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

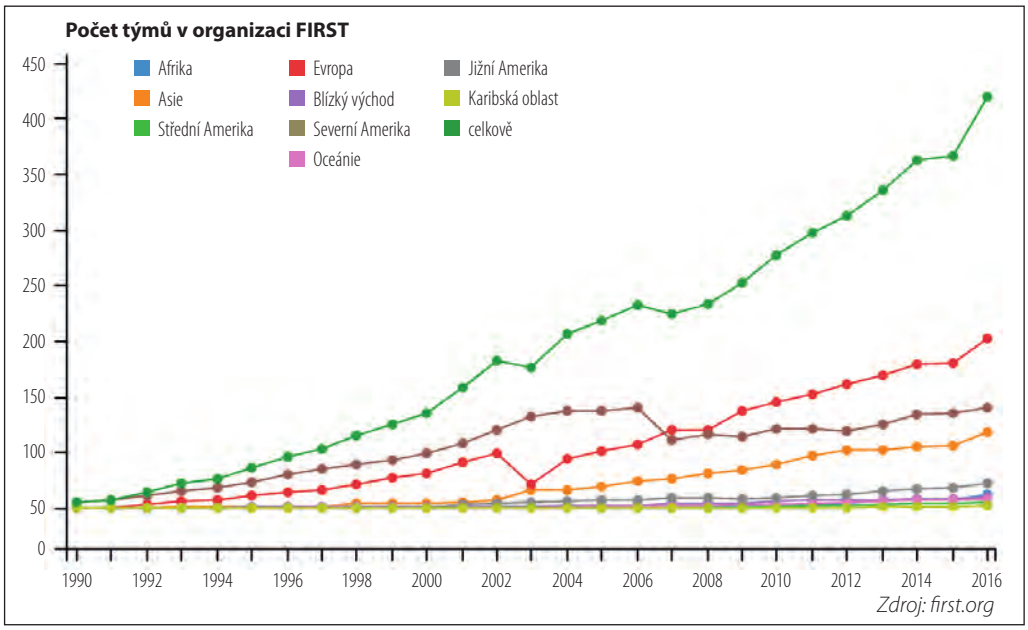
Na rozdíl od organizace FIRST jsou zde oddělené tři úrovně členství, které se odlišují způsobem ověření práce týmů a následně členským poplatkem. Nejnižší status, tzv. listed, je bezplatný a pro jeho získání stačí podpora dvou akreditovaných týmů a vyplnění formuláře s informacemi o týmu.

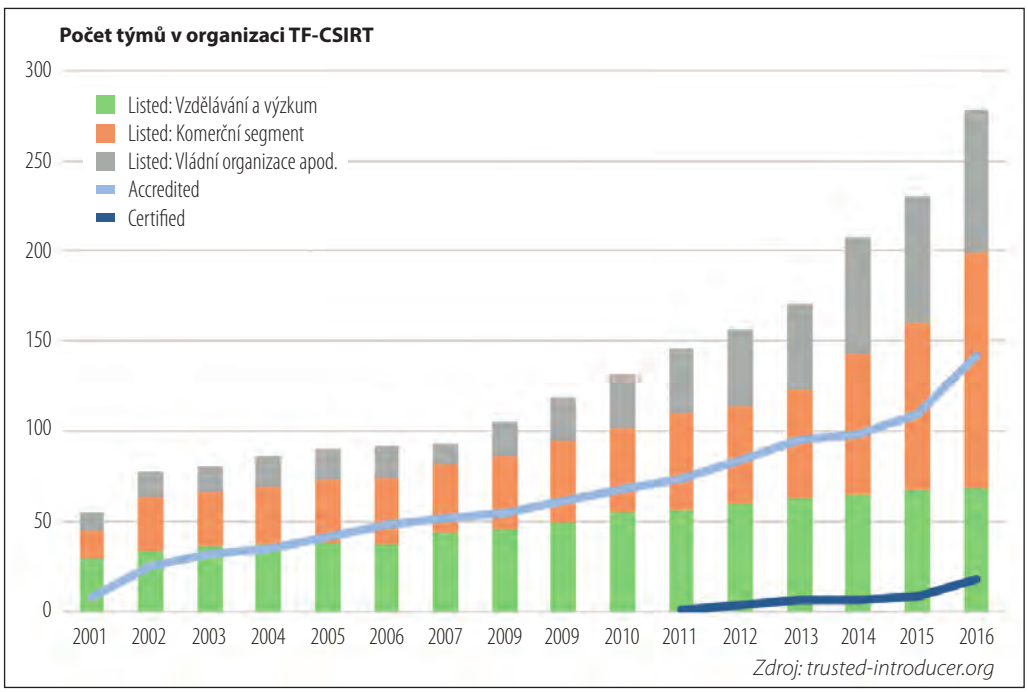
Nasleduje status „accredited“, který vyžaduje hlavně vyplnění formuláře v RFC 2350 popisujícího „best practice“ práce bezpečnostních týmů typu CSIRT. Tento status je už zpoplatněný sumou 1 200 eur ročně.

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