Existence a fungování platforem typu CSIRT/CERT v některých zemích světa

PRAHA 2009

Úvod

Jakékoli kroky v domácím bezpečnostním prostředí by bylo více než nezodpovědné konat bez toho, pokud by nebyla nejprve prostudována situace v zahraničí.

- V zemi existuje více či méně plnohodnotný "národní CERT", sloužící nejširší veřejnosti (Belgie, Dánsko, Estonsko, Finsko, Francie, Chorvatsko, Itálie, Litva, Lotyšsko, Maďarsko, Malta, Německo, Nizozemsko, Norsko, Polsko, Slovinsko, Spojené království, Španělsko, Švédsko, Ruská federace). Vedle nich může působit i více než deset platforem tohoto typu pro konkrétní zákazníky.
- V některých zemích existují pouze omezené struktury tohoto typu, které nicméně někdy (na požádání zahraničních partnerů) s větší nebo menší úspěšností "suplují" roli národních CERT (Česká republika, Irsko, Island, Kypr, Portugalsko, Rakousko). U těchto zemí je možné očekávat takový vývoj, že síť, původně omezená pro potřeby akademických subjektů, postupem času převezme roli národního CERT oficiálně a pokryje celé prostředí národní domény.
- Funkční CERT slouží zejména vládním a vojenským strukturám (Turecko).
- V zemi existují pouze firmy, plnící některé funkce CERT (Švýcarsko).
- V některých zemích tyto struktury vůbec neexistují (ze zemí EU je to Slovensko, Rumunsko, Bulharsko).

Národní CERT je proto v současnosti nejčastěji provozován nevládními (akademickými) subjekty se slabším nebo silnějším vlivem státu. Tak je tomu ve 14 zemích (Belgie, Dánsko, Estonsko, Francie, Chorvatsko, Itálie, Litva, Lotyšsko, Lucembursko, Maďarsko, Nizozemsko, Polsko, Slovinsko a Španělsko). **V pěti zemích** (Finsko, Malta, Německo, Norsko a Spojené království) **provozují národní CERT pouze (především) orgány státní správy.**

Sledovány byly i vazby platforem typu CERT na produkty firmy Microsoft. Úvodem je třeba poznamenat, že **spolupráce platforem typu CERT s firmou Microsoft je velmi diskutabilní** vzhledem k nejasnostem účelu sběru informací o incidentech ze strany Microsoftu a není tak nastavena potřebná důvěryhodnost. V zásadě existují následující možné přístupy k nim:

- Země, jejichž národní (nebo omezenější) platformy typu CERT s firmou Microsoft udržují nadstandardní vztahy: USA, zprostředkovaně i Ruská federace, patrně i Island.
- Země, jejichž národní (nebo omezenější) platformy typu CERT s firmou Microsoft udržují standardní vztahy (pracoviště standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích): Dánsko, Finsko, Francie, Chorvatsko, Irsko, Lucembursko, Maďarsko, Malta, Německo, Polsko, Portugalsko, Slovinsko, Spojené království, Turecko).
- Země, jejichž národní (nebo omezenější) platformy typu CERT firmu Microsoft a její produkty ignorují: Belgie, Estonsko, Lotyšsko, Nizozemí, Norsko, Španělsko.
- U ostatních zemí nebyl vztah národní (nebo omezenější) platformy typu CERT s firmou Microsoft prozatím zjištěn.

země	**počet členů akreditovaných v ENISA**	**počet členů akreditovaných ve FIRST**	**existuje zde národní CERT**	**jaká instituce jej provozuje**	**poznámka**	**spolupráce s firmou Microsoft**	**napojení na CETS Microsoft**
Belgie	2	2	ano (BELNET, od roku 2004)	universitní pracoviště, veřejná správa a výzkumné ústavy	vedle toho v Belgii existuje CERT pro vojenské účely (NCIRC), vybudovaný roku 2004 a používaný strukturou celé Severoatlantické aliance	stránka BELNET o operačním systému Windows vůbec nehovoří, obsahuje jen odkazy na systémy LINUX, SOLARIS, HPUX a APPLE; uživatele produktů Microsoft odkazuje pouze na stránky této firmy[1]; firma Microsoft o přímou spolupráci opakovaně usilovala, ale zřejmě bez výsledku	ne
Bulharsko	0	0	ne	-	-	nepodařilo se zjistit	připravuje se
Česká republika	1 (CESNET)	0[2]	ne	-	akademické pracoviště CERT je jediným certifikovaným pracovištěm v ČR, v oblasti bezpečnostních incidentů komunikuje s TF CERT a FIRST;	základem spolupráce je dohoda z února 2005 mezi firmou Microsoft a Národním bezpečnostním úřadem; pracoviště CESNET se případné spolupráci nebrání	ne, téma spadá do působnosti Policie České republiky
Dánsko	3	6	ano (DK-CERT, od roku 1991, po USA jeden z prvních CERT světa)	výzkumné a vzdělávací instituce, platforma, provozující CERT je nyní přidruženou agenturou Státního střediska pro výzkum v oblasti informačních technologií, financovanou Ministerstvem vzdělávání	vedle toho v zemi existuje dalších 5 omezenějších pracovišť podobného typu (CSIRT od roku 1999, vybudovaný komerčními internetovými a telekomunikačními operátory; KMD, vybudovaný rok 1997 pro účely místních úřadů, NORDUNET z roku 2002, SWAT a SECUNIA RESEARCH.	pracoviště standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích	ne
Estonsko	1	0	ano (CERT-EE, od roku 2006)	subjekty veřejného a soukromého sektoru (vládním subjektům je v platformě určeno zvláštní „podokno“)	-	stránka CERT-EE o produktech Microsoft de facto vůbec nehovoří a ani na ně neodkazuje	ne
Finsko	4	5	ano (CERT-FI, od roku 2002)	vládní subjekty, telekomunikační operátoři, vlastníci přenosových soustav	v zemi existuje ještě čtyři soukromé platformy: PSIRT Ericsson (založen roku 2000); NIRT Nokia (založeno 1998), FUNET (od roku 1995) a FS-Laboratories (od roku 1991)	pracoviště standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích	ne

[1] http://www.microsoft.com/security/default.mspx

[2] Ve dnech 28. – 31. ledna 2008 CESNET v Praze hostil konferenci FIRST, kde se chtěl přihlásit jako její plnoprávný člen, nicméně s ohledem na nejasnosti okolo budování CERT-CZ se tak nestalo.

Francie	4	3	ano (RENATER, od roku 1993)	ústřední orgány státní správy, výzkumná pracoviště	struktura CERTA, určená pro potřeby veřejné správy v území (obce, regiony), fungující od roku 1999 a dvě soukromé platformy CERT-IST (od roku 1999) a LEXSI (od roku 2003)	pracoviště CERTA standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích	ne
Kypr	1	0	ne	-	v zemi existuje jen akademická platforma CYNET (od roku 2001)	nepodařilo se zjistit, stránka je pouze v řečtině	ne
Chorvatsko	1	1	ano (CARNET od roku 1996)	akademické subjekty, operátoři, správci domén	-	výstrahy jsou vždy specifikovány podle toho, jakého operačního systému se týkají (UNIX, LINUX, WINDOWS, ostatní), pracoviště standardně upozorňuje na bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích	ne
Irsko	1	0	ne	-	v zemi působí pouze omezenější platforma HEANET (CERT-IE), od roku 2002, pokrývají sítě akademických institucí	pracoviště standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích	ne
Island	1	0	ne	-	v zemi pouze existuje akademická platforma RHNET (od roku 2003)	nepodařilo se s určitostí zjistit (většina textu je v islandštině); firma Microsoft patrně uzavřela smlouvy s universitami, které RHNET provozují (slevy na produkty pro pedagogy i studenty), ale nikoli s platformou RHNET jako takovou	ne
Itálie	8	1	ano (CERT-IT, od roku 1994)	Universita Miláno a operátoři	vedle toho existuje ještě vládní platforma GOVCERT pro potřeby veřejné sféry, struktura DIFESA pro potřeby armády a pět dalších (akademické, soukromé) subjektů tohoto typu	nepodařilo se s určitostí zjistit (stránky jsou značně neuspořádané); za zmínku stojí skutečnost, že některé regionální správy (prefektury, provincie) přešly na LINUX	ano (říjen 2006)
Litva	2	1	ano (LITNET, od roku 1998)	vysoké školy, výzkumné ústavy, nevládní organizace[3]	v zemi navíc od roku 2006 funguje platforma RRT, sloužící potřebám telekomunikačních operátorů	nepodařilo se s určitostí zjistit (informace jsou pouze v litevštině)	ne

[3] Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Pospíšilová, M., Velvyslanectví České republiky v Litvě, Vilnius, 18. VIII. 2006 (č. j. 999/2006 – Vilnius); National Contributions to be Taken into Account in the Preparation of the Independent Report on the use of the Internet for Terrorist Purposes and Cyberterrorism; CODEXTER (2006) 38 prov, 3. X. 2006.

Lotyšsko	2	0	ano (LATNET od roku 2006)	akademické a soukromé subjekty	v zemi navíc od roku 2007 funguje platforma DDIRV, sloužící potřebám vládních institucí, včetně armády	LATNET o produktech Microsoft vůbec neinformuje; DDIRV jen velmi sporadicky, spíše v dílčích anketách, nikoli co se týče konkrétních incidentů	ne
Lucembur-sko	1	0	nepodařilo se zjistit s jistotou	patrně akademická pracoviště	-	pracoviště standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích	ne
Maďarsko	3	1	ano (HUN-CERT, od roku 2003)	členové asociace poskytovatelů telekomunikačních služeb	v zemi existuje dvě další platformy: CERT-HU (funguje od roku 2004, pro potřeby veřejné správy, provozovaný obdobou Národního bezpečnostního úřadu) a NIIF (od roku 2003, pro potřeby některých akademických subjektů)	pracoviště standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích	ne
Malta	1	0	ano (MTCERT, od roku 2002)	orgány státní správy	-	pracoviště standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích	ne
Německo	19	16	ano (CERT-BUND, od roku 2001)	Spolkový úřad pro bezpečnost informační techniky (BSI, vládní agentura)	vedle toho existuje vojenská platforma CERT-Bundeswehr (od roku 2003) a sedmnáct dalších institucí typu CERT s omezenějším záběrem (soukromé firmy, banky atd.)	CERT-BUND standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích; státní správa v Německu od roku 2002 plošně přešla na LINUX,[4] ale firma Microsoft státní správě dále dodává celou řadu dalších aplikací[5]	ne
Nizozemsko	10	5	tuto roli patrně splňuje GOVCERT (založený roku 2002)	vládní a veřejné subjekty	vedle toho v zemi existuje dalších 9 subjektů, plnících funkci CERT pro určité úzce specifikované klienty (banky, zdravotnická zařízení, operátory, university, zákazníky soukromých firem)	o produktech firmy a incidentech, které s nimi souvisí, je informováno jen velmi sporadicky, spíše v oblasti všeobecných rad a odkazů na stránky firmy	ne

[4] http://www.theregister.co.uk/2002/06/04/german_gov_deal_offers_linux/
http://www.heise.de/english/newsticker/news/25006
[5] http://www.microsoft.com/presspass/press/2004/may04/05-03germanymoupr.mspx

Norsko	2	2	ano (NORCERT od roku 2004)	státní subjekty, operátoři, majitelé přenosových soustav	vedle toho v zemi existuje akademická síť UNINETT (od roku 1995)	o produktech firmy a incidentech, které s nimi souvisí, je informováno jen velmi sporadicky, spíše v oblasti všeobecných rad a odkazů na stránky firmy	ne
Polsko	3	1	ano (CERT POLSKA, od roku 1996)	hlavním subjektem, který v Polsku provozuje CERT, jsou správci tzv. Vzdělávací a akademické počítačové sítě (Naukowa i Akademiczna Siet Komputerowa, NASK); jedná se o akademické pracoviště, které začalo se zaváděním Internetu v Polsku	vedle toho v zemi existují dvě omezené CERT sítě na akademické půdě (PIONEER a TPCERT, vybudované obě na přelomu let 2001 a 2002), pokrývající jen sítě konkrétních akademických pracovišť	pracoviště standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích	připravuje se
Portugalsko	2	0	ne	-	v zemi fungují pouze dvě omezené akademické platformy (CERT-PT z roku 2002 a FEUP z roku 2006)	pracoviště standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích	ne
Rakousko	1	1	ne	-	v zemi funguje (od roku 2003) pouze akademická síť ACONET	o produktech firmy a incidentech, které s nimi souvisí, je informováno jen velmi sporadicky, spíše v oblasti všeobecných rad	ne
Rumunsko	0	0	ne[6]	-	-	-	ano (od října 2007)[7]
Řecko	2	0	ne	-	v zemi existují dvě omezené CERT sítě na akademické půdě (GRNET z roku 2000 a AUTH z roku 2004), pokrývající jen sítě konkrétních akademických pracovišť	pracoviště GRNET standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích	ne
Slovensko	0	0	ne	-	-	-	ne

[6] Bezpečnostní rada již roku 2006 schválila rezoluci k podpoře ochrany kritické infrastruktury (obsahující výslovné zmínky o nutnosti zvýšení obecného povědomí o informační bezpečnosti a vytvoření platformy typu CERT).

[7] http://www.alertnet.org/thenews/newsdesk/l25810282.htm

Slovinsko	1	1	ano (SI-CERT, od roku 1994)	akademická obec (Akademická a výzkumná síť Slovinska - Akademska in Raziskovalna Mreža Slovenije, ARNES)[8]	-	pracoviště standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích	ne
Spojené království	19	17	tuto roli splňuje GOVCERT (založený roku 2007)	vládní subjekty	vedle toho v zemi existuje dalších 18 subjektů, plnících funkci CERT pro určité klienty (MODCERT pro armádu, další pro konkrétní operátory, univerzity, zákazníky soukromých firem či výzkumných ústavů)	pracoviště GOVCERT standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích	ano (začátek roku 2007)
Španělsko	4	4	ano (IRIS, od roku 1995)	původně akademické subjekty, časem převážili správci domén (kteří nezřídka vyšli z akademického prostředí)	v zemi existují i omezenější platformy (UPC – od roku 1994, universita Barcelona; CCN – od roku 2006 – obecní úřady; INTECTO – od roku 2007, soukromé firmy)	o produktech firmy a incidentech, které s nimi souvisí, je informováno jen velmi sporadicky, spíše v oblasti všeobecných rad; za zmínku stojí i skutečnost, že mezi lety 2002 - 2005 Ministerstvo pro veřejné záležitosti začalo plošně užívat LINUX (namísto dosavadní platformy SOLARIS)[9]	připravuje se
Švédsko	3	3	tuto roli nejlépe splňuje SITIC (založený roku 2003)	vládní a nevládní sektor (realizační tým stojí na základech akademického sektoru, stejně jako zde působí konkrétní soukromé subjekty: operátoři, provideři, asociace výrobců)[10]	v zemi existuje ještě akademická platforma SUNET (od roku 2000) a TSCERT (telekomunikační firma Telia, od roku 1997)	nepodařilo se zjistit	ne
Švýcarsko	5	4	ne	-	v zemi existuje pět platforem, omezených na konkrétní klientelu (zákazníci telefonních firem a operátorů, jaderný výzkum atd.)	nelze v konečném důsledku zjistit, konkrétní platformy nejsou neautorizovaným subjektům přístupné	ne

[8] http://www.cert.si/
[9] http://www.advogato.org/article/524.html
http://ec.europa.eu/idabc/servlets/doc?id=22054
[10] http://www.sitic.se/ (presentace CERT-SE)

Turecko	2	0	ne	-	v zemi existuje platforma TR-CERT (od roku 2003), sloužící vládním a vojenským strukturám[11] a akademická struktura ULAK (od roku 2007)	platforma ULAK standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích	ne
Ruská federace	2	1	ano (RU-CERT, od roku 1998)	dominantní polostátní telekomunikační společnost	vedle toho existuje omezenější soukromá platforma WEBPLUS (od roku 2000)	obecně jsou vztahy Ruské federace a firmy Microsoft proměnlivé a do značné míry zpolitizované; otevřeně prezentované snahy o plošné zavedení platformy LINUX ve státní správě Ruské federace (o kterém se hovořilo roku okolo 2003), bylo nahrazeno mnohem vstřícnějšími vztahy s firmou Microsoft; nyní je Microsoft uváděn jako jeden ze sponzorů RU-CERT	ne

[11] Klíčovou roli při zajišťování kybernetické bezpečnosti Turecka sehrávají ozbrojené síly (včetně aspektu financováním laboratoří k testování a auditu informačních technologií). TR-CERT dnes slouží takřka výlučně k monitorování incidentů v rámci vojenské infrastruktury (a jeho provoz je rovněž financován z armádního rozpočtu).