Výroční zpráva Oddělení bezpečnosti datové sítě ÚVT MU 2012

14. 3. 2013

Přehled činností zajišťovaných pro MU týmem CSIRT-MU

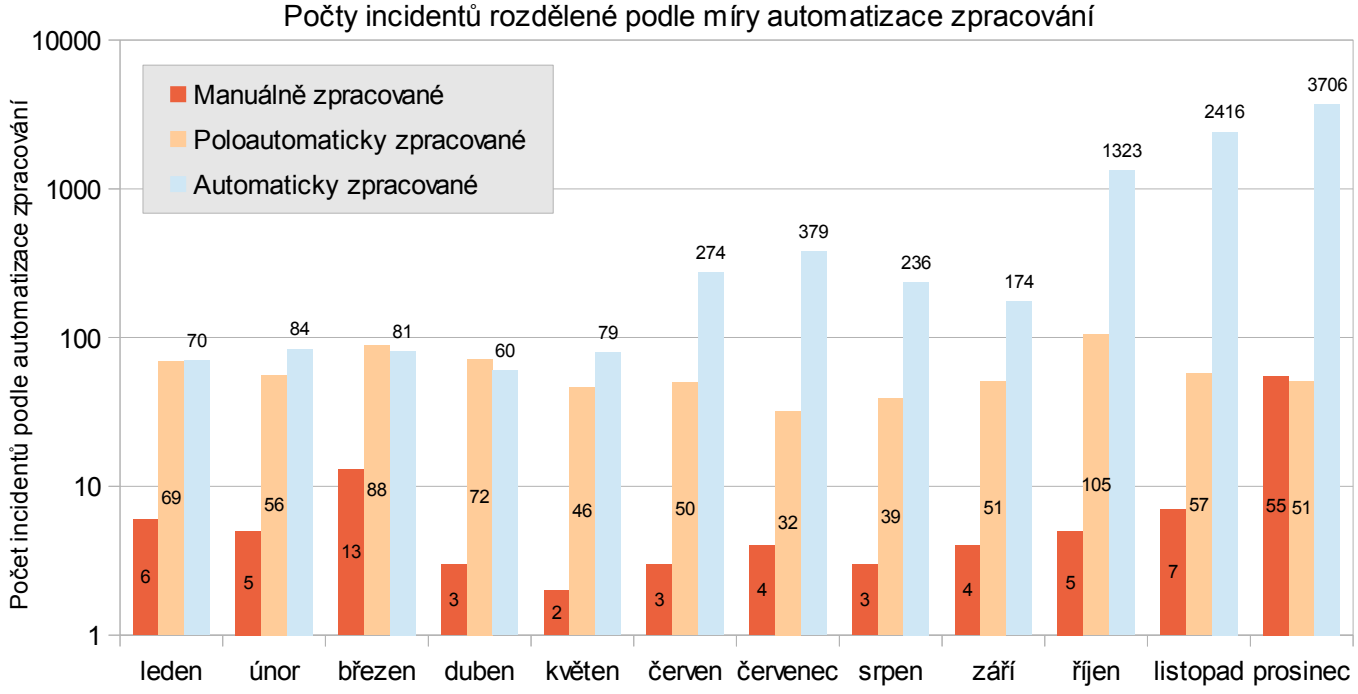
- **Koordinace řešení** počítačových bezpečnostních incidentů pro celou síť MU pomocí ticketovacího systému RT.
- **Monitorování síťového provozu** MU pro bezpečnostní a provozní účely a z toho plynoucí **automatická detekce** počítačových bezpečnostních incidentů analýzou síťového provozu.
- **Vzdělávání** nejen univerzitních správců, ale i koncových uživatelů v oblasti bezpečnosti; informování o aktuálních hrozbách a útocích.

Provozní činnosti CSIRT-MU

Obsluha bezpečnostních incidentů v síti MU

V průběhu roku 2012 se podařilo prohloubit zapojení automatizovaných procesů sloužících ke zpracování nejčastěji detekovaných incidentů v síti MU tak, že drtivá většina detekovaných incidentů je nově obsluhována automaticky bez nutnosti manuálního zásahu.

Graf 1. Struktura incidentů řešených v roce 2012



Rozložení řešených bezpečnostních incidentů dle úrovně automatizace ilustruje Graf 1 (nárůst je tak markantní, že bylo nutno v grafu zvolit na ose Y logaritmické měřítko). Tato míra automatizace

procesů umožňuje pokrytí výrazně širšího spektra potenciálních hrozeb v síti bez nutnosti navyšování lidských zdrojů.

V rámci automatizace procesů jsme vyvinuli řadu nástrojů, jež jsou primárně koncipovány tak, aby po nasazení v rámci ticketovacího systému RT fungovaly bez nutnosti lidské rutinní obsluhy. Nově nám tak přibyl například detektor útoků na přihlášení ke vzdálené ploše (RDP), který chrání univerzitní síť před tisíci útoků. V žádném případě by nebylo v lidských silách toto řešit bez dostatečné automatizace.

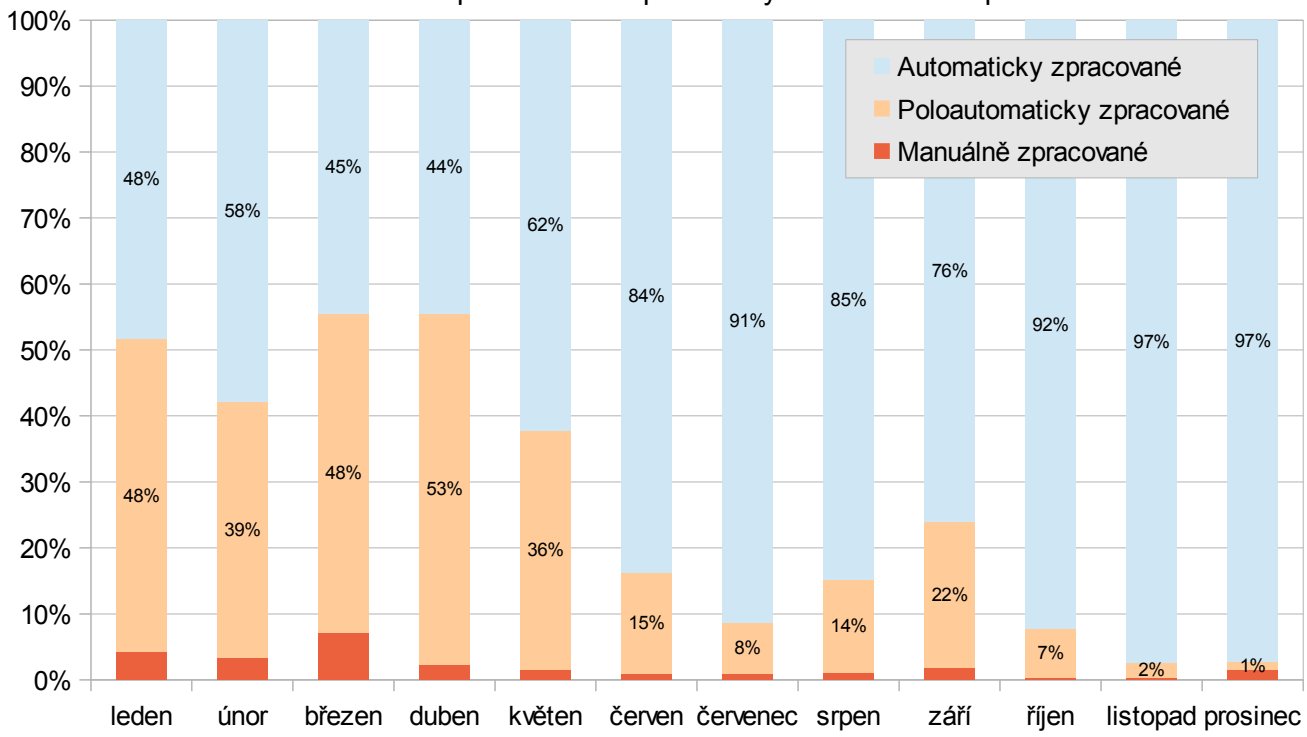
Podobně jsme na základě rozsáhlých zkušeností s časově a kapacitně náročným řešením důsledků úspěšných phishingových útoků v síti MU vyvinuli a nasadili nástroj PhiGARo, umožňující provést celou agendu reakce na phishingový útok, jež dříve zaměstnala jednotky až desítky pracovníků na hodiny práce, pouhým „kliknutím“.

V případě nově nasazeného penetračního testování zranitelných síťových zařízení se nám podařilo identifikovat desítky nezabezpečených tiskáren, z nichž bylo bez jakýchkoliv problémů možno získat informace např. o obsahu tištěných dokumentů.

Graf 2 ukazuje praktickou výhodu nastoleného trendu automatizace, v němž se drtivá většina incidentů zpracovává automatizovaně s využitím připravených nástrojů. Členové týmu tak mohou věnovat více pozornosti negenerickým a složitým incidentům.

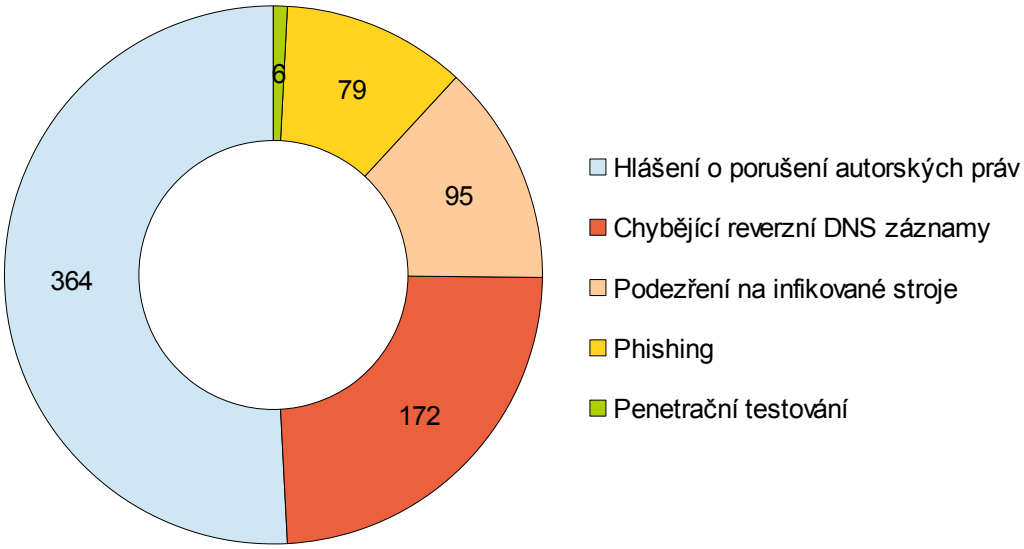
Graf 2. Trend automatizace zpracování incidentů v roce 2012

Poměrné zastoupení incidentů podle míry automatizace zpracování

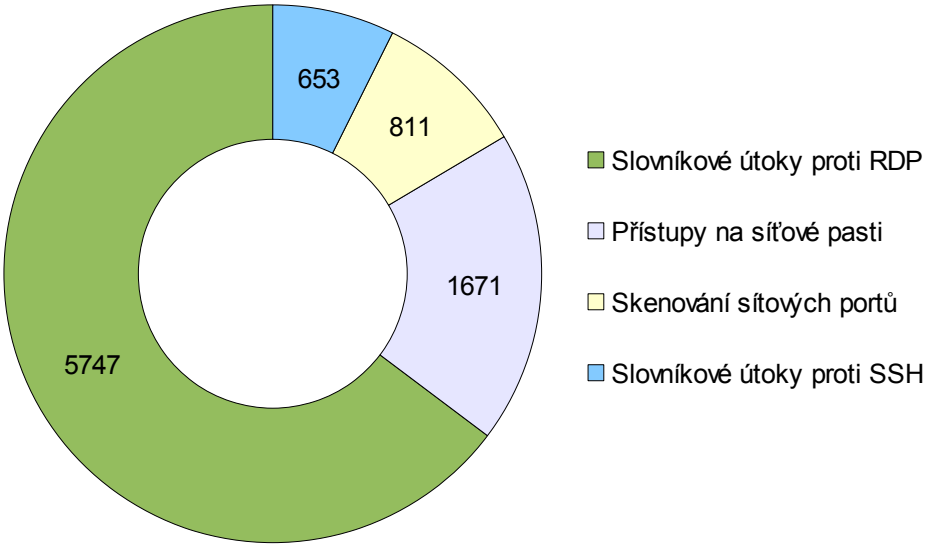


Tým CSIRT-MU řešil a zpracoval celkem 9708 hlášení unikátních bezpečnostních incidentů týkajících se sítě MU. Nejvýznamnější část představují právě detekce, které tým v minulosti z kapacitních důvodů nemohl provádět a zpracovávat. Typy incidentů s ohledem na automatizaci zpracování ilustrují Graf 3 a Graf 4.

Graf 3. Rozložení typů poloautomaticky zpracovaných incidentů



Graf 4. Rozložení typů automaticky zpracovaných incidentů



Útoků proti síťové infrastruktuře nebo službám neustále přibývá, proto tým nadále pracuje na pokrytí ještě většího spektra potenciálních hrozeb s maximálním ohledem na automatizaci zpracování. Činnost jednotlivých pracovníků se tak přenáší z běžné manuální obsluhy e-mailových hlášení do roviny vývoje nástrojů s vysokou přidanou hodnotu právě v oblasti detekce a zpracování počítačových bezpečnostních incidentů. Tento trend v neposlední řadě vytváří prostor pro zapojení studentů bakalářských a magisterských programů informatických oborů, kteří se mohou účastnit nejen vývoje specializovaných nástrojů, ale dokonce i samotných detekčních mechanismů. Získávají tak neocenitelné zkušenosti a praxi v každodenní realitě ochrany počítačové sítě.

Vzdělávací a jiné aktivity

Tým CSIRT-MU vnímá rozšiřování povědomí o základní počítačové bezpečnosti jako jednu ze svých priorit. V roce 2012 proto uveřejnil na svém webu https://security.ics.muni.cz řadu především interaktivních materiálů nejen pro studenty a běžné uživatele, ale i odborné texty a doporučení pro samotné správce služeb provozovaných v síti MU. Na webu byl uveřejněn například článek poukazující na atypické zranitelnosti v podobě malých síťových zařízení (tiskáren, webových kamer, atd.) a rady, jak případné slabiny eliminovat. Naproti tomu běžným uživatelům jsme nabídli interaktivní ilustraci typického scénáře phishingového útoku, nebo jsme rozebrali v té době aktuální hrozbu tzv. „ransomware“, který si našel cestu i do prostředí českého internetu.

Tým CSIRT-MU se aktivně zapojil do cvičení mezi světovými CSIRT týmy pořádaného bezpečnostním týmem Carnegie Mellon University. Prostřednictvím fiktivních bezpečnostních incidentů byla analyzována schopnost rychlé výměny dat nutných k eliminaci potenciálních rizik. Bezpečnostní tým musí být připraven na možnost globálního incidentu a musí být schopen rychlé a včasné komunikace s mnoha dalšími týmy, které jsou do řešení incidentu zapojeny. I proto se akcí tohoto typu tým CSIRT-MU účastnil a nadále účastní.

CSIRT-MU v číslech roku 2012

- **9707** bezpečnostních incidentů tým vyřešil v uplynulém roce. Z toho bylo:
  - **8882** vyřešeno plně automaticky,
  - **716** poloautomaticky,
  - pouhých **110** hlášení bylo nutné obsloužit manuálně.
- **5747** zneškodněných útoků na přihlašování ke vzdálené ploše (RDP) vlastním nástrojem RdpMonitor.
- **3160** unikátních uživatelů navštívilo edukační web https://security.ics.muni.cz.
- **1671** útočníků chycených v síťových pastech vlastním nástrojem Honeyscan.
- **1079** uživatelů si na webu https://security.ics.muni.cz ověřilo bezpečnost **7300** hesel.
- **79** vyřešených phishingových incidentů prostřednictvím vlastního nástroje PhiGARo.
- **64** nezabezpečených síťových zařízení (tiskáren, kamer, telekonferenční techniky, …) objeveno v rámci rozsáhlého testu zabezpečení.
- **44** síťových sond monitorovalo každý den provoz **16 500** aktivních strojů v síti MU.
- **poprvé** v historii se tým zapojil do vyšetřování počítačové kriminality s Policií ČR.

Výzkum a vývoj v oblasti síťové bezpečnosti

CYBER – Bezpečnost informačních a komunikačních systémů Armády ČR

V posledním, pátém roce řešení projektu bylo provedeno ověření hardwarové sondy při aktivní obraně sítě prostřednictvím několika testovacích scénářů v laboratorním i produkčním prostředí. Zvláštní pozornost byla věnována útokům odepřením služby (DoS). Dále byl finalizován obsáhlý katalog bezpečnostních hrozeb shrnující současné poznatky i původní výsledky výzkumu a vývoje v oblasti behaviorální analýzy, které vznikly za celou dobu řešení projektu.

Warden

Pracovníci oddělení se přímo podílí na vývoji systému WARDEN, který je určen k jednoduché a rychlé výměně detekovaných hrozeb mezi bezpečnostními týmy v síti CESNET2. Do projektu jsou zapojeny i další akademické bezpečnostní týmy z ČR. V rámci pilotního provozu byly sdíleny vybrané útoky detekované v síti MU a bylo ověřeno, že většina útoků necílí pouze na jednu síť, ale na více členských sítí CESNET2.

Analýza provozu sítě

V rámci výzkumu a vývoje nástrojů pro bezpečnostní monitorování počítačové sítě MU jsme se zaměřili na oblast geolokace IP toků, monitorování HTTP provozu a export dat ve formátu IPFIX (RFC 5101). Věnovali jsme se použití geolokace pro analýzu síťového provozu a detekci anomálií. Programové vybavení pro monitorování HTTP umožnilo rozšířit klasické IP toky tak, aby je bylo možné do budoucna použít pro řešení phishingových útoků vůči uživatelům sítě MU. Vytváření a sběr detailnějších statistik o síťovém provozu si vyžádal přechod na export dat ve formátu IPFIX, kterým bychom chtěli do budoucna nahradit provozně používaný formát NetFlow verze 9.

Nové výzkumné a vývojové projekty

Odborný a vědecko-výzkumný rozvoj bezpečnostního oddělení vyžaduje průběžné zapojování se do národních a mezinárodních projektů. V roce 2012 jsme podali pět návrhů projektů: Czech Cybercrime Centre of Excellence (EU - Cybercrime), Aktuální kybernetické hrozby v České republice a jejich eliminace (MV - Ministerstvo vnitra ČR), Bezpečnost optických prvků v datových a komunikačních sítích (MV), Kybernetický polygon (MV) a Mobilní dedikované zařízení pro naplňování schopností reakce na počítačové incidenty (CIRC) (MO - Ministerstvo obrany). Řešení projektů v případě jejich přijetí je plánované na období 2013-2015.