní smlouvy s NBÚ za účelem spolupráce v oblasti kybernetické bezpečnosti a zajištění činností podle § 17 odst. 2 ZKB - výběr provozovatele národního CERT, vyhlášeného dne 15. dubna 2015 jako č.j. 2688/2015-NBÚ/80, a která je Přílohou č. 1 této Smlouvy.
4. Na základě této Smlouvy budou k upřesnění podmínek provozování Národního CERT a za účelem podrobné úpravy vzájemné Spolupráce uzavírány vzestupně číslované písemné **Prováděcí protokoly**.

Za NBÚ bude Prováděcí protokoly podepisovat:

- náměstek sekce kybernetické bezpečnosti, nebo
- ředitel Národního centra kybernetické bezpečnosti.

Ke dni podpisu této Smlouvy je náměstkem sekce kybernetické bezpečnosti Ing. Jaroslav Šmíd a ředitelem Národního centra kybernetické bezpečnosti Mgr. Vladimír Rohel.

Za CZ.NIC bude Prováděcí protokoly podepisovat:

- představenstvo, nebo
- výkonný ředitel CZ.NIC.

Ke dni podpisu této Smlouvy je výkonným ředitelem CZ.NIC Mgr. Ondřej Filip, MBA.

Případná budoucí změna v osobách oprávněných podepisovat Prováděcí protokoly není důvodem pro změnu této Smlouvy; změna osob oprávněných k podpisu Prováděcích protokolů bude druhé Smluvní straně oznámena prostřednictvím informačního systému datových schránek (dále jen „ISDS"), umožní-li to povaha datových schránek Smluvních stran.

Část II.
Provozování Národního CERT

Čl. II.
Práva a povinnosti CZ.NIC při provozování Národního CERT

1. CZ.NIC se zavazuje k řádnému provozování Národního CERT v souladu s nejlepší praxí CERT/CSIRT týmů a dalšími národními a mezinárodními standardy zejména z oblasti kybernetické bezpečnosti. Provoz dohledového pracoviště – Národního CERT bude vykonávat bezpečnostní tým CSIRT.CZ provozovaný CZ.NIC. CZ.NIC se zavazuje provozovat Národní CERT prostřednictvím bezpečnostního týmu CSIRT.CZ na vlastní odpovědnost.
2. CZ.NIC se zavazuje věnovat se v přiměřené míře prevenci před kybernetickými útoky, například provozováním pasivních detekčních nástrojů, či v případě potřeby také aktivním vyhledáváním zranitelných či nevhodně zkonfigurovaných zařízení dostupných zejména prostřednictvím sítě Internet.
3. CZ.NIC se zavazuje udržovat členství bezpečnostního týmu CSIRT.CZ v nadnárodních organizacích působících v oblasti kybernetické bezpečnosti, zejména v těch, které byly uvedeny v Žádosti.
4. CZ.NIC se zavazuje, že
   a) bude oprávněn k přístupu k utajovaným informacím stupně utajení Vyhrazené podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „ZOUI"), a to na základě prohlášení podnikatele podle § 15a ZOUI anebo na základě platného osvědčení podnikatele stupně utajení Důvěrné, Tajné nebo Přísně tajné, a to nejméně pro formu přístupu podle § 20 písm. b) ZOUI, a
   b) fyzické osoby, jejichž činnost při plnění předmětu Smlouvy bude vyžadovat přístup k utajovaným informacím, tj. výkonný ředitel, provozní ředitel a analytici, budou držiteli platného osvědčení fyzické osoby pro přístup k utajovaným informacím stupně utajení Důvěrné nebo oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené ve smyslu ZOUI.
5. CZ.NIC se zavazuje, že bude zveřejňovat pravidelné zprávy o činnosti Národního CERT, a to jedenkrát ročně, nejpozději však do konce měsíce března následujícího kalendářního roku. Nejpozději do konce února předloží CZ.NIC zprávu k připomínkám NBÚ; NBÚ je povinen připomínky ke zprávě předat CZ.NIC nejpozději do 14 dnů od předložení zprávy k připomínkám. Informace ze zprávy budou jedním z podkladů pro tvorbu Zprávy o stavu kybernetické bezpečnosti v České republice, kterou každoročně zpracovává NBÚ a předkládá ji vládě České republiky; nejméně 1 měsíc před předložením vládě České republiky zašle NBÚ tuto Zprávu CZ.NIC k případným připomínkám.
6. CZ.NIC se v souladu s Žádostí zavazuje udržovat systém managementu bezpečnosti informací na úrovni normy ČSN ISO/IEC 27001, popř. obdobné uznávané normy zajišťující ochranu informací na stejné nebo lepší úrovni. NBÚ si vyhrazuje právo požadovat předložení zprávy z posledního vypracovaného dozorového/recertifikačního

auditu prokazujícího plnění výše uvedené normy, a to nejpozději do 30 dnů od doručení žádosti NBÚ.

7. CZ.NIC je oprávněn v souladu s § 17 odst. 3 ZKB vykonávat vlastním jménem a na vlastní odpovědnost i další činnosti v oblasti kybernetické bezpečnosti neupravené v ZKB, a to včetně hospodářských, za předpokladu, že tato činnost nenaruší plnění povinností uvedených v § 17 odst. 2 ZKB.

8. V případě důvodného podezření, že CZ.NIC při výkonu činnosti Národního CERT nedodržuje podmínky stanovené zákonem a Smlouvou, je NBÚ oprávněn požádat o předložení zprávy z posledního vypracovaného dozorového/recertifikačního auditu podle normy ČSN ISO/IEC 27001, popř. obdobné uznávané normy zajišťující ochranu informací na stejné nebo lepší úrovni, a to nejpozději do 30 dnů od doručení žádosti NBÚ. V případě nedoložení takové zprávy je pak NBÚ oprávněn vykonat u CZ.NIC kontrolu výkonu činnosti Národního CERT podle § 23 ZKB.

Čl. III.
Zákonné povinnosti Národního CERT

1. Národní CERT bude v souladu s § 17 odst. 2 písm. a) ZKB přijímat oznámení kontaktních údajů od orgánů a osob uvedených v § 3 písm. a) a b) ZKB a tyto údaje evidovat a uchovávat. CZ.NIC jako provozovatel Národního CERT umožní přijímání těchto kontaktních údajů rovněž prostřednictvím ISDS. NBÚ pro tento účel vyslovuje souhlas, aby CZ.NIC v souladu s ustanovením § 5a zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, disponoval datovou schránkou orgánu veřejné moci.

2. Národní CERT bude v souladu s § 17 odst. 2 písm. b) ZKB přijímat hlášení o kybernetických bezpečnostních incidentech od orgánů a osob uvedených v § 3 písm. b) ZKB a tyto údaje evidovat, uchovávat a chránit, přičemž

   a) CZ.NIC se zavazuje zřídit a udržovat v provozu dohledové centrum a zákaznickou podporu s nepřetržitým provozem plnící funkci posledního záchytného bodu (tzv. last resort), prostřednictvím kterého budou orgány a osoby uvedené v § 3 písm. b) ZKB hlásit Národnímu CERT kybernetické bezpečnostní incidenty, a

   b) Národní CERT je oprávněn přijímat hlášení o kybernetických bezpečnostních událostech a o kybernetických bezpečnostních incidentech i od dalších subjektů; pomoc při řešení těchto událostí a incidentů bude Národní CERT poskytovat přiměřeně a pouze v případě dostatečné kapacity, přičemž není povinen poskytovat podporu a pomoc koncovým uživatelům.

3. Národní CERT bude v souladu s § 17 odst. 2 písm. c) ZKB vyhodnocovat kybernetické bezpečnostní incidenty u orgánů a osob uvedených v § 3 písm. b) ZKB.

4. Národní CERT bude v souladu s § 17 odst. 2 písm. d) ZKB poskytovat orgánům a osobám uvedeným v § 3 písm. a) a b) ZKB metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu. Pomocí se rozumí především pomoc koordinační a metodická. Národní CERT není povinen poskytovat fyzickou podporu.

5. Národní CERT bude v souladu s § 17 odst. 2 písm. e) ZKB působit jako kontaktní místo pro orgány a osoby uvedené v § 3 písm. a) a b) ZKB.

6. Národní CERT bude v souladu s § 17 odst. 2 písm. f) ZKB provádět hodnocení zranitelností v oblasti kybernetické bezpečnosti.

7. Národní CERT bude v souladu s § 17 odst. 2 písm. g) ZKB předávat NBÚ údaje o kybernetických bezpečnostních incidentech bez uvedení ohlašovatele kybernetického bezpečnostního incidentu. Rozsah předávaných údajů a způsob jejich předávání bude stanoven prostřednictvím Prováděcího protokolu.

8. Národní CERT bude v souladu s § 17 odst. 2 písm. h) ZKB předávat na vyžádání NBÚ za stavu kybernetického nebezpečí kontaktní údaje orgánů a osob uvedených v § 3 písm. a) a b) ZKB. Národní CERT je povinen předat NBÚ tyto údaje neprodleně po jejich vyžádání.

9. Při výkonu povinností Národního CERT podle odstavce 1 až 8 je CZ.NIC v souladu s § 17 odst. 5 ZKB povinen postupovat nestranně a v souladu s § 17 odst. 4 ZKB je při výkonu těchto povinností povinen koordinovat svou činnost s NBÚ, a to zejména, pokud takovou spolupráci vyžadují okolnosti, které mají významný dopad na kybernetickou bezpečnost České republiky, tedy především v případech vyhlášeného stavu kybernetického nebezpečí podle § 21 ZKB a dalších krizových stavech způsobených zejména významným narušením kybernetické bezpečnosti České republiky.

10. V případě, že se v průběhu řešení kybernetického bezpečnostního incidentu Národním CERT objeví situace, která má nebo může mít významný bezpečnostní dopad na kritickou informační infrastrukturu, významný informační systém nebo informační systém veřejné správy, a pokud lze po CZ.NIC v takovém konkrétním případě a při znalosti jemu dostupných informací rozumně požadovat, aby takový významný bezpečnostní dopad rozpoznal, postoupí Národní CERT neprodleně tuto informaci NBÚ a dále bude při řešení tohoto incidentu postupovat v koordinaci s ním.

11. Národní CERT bude dále shromažďovat a vyhodnocovat údaje o kybernetických bezpečnostních událostech, kybernetických bezpečnostních incidentech a dalších kybernetických bezpečnostních hrozbách, které se při své činnosti dozví. Tyto informace bude předávat NBÚ a dalším subjektům působícím v oblasti kybernetické bezpečnosti v souladu s ujednáními v čl. IV.

Čl. IV.
Výměna informací

1. Národní i mezinárodní výměna informací o kybernetických hrozbách a rizicích mezi Národním CERT, dalšími CERT/CSIRT týmy a dalšími subjekty působícími v oblasti kybernetické bezpečnosti bude probíhat v závislosti na jejich citlivosti a závažnosti situace v souladu s platnými právními předpisy, nejlepší praxí CERT/CSIRT týmů a dalšími národními a mezinárodními standardy zejména z oblasti kybernetické bezpečnosti (např. Traffic Light Protocol – TLP) s cílem zabránit zneužití těchto informací. Ustanovení čl. III odst. 7 tímto není dotčeno.

2. NBÚ bude v souladu s § 9 odst. 4 ZKB poskytovat údaje z evidence incidentů CZ.NIC v rozsahu nezbytném pro zajištění ochrany kybernetického prostoru, a to podle závažnosti zjištění, stavu řešení kybernetického bezpečnostního incidentu a v souladu s principem proporcionality ve vztahu k závažnosti obsahu poskytovaných údajů.

3. CZ.NIC se zavazuje chránit a zabránit zneužití údajů získaných v souvislosti s výkonem činností uvedených v § 17 odst. 2 ZKB. Tyto údaje zejména nepředá třetím stranám mimo případy sdílení informací stanovené v této Smlouvě a neposkytne a nevyužije je ke komerčním účelům. Tato povinnost trvá i po skončení platnosti Smlouvy, ustanovení čl. VIII odst. 2 Smlouvy platí obdobně.
4. CZ.NIC se zavazuje, že bude na jím provozovaných webových stránkách Národního CERT průběžně zveřejňovat aktualizované informace a statistiky o počtu a druhu řešených kybernetických bezpečnostních incidentů.
5. Technické podrobnosti a způsob výměny informací Smluvní strany stanoví prostřednictvím Prováděcích protokolů.

Čl. V.
Finanční zajištění provozování Národního CERT

1. Náklady spojené s provozováním Národního CERT ponese CZ.NIC.
2. CZ.NIC bude vykonávat povinnosti podle čl. III odst. 1, 2, 3, 5, 7 a 8 Smlouvy bezúplatně.
3. CZ.NIC je oprávněn požadovat finanční plnění od třetích osob za výkon činností uvedených v čl. III odst. 4 a 6 Smlouvy a rovněž za výkon další hospodářské činnosti v oblasti kybernetické bezpečnosti podle § 17 odst. 3 ZKB.
4. CZ.NIC je oprávněn žádat o podporu financování provozu Národního CERT ze soukromých, resortních, vládních, či mezinárodních zdrojů, a to zejména formou grantů či čerpání fondů.
5. NBÚ bude podporovat CZ.NIC při případném získávání financování činnosti Národního CERT podle této Smlouvy, zejména z národních a mezinárodních zdrojů formou grantů či čerpání fondů a to pokud to nebude možno považovat za střet zájmů vzhledem k zapojení NBÚ v orgánech, které budou o poskytnutí financí rozhodovat.
6. NBÚ je oprávněn každoročně požadovat od CZ.NIC prokázání finanční stability a schopnosti udržet řádný provoz Národního CERT.

Část III.
Spolupráce

Čl. VI.
Obsah Spolupráce

1. Obsahem Spolupráce je zejména:
   a) odborná pomoc CZ.NIC při kontrolách v oblasti kybernetické bezpečnosti, které NBÚ provádí podle § 23 ZKB, a rovněž při forenzní činnosti; CZ.NIC za tímto účelem bude NBÚ po předchozí dohodě poskytovat personální a technickou pomoc,
   b) vzdělávání a šíření osvěty v oblasti kybernetické bezpečnosti, a to formou pořádání seminářů, přednášek, konferencí, školení, účasti na akcích týkajících se této oblasti a případným vydáváním materiálů k těmto tématům v elektronické i tištěné podobě;

obě Smluvní strany se budou navzájem v dostatečném předstihu informovat o jimi připravovaných aktivitách a budou koordinovat jejich přípravu,

c) rozvoj spolupráce se třetími subjekty působícími zejména v oblasti kybernetické bezpečnosti na národní i mezinárodní úrovni, přičemž Smluvní strany budou koordinovat svou pozici a spolupracovat na propagaci a jednotném obrazu kybernetické bezpečnosti České republiky při práci v mezinárodních organizacích, ve kterých jsou členy, působením na akcích v zahraničí i v České republice a vzájemnou podporou a propagací svých aktivit v této oblasti,

d) součinnost při zřizování dalších CERT/CSIRT týmů v České republice, přičemž obě Smluvní strany budou podporovat vznik nových kybernetických bezpečnostních týmů u akademických institucí a soukromých společností,

e) vzájemná výměna zkušeností, znalostí, know-how a informací zejména z oblasti kybernetické bezpečnosti, přičemž Smluvní strany se zavazují si v co největší možné míře poskytovat výsledky výzkumných projektů, úkolů a řešení, které vedou nebo se jich účastní; nestanoví-li poskytující Smluvní strana jinak, budou tyto výsledky prostřednictvím NBÚ k dispozici pro využití všemi subjekty spolupracujícími na ochraně kybernetického prostoru, včetně orgánů veřejné správy, subjektů kritické informační infrastruktury, orgánů nebo osob zajišťujících významnou síť a správců významného informačního systému,

f) společná účast na cvičeních kybernetické bezpečnosti a obrany; CZ.NIC se bude na požádání NBÚ po vzájemné dohodě účastnit národních a mezinárodních cvičení a případných dalších akcí souvisejících s provozem Národního CERT a kybernetickou bezpečností České republiky a NBÚ bude CZ.NIC k účasti na takových akcích zvát,

g) spolupráce při přípravě návrhů právních předpisů a navazujících dokumentů v oblasti kybernetické bezpečnosti,

h) další spolupráce v závislosti na aktuální potřebě činností k zajištění kybernetické bezpečnosti České republiky.

2. CZ.NIC se bude na základě žádosti NBÚ účastnit jednání Rady pro kybernetickou bezpečnost a zasedání pracovních orgánů zřizovaných NBÚ při řešení závažných kybernetických bezpečnostních incidentů, které mohou mít významný bezpečnostní dopad na kybernetickou bezpečnost České republiky, pokud v konkrétním případě nebude jeho účast ze závažných důvodů vyloučena. CZ.NIC poskytne NBÚ kontaktní údaje na osoby, které budou při plnění této povinnosti CZ.NIC zastupovat a které splňují podmínky pro přístup k utajovaným informacím, k nimž mohou mít v této souvislosti přístup, a to nejméně pro stupeň utajení, který je nutný k účasti na takovém jednání. V případě projednávání utajovaných informací vyššího stupně utajení učiní NBÚ potřebná opatření, aby nedošlo k neoprávněnému přístupu k těmto utajovaným informacím. V případě neúčasti CZ.NIC na jednání Rady pro kybernetickou bezpečnost nebo na zasedání pracovních orgánů zřizovaných NBÚ při řešení závažných kybernetických bezpečnostních incidentů je NBÚ povinen seznámit CZ.NIC se závěry jednání, pokud mohou ovlivňovat činnost Národního CERT podle této Smlouvy.

3. Podrobnější úprava podmínek Spolupráce bude Smluvními stranami stanovena formou Prováděcích protokolů, a to včetně finančního zajištění konkrétně specifikované

Spolupráce, pokud se na něm Smluvní strany písemně dohodnou. Smluvní strany mohou průběžně rozvíjet Spolupráci rovněž neformální cestou.

4. Spolupráce mezi CZ.NIC a NBÚ bude ze strany CZ.NIC poskytována v rozsahu odpovídajícím jeho kapacitním, personálním, časovým či finančním možnostem.

Část IV.
Další ujednání

Čl. VII.
Úprava práva duševního vlastnictví

1. Smluvní strany se zavazují při realizaci této Smlouvy k dodržování a ochraně práv průmyslového a jiného duševního vlastnictví, jakož i práv spadajících do autorského práva a ochrany obchodního tajemství.
2. V případě, že při plnění předmětu Smlouvy vznikne činností Smluvních stran dílo nesoucí znaky autorského díla podle zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, a to zejména v důsledku provádění výzkumu a vývoje nebo osvětové činnosti v oblasti kybernetické bezpečnosti, mohou si Smluvní strany formou Prováděcího protokolu dohodnout podmínky poskytnutí práva k užívání takového díla.

Čl. VIII.
Mlčenlivost

1. Smluvní strany jsou povinny zachovávat mlčenlivost o
   a) informacích v případech stanovených platnými právními předpisy a dalšími národními a mezinárodními standardy zejména z oblasti kybernetické bezpečnosti (např. Traffic Light Protocol – TLP),
   b) údajích o kybernetických bezpečnostních incidentech evidovaných v souladu se ZKB s výjimkou takových údajů, které mají být v souladu s touto Smlouvu nebo ZKB zveřejněny, a
   c) informacích, o kterých se dozvěděly při uzavírání této Smlouvy nebo za doby jejího trvání při výkonu práv a povinností z ní vyplývajících, jimiž se rozumí veškeré informace v ústní nebo v písemné formě, jakož i know-how, za které se považují veškeré poznatky obchodní, výrobní, bezpečnostní, technické či ekonomické povahy včetně software a dokumentace, související s činností Smluvní strany, které mají skutečnou nebo alespoň potenciální hodnotu a které nejsou běžně dostupné, přičemž příslušná Smluvní strana projevila vůli, aby se na tyto informace vztahovala povinnost mlčenlivosti, nebo lze tento projev vůle vzhledem k jejich povaze oprávněně předpokládat.
2. Smluvní strany se zavazují, že nesdělí informace podle tohoto článku třetí osobě a přijmou taková opatření, která znemožní jejich zpřístupnění třetím osobám. Ustanovení předchozí věty se nevztahuje na případy, kdy
   a) mají Smluvní strany povinnost poskytnout informace stanovenou zákonem,

b) Smluvní strany na základě této Smlouvy poskytují informace třetím subjektům nebo je zveřejňují,

c) se takové informace stanou veřejně známými či dostupnými jinak než porušením povinností Smluvní strany; nebo

d) druhá Smluvní strana dá ke zpřístupnění konkrétní informace souhlas.

3. Získá-li v souvislosti s výkonem práv a povinností vyplývajících z této Smlouvy kterákoli ze Smluvních stran přístup k osobním údajům ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, je tato Smluvní strana povinna zajistit nakládání s těmito údaji v souladu s tímto zákonem a je odpovědná za újmu vzniklou druhé Smluvní straně nebo třetím osobám v případě porušení této povinnosti.
4. Povinnosti podle odstavce 1 až 3 trvají i po skončení platnosti Smlouvy.
5. Smluvní strany se dohodly, že informace o uzavření této Smlouvy, jakož i obsah této Smlouvy s výjimkou Prováděcích protokolů, které budou obsahovat utajované informace nebo budou označeny jako neveřejné, nepodléhají povinnosti mlčenlivosti a Smluvní strany jsou oprávněny je uveřejnit, a to i způsobem umožňujícím dálkový přístup.
6. Smluvní strany se dohodly, že informace týkající se činnosti Národního CERT podle této Smlouvy a ZKB bude na základě právních předpisů o svobodném přístupu k informacím poskytovat NBÚ. CZ.NIC je povinen poskytnout k tomu NBÚ potřebnou součinnost.

Čl. IX.
Doba trvání Smlouvy a její ukončení

1. Smlouva nabývá v souladu s § 164 odst. 2 správního řádu platnosti a účinnosti okamžikem připojení podpisu poslední Smluvní strany, jsou-li Smluvní strany přítomny současně. Nejsou-li Smluvní strany přítomny současně, je Smlouva uzavřena okamžikem, kdy její návrh opatřený podpisy ostatních osob, jimž byl určen, dojde navrhovateli Smlouvy.
2. Smlouva se uzavírá na dobu neurčitou.
3. Smlouva může být ukončena

   a) písemnou dohodou Smluvních stran;

   b) písemnou výpovědí kterékoli ze Smluvních stran, a to i bez udání důvodu. Výpovědní lhůta je 6 měsíců a počíná běžet od prvního dne měsíce následujícího po měsíci, ve kterém byla výpověď doručena druhé Smluvní straně;

   c) odstoupením od Smlouvy v případě, kdy druhá Smluvní strana poruší Smlouvu podstatným způsobem a k odstranění porušení nedojde v přiměřené době poskytnuté druhou Smluvní stranou. Odstoupení od Smlouvy musí být písemné, jinak je neplatné; odstoupení od Smlouvy nabývá účinnosti okamžikem jeho doručení druhé Smluvní straně. Za podstatné porušení Smlouvy se považuje zejména:

      i. porušení povinnosti mlčenlivosti stanovené v čl. VIII Smlouvy, a to zejména formou neoprávněného zveřejnění informací, jejich zneužitím pro komerční či jiné účely nebo nedostatečným zajištěním jejich ochrany, které způsobí nebo může způsobit rozsáhlý únik informací,

ii. nedodržení potřebné organizační a institucionální kapacity, finanční stability a technického a technologického zajištění plnění předmětu Smlouvy ze strany CZ.NIC,

iii. nedodržení dalších předpokladů pro provozování Národního CERT stanovených v § 18 odst. 2 ZKB ze strany CZ.NIC,

iv. porušení povinnosti provozovat Národní CERT nestranně,

v. porušení povinnosti stanovené v čl. II odst. 7 Smlouvy,

vi. opakované nepřizvání k účasti nebo opakovaná neúčast CZ.NIC na jednání Rady pro kybernetickou bezpečnost nebo zasedání pracovních orgánů zřizovaných NBÚ při řešení závažných kybernetických bezpečnostních incidentů, které mohou mít významný bezpečnostní dopad na kybernetickou bezpečnost České republiky,

vii. neposkytnutí informací o závěrech jednání, která mohou mít významný dopad na činnost druhé Smluvní strany v případě, že nebyla na tato jednání přizvána.

d) písemným návrhem kterékoli ze Smluvních stran na zrušení Smlouvy ve smyslu § 167 odst. 1 správního řádu. Pokud s návrhem druhá Smluvní strana vysloví souhlas, zaniká Smlouva dnem, kdy tento písemný souhlas dojde Smluvní straně, která návrh podala. Pokud druhá Smluvní strana se zrušením Smlouvy nesouhlasí, může o zrušení Smlouvy na žádost Smluvní strany, která podala návrh, rozhodnout správní orgán příslušný podle § 169 odst. 1 správního řádu. Smluvní strana může podat návrh na zrušení Smlouvy:

i. změní-li se podstatně poměry, které byly rozhodující pro stanovení obsahu Smlouvy, a plnění Smlouvy nelze na Smluvní straně z tohoto důvodu spravedlivě požadovat,

ii. jestliže se Smlouva dostala do rozporu s právními předpisy,

iii. z důvodu ochrany veřejného zájmu, nebo

iv. jestliže vyšly najevo skutečnosti, které existovaly v době uzavírání Smlouvy a nebyly Smluvní straně bez jejího zavinění známy, pokud tato Smluvní strana prokáže, že by s jejich znalostí Smlouvu neuzavřela.

4. Ke dni ukončení Smlouvy je CZ.NIC povinen předat NBÚ písemně (tj. v elektronické strojově čitelné podobě) veškeré kontaktní údaje, evidence hlášení kybernetických bezpečnostních událostí a incidentů a výsledky další činnosti a Spolupráce vzniklé nebo získané v souvislosti provozováním Národního CERT.

Čl. X.
Závěrečná ustanovení

1. Právní vztahy Smlouvou výslovně neupravené a z ní vyplývající nebo s ní související se řídí příslušnými ustanoveními zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, a přiměřeně ustanoveními zákona č. 89/2012 Sb., občanského zákoníku.

2. Vyžaduje-li Smlouva u některého úkonu Smluvní strany písemnou formu, oznámení takového úkonu musí být druhé Smluvní straně doručeno prostřednictvím ISDS, umožní-li to povaha datových schránek Smluvních stran, nebo doporučeně poštou, doručovací

službou či osobně proti podpisu na adresu jejího sídla uvedenou v záhlaví Smlouvy. Odmítne-li Smluvní strana převzít oznámení o úkonu druhé Smluvní strany, považuje se oznámení za doručené dnem odmítnutí. V případě, že je oznámení o úkonu zasláno poštou, považuje se za den doručení třetí den po podání oznámení k poštovní přepravě.

3. Jakékoli změny či doplňky Smlouvy je možné platně učinit pouze formou písemných a vzestupně číslovaných dodatků, podepsaných oprávněnými zástupci obou Smluvních stran. Prováděcí protokoly mohou být měněny pouze písemně.

4. V případě jakýchkoli neshod nebo rozporů mezi Smluvními stranami se tyto zavazují vynaložit veškeré úsilí k jejich smírnému řešení.

5. Stane-li se některé ustanovení Smlouvy neplatným či neúčinným v důsledku změny právní úpravy, nedotýká se tato neplatnost či neúčinnost ostatních ustanovení Smlouvy. Smluvní strany se v tomto případě zavazují vyvinout maximální možné úsilí k uzavření dodatku ke Smlouvě, jímž nahradí toto neplatné či neúčinné ustanovení ustanovením novým, které bude svým obsahem nejvíce odpovídat původní vůli Smluvních stran a bude v souladu s platnými právními předpisy. Do doby uzavření dodatku se vztah Smluvních stran bude v této záležitosti řídit obecně závaznými právními předpisy.

6. Smlouva se pořizuje ve čtyřech (4) vyhotoveních s platností originálu, z nichž obě Smluvní strany obdrží po podpisu každá dvě vyhotovení. Smlouva zároveň bude v souladu s § 19 odst. 3 ZKB zveřejněna ve Věstníku NBÚ.

7. Smluvní strany prohlašují, že Smlouva byla sepsána na základě jejich pravé a svobodné vůle, že si ji před jejím podpisem přečetly a s celým jejím obsahem souhlasí, což stvrzují vlastnoručními podpisy.

8. Nedílnou součástí Smlouvy jsou tyto přílohy:

   Příloha č. 1 Smlouvy – Žádost o uzavření veřejnosprávní smlouvy za účelem spolupráce v oblasti kybernetické bezpečnosti a zajištění provozu národního bezpečnostního týmu

   Příloha č. 2 Smlouvy – Plná moc ze dne 22.5. 2015

V Praze dne 18.12.2015

Národní bezpečnostní úřad:

.....

V Praze dne 18.12.2015

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

.....

Příloha č. 1 k čj. 9625/2015-NBÚ/41

Žádost o uzavření veřejnosprávní smlouvy

za účelem spolupráce v oblasti kybernetické bezpečnosti a zajištění provozu národního bezpečnostního týmu

CZ.NIC, z. s. p. o.
Milešovská 1136/5
130 00 Praha 3

CZ.NIC

CSIRT.CZ
powered by CZ.NIC

Obsah

1. Identifikační údaje

Název:	CZ.NIC, z. s. p. o.
Sídlo:	Milešovská 1136/5 130 00 Praha 3
ID datové schránky:	h4axdn8
IČ:	67985726
DIČ:	CZ67985726

Sdružení je zapsáno ve spolkovém rejstříku vedeném u Městského soudu v Praze, spisová značka L 58624.

2. Organizační a institucionální kapacity

2.1. Zkušenosti s provozem bezpečnostního týmu CSIRT a koordinací činností při řešení rozsáhlejších kybernetických útoků

Sdružení CZ.NIC disponuje rozsáhlými zkušenostmi nutnými ke spolehlivému zajištění provozu národního bezpečnostního týmu typu CERT/CSIRT a jeho dalšímu rozvoji.

Na základě dohody s Ministerstvem vnitra České republiky a podpisu společného memoranda převzalo sdružení CZ.NIC **1. ledna 2011** provoz a zabezpečení národního CSIRT České republiky, který souvisel s ukončením výzkumného projektu, v jehož rámci byl CSIRT.CZ v minulosti provozován. V souvislosti s převodem kompetencí v oblasti kybernetické bezpečnosti z Ministerstva vnitra ČR na Národní bezpečnostní úřad bylo od 1. dubna 2012 zmíněné memorandum nahrazeno obdobným dokumentem uzavřeným mezi sdružením CZ.NIC a **Národním bezpečnostním úřadem**. Na základě tohoto memoranda sdružení CZ.NIC zabezpečuje provoz národního CSIRT České republiky v současné době.

CZ.NIC chrání důvěrnost aktiv proti neautorizovanému vyzrazení. Sdružení implementuje bezpečnostní politiku informací konzistentně, plánovitě a ekonomicky efektivně. V roce 2013 získal správce české národní domény mezinárodně uznávanou **certifikaci systému managementu bezpečnosti informací (ISMS)**, podle normy **ISO 27001**.

Kromě zkušeností z více než čtyřletého provozu národního bezpečnostního týmu CSIRT.CZ má sdružení CZ.NIC zkušenost též s provozem vlastního interního bezpečnostního týmu CZ.NIC-CSIRT. Ten je evidován u úřadu Trusted Introducer od října 2008 a od srpna 2010 patří mezi akreditované týmy. Za dobu své existence řešil CZ.NIC-CSIRT řadu bezpečnostních incidentů jak v příslušném autonomním systému, tak také v doméně .CZ. Nejrozsáhlejším incidentem řešeným CZ.NIC-CSIRT v rámci domény .CZ pak byl incident z února 2010, kdy ve dnech 1.- 8. února 2010 rozhodlo sdružení CZ.NIC na základě doporučení CZ.NIC-CSIRT o zablokování 150 doménových jmen, které se staly součástí útoku na IRS (úřad pro správu daní při ministerstvu financí USA).

2.1.1. Typová schémata řešení kybernetických bezpečnostních incidentů

Národní bezpečnostní tým CSIRT.CZ má na základě svých zkušeností i mezinárodních best-practice vypracována typová schémata řešení nejběžnějších kybernetických bezpečnostních incidentů. Tato schémata řešení, dle kterých národní bezpečnostní tým postupuje, jsou k dispozici pro řešení DDoS útoků, phishingu, malwaru a dále pro obecné řešení. Typová schémata řešení těchto incidentů jsou v příloze této žádosti.

2.1.2. Zkušenosti s koordinací činností při řešení rozsáhlejších kybernetických útoků

Národní bezpečnostní tým CSIRT.CZ má dlouhodobé zkušenosti s koordinací při řešení rozsáhlejších kybernetických útoků. Jedním z předpokladů pro koordinaci takovýchto incidentů je vybudování vzájemné důvěry a udržování vysokého stupně znalostních kapacit.

Za účelem koordinace řešení rozsáhlých kybernetických útoků podporuje Národní bezpečnostní tým CSIRT.CZ **ustanovení týmů typu CERT/CSIRT** u významných subjektů české internetové scény, především poskytovatelů připojení a internetového obsahu (ISP). Díky úsilí CSIRT.CZ bylo jen v loňském roce v České republice ustanoveno a úřadem Trusted Introducer statusem *listed* nebo accredited označeno minimálně 8 týmů. Významnou motivací pro tyto týmy, resp. jejich zřizovatele, představovala možnost zapojení do **projektu FENIX**, který vznikl jako reakce na intenzivní DoS útoky, kterým v březnu 2013 čelila významná česká média, banky a operátoři. Smyslem projektu je umožnit v případě DoS útoku dostupnost internetových služeb v rámci subjektů zapojených do této aktivity. Významnou roli při koordinaci kybernetických útoků představuje též **Pracovní skupina CSIRT.CZ**, jejíž zasedání se pravidelně zúčastní přibližně 60 zástupců ze soukromé, veřejné i akademické půdy a na jednom místě diskutují aktuální témata kybernetické bezpečnosti včetně otázek, jak zvýšit svoji odolnost a připravenost proti těmto incidentům.

Klíčovou součástí schopnosti reakce na rozsáhlé bezpečnostní incidenty dotýkající se České republiky je udržování úzké spolupráce mezi oběma vrcholovými týmy. V tomto směru udržuje CSIRT.CZ úzkou spolupráci s vládním bezpečnostním týmem GovCERT.CZ na mnoha úrovních.

Pro koordinaci řešení rozsáhlých kybernetických útoků dále CSIRT.CZ udržuje spolupráci též s akademickým sektorem, s policií ČR, s Českou bankovní asociací, či s komunitou bezpečnostních týmů v ČR, kdy pro členy bezpečnostních týmů typu CSIRT provozuje společný komunikační kanál pro on-line diskutování aktuálních bezpečnostních událostí. Kromě toho spravuje CSIRT.CZ několik e-mailových konferencí, které jsou připraveny a udržovány pro případ potřeby řešení rozsáhlých kybernetických útoků. Níže je uvedeno několik příkladů, které ilustrují schopnost bezpečnostního týmu CSIRT.CZ pružně reagovat na rozsáhlejší bezpečnostní incidenty se závažným dopadem, ohrožující větší množství uživatelů, či zahrnující velké množství cílů.

V **květnu 2014** se v České republice objevila série útoků na routery domácích uživatelů, při jejichž řešení sehrál CSIRT.CZ klíčovou roli. Jeden z napadených routerů byl podroben analýze, která umožnila odhalit způsob napadení a navzdory již neexistující podpoře ze strany výrobce nalezl CSIRT.CZ způsob jakým se uživatelé těchto zařízení mohou chránit. CSIRT.CZ využil všech možností k informování veřejnosti prostřednictvím médií. Dále byl vytvořen portál www.rom-0.cz, na kterém si mohou uživatelé svá zařízení otestovat a zjistit tak, zda jsou zranitelná. V rámci koordinace obrany byla také navázána spolupráce s bankovním sektorem a bankám, které projevily zájem, byl poskytnut seznam IP adres, na kterých byla zranitelnost detekována. Banky pak zahrnuly tento seznam do svých detekčních mechanismů, případně rovnou informovali své klienty o možném riziku.

V **dubnu 2014** se v ČR poprvé objevil velmi nebezpečný spam, který se vydával za informaci o neuhrazené pohledávce. Tým CSIRT.CZ byl prvním, kdo na tento nebezpečný spam upozornil a kdo udělal prvotní analýzu přiloženého malware. Díky tomu došlo k varování široké veřejnosti prostřednictvím médií a pravděpodobně se tak podařilo předejít větším škodám. Účinnost použité metody byla totiž v této první vlně velmi vysoká, a to především díky zastrašování uživatelů údajným dluhem.

V březnu **2013** sehrál Národní bezpečnostní tým CSIRT.CZ klíčovou roli při koordinaci, řešení a analýze **DDoS útoků**, které zasáhly webové stránky významných českých médií, bank a telekomunikačních operátorů nebo portál Seznam.cz. Na základě zkušeností s těmito útoky byla spuštěna služba umožňující otestovat danou infrastrukturu na odolnost vůči DoS/DDoS útokům. Nabízené testy zahrnují UDP flood, slowloris, ICMP flood a SYN flood. Cílem služby, které v reakci na útoky a roli Národního bezpečnostního týmu CSIRT.CZ využily společnosti jako např. GTS Czech či ČD Telematika je otestovat chování testované infrastruktury v případě reálného útoku a včas tak odhalit případná slabá místa.

V oblasti zkušeností s koordinací řešení rozsáhlejších kybernetických bezpečnostních incidentů je důležité též zmínit roli CSIRT.CZ při **útocích skupiny Anonymous** v roce **2012**, při kterých se členové CSIRT.CZ aktivně podíleli na preventivní ochraně cílů před útoky této skupiny a také na analýzách touto skupinou používaných nástrojů. Výsledky této analýzy pomáhaly společně se schopností CSIRT.CZ včas varovat správce před chystanými útoky, snížit dopady útoků této skupiny.

2.1.3. Členství v nadnárodních organizacích působících v oblasti kybernetické bezpečnosti

Sdružení CZ.NIC, resp. bezpečnostní tým CSIRT.CZ, a jeho zaměstnanci jsou členy následujících nadnárodní organizací působících v oblasti kybernetické bezpečnosti. Organizace jsou řazeny v abecedním pořadí.

- APWG (Anti-Phishing Working Group) - globální koalice soukromých společností, státních institucí a bezpečnostních složek zaměřená na celosvětový boj s kybernetickým zločinem, především phishingem.
- CECSP (Central European Cyber Security Platform) - společná iniciativa České republiky, Slovenska, Polska, Maďarska a Rakouska, jejímž cílem je sdílení informací, osvědčených postupů a know-how v oblasti kybernetických hrozeb a potencionálních útoků. Platforma podporuje koordinaci činnosti týmů, společné vzdělávaní a cvičení. Státy by přes platformu měly rovněž hledat společné pozice na mezinárodní otázky. Pravidelná setkání slouží k budování důvěry mezi týmy a sdílení informací.
- DNSSEC Industry Coalition - organizace, která se stará o prosazování bezpečnostní technologie DNSSEC na mezinárodní úrovni. Úkolem této organizace je jednotný postup při prosazování a zavádění DNSSEC u všech potenciálních uživatelů, mezi kterými nemohou chybět ani doménové registry národních i generických TLD.

- DNS-OARC (The Domain Name System Operations, Analysis and Research Center) - důvěryhodná platforma, na které se setkávají klíčové subjekty a sdílejí své zkušenosti z DNS provozu, analýz a výzkumu tak, aby mohly co nejlépe a nejúčinněji koordinovat svoji činnost, především v oblasti bezpečnosti. Od roku 2010 organizaci předsedá Ondřej Filip, výkonný ředitel sdružení CZ.NIC, který byl v roce 2014 zvolen do svého již třetího funkčního období.

- ICANN (Internet Corporation for Assigned Names and Numbers) - mezinárodní nezisková organizace založená v roce 1998, jejímž hlavním úkolem je nejen správa a přidělování generických doménových jmen nejvyšší úrovně (gTLD) a národních doménových jmen nejvyšší úrovně (ccTLD), ale také IP adres. Sdružení CZ.NIC jako správce národní domény vysílá své zástupce na pravidelná jednání a jeho odborníci se aktivně zapojují do činnosti pracovních skupin. Ondřej Filip, výkonný ředitel sdružení CZ.NIC, například působí jako člen prestižního Poradního výboru pro bezpečnost a stabilitu (SSAC). V březnu 2015 se Ondřej Surý, vedoucí výzkumného a vývojového oddělení CZ.NIC, stal v rámci ICANN členem týmu, který připraví plán na změnu kořenového klíče používaného pro zabezpečení internetových domén pomocí technologie DNSSEC.

- Trusted Introducer - jedná se o jednu z aktivit organizace TERENA sdružující CSIRT týmy v rámci Evropy; představuje důvěryhodné centrum pro výměnu citlivých informací a know-how mezi jednotlivými CSIRT týmy. **CZ.NIC** je členem a patří mezi **akreditované CSIRT týmy,** což představuje vyšší stupeň důvěryhodnosti v rámci komunity oproti běžnému členství.

Aktuálně probíhá proces přijetí týmu CSIRT.CZ do mezinárodní organizace bezpečnostních týmů FIRST (Forum of Incident Response and Security Teams).

Vedle výše uvedených institucí sdružení CZ.NIC koordinuje též evropský projekt zaměřený na posílení spolupráce v oblasti kybernetické bezpečnosti.

- CS Danube (Cyber Security in Danube Region) - cílem projektu CS Danube zahájeného v dubnu 2015 je především posílit důvěru a spolupráci mezi bezpečnostními týmy CERT/CSIRT, sdílet jejich know-how a nástroje. Nedílnou součást projektu představuje posílení kapacit v podobě školení zaměřeného na zabezpečení webových stránek. Na realizaci projektu podpořeného z programu START Strategie EU pro Podunají se vedle sdružení CZ.NIC, resp. bezpečnostního týmu CSIRT.CZ, dále podílejí také partneři z Rakouska, Slovenska, Chorvatska, Srbska a Moldavska.

2.1.4. Účast na kybernetických cvičeních

Neocenitelné zkušenosti s koordinací činností při řešení rozsáhlejších kybernetických útoků a jejich řešení získává tým CSIRT.CZ v rámci pravidelných kybernetických cvičení. V roce 2014 se národní bezpečnostní tým CSIRT.CZ zúčastnil následujících cvičení:

- **Cyber Europe 2014** - za Českou republiku jsme se zhostili role národního koordinátora při přípravě zatím největšího evropského kybernetického cvičení, které zastřešovala Evropská agentura pro

síťovou a informační bezpečnost (ENISA) – Cyber Europe 2014. Vzhledem ke komplexnosti navržených technických a operačních úloh se cvičení odehrálo ve třech fázích, přičemž do první technické fáze, která trvala dva dny, jsme kromě týmu CSIRT.CZ zapojili dalších sedm subjektů z České republiky (vládní CERT tým GovCERT.CZ, sdružení CESNET, české peeringové centrum NIX.CZ, společnost Unicorn, bezpečnostní tým Masarykovy univerzity CSIRTMU, registrátor Active24 a Policejní akademie v Praze). Do operační fáze (OLEx) cvičení jsme zapojili ještě v té době čerstvě konstituovaný CSIRT tým společnosti Casablanca.

- **Cvičení CECSP** - v rámci vytvořené platformy CECSP pro spolupráci států Visegrádské čtyřky a Rakouska jsme se podíleli na přípravě společného cvičení, které odstartovalo další spolupráci vrcholových CSIRT/CERT týmů střední Evropy v oblasti řešení incidentů a budování spolupráce. Cvičení se kromě týmu CSIRT.CZ zúčastnili další zástupci přibližně 11 vrcholových bezpečnostních týmů ze zemí V4 a Rakouska. Vedle operačních úkolů jsme v průběhu cvičení řešili také právní otázky v rámci legislativy jednotlivých zapojených států.

- **Cvičení NATO CC2014** – v pozici hráče jsme se zúčastnili prestižního cvičení NATO Cyber Coalition 2014, které připravila Severoatlantická aliance (NATO). V rámci cvičení se členové CSIRT.CZ podíleli na vysoce technických úkolech – analýze základní desky a jejího programového vybavení (BIOS apod.). Při tomto cvičení jsme úzce spolupracovali s bezpečnostními experty z Národního centra kybernetické bezpečnosti.

- **Národní cvičení** - posledním cvičením, kterého jsme se v roce 2014 zúčastnili, bylo národní cvičení, které uspořádal Národní bezpečnostní úřad. Cvičení bylo určeno pro správce sítí ze státní správy, přičemž cvičení se v roli odborné poroty zúčastnili také odborníci na legislativu, členové etablovaných bezpečnostních týmů (včetně zástupce CSIRT.CZ), bezpečnostních složek, úřadů státní správy atd. Hráči, správci sítí ze státní správy, řešili v průběhu dne dva zajímavé bezpečnostní problémy, kde jeden měl charakter záplavového útoku na infrastrukturu a druhý ohrožoval koncového uživatele. Hráči si s oběma úkoly poradili velice dobře a celé cvičení se neslo v duchu živé diskuse a výměny názorů a informací.

2.2. Personální a znalostní kapacity

Na základě zkušeností s provozem a rozvojem národního bezpečnostního týmu CSIRT.CZ, který sdružení CZ.NIC zajišťuje od 1. ledna 2011, působí v rámci organizace níže ustálený tým národního bezpečnostního týmu CSIRT.CZ o devíti členech, z nichž každý disponuje unikátními znalostmi a dovednostmi v oblasti kybernetické bezpečnosti.

- Ing. Martin Peterka - vedoucí bezpečnostního týmu CSIRT.CZ a současně interního bezpečnostního týmu sdružení CZ.NIC - CZ.NIC-CSIRT. Martin Peterka vystudoval obor Automatizované systémy řízení na strojní fakultě VUT Košice. Poté pracoval na vývoji informačního systému řízení výroby ve společnosti VSŽ Informatika, kde se mimo jiné podílel na zavádění certifikátu kvality ISO 9000. V

letech 1999 až 2003 řídil projekt správy domény CZ ve společnosti KPNQwest Czechia, která pro sdružení CZ.NIC zajišťovala provoz domény CZ. Jako provozní ředitel sdružení CZ.NIC se dále stará o bezchybný provoz registru doménových jmen CZ, dohlíží na práci operátorů zákaznické podpory a pomáhá řešit závažné problémy držitelů domén. Martin Peterka se také zúčastnil speciálního kurzu pro členy CSIRT týmů organizovaného organizací TERENA – Transits I.

- Pavel Bašta - bezpečnostní analytik senior. Pavel začínal jako správce sítě v malé personální společnosti, z níž se přesunul do společnosti Český Telecom, respektive Internet OnLine, kde se věnoval technické podpoře. V rámci společnosti Telefónica poté působil v dohledovém centru datových okruhů, v němž se detailněji seznámil s konfiguracemi Cisco routerů. Do náplně jeho práce patřilo i řešení problémů zákazníků s mailovými, webhostingovými a doménovými službami, včetně problémů týkajících se bezpečnosti zákaznických služeb. Poslední roky zastával pozici administrátora informačních systémů - staral se o správné fungování serverů Telefóniky i jejích zákazníků běžící na platformě MS Windows. Pavel Bašta je **držitelem certifikací** Microsoft Certified Systems Engineer, Microsoft Certified Technology Specialist, Certified Ethical Hacker a Computer Hacking Forensic Investigator. Pavel Bašta rovněž absolvoval speciální kurzy pro členy CSIRT týmů organizované organizací TERENA - Transits I a Transits II.

- Mgr. Zuzana Duračinská – specialistka počítačové bezpečnosti. Zuzana Duračinská absolvovala v CZ.NIC v roce 2012 odbornou stáž, která se v lednu 2013 změnila v práci na plný úvazek. V červnu 2013 doplnila Zuzana týmy CZ.NIC-CSIRT a CSIRT.CZ. K její hlavním činnostem patří příprava a realizace kybernetických cvičení, příprava odborných článků a reprezentace týmů nebo provoz služby Skener webu. Mezi další činnosti patří rozvíjení národní a mezinárodní spolupráce s členy bezpečnostní komunity. Zuzana Duračinská je **držitelkou certifikace** Certified Ethical Hacker. Zuzana Duračinská se také zúčastnila speciálního kurzu pro členy CSIRT týmů organizovaného organizací TERENA – Transits I.

- Ing. Katarína Ďurechová – **analytička počítačové bezpečnosti.** Katarína Ďurechová se správě serverů věnovala již při studiích na vysoké škole v Bratislavě. Ve stejné době se začala zajímat také o penetrační testování a programování v Perlu. Ve sdružení CZ.NIC pracuje od května 2013. Nejdříve zde působila jako programátorka pro výzkum a vývoj (Laboratoře CZ.NIC), kde se zabývala hlavně provozováním honeypotů. Od února 2015 rozšířila tým CSIRT.CZ, kde se nadále věnuje honeypotům a podílí se na penetračních testech v rámci služby Skener webu.

- Ing. Jaroslav Kodet – analytik počítačové bezpečnosti. Jaroslav Kodet začínal jako programátor-analytik pro bytové družstvo Ocelář, pak vystřídal několik pozic v bankovním a průmyslovém IT, a to na pozicích od pobočkového administrátora přes centrálového programátora až po projektového manažera rozsáhlého IT projektu v oblasti bankovnictví (měnový dealing). Ve společnosti Nextel s.r.o, následně integrované do s. p. t. Telecom, působil v útvaru zodpovědném

za provoz a dohled datových okruhů a přístupové sítě. Po akvizici Telecomu společností Telefónica působil v útvaru zajišťujícím provoz a podporu interních koncových uživatelů korporátní sítě, následně se zabýval rozvojem a zajištěním rutinního provozu internetových služeb. V neposlední řadě řešil problémy zákazníků týkající se počítačové bezpečnosti, zejména útoky na hostované služby.

- Andrea Kropáčová - je jedním ze zakládajících členů týmu CSIRT.CZ. Andrea Kropáčová začínala jako správce sítí, síťových služeb a příležitostný programátor ve sdružení CESNET, odkud byl už jen krok k oblasti bezpečnosti sítí a služeb a následně k problematice CERT/CSIRT týmů. V roce 2004 sestavila první světovou komunitou oficiálně uznaný tým typu CSIRT v České republice - tým CESNET-CERTS. Zkušenosti z vybudování tohoto akademického týmu uplatnila v letech 2007 až 2010 při budování pracoviště CSIRT.CZ a po jeho přerod v Národní CSIRT České republiky zůstala v roli reprezentanta. Jejím úkolem je reprezentovat tým v mezinárodní infrastruktuře CERT/CSIRT týmů, národní i mezinárodní spolupráce, komunikace a strategický rozvoj týmu, jeho role a služeb.

- Bc. Bc. Edvard Rejthar, Bsc (Hons) – **bezpečnostní analytik a programátor.** Edvard Rejthar má v týmu CSIRT.CZ a CZ.NIC-CSIRT na starosti především analýzu škodlivého kódu na webových stránkách v české doméně, rozvoj systémů na automatické zpracovaní dat a analýzy pro projekt Turris. Edvard Rejthar získal bakalářský titul z aplikované informatiky na Fakultě informačních studií Vysoké školy ekonomické (VŠE) a též bakalářský titul v oboru Web a multimédia na Fakultě elektrotechniky Českého vysokého učení technického (ČVÚT). Část studia strávil na Coventry University ve Velké Británii, kde se zabýval softwarovým inženýrstvím a získal titul bakalář počítačových věd - Bachelor of Computer Science (Bcs.). V minulosti pracoval jako správce mobilního obsahu a webdesigner na volné noze. Edvard Rejthar mluví plynně francouzsky a anglicky.

- Michal Prokop – bezpečnostní analytik a operátor provozu. Michal Prokop se podílí na provozování interního bezpečnostního týmu CZ.NIC-CSIRT a národního CSIRT týmu ČR. Absolvoval Vyšší odbornou školu Institut informatiky a při studiu na České zemědělské univerzitě, kde studoval systémové inženýrství a informatiku, pracoval ve společnosti Global Payments Europe, s.r.o. jako tester. Do sdružení CZ.NIC přišel v roce 2008. Michal Prokop je **držitelem certifikací** Certified Ethical Hacker a Computer Hacking Forensic Investigator. Michal též absolvoval speciální kurzy pro členy CSIRT týmů organizované organizací TERENA - Transits I. a Transits II.

- Mgr. Robert Šefr – bezpečnostní analytik. Robert Šefr má v rámci národního bezpečnostního týmu CSIRT.CZ za úkol přípravu systémů pro automatizaci vyhledávání a zpracování incidentů v ČR a analýzu dat z projektu Turris. Svoje znalosti čerpal hlavně při studiu na Fakultě informatiky Masarykovy univerzity v Brně, kde se na bezpečnost zaměřoval a po obhajobě diplomové práce na téma „Reverzní inženýrství" získal titul magistr v oboru aplikovaná informatika. Praktické

zkušenosti v oblasti kybernetické bezpečnosti nabyl Robert Šefr jako bezpečnostní konzultant ve společnosti Comguard.

Vedle výše uvedených členů bezpečnostního týmu se na činnosti národního bezpečnostního týmu CSIRT.CZ podílejí a budou podílet i další útvary, které svoji kapacitou mohou prakticky okamžitě posílit národní bezpečnostní tým při řešení specifických úkolů nebo ad-hoc záležitostí jako jsou např. rozsáhlé kybernetické incidenty. Mezi klíčové útvary sdružení spolupracující v národním bezpečnostním týmem CSIRT.CZ patří zejména:

- Laboratoře CZ.NIC - laboratoře CZ.NIC představují organizačně oddělené výzkumné a vývojové pracoviště, které se zabývá zkoumáním v oblasti Internetu se zaměřením na internetové protokoly, analýzy síťového provozu, aktivním i pasivním monitoringem či návrhy prototypů pro další vývoj v rámci sdružení CZ.NIC. Práce Laboratoří se zaměřují jak na lokální, tak i zahraniční internetové komunity, se kterými úzce spolupracují zejména při výzkumu v oblasti kybernetické bezpečnosti a nových technologií a jejich nasazení do praxe. V laboratořích CZ.NIC pracuje celkem 34 zaměstnanců (29 dle přepočtených úvazků), z nichž většina může posílit národní bezpečnostní tým CSIRT.CZ.

  Mezi nejvýznamnější projekty laboratoří CZ.NIC patří bezpečnostní projekt Turris, jehož cílem je analýza bezpečnostní situace v sítích koncových uživatelů a výzkum v oblasti ochrany proti kybernetickým útokům. V rámci projektu získávají vybraní dobrovolníci bezpečnostní sondu v podobě routeru Turris, který kromě funkcí běžného domácího směrovače dokáže analyzovat provoz mezi Internetem a domácí sítí a identifikovat podezřelé datové toky. Při jejich odhalení upozorní na možný útok centrálu Turris, která porovnává data z ostatních připojených routerů a vyhodnocuje nebezpečnost detekovaného provozu. V případě útoku centrála vytvoří a distribuuje aktualizaci do celé sítě, a začne tak chránit všechny uživatele zařízení Turris.

- Dohledové centrum a zákaznická podpora – dohledový tým zajišťující též tzv. zákaznickou podporu monitoruje v režimu 24/7 klíčové funkce nezbytné pro hladký a bezpečný provoz infrastruktury spojené se zajištěním provozu české národní domény .cz. Dohledové centrum také přijímá hlášení pro CSIRT.CZ a provádí jejich třídění. Reálné incidenty jsou pak předávány týmu CSIRT.CZ k dořešení.

- Tým projektů EU – poskytuje podporu při zapojování bezpečnostního týmu CSIRT.CZ do mezinárodních projektů a jejich předkládání. Ve vztahu ke kybernetické bezpečnosti se jedná především o projekt CS Danube (viz. výše). Další podpora národního bezpečnostního týmu CSIRT.CZ směruje do analýz evropské legislativy a dopadů regulatorního rámce na subjekty v České republice, kdy mezi nejaktuálnější otázky patří Směrnice o síťové a informační bezpečnosti (NIS). Tým projektů EU poskytoval v této otázce též podporu zástupcům ČR na pracovní skupině Rady Evropské unie pro telekomunikace a informační společnost (H.05).

- Právní/sekretariát – součinnost právního oddělení je vyžadována především při zpracování právních analýz spojených se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a jeho dopadů na fungování národního bezpečnostního týmu CSIRT.CZ a na subjekty podnikající v oblasti elektronických komunikací. Právní oddělení se též významně podílí na analýzách právního rámce pro bezpečnostní výzkum, např. skenování zranitelností.

Všechny výše uvedené aktivity jsou pak organizačně i odborně zastřešeny Mgr. Ondřejem Filipem, výkonným ředitelem sdružení CZ.NIC a jedním z předních českých i světových expertů na oblast kybernetické bezpečnosti.

2.3. Zkušenosti s provozováním dohledového centra

Sdružení CZ.NIC provozuje **od roku 2005** vlastní dohledové centrum, jehož cílem je především zajištění monitoringu nad klíčovými funkcemi nezbytnými pro hladký a bezpečný provoz infrastruktury spojené se zajištěním provozu české národní domény .cz. Dohledové centrum, fungující v nepřetržitém režimu **24/7** zajišťuje též zákaznickou podporu držitelům domén, a to zejména v situacích, kdy by mělo dojít ke zrušení doménového jména, dochází ke změně údajů kontaktu či změně držitele. Dohledové centrum také tvoří důležitý pilíř při filtrování hlášených incidentů, tak aby byly předávány relevantní incidenty správnému řešitelskému týmu, tedy CSIRT.CZ, případně internímu týmu CZ.NIC-CSIRT.

2.4. Osvětová činnost v oblasti kybernetické bezpečnosti

2.4.1. Publikační činnost

Členové bezpečnostního týmu CSIRT.CZ i další pracovníci, podporující činnost národního bezpečnostního týmu, disponují rozsáhlou publikační činností v odborných médiích i médiích určených široké veřejnosti. Níže uváděný seznam obsahuje výběr publikační činnosti za posledních 5 let.

2015

BAŠTA, Pavel. *Postřehy z bezpečnosti: Logjam – nový útok proti TLS* . Root.cz [online] 2015. Dostupné na:http://www.root.cz/clanky/postrehy-z-bezpecnosti-logjam-novy-utok-proti-tls/

BAŠTA, Pavel. *Postřehy z bezpečnosti: Rombertika mast na MBR past.* Root.cz [online] 2015. Dostupné na: http://www.root.cz/clanky/postrehy-z-bezpecnosti-rombertika-mast-na-mbr-past/

BAŠTA, Pavel. *Postřehy z bezpečnosti: FBI radí, pátrá, informuje.* Root.cz [online] 2015. Dostupné na: http://www.root.cz/clanky/postrehy-z-bezpecnosti-fbi-radi-patra-informuje/

DURAČINSKÁ, Zuzana. BAŠTA, Pavel. *DDoS – sofistikovaný útok nebo služba na objednávku?* IT Systems 04/2015. Str. 2-3. Dostupné též na: https://www.nic.cz/files/nic/doc/IT_Security_DDoS_042015.pdf

BAŠTA, Pavel. *Postřeh□□be□pečnosti: persistentní XSS v pluginech pro WordPress.* Root.cz [online] 2015. Dostupné na: http://www.root.cz/clanky/postrehy-z-bezpecnosti-persistentni-xss-v-pluginech-pro-wordpress/

BAŠTA, Pavel. *Postřeh□□be□pečnosti: přenos dat s pomocí tepla.* Root.cz [online] 2015. Dostupné na: http://www.root.cz/clanky/postrehy-z-bezpecnosti-prenos-dat-s-pomoci-tepla/

DURAČINSKÁ, Zuzana. *Základní minimum □abe□pečení webových stránek.* SecurityWorld 01/2015. Str.38-39. Dostupné též na: https://www.nic.cz/files/nic/doc/SW_bezpecnost_032015_1.pdf/

BAŠTA, Pavel. *Postřeh□□be□pečnosti: Kaspersk□ popsal platformu EquationDrug.* Root.cz [online] 2015. Dostupné na: http://www.root.cz/clanky/postrehy-z-bezpecnosti-kaspersky-popsal-platformu-equationdrug/

DURAČINSKÁ, Zuzana. *Postřeh□□be□pečnosti: podvodné e-mail□ ešte nedali posledné slovo.* Root.cz [online] 2015. Dostupné na: http://www.root.cz/clanky/postrehy-z-bezpecnosti-podvodne-e-maily-este-nedali-posledne-slovo/

BAŠTA, Pavel. *Postřeh□□be□pečnosti: mnoho □ranitelností – androidova smrt.* Root.cz [online] 2015. Dostupné na: http://www.root.cz/clanky/postrehy-z-bezpecnosti-mnoho-zranitelnosti-androidova-smrt/

BAŠTA, Pavel. *Postřeh□□be□pečnosti: krocení duchů v Linuxu.* Root.cz [online] 2015. Dostupné na: http://www.root.cz/clanky/postrehy-z-bezpecnosti-kroceni-duchu-v-linuxu/

BAŠTA, Pavel. *Postřeh□□be□pečnosti: Malvertising kampaň na AdSense.* Root.cz [online] 2015. Dostupné na: http://www.root.cz/clanky/princip-amplification-utoku-zneuzivajicich-dns-ntp-a-snmp/

DURAČINSKÁ, Zuzana. BAŠTA, Pavel. *Princip amplification útoků □neužívajících DNS, NTP a SNMP.* Root.cz [online] 2015. Dostupné na: http://www.root.cz/clanky/princip-amplification-utoku-zneuzivajicich-dns-ntp-a-snmp/

BAŠTA, Pavel. *Postřeh□□be□pečnosti: Microsoft Office, Epi□oda 5 – Makra vrací úder.* Root.cz [online] 2015. Dostupné na: http://www.root.cz/clanky/postrehy-z-bezpecnosti-microsoft-office-epizoda-5-makra-vraci-uder/

2014

BAŠTA, Pavel. *Postřehy z bezpečnosti: 100 000 napadených stránek s CMS WordPress.* Root.cz [online] 2014. Dostupné na: http://www.root.cz/clanky/postrehy-z-bezpecnosti-100-000-napadenych-stranek-s-cms-wordpress/

BAŠTA, Pavel. *Postřehy z bezpečnosti: chyby PayPal umožňující převzetí cizího účtu.* Root.cz [online] 2014. Dostupné na: http://www.root.cz/clanky/postrehy-z-bezpecnosti-chyba-v-microsoft-windows-kerberos-ohrozuje-cele-pocitacove-site/

BAŠTA, Pavel. *Postřehy z bezpečnosti: chyba v Microsoft Windows Kerberos ohrožuje celé počítačové sítě.* Root.cz [online] 2014. Dostupné na: http://www.root.cz/clanky/postrehy-z-bezpecnosti-chyba-v-microsoft-windows-kerberos-ohrozuje-cele-pocitacove-site/

DURAČINSKÁ, Zuzana. *Zatočte se spamem.* SecurityWorld 04/2014. Str.38 - 39. Dostupné též na: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTcz_11212014_1.pdf

DURAČINSKÁ, Zuzana. *Jak probíhá kybernetické cvičení?* IT Systems 09/2014. Str.33. Dostupné též na: https://www.nic.cz/files/nic/doc/ITSystems_bezpecnost_092014.pdf

DURAČINSKÁ, Zuzana. *Zatočte s amplification ataky.* SecurityWorld 3/2014. Str.42-43. Dostupné též na: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTcz_09042014_1.pdf

BAŠTA, Pavel. *Atak na české routery.* Computerworld [online] 2014. Str.31. Dostupné na: https://www.nic.cz/files/nic/doc/Computerworld_routery_06062014.pdf

DURAČINSKÁ, Zuzana. *Skener webov pre mestá a obce.* Sborník konference ISSS 2014. str 30-31. Dostupné též na: https://www.isss.cz/archiv/2014/download/isss2014.pdf

KŘÍŽ, Lukáš. *Braňte se počítačovým útokům: Rozhovor s Pavlem Baštou.*. BusinessIT [online] 02/2014. Dostupné na: http://www.businessit.cz/cz/uzivatele-rady-tipy_0.php

SEDLÁK, Ján. *Jak pracuje český kyberbezpečnostní tým – rozhovor s Martinem Peterkou.* Connect.cz [online] 02/2014. Dostupné na: http://connect.zive.cz/clanky/martin-peterka-jak-pracuje-cesky-kyberbezpecnostni-tym/sc-320-a-172394

2013

DURAČINSKÁ, Zuzana. *Skener webu.* Veřejná správa. č. 13/2013. Str. 28. Dostupné též na: https://www.nic.cz/files/nic/doc/VS_Skener_webu_092013.png

PETERKA , Martin: *Bezpečnost je vždy až na prvním místě aneb Role expertních týmů roste.* Veřejná správa. č.13/2013. Str.18-19. Dostupné též na: https://www.nic.cz/files/nic/doc/Verejna_sprava_CSIRT_072013.pdf

KROPÁČOVÁ, Andrea. *Za hranice síťařského desatera.* Root.cz [online] 2013. Dostupné na: http://www.root.cz/clanky/za-hranice-sitarskeho-desatera/

KROPÁČOVÁ, Andrea. *Síťařské desatero při připojování sítě do internetu.* Root.cz [online] 2013. Dostupné na: http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

KROPÁČOVÁ, Andrea. *CERT/CSIRT týmy a jejich role.* Root.cz [online] 2013. Dostupné na: http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

BAŠTA, Pavel. *Role uživatelů při boji s kybernetickými útoky.* Root.cz [online] 2013. Dostupné na: http://www.root.cz/clanky/role-uzivatelu-pri-boji-s-kybernetickymi-utoky/

2012

BAŠTA, Pavel. *Reportáž: cvičný útok na EU na vlastní kůži.* Root.cz [online] 2012. Dostupné na: http://www.root.cz/clanky/reportaz-cvicny-utok-na-eu-na-vlastni-kuzi/

KROPÁČOVÁ, Andrea. *Cvičný útok na sítě EU očima CSIRT.CZ.* Root.cz [online] 2012. Dostupné na: http://www.root.cz/clanky/cvicny-utok-na-site-eu-ocima-csirt-cz/

2011

KOVALIK, Jan, . *ČR střeží před kyberútokem čtyři lidé na půl úvazku* - rozhovor s Andreou Kropáčovou. Aktualne.cz [online] Dostupné na: http://zpravy.aktualne.cz/ekonomika/technika/cr-strezi-pred-kyberutokem-ctyri-lide-na-pul-uvazku/r~i:article:721812/

KROPÁČOVÁ, Andrea. *Jak CSIRT.CZ došel k akreditaci.* Lupa.cz [online]. 2011. Dostupné na: http://www.lupa.cz/clanky/jak-csirt-cz-dosel-k-akreditaci/

KROPÁČOVÁ, Andrea. *Týmová práce pro zajištění bezpečnosti komunikačních sítí.* Computer. č. 05/2011. Dostupné též: https://www.nic.cz/files/nic/doc/Computer_CSIRT.CZ_052011.pdf

PETERKA, Martin. *Role a počet bezpečnostních týmů rostou. Co o nich ale víme?* Lupa.cz [online]. 2011. Dostupné na: http://www.lupa.cz/clanky/role-a-pocet-bezpecnostnich-tymu-rostou-co-o-nich-ale-vime/

2.4.2. Provozování informačních kanálů

Sdružení CZ.NIC, resp. národní bezpečnostní tým CSIRT.CZ provozuje pod názvem **„Aktuálně z bezpečnosti" (AZB)** informační kanál zaměřený především na varování před aktuálními kyber-bezpečnostními hrozbami a zranitelnostmi.

Tento kanál dostupný na internetových stránkách CSIRT.CZ - https://www.csirt.cz/news/security/ je dostupný též v angličtině. Informace z tohoto informačního zdroje je možné získávat též prostřednictvím RSS kanálu. Zprávy z AZB jsou pak často přebírány dalšími médii či využívány orgány veřejné správy (Národní centrum kybernetické bezpečnosti, Ministerstvo vnitra).

V roce 2014 bylo prostřednictvím tohoto informačního kanálu publikováno celkem 663 aktualit (tj. průměrně dvě denně) souvisejících s kybernetickou bezpečností.

Mezi další z informačních kanálů patří **blog** (http://blog.nic.cz), na kterém členové bezpečnostního týmu uveřejňují rozsáhlejší a podrobnější informace o tématech spojených s kybernetickou bezpečností jako jsou aktuální zranitelnosti a jejich dopad na český Internet nebo účast na kybernetických cvičeních.

CSIRT.CZ rovněž provozuje na svých internetových stránkách sekci **Rady a návody**, ve které publikuje návody pro uživatele i administrátory k nejrůznějším tématům počítačové bezpečnosti. V sekci tak lze najít informace k zabezpečení osobních údajů, webové stránky, či třeba informace k DoS a DDoS útokům.

2.4.3. Účast na konferencích

Zástupci Národního bezpečnostního týmu CSIRT.CZ se za účelem sledování nejnovějších poznatků i šíření zúčastní celé řady konferencí a seminářů na národní i mezinárodní úrovni.

Na **mezinárodní úrovni** se členové Národního bezpečnostního týmu zúčastnili např. následujících významných konferencí a workshopů:

- **FIRST** (Forum of Incident Response and Security Teams) – výroční konference společného fóra bezpečnostních týmů. Zástupci sdružení CZ.NIC, Andrea Kropáčová a Martin Peterka se pravidelně účastní této konference od roku 2009.

- **NatCSIRT** – pravidelné setkání národních bezpečnostních týmů, které organizuje CERT Coordination Centre CERT/CC vždy po konferenci FIRST na níž se probírají aktuální témata týkající se práce národních bezpečnostních týmů. Setkání se za sdružení CZ.NIC pravidelně od roku 2011 účastní Martin Peterka a Andrea Kropáčová.

- **TF-CSIRT** – konference pořádaná pod záštitou organizace TERENA je určená pro členy CSIRT týmů. Na této konferenci si zástupci bezpečnostních týmů vyměňují praktické poznatky z řešení incidentů a další relevantní informace. Za sdružení CZ.NIC se těchto akcí od roku 2009 vždy účastní minimálně jeden z následujících členů CSIRT.CZ - Martin Peterka, Andrea Kropáčová, Michal Prokop,

Zuzana Duračinská a Pavel Bašta . Zástupci CSIRT.CZ na akci také několikrát prezentovali vlastní poznatky a aplikace, jako například program Malicious Domain Manager, či informace o ROM-0 zranitelnosti, projektu Turris, či o projektu FENIX.

- **0ct0b3rf3st** – Konference pro členy bezpečnostní komunity, přístupná pouze na základě osobní pozvánky. Konferenci pravidelně pořádal tým CERT.EE. V červnu 2012 se akce zúčastnil Michal Prokop, v červnu 2013 Pavel Bašta s prezentací o DDoS útocích z března roku 2013 a v červnu 2014 se zúčastnil akce Michal Prokop a Pavel Bašta, který na akci prezentoval projekt Turris.

- **Brucon** - ryze technická konference zaměřená především na informace o nových způsobech útoků a na nové zranitelnosti. Konference se v září 2012 zúčastnil Pavel Bašta.

- **BlackHat** – ryze technická konference zaměřená především na informace o nových způsobech útoků a na nové zranitelnosti. V říjnu 2014, a v březnu let 2013 a 2012 se Pavel Bašta a Michal Prokop zúčastnili této konference v Amsterdamu.

- **CeCOS** (Counter-eCrime Operations Summit) - konference pořádaná v rámci Anti-Phishing Working Group (APWG) zaměřená na boj s kybernetickým zločinem. V dubnu 2014 se Pavel Bašta zúčastnil této konference v Hong-Kongu (Čína), kde přednesl příspěvek na téma ochrana webových stránek v doméně první úrovně s pomocí aplikace Malicious Domain Manager (MDM).

- **eCrime Research Summit** - konference pořádaná v rámci Anti-Phishing Working Group (APWG) se zaměřuje na informace o nových hrozbách pro nové uživatele a na boj proti kybernetické kriminalitě. V září 2013 se Pavel Bašta a Michal Prokop zúčastnili této konference v San Franciscu (USA). **V květnu 2015 se akce zúčastnil Pavel Bašta.**

Na **národní úrovni** sdružení CZ.NIC, dvakrát ročně realizuje vlastní konferenci **Internet a Technologie**, v jejímž rámci členové týmu CSIRT.CZ pravidelně vystupují s aktuálními tématy z oblasti bezpečnosti, případně pořádají workshopy se zaměřením na problematiku bezpečnosti. Sdružení CZ.NIC dále v roce 2013 hostilo speciální kurz pro členy bezpečnostních týmů pořádaný organizací TERENA. Kurzu bylo poskytnuto potřebné technické zázemí, prostory v rámci akademie CZ.NIC a technická podpora. Vedle toho se členové CSIRT.CZ účastní např. následujících odborných konferencí:

- **ICT Day** – konference pořádaná časopisem STECH se pravidelně zaměřuje na otázky bezpečnosti v kyberprostoru. V květnu 2012 se akce účastnili Michal Prokop a Pavel Bašta, který návštěvníky seznámil s činností CSIRT.CZ v roce 2011. V červnu 2013 akci navštívil Pavel Bašta a Michal Prokop, který zde prezentoval nejzajímavější incidenty v kyberprostoru za první pololetí roku 2013. V červnu 2014 se akce účastnil Michal Prokop, který na ní prezentoval aktuální bezpečnostní incidenty. V červnu 2015 akci navštívili Jaroslav Kodet a Pavel Bašta, který zde prezentoval průřez incidenty za poslední rok a trendy, které lze podle těchto incidentů očekávat v dalších letech.

- **ITTE 2013** – konference pořádaná českou pobočkou AFCEA pod záštitou ředitele NBÚ zaměřená na kyber útoky a kybernetickou bezpečnost. Akce se zúčastnil Pavel Bašta, který na ní prezentoval zkušenosti z DDoS útoků z března roku 2013.

- **Soom** – Konference pořádaná serverem soom.cz je zaměřena především na odborníky z české internetové komunity. Konference se v listopadu 2014 zúčastnili Pavel Bašta a Michal Prokop.

2.4.4. Osvěta směrem k široké veřejnosti: Jak na Internet

Za účelem zvyšování povědomí široké laické veřejnosti o využití Internetu a internetových technologiích připravilo v roce 2012 sdružení CZ.NIC ve spolupráci s Českou televizí sérii osvětových videí „Jak na Internet". Ta byla podpořena rovněž komunikací na sociálních sítích a vlastní internetové stránce www.jaknainternet.cz, kde mohou návštěvníci najít další informace.

Celkem bylo připraveno 100 dílů, které jsou od roku 2012 průběžně vysílány na různých kanálech České televize (ČT1 a ČT Sport), ale též k dispozici např. v rámci zábavního kanálu autobusů Student Agency a vlaků RegioJet.

Tématem internetové bezpečnosti se přímo zabývá hned několik dílů, kdy video „Bezpečnostní týmy" výslovně zmiňuje též pozitivní roli vládního týmu CERT a Národního bezpečnostního úřadu (NBÚ). Vybrané díly zabývající se různými úhly kybernetické bezpečnosti jsou řazeny v abecedním pořadí:

- Bezpečnost počítače (http://www.jaknainternet.cz/page/1179/bezpecnost-pocitace/)
- Bezpečnostní týmy (http://www.jaknainternet.cz/page/1790/bezpecnostni-tymy/)
- Ochrana dětí na Internetu (http://www.jaknainternet.cz/page/1201/ochrana-deti-na-internetu/)
- On-line bezpečnost (http://www.jaknainternet.cz/page/1741/online-bezpecnost/)
- Počítačová hesla (http://www.jaknainternet.cz/page/1178/pocitacova-hesla/)
- Rizika sociálních sítí (http://www.jaknainternet.cz/page/1185/rizika-socialnich-siti/)

Od roku 2012 zaznamenal seriál v televizi již více než **100 mil. shlédnutí**. Podle výzkumu provedeného v říjnu 2014 agenturou Markent zná seriál Jak na Internet 24 % uživatelů Internetu v České republice. 92 % z nich považuje seriál jako poučný, téměř 70 % ohodnotilo seriál jako přinášející informace užitečné pro práci a 50 % se v epizodách dozvědělo něco nového.

2.4.5. Osvěta směrem k odborné veřejnosti: přednášková činnost

Nedílnou součást osvětových aktivit sdružení CZ.NIC, resp. bezpečnostního týmu CSIRT.CZ, představuje vzdělávací a výukové středisko Akademie CZ.NIC. Mezi již ustálené kurzy určené odborné veřejnosti patří i

vzdělávání v oblasti kybernetické a počítačové bezpečnosti. Součástí nabídky Akademie CZ.NIC jsou rovněž kurzy na míru uspořádané např. pro Policii České republiky nebo Bezpečnostní informační službu (BIS).

Přehled vyučovaných kurzů, počet běhů a účastníků v jednotlivých letech jsou uvedeny níže v tabulce.

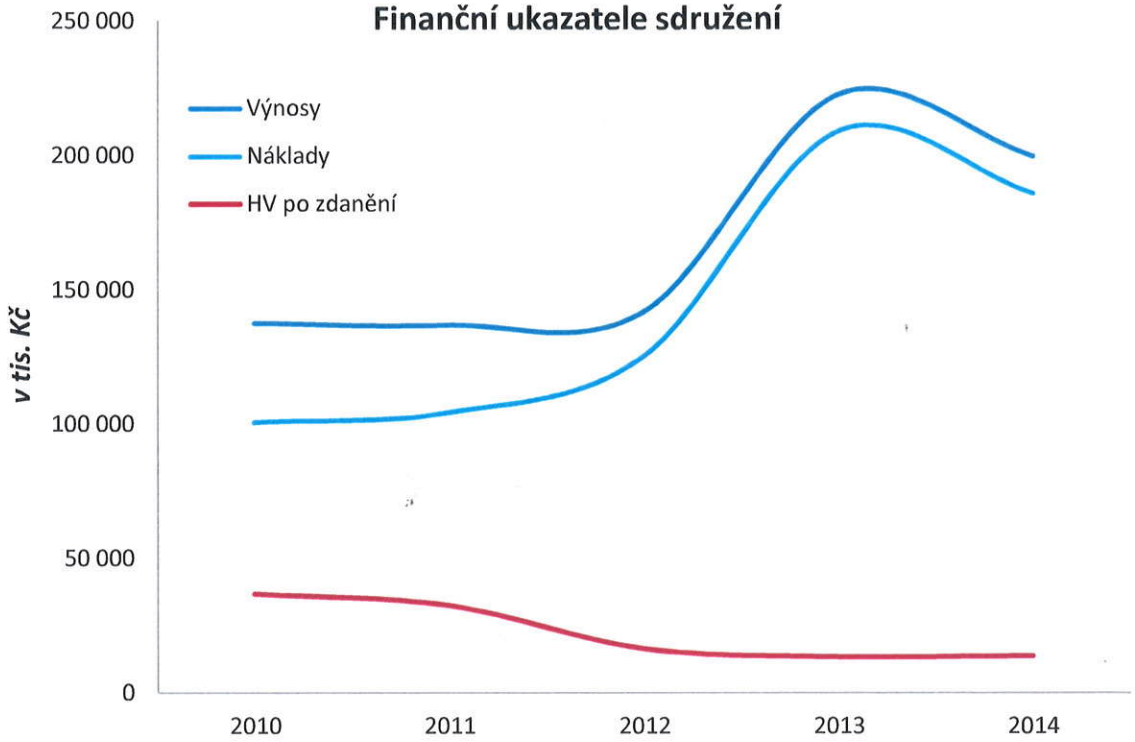
	2013		2014	
	Běhů	Účastníků	Běhů	Účastníků
Bezpečnost webových aplikací			2	34
DNSSEC – zabezpečení DNS	1	6	4	28
Počítačová bezpečnost prakticky			5	94
Svobodná aplikační bezpečnost I.	4	47	2	15
Svobodná aplikační bezpečnost II.			4	23
Celkem	**5**	**53**	**15**	**160**

Mezi účastníky výše uvedených kurzů patřily jak zástupci podnikatelů v oblasti elektronických komunikací (ISP), tak zástupci veřejné správy.

3. Finanční stabilita

Sdružení CZ.NIC představuje zájmové sdružení právnických osob, jehož **cílem není dosahování zisku**, ale naopak za pomoci prostředků kterými disponuje rozvíjet internetové prostředí v České republice a napomáhat internetové komunitě. Tyto aktivity může sdružení financovat ze své hlavní činnosti – provozování a správy doménových jmen .CZ.

V roce 2014 dosahovaly příjmy sdružení téměř 200 mil. Kč a hospodářský výsledek po zdanění 13,8 mil. Kč, což vytváří více než dostatečné zdroje pro provoz národního bezpečnostního týmu CSIRT.CZ a zajištění jeho činností v souladu s § 17, zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Klíčové finanční ukazatele vypovídající o finanční stabilitě sdružení za posledních 5 let jsou znázorněny v níže uvedeném grafu.



Pro další rozvoj a posilování kapacit Národního bezpečnostního týmu CSIRT.CZ využívá sdružení též formu grantů. V roce 2015 se podařilo takto získat od Evropské komise grant „CS Danube" (Kybernetická bezpečnost v Podunají), v rámci bezpečnostního výzkumu Ministerstva vnitra pak byl schválena na komplexní projekt zaměřený na Predikci a ochranu před kybernetickými incidenty (PROKI), který bude realizován v letech 2015 – 2020 a zajistí tak další dlouhodobý cíl financování národního bezpečnostního týmu.

4. Technické a technologické zajištění

4.1. Nástroje pro analýzu aktuálních hrozeb zranitelnosti z oblasti kybernetické bezpečnosti

Základ pro analýzu hrozeb a zranitelností představuje přístup do databází, informujících o aktuálních útocích, jako jsou **Google Safe Browsing** (permanentně updatovaný seznam stránek s phishing, či malware), **Phishtank** (databáze phishingových stránek), malwarepatrol (databáze zdrojů malware), **PassiveDNS** (databáze udržující historii DNS záznamů pro IP adresy a doménová jména), **CleanMX** (zdroj informací o různých hrozbách na IP adresách v ČR) a **Shadowserver** (informace o IP adresách v ČR s konkrétními zranitelnostmi, dostupnými službami, či například zapojenými do konkrétních botnet sítí).

Sdružení CZ.NIC dále provozuje vlastní systémy pro detekci a analýzu incidentů - projekt **Turris** a **vlastní sadu honeypotů**. Projekt Turris vyhodnocuje provoz v sítích koncových uživatelů v ČR a automaticky upozorňuje na anomálie v síťovém provozu. Ve spolupráci se sdružením CESNET také provozujeme systém pro detekci podezřelých síťových toků známý jako **IDS** (Intrusion Detection System). Důležitým zdrojem informací jsou také samotné incidenty, reportované týmu CSIRT.CZ a uchovávané v ticketovacím systému OTRS. Tento systém umožňuje vyhledávání informací dle konkrétních parametrů, lze tak například získat přehled o historii incidentů na konkrétní IP adrese, či v konkrétní síti. Uvedené zdroje informací o bezpečnostních incidentech jsou následně využívány pro další analýzy incidentů a data jsou v projektech křížově využívána pro získání globálního přehledu, případná reaktivní opatření, či varování uživatelů před aktuálními hrozbami.

4.2. Nástroje pro analýzu zranitelností souvisejících s českými doménovými jmény

Pro analýzu zranitelností souvisejících s českými doménami je využíván vlastní open-source nástroj **Malicious Domain Manager (MDM)** umožňující včas informovat držitele doménových jmen o napadení jejich webových stránek. Tato služba je velice důležitá nejen z pohledu držitelů doménových jmen, ale také z pohledu běžných uživatelů internetu. Napadené webové stránky se nezřídka stávají ohniskem šířícím různé virové záplaty, využívajíce špatně záplatované aplikace na koncových stanicích uživatelů. Od spuštění aplikace v polovině roku 2011 byla nějaká z forem úspěšného napadení stránek řešena na více než 8 400 doménách, což představuje více než 122 000 jednotlivých URL šířících malware, či obsahujících phishingovou stránku. Zdrojem informací o napadených doménách jsou převážně veřejně dostupné zdroje, sdružení CZ.NIC má však rovněž uzavřenu exkluzivní smlouvu se společností Google na poskytování rozšiřujících dat týkajících se jednotlivých napadených domén.

Na základě Usnesení vlády č. 982 z 18. prosince 2013 a spolupráci s Ministerstvem průmyslu a obchodu sdružení CZ.NIC provádí jednak pravidelný monitoring a vyhodnocení **zabezpečení doménových jmen prostřednictvím technologie DNSSEC** pro všechny domény v zóně .CZ, tak zabezpečení domén ústředních orgánů státní správy dotčených výše uvedeným usnesením. Ověřit zabezpečení DNSSEC jak pro konkrétní doménu úřadu, tak v rámci internetové připojení (konektivity), umožňuje webový nástroj umístěný na adrese www.982.cz. Pro možnost snadné kontroly důvěryhodnosti poskytovaných informací ze strany laické veřejnosti pak sdružení vyvinulo **DNSSEC validátor**, doplněk pro internetové prohlížeče názorně zobrazující zabezpečení domény prostřednictvím technologie DNSSEC. Tento doplněk je dostupný pro všechny rozšíření internetové prohlížeče – Mozilla Firefox, Google Chrome a Internet Explorer.

Sdružení rovněž dlouhodobě sleduje nová rizika spojená s DNS a s doménovými jmény a na takováto rizika upozorňuje odbornou veřejnost, případně provádí vlastní analýzy těchto rizik. Příkladem může být informační kampaň k nebezpečí **Amplification útoků** zneužívajících otevřené rekurzivní DNS servery, či úspěšná preventivní akce realizovaná ve spolupráci s Bezpečnostní infomační službou (BIS), která se zaměřovala na DNS servery, které byly identifikovány sdružením CZ.NIC jako nedostatečně zabezpečené. Správci těchto serverů obdrželi od sdružení CZ.NIC dopis s upozorněním na daný problém.

4.3. Nástroje a techniky pro penetrační testování a skenování zranitelností

Od roku 2013 provozuje sdružení projekt **Skener webu** (www.skenerwebu.cz). Tento projekt je určen provozovatelům a správcům webů, kterým pomáhá bezplatně odhalit potenciální zranitelnosti jejich internetových prezentací. Služba je určena především veřejné správě neziskovým organizacím a malým a středním podnikům, které nemohou vynaložit prostředky na získání komerčního řešení, avšak přesto jsou si vědomy, že zranitelnost jejich webu se může snadno stát problémem pro ostatní uživatele Internetu.

Analýza zranitelnosti probíhá ve dvou fázích. Nejdříve pomocí automatických nástrojů a následně je proveden manuální test webu zkušeným testerem, který mimo jiné vyhodnotí nalezené zranitelnosti v kontextu celého webu a navrhne vhodná řešení. Na konci je žadateli poslána zpráva, která obsahuje nalezené zranitelnosti, jejich ohodnocení dle závažnosti a také návrhy na možná řešení dané zranitelnosti. Při analýze potenciálních zranitelností služba staví jak na vlastních měřeních a zkušenostech bezpečnostního týmu, tak na seznamu Top 10 obecně nejzávažnějších bezpečnostních rizik projektu Open Web Application Security (OWASP).

V roce 2014 otestovalo sdružení CZ.NIC v rámci svého projektu celkem 99 webových aplikací. V rámci jejich testování bylo odhaleno celkem 1319 zranitelností.

Kromě projektu Skener webu se sdružení CZ.NIC dlouhodobě věnuje testování internetového prostoru vymezeného IP adresními rozsahy dedikovanými pro Českou republiku na aktuální zranitelnosti, či preventivní hledání již známých zranitelností. V minulosti tak například proběhlo skenování na zranitelnost HeartBleed, či hledání routerů zranitelných vůči ROM-0. Výsledky těchto testů jsou pak využity v procesu

řešení celé řady incidentů, v případě potřeby mohou pak být předány i důvěryhodným partnerům, schopným zajistit distribuci informací v rámci své působnosti (např. NCKB, ČBA).

V rámci navrhované veřejnoprávní smlouvy o spolupráci v oblasti bezpečnosti uzavřené s Národním bezpečnostním úřadem dle zákona č. 181/2014 Sb., plánuje sdružení CZ.NIC v této činnosti pokračovat a rozšířit ji o pravidelné testování úrovně zabezpečení internetových služeb provozovaných v rámci adresních prostorů alokovaných do České republiky. V rámci těchto testů se zaměříme například plošné vyhledávání webových prezentací provozovaných na zastaralých verzích CMS (Content Management System), jako jsou Joomla, WordPress, či Drupal, případně detekci zranitelných doplňků v těchto CMS. Dalším příkladem může být plánované testování zabezpečení SSH přístupů a kvality používaných hesel.

4.4. Nástroje pro příjem hlášení kybernetických bezpečnostních incidentů ze strany povinných subjektů a nástroje potřebné pro spolupráci při řešení kybernetických bezpečnostních incidentů u povinných subjektů

V souvislosti s nabytím účinnosti zákona č. 181/2014 Sb., o kybernetické bezpečnosti, umožnil Národní bezpečnostní tým CSIRT.CZ povinným subjektům dle § 3 písm. a) a b) (zejm. poskytovatelé služeb a sítí a osoby zajišťující významnou síť el. komunikací) možnost ohlásit své kontaktní údaje a také provést hlášení kybernetických bezpečnostních incidentů. Povinné subjekty mohou své údaje a kybernetické bezpečnostní incidenty nahlásit prostřednictvím webových formulářů umístěných na stránkách www.csirt.cz, ale též e-mailem, datovou schránkou, telefonicky či klasickou poštou. Všechna hlášení jsou následně zpracovávána v rámci systému OTRS (Open-source Ticket Request System).

Použití tohoto systému zaručuje včasnou a dohledatelnou reakci obsluhy na nahlášený incident, či informaci a splňuje všechny nároky potřebné pro spolupráci při řešení kybernetických bezpečnostních incidentů u povinných subjektů. Za využití některé z výše uvedených možností svoje údaje dosud ohlásilo 98 subjektů.

V rámci předloženého projektu bezpečnostního výzkumu vyhlášeného Ministerstvem vnitra je mj. tento proces zefektivnit a vytvořit efektivní správu kontaktních údajů s možností jejich předání vládnímu CERT v zákonem stanovených případech.

4.5. Technologie PGP k zajištění bezpečné elektronické komunikace

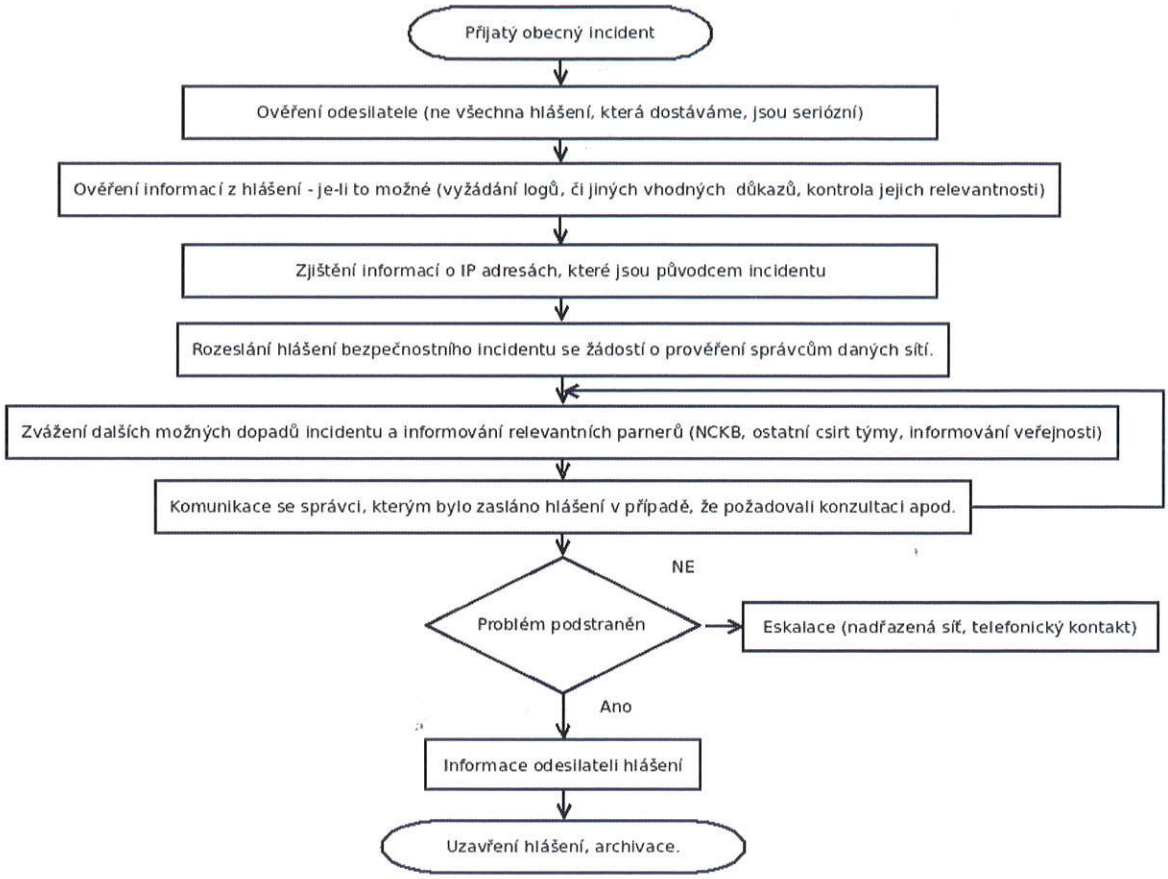
V rámci komunikace národního bezpečnostního týmu je pro společnou e-mailovou adresu abuse@csirt.cz i e-mailové adresy jednotlivých členů týmu využívána zabezpečená elektronická komunikace prostřednictvím PGP klíče o velikosti 1024 bitů.

Informace o používaných klíčích, včetně jejich fingerprintů lze nalézt v popisu týmu CSIRT.CZ vytvořeném v souladu s RFC23501[1].

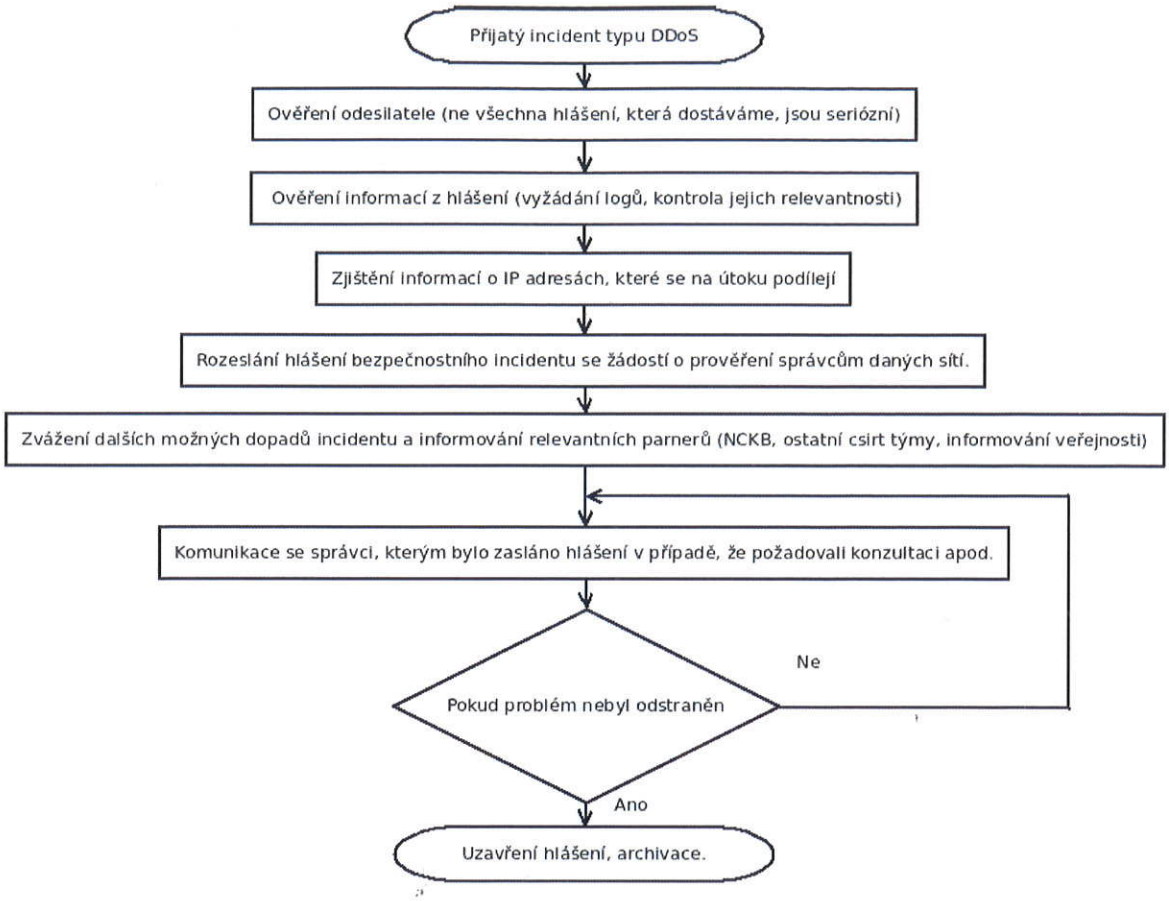
[1] https://www.nic.cz/files/csirt/rfc2350_CSIRT.CZ.2015_06_05.pdf

5. Příloha - Typová schémata řešení kybernetických bezpečnostních incidentů

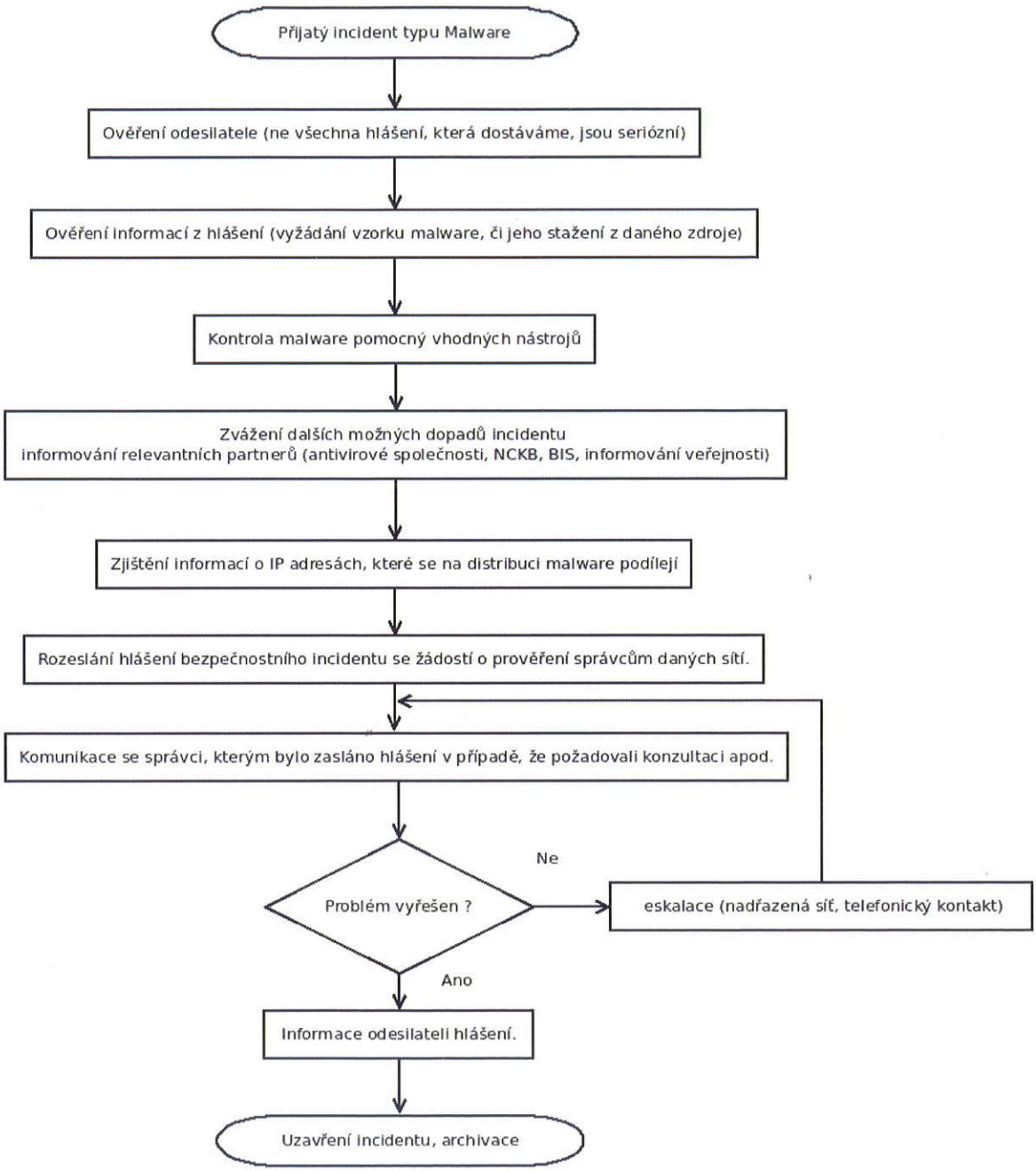
5.1. Obecný incident



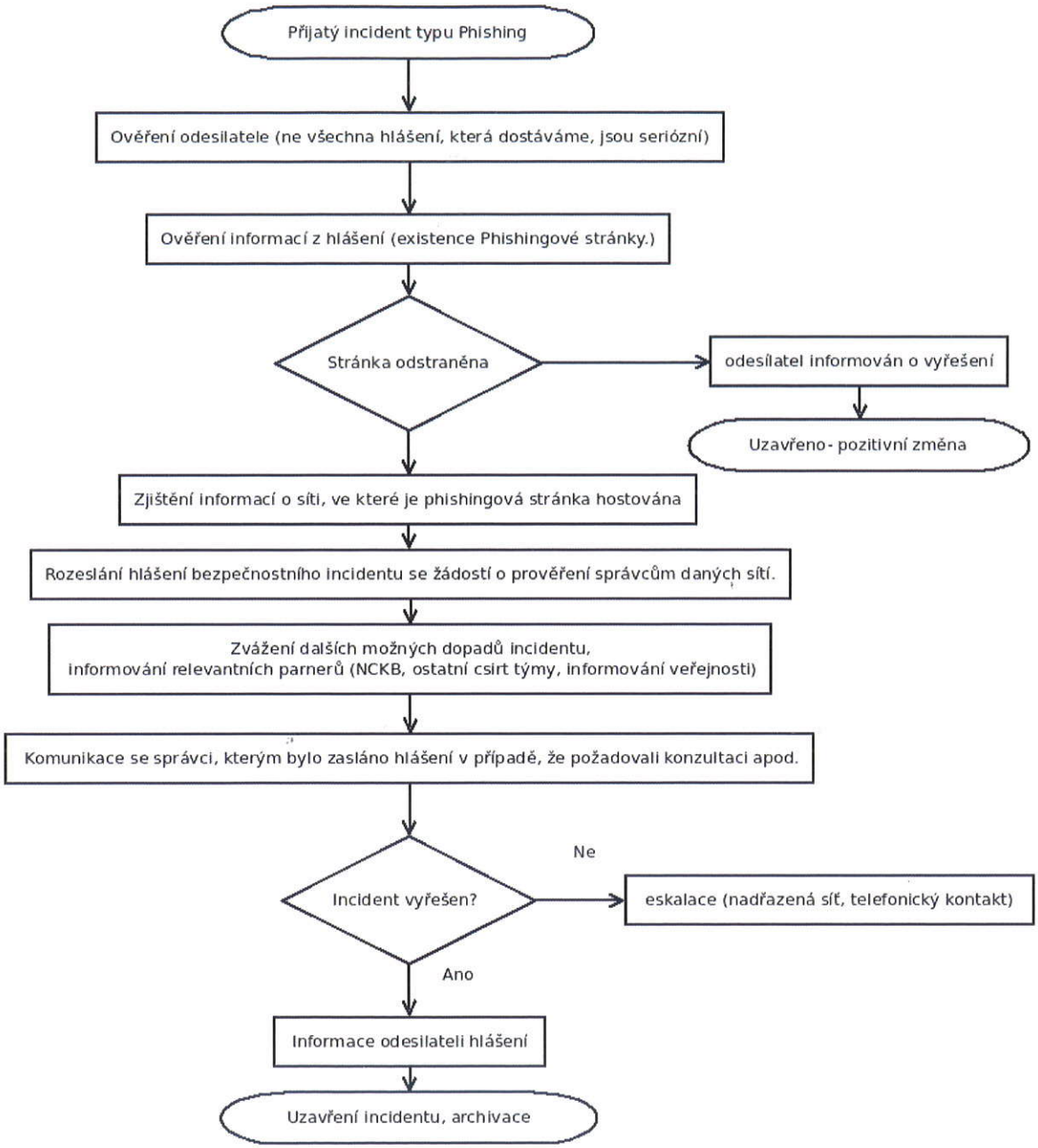
5.2. DDoS


Přijatý incident typu DDoS
Ověření odesilatele (ne všechna hlášení, která dostáváme, jsou seriózní)
Ověření informací z hlášení (vyžádání logů, kontrola jejich relevantnosti)
Zjištění informací o IP adresách, které se na útoku podílejí
Rozeslání hlášení bezpečnostního incidentu se žádostí o prověření správcům daných sítí.
Zvážení dalších možných dopadů incidentu a informování relevantních parnerů (NCKB, ostatní csirt týmy, informování veřejnosti)
Komunikace se správci, kterým bylo zasláno hlášení v případě, že požadovali konzultaci apod.
Pokud problém nebyl odstraněn
Ne
Ano
Uzavření hlášení, archivace.

5.3. Malware


Přijatý incident typu Malware
Ověření odesilatele (ne všechna hlášení, která dostáváme, jsou seriózní)
Ověření informací z hlášení (vyžádání vzorku malware, či jeho stažení z daného zdroje)
Kontrola malware pomocný vhodných nástrojů
Zvážení dalších možných dopadů incidentu
informování relevantních partnerů (antivirové společnosti, NCKB, BIS, informování veřejnosti)
Zjištění informací o IP adresách, které se na distribuci malware podílejí
Rozeslání hlášení bezpečnostního incidentu se žádostí o prověření správcům daných sítí.
Komunikace se správci, kterým bylo zasláno hlášení v případě, že požadovali konzultaci apod.
Problém vyřešen ?
Ne
eskalace (nadřazená síť, telefonický kontakt)
Ano
Informace odesilateli hlášení.
Uzavření incidentu, archivace

5.4. Phishing


Přijatý incident typu Phishing
Ověření odesilatele (ne všechna hlášení, která dostáváme, jsou seriózní)
Ověření informací z hlášení (existence Phishingové stránky.)
Stránka odstraněna
odesílatel informován o vyřešení
Uzavřeno - pozitivní změna
Zjištění informací o síti, ve které je phishingová stránka hostována
Rozeslání hlášení bezpečnostního incidentu se žádostí o prověření správcům daných sítí.
Zvážení dalších možných dopadů incidentu,
informování relevantních parnerů (NCKB, ostatní csirt týmy, informování veřejnosti)
Komunikace se správci, kterým bylo zasláno hlášení v případě, že požadovali konzultaci apod.
Incident vyřešen?
Ne
eskalace (nadřazená síť, telefonický kontakt)
Ano
Informace odesilateli hlášení
Uzavření incidentu, archivace

6. Seznam povinných příloh

1. Čestné prohlášení vztahující se k bodu I. 1. písm. a) až d), g) a h) Výzvy;
2. Potvrzení o neexistenci daňových nedoplatků vůči orgánům Finanční správy ČR;
3. Potvrzení o neexistenci jakýchkoliv nedoplatků vůči Celní správě ČR;
4. Potvrzení o neexistenci nedoplatků na pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti, penále a přirážce k pojistnému;
5. Potvrzení závazků vůči zdravotním pojišťovnám:
    - 5.1. Odborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví
    - 5.2. Zdravotní pojišťovna ministerstva vnitra České republiky
    - 5.3. Česká průmyslová zdravotní pojišťovna
    - 5.4. Všeobecná zdravotní pojišťovna České republiky
    - 5.5. Revírní bratská pokladna
    - 5.6. Vojenská zdravotní pojišťovna České republiky
6. Plná moc