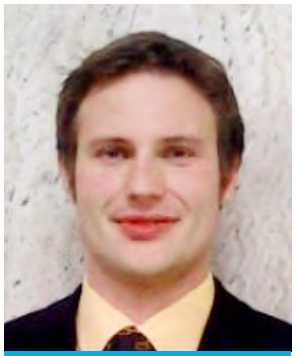
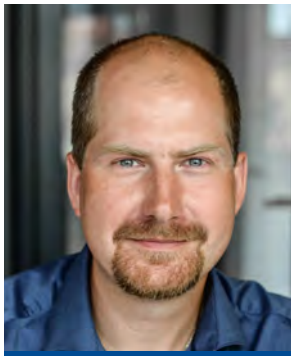
GovCERT.CZ a CZ.NIC

# Rozhovor se státními CERT týmy

Naše duo státních CERT týmů (organizace CSIRT.cz, resp. CZ.NIC a GovCERT.CZ) spolu již nějakou dobu koexistuje, avšak ne vždy měly týmy na různá témata stejné názory. To je logické, vezmeme-li v úvahu, že jde o organizace s rozdílným původem i agendou. Při čtení rozhovorů s nimi nás vždy napadlo, jaký názor by na danou otázku asi měla organizace druhá. Přišlo nám tedy jako zajímavý nápad zkusit provést rozhovor s oběma subjekty a dotazy strukturovat tak, aby odpovědi ilustrovaly rozdíly v přístupu k jednotlivým problematikám. Za GovCERT.CZ souhlasil s rozhovorem jeho ředitel a spoluzakladatel Radim Ošťádal, za CZ.NIC nás pak poctili Ondřej Filip, výkonný ředitel sdružení, ve spolupráci s Pavlem Baštou, bezpečnostním analytikem týmu CSIRT.cz.



GovCERT.CZ
Radim Ošťádal



CZ.NIC
Ondřej Filip

**Vaše organizace se pohybuje na českém kybernetickém poli již nějakou dobu. Jak byste zhodnotil její dosavadní fungování, jak se daří naplňovat cíle, které si jako organizace kladete?**

**GovCERT.CZ** Národní centrum kybernetické bezpečnosti, které je v současné době součástí Národního úřadu pro kybernetickou a informační bezpečnost, vzniklo na přelomu let 2012 a 2013, kdy nás v týmu bylo pět. Máme za sebou pět let činnosti, kdy se z malého týmu stal v tomto roce samostatný ústřední správní orgán, který se primárně stará o kybernetickou bezpečnost v ČR. Za tu dobu se nám podařilo vybudovat dobře fungující tým plný schopných lidí, které ta práce baví. Umíme řešit celou škálu kybernetických incidentů a útoků, pravidelně provádíme penetrační testy, nasazujeme síťové sondy do státní správy. Přijali jsme národní legislativu, připravili Národní strategii kybernetické bezpečnosti a akční plán, který bude následující tři roky udávat směr v této oblasti. Pořádáme technická a operační cvičení Cyber Czech, podíleli jsme se na přípravě vzdělávacích programů kybernetické bezpečnosti na vysokých i středních školách a Česká republika je ve světě vnímána jako jeden z lídrů v oblasti kybernetické bezpečnosti. Celkově můžu říct, že jsem s vývojem

za těch pět let velmi spokojen. Ale před námi je stále velké množství výzev, kterých každým dnem přibývá.

**CZ.NIC** My se ve sdružení CZ.NIC zabýváme kybernetickou bezpečností v mnoha ohledech. Kromě provozování národního bezpečnostního týmu CSIRT.CZ se sdružení věnuje mnoha aktivitám spojeným s bezpečností. Jako příklad bych mohl uvést projekty Honeypot as a Service nebo projekt bezpečných routerů Turris Omnia. Pokud se zaměříme přímo na CSIRT.CZ, tak ten se věnuje bezpečnosti od reakcí na incidenty přes vzdělávání a prevenci až po výzkum. Při realizaci našich projektů vždy sledujeme i případné synergie mezi nimi. Výsledná data z jednoho projektu tak často slouží v projektu jiném. Celé je to taková skládačka, jejíž jednotlivé kostky do sebe zapadají. Právě vytvořit takovýto funkční celek, který bude pomáhat uživatelům Internetu podporou všech oblastí bezpečnosti, bylo naším velkým cílem, který se nám postupně daří naplňovat.

**Jednou z vašich hlavních činností, jak je uvedeno na vašem webu, je výzkum a vývoj v oblasti kybernetické bezpečnosti. Jakému výzkumu se v současné době věnujete? Má tento vývoj již nějaké konkrétní výstupy?**

**GovCERT.CZ** Zatím se jedná pouze o pár výzkumných projektů, ale do budoucna se chceme na oblast výzkumu a vývoje více zaměřit. Před pár měsíci jsme navázali úzkou spolupráci s Technologickou agenturou ČR, abychom mohli lépe spolupracovat se soukromou i akademickou sférou na výzkumných projektech a poskytovat potřebné informace o možnostech výzkumu a vývoje v kybernetické bezpečnosti stejně jako i strategické vedení. Na projektech jako takových participujeme většinou v pozici aplikačního garanta, kdy do projektu můžeme vstupovat ve všech jeho fázích, podílet se na realizaci a především využít v praxi, resp. aplikovat jeho výsledky. Co se týče zmiňovaných výzkumných projektů NÚKIB, jedná se aktuálně o projekt s názvem „Kyberliga – dobrovolnické kybernetické kapacity státu“ realizovaný ve spolupráci s Univerzitou Karlovou. Výstupem bude návrh možných variant vytvoření dobrovolnických kybernetických kapacit státu na základě analýzy aktuálních a předpokládaných potřeb zajišťování kybernetické bezpečnosti státu včetně stanovení pozitiv, problematických bodů a negativ, která vytvoření dobrovolnických kybernetických kapacit státu mohou přinést. Dále např. „Experimentální výzkum individuálních reakcí na hrozby v kyberprostoru“, který budeme řešit s Masarykovou univerzitou a jehož cílem je pomocí biometrických měření zachycení a analýza individuálních emočních reakcí v závislosti na kybernetických hrozbách a srovnání s reakcemi na konvenční hrozby.

**Sdružení CZ.NIC se také mimo jiné zabývá různorodým vývojem. Nejznámější budiž patrně modem Turris Omnia, ale slyšel jsem, že také pracujete na vlastním DNS resolveru. Probíhá nějaká výzkumná / vývojová činnost v rámci týmu CSIRT.CZ, resp. dotýká se nějaká z těchto činností přímo kybernetické bezpečnosti?**

**CZ.NIC** CSIRT.CZ je plnohodnotnou součástí firmy a podílí se na projektech, které s bezpečností nějak souvisí nebo jsou na ni přímo zaměřené. Kromě toho má i svůj vlastní výzkumný projekt PROKI (Predikce a Ochrana Před Kybernetickými Incidenty). Ten je zaměřen na včasné informování koncových sítí o možných rizicích spojených s jejich IP rozsahy a dále se věnuje analýzám a vyhodnocování bezpečnostních incidentů. Kromě toho CSIRT.CZ udržuje a vyvíjí systém MDM (Malicious Domain Manager), který slouží k upozorňování držitelů domén, když dojde k napadení jejich webové prezentace, a ta je např. zneužívána k šíření malware nebo k phishingovým útokům. MDM také umí analyzovat obsah webu a zjistit např. skutečné umístění útočníkem používaného exploit kitu. Jak už jsem naznačil výše, data vystupující z projektů jsou také dále využívána v ostatních projektech. Některé výstupy z MDM využíváme k lepšímu zabezpečení vlastníků routerů Turris Omnia. Jiné výstupy z projektu Turris jsou využívány v rámci projektu PROKI.

**Spolupracujete na výzkumu s akademickou a na vývoji se soukromou sférou? Jak tato spolupráce probíhá?**

**CZ.NIC** Ano, pokud bych se podržel projektu Turris, tak tam přímo spolupracujeme s českými univerzitami. Jde o oblast hardwarového vývoje a např. také o výzkum, kde jsou pomocí teorie her zkoumána některá specifika útoků zachycených v rámci sítě routerů Turris. Naopak soukromá sféra má zájem o využívání výstupů z projektu PROKI, dokonce s jedním konkrétním zájemcem již máme uzavřenou dohodu o využívání těchto dat a aktuálně jednáme s dalšími dvěma zájemci.

**Jak nahlížíte na připravenost ČR jako celku na skutečně rozsáhlý a dlouhotrvající kyberneticky útok? Je realisticky možné v současných kapacitách zvládnout veškeré agendy plynoucí ze stavu kybernetic-**

**kého nebezpečí? Kde vidíte největší mezery a jakým způsobem myslíte, že by bylo nejlepší je zaplnit?**

**GovCERT.CZ** Zde hodně záleží na typu útoku – zda se jedná o dlouhodobou špionážní kampaň s cílem získat důležité informace a data, nebo zda se jedná o útoky typu odepření služby Denial-of-Service (DoS). V prvním případě je nejdůležitější částí samotná detekce takového útoku. Zde má ČR určitě nedostatky, které se snažíme dlouhodobě řešit. V současné době probíhá nasazování síťových sond na vybraná ministerstva. Data z perimetru sítě potom půjdou přímo do vládního CERTu, kde budou analyzována. Cílem je pomoci jednotlivým organizacím právě s detekcí incidentů nebo probíhajících útoků. Celkově je ale potřeba pracovat na schopnostech jednotlivých organizací incidenty včas detekovat a řešit je. A to nejen technickým vybavením, ale hlavně najímáním schopných lidí, kteří se budou této problematice naplno věnovat. Pokud se budeme bavit o opravdu rozsáhlém a dlouhodobém DoS útoku, pro tento případ vznikl projekt Fénix realizovaný českým peeringovým uzlem, sdružením NIX.CZ. Do projektu je zapojena většina významných operátorů poskytujících internetovou konektivitu jak koncovým uživatelům v ČR, tak významným českým internetovým službám. V případě rozsáhlého DoS útoku by měla komunikace mezi těmito operátory fungovat a díky vytvoření tzv. bezpečné VLANy by měla být zajištěna také dostupnost služeb daných operátorů.

**CZ.NIC** Hodně záleží na tom, jak sofistikovaný útok by to byl a v čem by spočíval. Pokud by se jednalo např. o DDoS útoky, jaké zažilo před pár lety Estonsko, tak jsem mírně optimistický. Díky projektu Fénix bychom pravděpodobně ustáli tento druh útoků mnohem lépe než zmiňovaná pobaltská republika. Sítě sdružené v tomto projektu by měly být schopné vytvořit funkční ostrov, v němž by pro firmy i koncové uživatele zůstaly skutečně klíčové služby dostupné i v případě masivního DDoS útoku. Proto se osobně snažím, aby počet sítí zapojených do tohoto projektu byl co nejvyšší. Pokud se ale bavíme o masivním zneužívání nějaké nové zranitelnosti, např. k šíření škodlivého kódu, tam je otázkou, zda má naše země v současné chvíli dostatek erudovaných odborníků, kteří by se dokázali s takto sofistikovaným útokem vypořádat. Obávám se ale, že nedostatek specialistů v oblasti bezpečnosti není jen specifikem České republiky.

**Jak často řešíte vážné kybernetické incidenty? Jedná se v těchto případech o váš konkrétní zásah nebo jde většinou o koordinační či konzultační činnost?**

**GovCERT.CZ** Kybernetické incidenty v rámci kategorizace dle závažnosti rozdělujeme do tří skupin. Méně závažné, závažné a velmi závažné. Většina námi řešených kybernetických incidentů spadá do kategorií nižších, tedy méně závažných až závažných. Těch velmi závažných řešíme spíše jednotky případů za rok, za rok 2017 jich zatím evidujeme šest. Avšak řešení takovýchto incidentů může trvat i několik měsíců. Většinou se jedná o náš konkrétní zásah v dané organizaci, kde se incident stal, a o spolupráci na analýze a vyřešení toho incidentu. V první řadě se snažíme zabránit pokračování incidentu, poté následuje samotné forenzní vyšetřování. Snažíme se zjistit vektor útoku, činnost útočníka a např. zcizená data. Součástí řešení je i navržení opatření, aby k podobnému incidentu znovu nedošlo. Získané poznatky poté často anonymizujeme a sdílíme je s dalšími organizacemi, aby se i tyto organizace mohly na podobný incident připravit nebo mu přímo zabránit.

**CZ.NIC** Těžko říci, protože co někomu připadá jako méně vážný bezpečnostní incident, může být pro jiného velmi závažné. My to z pohledu zvenčí nemusíme správně posoudit, a proto bych tu nechtěl dávat nějaká čísla. Mohu ale říci, že v tomto roce jsme zatím řešili 853 incidentů, což zahrnuje vše od phishingu přes škodlivý kód až po DDoS útoky. V každém případě je role národního CSIRT při řešení incidentů především koordinační a konzultační. Nemáme určitě ambice chodit do firem a někde něco přenastavovat v cizí infrastruktuře. Osobně považuji za velmi důležitou součást práce CSIRT.CZ právě vzdělávání a prevenci.

**Na jaké úrovni probíhá při kybernetických incidentech spolupráce mezi oficiálními CERT týmy, policií a např. zpravodajskými službami? Existuje jasně daný scénář, v jaké míře a posloupnosti do vyšetřování vstupují, nebo se postupuje ad-hoc podle konkrétní situace?**

**GovCERT.CZ** My jako vládní CERT spolupracujeme jak s Policií ČR, tak se zpravodajskými službami. Spolupráce má dvě základní úrovně. Nejprve se jedná o spolupráci v technické oblasti, ta je převážně neformální. Vyměňujeme si zkušenosti, postupy řešení kybernetických útoků, technické nástroje, účastníme se společně kybernetických cvičení atd. S policií dále spolupracujeme, pokud je bezpečnostní incident zároveň trestným činem a napadená organizace podala trestní oznámení. Tady je spolupráce spíše ad-hoc a hodně záleží na konkrétní situaci. Musíme se s policií koordinovat, protože máme z principu našich kompetencí rozdílnou agendu. My se snažíme co nejdříve systém zabezpečit a zamezit pokračování incidentu. Policie se snaží dopadnout pachatele. Ve většině případů tyto cíle

nejdou proti sobě, ale i to se někdy může stát. Každopádně se musíme vzájemně informovat a postupovat koordinovaně. Při nejvážnějších incidentech můžou být zapojeny do řešení i zpravodajské služby. Dále jsme do některých policejních případů zapojeni jako odborní konzultanti. Většinou se nejedná o incidenty a spolupráce musí být jasně formalizována. Od zpravodajských služeb potom dostáváme informace o hrozbách, které dále sdílíme organizacím spadajícím do naší působnosti.

**Probíhá spolupráce mezi CSIRT.CZ a GovCERT.CZ?**

**GovCERT.CZ** Ano, ta spolupráce probíhá téměř na denní bázi. Sdílíme spolu informace a zkušenosti, spolupracujeme na různých projektech. Zde bych zmínil alespoň ty nejdůležitější. V rámci české kapitoly projektu The Honeynet Project pracujeme na vývoji honeypotů a na sdílení informací z nich získaných. Dále spolupracujeme na projektech PROKI (Predikce a obrana před kybernetickými hrozbami) a CTI (Cyber Threat Intelligence). V obou případech se snažíme zvýšit schopnosti organizací v ČR detekovat kybernetické incidenty. V rámci řešení incidentů si vyměňujeme aktuální data, co se děje a čím se zabýváme, to platí i pro informace o nových zranitelnostech. Společně se také účastníme kybernetických cvičení.

**CZ.NIC** Ano, s kolegy z GovCERT.CZ se pravidelně potkáváme na našich i jejich akcích, vyměňujeme si zkušenosti a informace o incidentech, které by mohly jednu či druhou stranu zajímat.

**Jak byste hodnotil dosavadní činnost CSIRT.CZ vzhledem k povinnostem daným legislativou a k agendě, kterou si předsevzal plnit?**

**GovCERT.CZ** Se spoluprací a celkově s činností národního bezpečnostního týmu CSIRT.CZ jsme dlouhodobě velmi spokojeni. Nejedná se o žádného nováčka a tým fungoval dlouho před platností národní legislativy v oblasti kybernetické bezpečnosti. Tým CSIRT.CZ je provozován sdružením CZ.NIC, který je správcem domény .CZ, dlouhodobě zprostředkovává řešení incidentů primárně s českými operátory a věnuje se prevenci na různých úrovních. Do prevence lze zahrnout např. vzpomínaný projekt PROKI nebo letošní akci upozorňování na zranitelné redakční systémy. Co se týče prevence pro koncové uživatele, úspěšným počinem byly seriály „Jak na Internet“ nebo „Nauč tetu na netu“. Dlouholeté zkušenosti týmu CSIRT.CZ a sdružení CZ.NIC se využívají také při připomínkování právních předpisů.

**Jak byste hodnotil dosavadní činnost GovCERT.CZ (NÚKIB) vzhledem k povinnostem daným legislativou a k agendě, kterou si předsevzal plnit?**

**CZ.NIC** Já myslím, že se jim to daří. Když si uvědomíme, jak se kybernetická bezpečnost spíše neřešila na úrovni státních institucí před vznikem NKCB, dnes NÚKIB, jedná se v podstatě o heroický výkon.

**Co si myslíte o úrovni kybernetické bezpečnosti na českých úřadech a ministerstvech v porovnání se soukromým sektorem ve firmách srovnatelné velikosti?**

**GovCERT.CZ** To se nedá takto generalizovat. Máme tu úřady a ministerstva s kybernetickou bezpečností na špičkové úrovni a naopak ty, které nemají nastaveny ani základní bezpečnostní mechanismy, jako je centrální vyhodnocování bezpečnostních logů nebo síťový monitoring. To stejné ovšem platí i pro firmy ze soukromého sektoru. Hlavní nedostatky u ministerstev jsme odhalili během letošního auditu kybernetické bezpečnosti, který probíhal na základě usnesení Vlády ČR z února 2017. Mezi největší problémy patřily např. nedostatek lidských zdrojů, nevhodný rozsah systému řízení bezpečnosti, neexistující bezpečnostní monitoring a další. To budou naše priority pro zlepšení na příští rok.

**Státní správa se dlouhodobě potýká s nedostatkem kvalitních odborníků, což se projevuje mimo jiné tím, že často kritizované IT zakázky nejsou schopny implementovat v požadující kvalitě a plánovaném časovém horizontu. Tento nedostatek povětšinou vysvětlují tím, že IT odborníci nemají zájem u nich za nízké tabulkové platy pracovat. V kontrastu s tím zaznívají z oficiálních pozic zabývajících se touto problematikou názory, že zákon o státní službě výrazně napomohl řešit tuto otázku a že platy státních zaměstnanců jsou srovnatelné s těmi v soukromé sféře. Jaký na tento rozpor máte názor vy?**

**GovCERT.CZ** Ano, tohle je dlouhodobě opravdu velký problém a zákon o státní službě ho rozhodně nevyřešil. Problém je ještě větší, pokud se zaměříme na lidi zabývající se v oblasti IT přímo kybernetickou bezpečností. My na to dlouhodobě upozorňujeme, ale bohužel není v našich silách prosadit výraznější zlepšení v podobě zvýšení platů. Peníze však často nejsou tím nejdůležitějším, o co se tito odborníci zajímají. V průzkumech realizovaných různými personálními agenturami je plat často až na druhém nebo třetím místě. Důležitou roli hraje, jak je práce zajímavá, jak může člověk odborně růst a v jakém kolektivu pracuje. Na to se u nás zaměřujeme a zatím se nám daří sehnat

schopné lidi. Nejedná se samozřejmě o řešení výše popsaného problému, spíše je to způsob, jak mu čelit, když chybí koncepční řešení.

**CZ.NIC** S tímto tvrzením souhlasím pouze částečně. Je nepochybné, že zákon o státní službě pomohl, ale rozhodně nelze říct, že tím byla tato oblast zcela vyřešena. Jen těžko si lze představit, že by např. v rámci nějakého úřadu vzniklo vývojové oddělení, které by se staralo o programování nějaké klíčové části e-Governmentu.

**Vzhledem k zákonu o veřejných zakázkách není ve státním sektoru možné cílit na konkrétní dodavatele technologií, resp. se některým dodavatelům vyhnout. Považujete za rozumné, aby byly významné informační systémy či kritická informační infrastruktura závislé na technologiích firem ze zemí, které se v současné geopolitické situaci nacházejí na opačném konci spektra mezinárodního společenství?**

**GovCERT.CZ** Toto je velmi složitá otázka a v poslední době se hodně řeší v souvislosti se společností Kaspersky. Pokud necháme jakoukoli firmu přistupovat do našich kritických a významných systémů a pokud tato firma pochází ze země s rozdílnými bezpečnostně-strategickými zájmy, představuje to vždy určité bezpečnostní riziko. Podle mého názoru je potřeba u technologií nasazovaných do prostředí kritické informační infrastruktury a významných informačních systémů hodnotit původ dodavatele a politicko-legislativní kontext, ve kterém dodavatel působí. Na druhou stranu tu máme zákon o veřejných zakázkách a celkově v této oblasti neexistuje jednotná národní strategie. Je to každopádně oblast, které by se Česká republika měla v budoucnu intenzivně věnovat.

**CZ.NIC** Účastníme se cvičení, která pro nás mají pozitivní přínos. Jsou to např. cvičení organizovaná v rámci NATO nebo v rámci EU organizací ENISA. Některá z těchto cvičení jsou vyloženě technická a zaměřená např. na forenzní analýzu, některá na řešení incidentů na mezinárodní i lokální úrovni a některá na strategické rozhodování. Z toho také plynou jednotlivá pozitiva. Pro techniky je to možnost vyzkoušet si své znalosti a schopnosti a případně si rozšířit obzory, pro kolegy řešící incidenty je to příležitost vyzkoušet si krizové komunikační kanály a pro management je to možnost odhalit nedostatky v zákonech, které znemožňují provedení konkrétních ochranných opatření.

**Jak je na tom Česká republika z hlediska kyberbezpečnosti na mezinárodní scéně? České týmy se pravidelně v různých cvičeních umisťují na předních pozicích. Je to indikativní pro kvalitu českých expertů obecně nebo se jedná o omezenou skupinku skutečně elitních odborníků, kteří vyčnívají nad zbytkem kyberbezpečnostní komunity?**

**GovCERT.CZ** Česká republika se v oblasti kybernetické bezpečnosti řadí k lídrům. V mezinárodním srovnání patří k předním státům a každým rokem se posouváme dopředu. U cvičení, která zmiňujete, se jedná o nějakou skupinu odborníků. Ale jak už jsem říkal, složení je opravdu napříč organizacemi z veřejného, soukromého i akademického sektoru. A taková spolupráce v mnoha státech vůbec není samozřejmostí. Celkově bych chtěl říct, že v ČR máme opravdu skvělou bezpečnostní komunitu. Ale zpět k otázce. Kromě cvičení zde máme mezinárodní srovnání kybernetické bezpečnosti, kde jsme se podle estonského National Cyber Security Index (NCSI) umístili na 1. místě ze 41 zemí, které se hodnocení účastnily. V hodnocení OSN (ITU) jsme se od roku 2015 zlepšili o minimálně šest příček – z 41.–43. místa na 35. místo.

**CZ.NIC** Myslím, že úroveň českých expertů je velmi dobrá, těch zmíněných cvičení se neúčastní pouze členové CSIRT.CZ či GovCert, ale zapojují se i zástupci jiných bezpečnostních týmů. Také díky projektu FENIX je kybernetická bezpečnost aktuálním tématem v internetové komunitě.

**V rámci EU se kyberbezpečnosti dostává stále více pozornosti. V připravovaném kyber balíčku se např. počítá s rozšířením působnosti agentury ENISA či o zavedení certifikovaných dodavatelů technologií. Je tento přístup dostatečně produktivní nebo jde o návrhy, které reálné situaci nijak nepomohou, a bylo by potřeba prosazovat změny výraznějšího charakteru?**

**GovCERT.CZ** EU v poslední době nedostatkem nápadů na poli kybernetické bezpečnosti rozhodně netrpí. Podle mě je ale důležité řádně implementovat existující projekty než přicházet se stále novými iniciativami. Rozšíření působnosti agentury ENISA navržené ve zmiňovaném nařízení v principu vítáme. ENISA může jednotlivým státům nabídnout metodickou podporu, osvědčené postupy a vodítka pro implementaci NIS směrnice. Obdobnou roli může sehrát ve vzdělávání a osvětě. Tam se snažíme uvést v život síť národních kontaktních osob/institucí, které by mohly sdílet znalosti a postupy či spolupracovat na společných projektech, a ENISA je podle nás přirozenou zastřešující platformou. U certifikace IT produktů a služeb vnímáme poptávku trhu. Podle mě je ale důležitější otázka konkrétní podoby evropského cer-

tifikačního systému než to, zda má existovat. To ale ještě bude předmětem mnoha jednání.

**CZ.NIC** Je ještě brzy návrhy hodnotit. Např. myšlenka certifikovaných dodavatelů může na jedné straně pomoci zviditelnit kvalitní společnosti, ale také může vést k nepružnosti trhu a zvýhodnění určitých dodavatelů se silným administrativním zázemím, a tím naopak omezit trh a ve svém důsledku bezpečnost snížit. Nerad používám klišé, ale ďábel se skutečné skrývá v detailech.

**Ve výše zmíněném balíčku je jako jedna z problematických oblastí identifikována komunikace a předávání informací mezi jednotlivými členskými státy a je předkládána řada opatření, jak tuto komunikaci zlepšit. Je reálné od těchto opatření očekávat zlepšení sdílení strategických informací v rámci EU, když některé členské státy na mezinárodní scéně např. otevřeně zastávají pozice Ruska?**

**GovCERT.CZ** Zajištění kybernetické bezpečnosti je primárně odpovědností jednotlivých členských států. Ty si samozřejmě hlídají, s kým sdílejí své informace, a výhrada národní bezpečnosti musí být respektována. V současnosti se však v rámci EU setkáváme i se situacemi, kdy sdílení informací nutně nesouvisí s národní bezpečností, ale přesto nefunguje jednoduše proto, že se lidé v jednotlivých institucích neznají či nemají nastaveny komunikační kanály. V tomto směru mohou mít opatření v rámci směrnice NIS nebo kybernetického balíčku pozitivní dopad. Na druhou stranu je potřeba vzít v potaz i již nastavené kanály mezi národními a vládními týmy v organizacích Trusted Introducer nebo FIRST, které sdružují právě CERT/CSIRT týmy.

**CZ.NIC** Někdy by stačilo, kdyby politici nedělali nic. V rámci EU někdy dochází k rozporuplným jevům, kdy z jedné strany je požadavek na zlepšení komunikace mezi členskými státy, z druhé strany pak ale přichází legislativa GDPR, která považuje IP adresu za osobní údaj a nutí bezpečnostní týmy zacházet s ní se zvýšenou opatrností. Nerad bych předbíhal, ale panuje určitá obava, že ochota sdílet informace o incidentech v rámci bezpečnostní komunity značně poklesne v květnu příštího roku, kdy nařízení GDPR vstoupí v platnost. Zatím je však naše zkušenost se sdílením těchto informací v bezpečnostní komunitě spíše pozitivní.

**Česká republika je v oblasti kyberbezpečnostní legislativy považována za jednoho z pionýrů. Je současný stav naší legislativy do dohledného časového období dostatečný nebo v tomto ohledu ještě vidíte prostor pro zlepšení?**

**GovCERT.CZ** Opravdu jsme pionýry v oblasti kyberbezpečnostní legislativy. Pomohlo nám to v implementaci evropské Směrnice NIS, na jejímž obsahu se podílela i ČR. Jelikož měla ČR již před účinností směrnice svůj kybernetický zákon, nebylo zapotřebí provádět výrazné změny v legislativě a v kompetencích úřadů jako u jiných členských států, které začínají od nuly. Nyní je ČR jednou z prvních zemí, která má značnou část požadavků Směrnice NIS již splněnou. Naši odborníci poskytují podporu při tvorbě legislativy jiným zemím. Prostor pro zlepšení tu do budoucna určitě je. Regulovaná oblast je natolik dynamická, že je nutné udržet s rozvojem ICT a rozvojem kybernetické bezpečnosti krok. Samotné uplatňování zákonů v praxi nám vždy přináší nové zkušenosti. Objevují se samozřejmě i nedostatky či slabá místa. Např. do budoucna bychom rádi upravili identifikaci informačních nebo komunikačních systémů kritické infrastruktury či významných informačních systémů, čímž bychom mohli zlepšit situaci, kdy se některé organizace zaměřují výlučně jen na kritické a významné systémy a neřeší bezpečnost jako celek.

**CZ.NIC** Prostor pro zlepšení se vždy najde. Nám by např. nyní pomohlo, kdyby národní CSIRT získal určitou výjimku právě ve vztahu k nařízení GDPR.

**Máte nějaká slova na závěr? Co byste vzkázal čtenářům DSM?**

**GovCERT.CZ** Popřál bych jim hlavě veselé Vánoce a úspěšný rok 2018. Dále bych je chtěl upozornit na naše webové stránky a twitterový účet, kde pravidelně zveřejňujeme informace o nejnovějších hrozbách, a na akce a semináře, kterých se účastníme nebo je přímo organizujeme. Vlajkovou lodí je dvoudenní konference CyberCon Brno, která probíhá každoročně v září. V roce 2018 se bude konat 19. - 20. září a všichni jsou srdečně zváni.

**CZ.NIC** Snad aby nepodléhali iluzi, že vrcholové bezpečnostní týmy na národní či mezinárodní úrovni jsou zde proto, aby je ochránily. Nejde o mocnou skupinu lidí, kteří přiletí v černých helikoptérách a budou řešit problémy každého. Naopak, kybernetická bezpečnost je odpovědností každého z nás, každého jednotlivce i instituce.

**Děkujeme za rozhovor.**
**Za DSM se ptal Adam Lamser.**