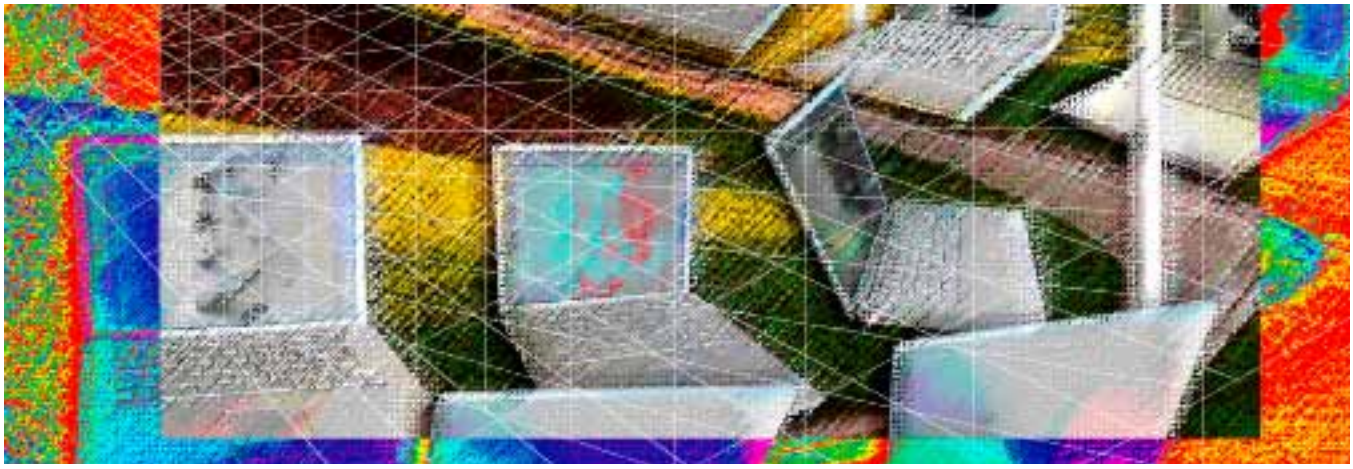

Tým CSIRT.CZ

Bezpečnost je vždy až na prvním místě aneb Role expertních týmů roste

Každá nová technologie v lidské společnosti znamená, že dříve nebo později nevyhnutelně přijdou také pokusy o její zneužití.

Martin Peterka

Podobně tomu bylo v případě počítačových sítí v osmdesátých letech dvacátého století, kdy vznikly první exempláře malwaru – škodlivého softwaru, sloužícího k různým účelům od vlastního pobavení programátorů až po závažnější případy snahy někoho poškodit či zcizit citlivé informace. První zaznamenaný případ masově se šířícího malwaru, který v prosinci 1987 napadl celosvětovou síť VNET, společnost IBM ještě zametla pod koberec. Jednalo se o takzvaného počítačového červa, který se replikoval rozesíláním na všechny e-mailové kontakty příjemce a ochromil řadu mezinárodních sítí.

Útok a organizovaná kyberobrana

O necelý rok později, v listopadu 1988, byl spuštěný první malware šířený po internetu. *Morrisův červ*, původně zamýšlený jako studentský test bez úmyslu škodit, se kvůli chybě v programu velmi agresivně množil a většinu napadených počítačů zpomalil k nepoužitelnosti. Tvůrce programu, Robert Morris, byl obžalován a odsouzen za porušení zákona o zneužití výpočetní techniky. Po odvolání mu byl vyměřen trest v podobě finanční pokuty a čtyři sta hodin veřejně prospěšných prací. Morrisovu programu se také někdy přezdívá *Velký červ* kvůli zničujícímu dopadu, jaký šíření software mělo na tehdejší internet. Podle dobových odhadů bylo napadeno šest tisíc počítačů s operačním systémem UNIX, tedy zhruba deset procent všech přístrojů připojených k internetu. Finanční újma dotčeným společnostem se podle některých odhadů mohla pohybovat v řádu milionů dolarů. Zjevná zranitelnost světového počítačového systému při napadení *Morrisovým červem* vedla americké ministerstvo obrany k myšlence založit speciální útvar počítačové bezpečnosti. Ještě v listopadu vzniklo také první koordinační centrum CERT (Computer Emergency Response Team) při Carnegie Mellon University v Pittsburghu, které dodnes funguje. Zodpovědnost za kybernetickou bezpečnost Spojených států vzal v roce 2003 na svá bedra tým US-CERT (United States Computer Emergency Readiness Team), operační odnož amerického ministerstva vnitra, která pracuje dvacet čtyři hodin denně.

Po zkušenostech s prvními útoky koncem osmdesátých let se v dalších zemích začaly po vzoru CERT vytvářet organizace s úkolem reagovat na ohrožení kybernetické bezpečnosti v jednotlivých národních internetových doménách. Obecně se nazývají CSIRT – Computer Security Incident Response Team. Vzhledem ke globální provázanosti jednotlivých počítačových sítí je mezinárodní spolupráce CSIRT týmů jedním z hlavních předpokladů jejich efektivity. V rámci Evropy je platformou pro pravidelná setkávání zástupců týmů CSIRT pracovní skupina TF-CSIRT, jejíž vznik iniciovalo a organizuje sdružení TERENA (Trans-European Research and Education Networking Association), evropská mezinárodní organizace podporující aktivity v oblasti internetu, infrastruktur a služeb v rámci akademické komunity. V celosvětovém měřítku má podobnou roli organizace FIRST (Forum for Incident Response and Security Teams).

Počítačová bezpečnost v Česku

První česká jednotka rychlého nasazení pro případ bezpečnostní hrozby počítačových sítí měla své počátky od roku 2004 v rámci sdružení CESNET. V rámci tohoto týmu potom v letech 2007 až 2010 vznikalo i národní pracoviště

CSIRT a k 1. lednu 2011 vznikl na základě memoranda mezi Ministerstvem vnitra oficiální Národní CSIRT České republiky neboli CSIRT.CZ. Jeho provozováním a financováním bylo pověřeno sdružení CZ.NIC, které spravuje národní internetovou doménu nejvyššího řádu .CZ. S platností od 1. dubna 2012 nahradila memorandum s Ministerstvem vnitra nová dohoda uzavřená s Národním bezpečnostním úřadem, který se v říjnu roku 2011 stal gestorem problematiky kybernetické bezpečnosti.

Mezi hlavní úkoly CSIRT.CZ spadá řešení bezpečnostních incidentů vzniklých v počítačových sítích, koordinace jejich odstranění a jejich prevence. CSIRT.CZ je zároveň prostředníkem programu budování pracovišť typu CSIRT v České republice. Jednotlivé týmy kybernetické bezpečnosti v tomto programu pracují nezávisle na CSIRT.CZ. CSIRT.CZ přitom poskytuje nezbytné know-how pro budování nových týmů CSIRT a přispívá k efektivnější spolupráci existujících týmů. Zároveň slouží jako instance „poslední záchrany" v případech, kdy napadená síť nedokáže kontaktovat správce sítě, která je zdrojem útoku, nebo kdy správa dané sítě na hlášení nereaguje.

Útoky na české weby

Činnost týmu pro kybernetickou bezpečnost je v období nízkého rizika pro počítačové sítě laickým okem neviditelná, ale o to víc se ukazuje jeho význam v případě ohrožení. Jednoznačně to ukázaly série útoků na české webové služby začátkem března 2013. Napadení postupně způsobilo nedostupnost významných portálů jako Seznam.cz, zpravodajských serverů (například iDNES.cz, IHNED.cz, Novinky.cz nebo Lidovky.cz), webů telefonních operátorů (Telefónica O2 a T-Mobile) nebo webů bank (ČSOB, Raiffeisen banky, České národní banky, FIO banky nebo České spořitelny, která se dokonce potýkala s výpadkem elektronických obchodních systémů a platebních terminálů). Tým CSIRT.CZ od prvního dne březnových útoků působil jako konzultant pro napadené společnosti, státní správu a veřejnost. V rámci krizového štábu v sídle sdružení CZ.NIC zajišťoval výměnu informací se správci dotčených sítí, koordinoval postup s poskytovateli připojení k internetu a zajišťoval komunikaci s bezpečnostními složkami, Národním centrem kybernetické bezpečnosti při Národním bezpečnostním úřadu, zahraničními partnery a s médii. Zároveň podával spolehlivé informace o útocích společnostem, které se obávaly možných útoků, a preventivně shromažďoval informace o infrastruktuře jejich sítí. Po ukončení útoků celou událost vyhodnotil a podal doporučení, která by měla pomáhat předejít budoucím napadením podobného typu.

Mezinárodní spolupráce

CSIRT.CZ vystupuje vůči jiným státům jako srozumitelný a uznávaný kontaktní bod pro záležitost kybernetické bezpečnosti a aktivně se zahraničními subjekty spolupracuje. Příkladem spolupráce CSIRT.CZ s mezinárodními institucemi je incident z počátku roku 2012, kdy byl tým CSIRT.CZ požádán týmem CERTEU o součinnost při vyšetřování úspěšného útoku na webové stránky oddělení průmyslových rizik společného výzkumného centra Evropské unie. Při tomto útoku došlo k úniku citlivých informací (uživatelských jmen a hesel) a k jejich zveřejnění na serveru Pastebin. Tým CSIRT.CZ dohledal příslušné kontakty na uživatele v České republice, jejichž emailové účty byly tímto způsobem kompromitovány, a všem těmto uživatelům rozeslal jak informaci o situaci jejich emailových účtů, tak doporučení ohledně dalšího vhodného postupu při nápravě této situace a prevence dalších případných škod. V říjnu 2012 pak požádal US-CERT tým CSIRT.CZ o pomoc při eliminaci útoku typu DDoS (tedy stejnou techniku útoku jako v březnu 2013 na české weby, kdy útočníci zahltí server takovým množstvím dotazů, že je nezvládá zpracovat) na cíle ve Spojených státech. Část útoků přicházela z IP adres na území České republiky a CSIRT.CZ odhalil řadu zneužitých počítačů.

V zahraničí je CSIRT.CZ dále aktivní zejména zmíněnou spoluprací se sdružením TERENA v rámci platformy TF-CSIRT – mezinárodního fóra umožňujícího spolupráci týmů CSIRT na evropské úrovni. Fórum se dělí na dvě skupiny – uzavřenou, která je přístupná pouze akreditovaným týmům, a otevřenou, do které mohou vstupovat všichni zájemci o práci týmů CSIRT. Pracovní skupina TF-CSIRT se obvykle schází několikrát ročně. Osvětová činnost CSIRT.CZ v rámci Akademie CZ.NIC zahrnuje zejména sérii školení Svět Internetu a domén primárně určených zaměstnancům státní správy a členům bezpečnostních složek České republiky. Kurzy jsou koncipovány jako základní exkurs do fungování internetu a speciální pozornost je věnována praktickým záležitostem z oblasti počítačové bezpečnosti, které pomohou zejména vyšetřovatelům Policie České republiky zorientovat se v základních typech počítačové kriminality a znát konkrétní subjekty, na které se mohou při práci obrátit.

Zájemci o činnost CSIRT.CZ mohou sledovat aktivity organizace na jejím webu **www.csirt.cz**, kde jsou zároveň v sekci novinek shromažďovány nejzajímavější aktuality z oblasti kybernetické bezpečnosti. CSIRT.CZ zároveň ke své činnosti vydává výroční hodnotící zprávy a informuje o ní také sdružení CZ.NIC na svých webových stránkách a blogu **blog.nic.cz**. ■

Jak postupovat při hlášení incidentů

Pokud máte podezření na počítačovou kriminalitu (například při příchodu nevyžádané pošty nebo podvodných e-mailů, při nestandardním chování počítače, automatickém přesměrování na podvodné weby nebo nelegální obsah), vždy se obraťte na vašeho správce počítačové sítě. Kontakty na CSIRT.CZ nejsou určeny koncovým uživatelům! Pokud jste správcem sítě a identifikované potíže přetrvávají, nejsou řešitelné vašimi zdroji nebo jsou závažného charakteru, incident nahlaste na adrese **abuse@csirt.cz**. Tipy na vhodnou formu a obsah hlášení najdete na webu CSIRT.CZ.

Martin Peterka působí ve sdružení CZ.NIC a je vedoucím bezpečnostního týmu CSIRT.CZ.