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.

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

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-