Bezpečnostní týmy v Evropě i ve světě

Zatímco v minulosti byla IT bezpečnost často úkolem jiných oddělení, dnes se vytvářejí samostatná oddělení, která se jí věnují. Jak narůstá důležitost bezpečnosti v elektronických službách, stejně stoupá i nutnost mít bezpečnostní týmy typu Csirt/CERT. Od vzniku prvního oficiálního týmu v roce 1988 se v dané oblasti mnoho změnilo.

ZUZANA DURAČINSKÁ

První CERT (Computer Emergency Response Team) vznikl ve Spojených státech amerických na půdě Carnegie Mellon University jako reakce na prvního „červa“, který výraznějším způsobem zasáhl tehdejší ještě poměrně malou síť, internet.

Důvodem pro vznik tohoto týmu bylo zajistit koordinovanou reakci na vzniklou situaci. A protože se toto řešení osvědčilo, rozhodlo se tým zachovat i pro řešení případných budoucích bezpečnostních incidentů.

Dodnes tato univerzita provozuje jeden z největších bezpečnostních týmů a pravidelně informuje o nových zranitelnostech. Univerzita zároveň drží ochrannou známku pro používání názvu CERT.

Aby o sobě jednotlivé týmy věděly a aby bylo jejich vzájemné kontaktování snadnější, vytvořily se postupně dvě větší organizace sdružující bezpečnostní týmy. Členství v těchto organizacích je dnes také jediným způsobem, jak nezávisle ověřit práci a fungování týmu.

Organizace First

První organizace s mezinárodní působností nese název First. Myšlenka organizace, která by sdružovala bezpečnostní týmy, vznikla v roce 1989, tedy rok po známém červu Morris. Již tehdy bylo jasné, že spolupráce a výměna informací je nevyhnutelná při řešení zranitelností a útoků, které se týkají provozu v rámci internetu.

Vzhledem k tomu, že First vznikal na americké půdě, přirozeně lákal více týmy ze stejného kontinentu. Až do roku 2006 tedy převládal počet týmů ze Severní Ameriky. V roce 2007 se tento trend ale otočil a začaly se co do počtu prosazovat týmy z Evropy.

V roce 2016 už měly evropské týmy převahu nad Severní Amerikou, a to v poměru 152 ku 90. Celkově má organizace First v současnosti 369 týmů ze 79 států světa. Co se týče skladby týmů, mnoho z nich je produktových, dále jsou ve značné míře zastoupené i týmy s národní působností v jednotlivých státech.

Pro členství v organizaci First musí jiný člen vykonat fyzickou kontrolu a audit práce týmu, který se o členství uchází. Tím se zabezpečí, že všechny týmy splňují minimální požadavky na členství, zároveň to umožňuje udržet profesní úroveň členské základny.

Hodnoceny jsou proces zpracování incidentů, vzdělanostní úroveň členů týmů, finanční prostředky na jeho provoz, fyzické zabezpečení pracoviště a tak dále.

Skupina Csirt

Druhou skupinou sdružující bezpečnostní týmy je TF-Csirt (The Task Force on Computer Security Incident Response Teams). Působí pod organizací Geant, jež poskytuje e-infrastrukturu pro vzdělávací a výzkumné instituce. První setkání této skupiny se konalo až deset let poté, co First již fungoval.

Cílem zakladatelů této druhé organizace bylo vytvořit podmínky pro bližší spolupráci mezi evropskými bezpečnostními týmy. Na těchto setkáních se probíraly služby, které by se členům měly poskytovat, a fungování této skupiny pod organizací Terena (dnes Geant).

Prvního oficiálního setkání se účastnili reprezentanti z 26 evropských týmů. Na rozdíl od Firstu vznikal TF-Csirt z určité členské základny. Již v roce 2001 měl přes 50 členů, přičemž většinu tvořily akademické týmy.

Ze zápisků z tehdejších setkání se lze dozvědět, že důvodem vzniku další organizace na lokální evropské úrovni byly požadavky na větší lokální obsah a zároveň narůstající členská základna Firstu, která způsobovala, že členové měli větší problém navázat bližší vztahy s jednotlivými týmy.

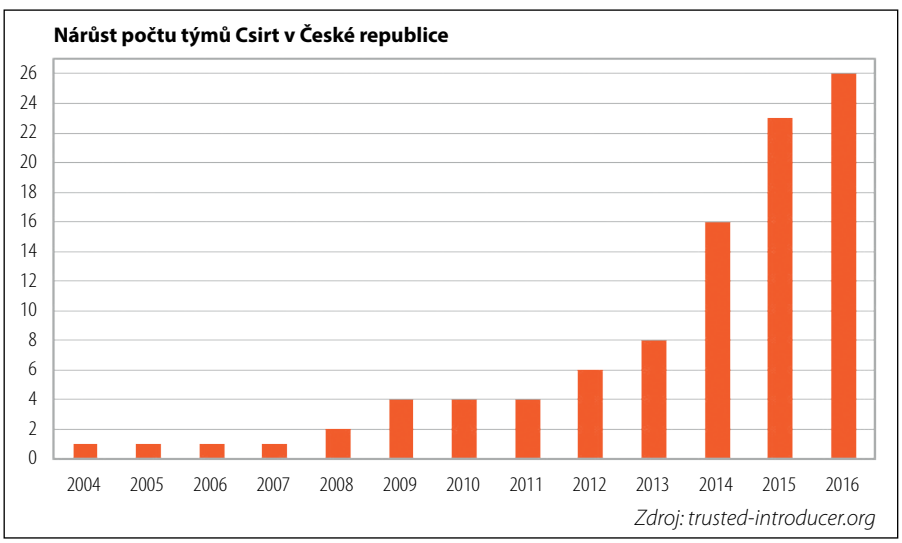
Co se však mezi rokem 2000 a současností změnilo ohledně členské základny a účastníků na pravidelných setkáních pořádaných třikrát ročně, je skladba týmů. V této skupině provozované organizací se zaměřením na vědu a výzkum výrazně stoupá od roku 2012 počet týmů z komerčního sek-

Počet bezpečnostních týmů podle zařazení do oblasti působení

Výzkum a vzdělávání	3
Poskytovatel internetu	18
Finanční sektor	1
Komerční organizace	5
Poskytovatel informačních služeb	4
Národní působnost	1
Vládní organizace	2
Nezisková organizace	1

Poznámka: Oblastí zaměření může být více

Zdroj: trusted-introducer.org



Zdroj: trusted-introducer.org

toru a od roku 2014 již začínají převládat nad akademickými týmy.

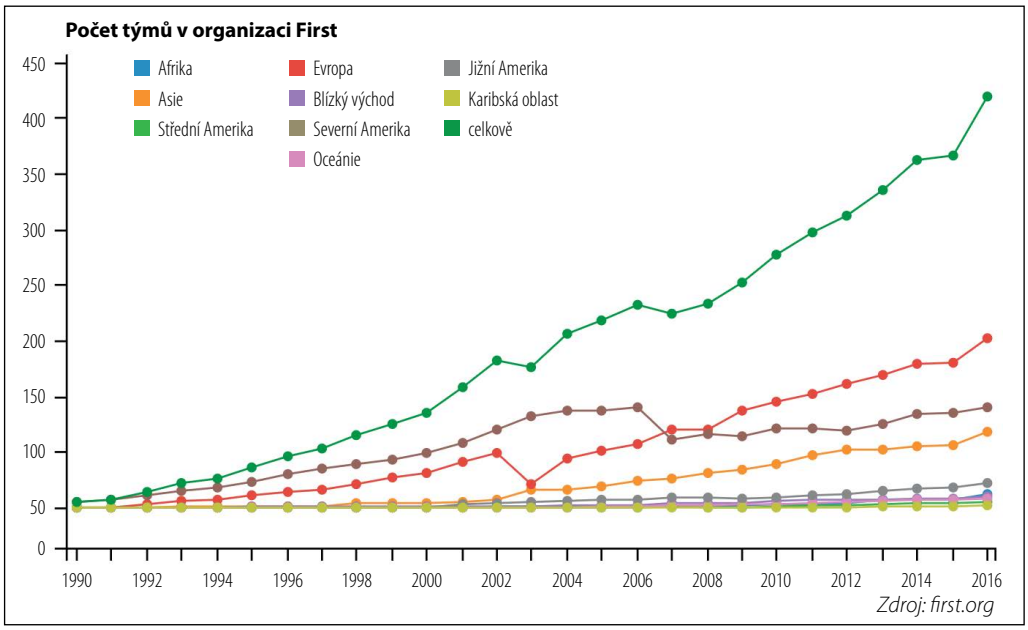
Na rozdíl od organizace First jsou zde oddělené tři úrovně členství, které se odlišují způsobem ověření práce týmů a následně členským poplatkem. Nejnižší status, tzv. listed, je bezplatný a pro jeho získání stačí podpora dvou akreditovaných týmů a vyplnění formuláře s informacemi o týmu.

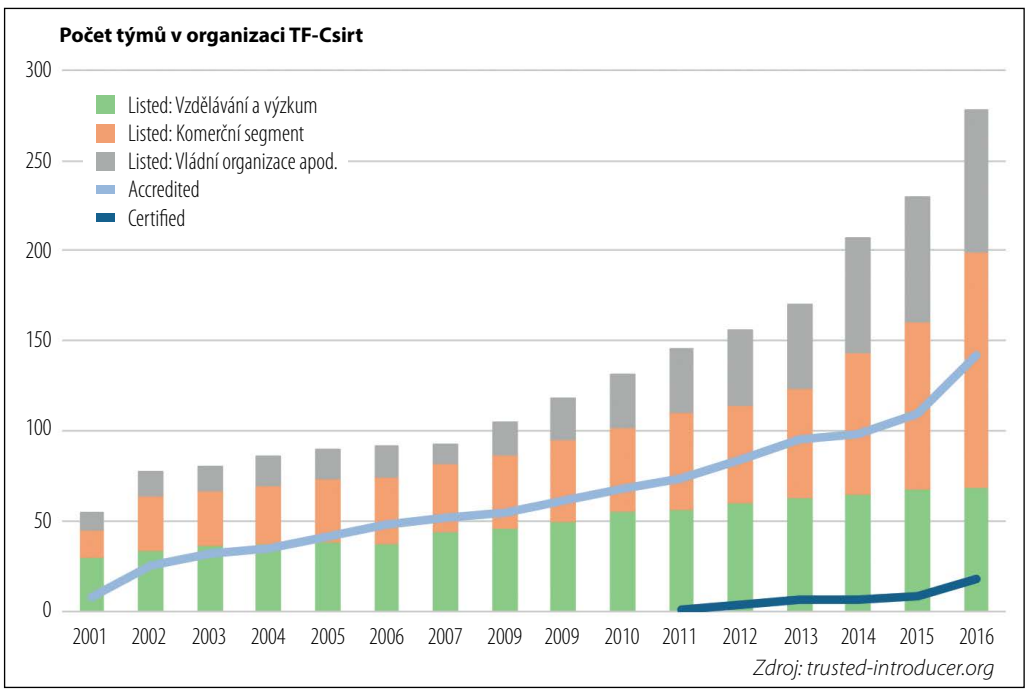
Nasleduje status „accredited“, který vyžaduje hlavně vyplnění formuláře v RFC 2350 popisujícího „best practice“ práce bezpečnostních týmů typu Csirt. Tento status je už zpoplatněný sumou 1 200 eur ročně.

Poslední úroveň členství je „certified“. Ta už vyžaduje splnění různých parametrů ve čtyřech oblastech: organizace, lidské zdroje, nástroje a procesy.

Certifikace se bere jako jeden ze způsobů externího auditu práce bezpečnostního týmu a je zpoplatněná. Vzhledem k nákladnosti a složitosti prošlo certifikací jenom 16 týmů z celkového počtu 289.

Jak TF-Csirt, tak First však kromě členství poskytují také různá školení, pomáhají vytvářet pracovní skupiny pro specifické oblasti, které Csirt týmy spojují, pomáhají vzniku nových týmů, organizují společná setkání a věnují se dalším aktivitám.





Situace v tuzemsku

První Csirt tým na území České republiky vznikl v rámci organizace Cesnet a do skupiny TF-Csirt se zařadil v roce 2004. Nástup dalších týmů byl však velice pozvolný – až v roce 2008 se přidal další tým, který shodou okolností také začalo provozovat sdružení Cesnet.

Tentokrát šlo o tým s národní působností, který pak přešel pod sdružení CZ.NIC, správce domény.CZ, a dodnes plní funkce národního CSIRT týmu, které byly v mezičase formálně zapsané v zákoně o kybernetické bezpečnosti.

Ve stejném roce se přidal interní tým sdružení CZ.NIC. V roce 2009 se pak staly členy týmy Masarykovy univerzity a Vysokého učení technického v Brně.

Týmy za Českou republiku sdružené ve skupině TF-Csirt tvořily až do roku 2011 výlučně skupiny z akademického a neziskového sektoru. Na celoevropské úrovni se k tomu přidávaly také týmy s národní a vládní působností, vytvořené ve státním sektoru.

Od roku 2011 se tento trend začal měnit a dnes tvoří akademické týmy v TF-Csirt na evropské úrovni jenom zhruba jednu pětinu z celkového počtu, v České republice jsou to dokonce jenom tři již zmíněné týmy ze současných 26 členů.

Co se týče celkového počtu týmů sdružených v TF-Csirt a v příslušné službě Trusted Introducer, Česká republika se řadí mezi státy s největším počtem oficiálních bezpečnostních týmů. Výrazný nárůst počtu týmů nastal v průběhu roku 2014 a pak v následných letech.

Jedním z důvodů vzestupu počtu členů byly DDoS útoky z března 2013, které také vedly ke vzniku projektu Fenix (provozuje sdružení NIX.CZ). Právě jednou z podmínek připojení se do tohoto projektu je vytvoření oficiálního Csirt týmu, který bude schopen v případě většího útoku rychle reagovat na vzniklou situaci.

Postupně se však přidávají týmy i z jiných soukromých společností a ustanovení oficiálního Csirt týmu se stává konkurenční výhodou a projevem systematického přístupu k řešení bezpečnostních otázek. ■

Autorka pracuje jako bezpečnostní analytička sdružení CZ.NIC, které provozuje Národní bezpečnostní tým Csirt.cz