Výroční zpráva Oddělení bezpečnosti datové sítě ÚVT MU 2011

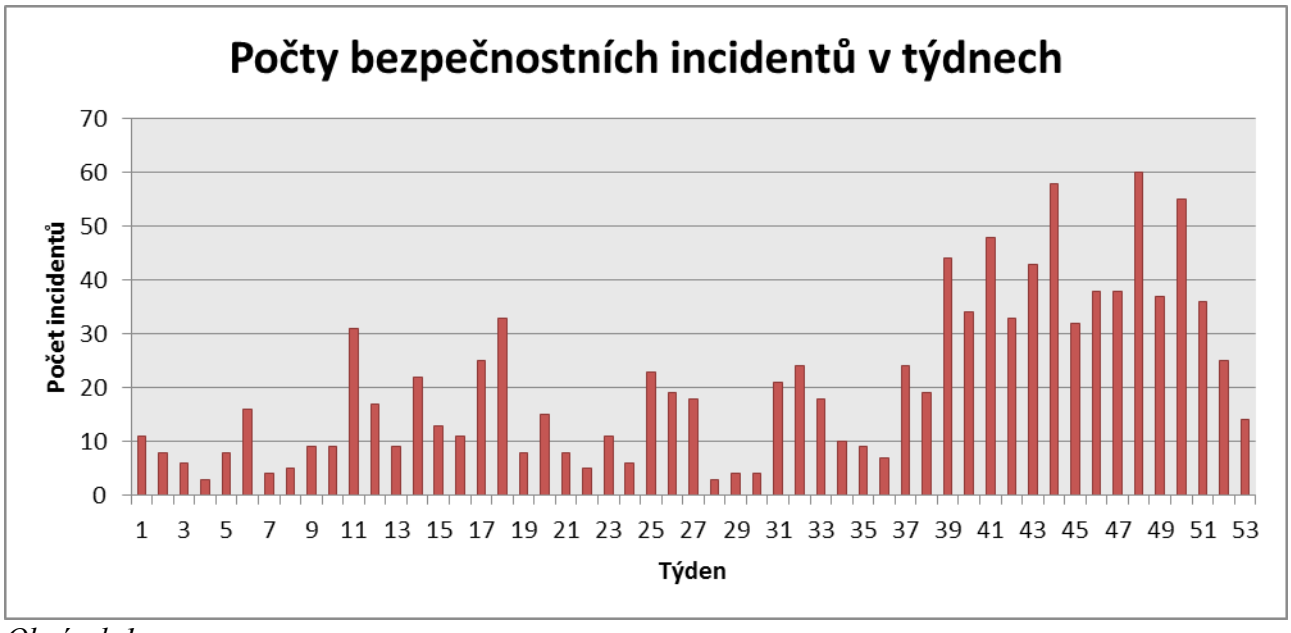
Jan Vykopal, 15. 2. 2012

Přehled činností zajišťovaných pro MU

- Koordinace řešení počítačových bezpečnostních incidentů pro celou síť MU; poloautomatická obsluha kontaktů abuse@muni.cz a csirt@muni.cz založená na požadavkovém systému RT.
- Monitorování síťového provozu Masarykovy univerzity pro bezpečnostní a provozní účely.
- Automatická a včasná detekce počítačových bezpečnostních incidentů analýzou síťového provozu, provoz síťových pastí (tzv. honeypotů).
- Automatická reakce na závažné bezpečnostní incidenty (urgence a blokování zdroje).
- Vzdělávání univerzitních správců IT systémů i koncových uživatelů v oblasti bezpečnosti; informování o aktuálních hrozbách a útocích.

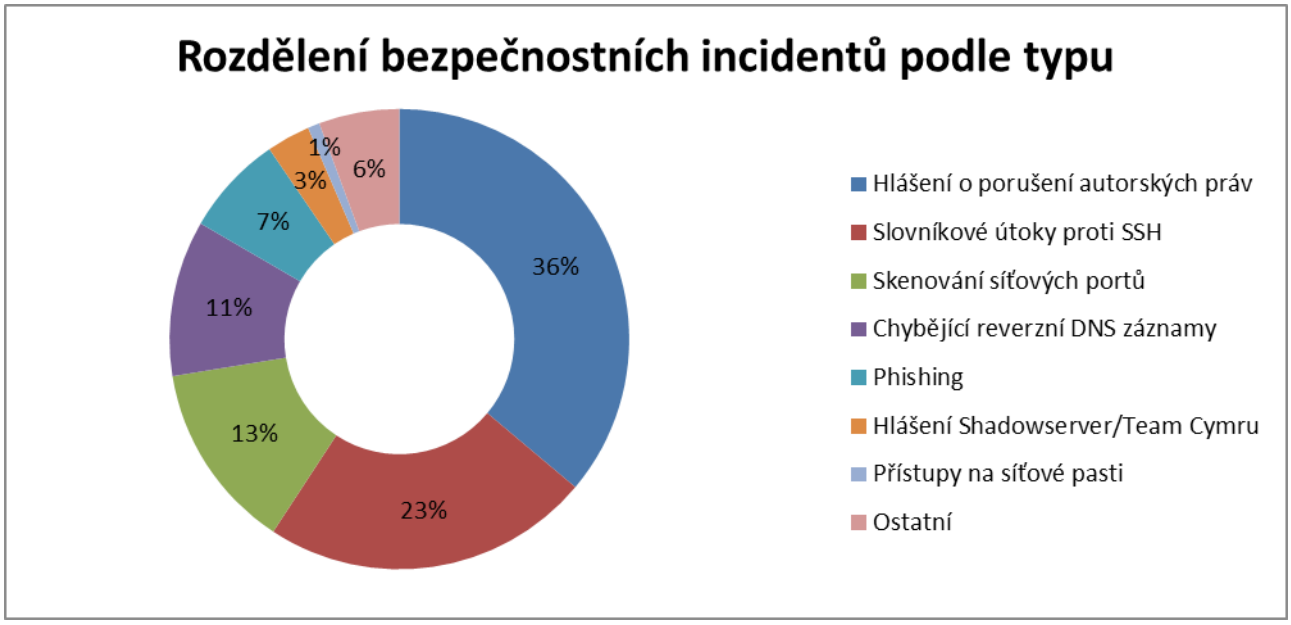
Provozní činnosti CSIRT-MU

Automatizace koordinace řešení bezpečnostních incidentů byla jednou z hlavních aktivit v průběhu celého roku 2011. Podařilo se nám minimalizovat dobu řešení a množství lidské práce potřebné k řešení hlášených incidentů, což umožnilo nasadit nové nástroje detekující dosud nehlášené typy událostí a incidentů. Toto pěkně ilustruje Obrázek 1, kde je vidět nárůst v počtu zpracovávaných hlášení v posledních týdnech roku 2011.



Obrázek 1

V roce 2011 obdržel tým CSIRT-MU celkem 1617 e-mailových hlášení, z toho 1091 vyhodnotil jako hlášení o bezpečnostních incidentech. Poloautomaticky bylo zpracováno 940 hlášení, ručně pouze 151 reportů. Rozdělení incidentů podle typu je uvedeno na Obrázku 1. Největší podíl zaujímají hlášení o porušení autorských práv (zejména sdílení multimediálního obsahu), dále masivní slovníkové útoky proti autentizaci služby SSH a skenování síťových portů. Příchozí hlášení o incidentech pocházela z automatické detekce síťových anomálií (48 %) nebo od třetích stran a univerzitních uživatelů a správců (52 %).



Obrázek 2

Nově jsme nasadili automatickou urgenci hlášení, pokud zodpovědný kontakt na MU neodpovídá včas na hlášení, blokování zdroje incidentů (IP adresy či identity v síti eduroam/VPN) v případě opakovaného či masivního výskytu útoku či nežádoucího provozu a agregaci hlášení vztahující se k jednomu stroji a incidentu.

Na konci roku 2011 bylo v provozu celkem 39 nezávislých síťových sond, které monitorují 10gigabitové přípojky MU do akademické sítě CESNET a provoz všech fakult, důležitých součástí a systémů MU. Tato data jsou použita zejména pro automatickou detekci útoků a podporu řešení bezpečnostních incidentů.

Z preventivních důvodů jsme zaregistrovali a provozujeme doménu mumi.cz, aby tato doména nemohla být využita k útoku (např. typosquattingu) proti prakticky jakýmkoliv službám provozovaným v síti MU a pod doménou muni.cz.

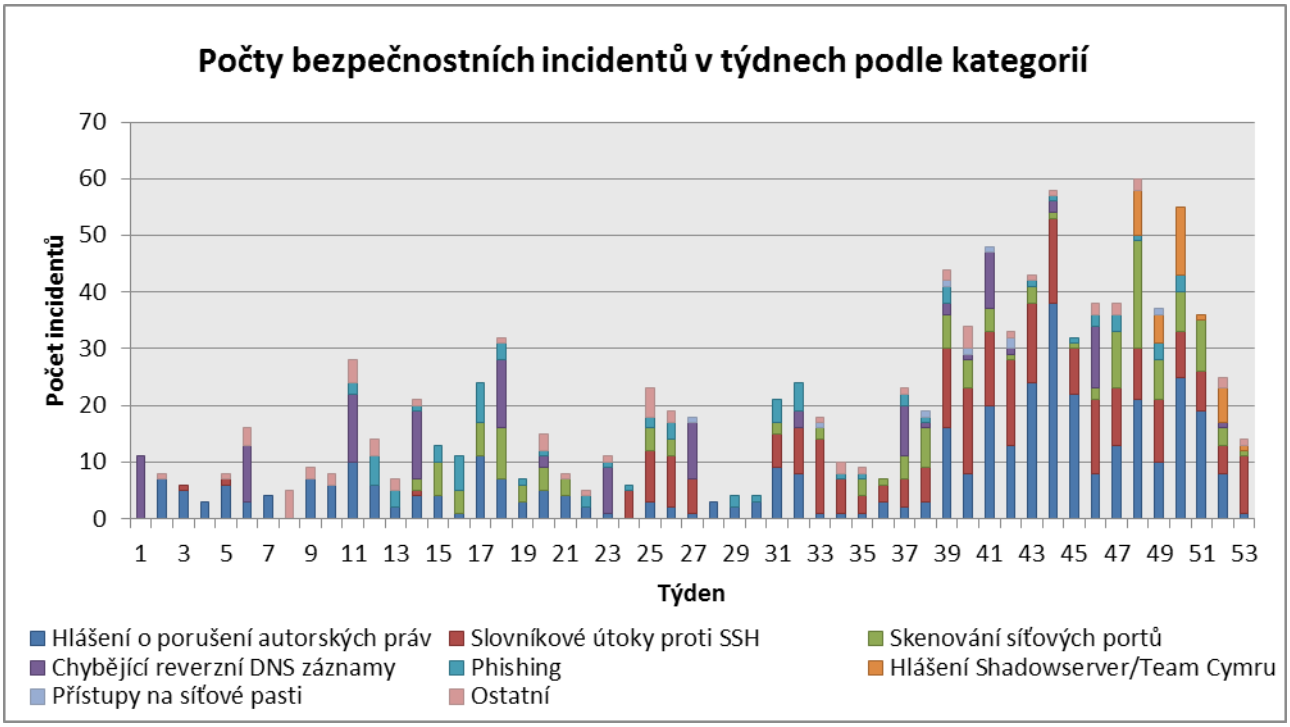
Kromě technické bezpečnosti sítě MU jsme se věnovali i procesní a organizační stránce. Na základě našeho návrhu vstoupila na konci května v platnost Směrnice rektora č. 6/2011 *Správa a užívání počítačové sítě,* která reaguje na podstatné změny v oblasti bezpečnosti ICT od doby vydání předcházející verze směrnice v roce 2003. Následně byl zpracován i výklad směrnice.

Vzdělaní a informování uživatelé jsou spolu s kvalitními technickými prostředky základem bezpečné sítě a v případě některých typů útoků jsou jediní, kteří jim mohou účinně zabránit. Proto byl počátkem roku zprovozněn informační web pro běžné uživatele https://security.ics.muni.cz. Tématicky byl nejprve zaměřen na hrozbu podvodných e-mailů (tzv. phishing). Uživatelé se mohli zapojit do interaktivního školení *Phishing na vlastní kůži,* kde si mohli vyzkoušet, zda dokáží rozpoznat podvodný e-mail od legitimního. Školením prošlo celkem 264 uživatelů (od studentů, provozních pracovníků až po profesory a vedoucí pracovníky). Další významným počinem byla aplikace a článek věnující se odolnosti hesel používaných pro přístup k informačním systémům a službám. Aplikace využívá hesla, která zkoušeli skuteční útočníci při pokusech o průnik do síťových pastí, které taktéž provozujeme. Uživatelé si nechali od konce října prověřit celkem 3245 hesel. Na webu byl publikovány i články o aktuálních útocích, které cílily na univerzitní uživatele, a tipy pro zabezpečení webových serverů pro správce a popis detekčních služeb CSIRT-MU. Články si přečetlo celkem 3690 návštěvníků, spokojenost čtenářů byla velmi vysoká (89 % kladných hodnocení). Nový obsah a způsob informování se osvědčil více než rozesílání pravidelného měsíčního bezpečnostního bulletinu e-mailem, proto jsme ke konci roku 2011 vydali poslední číslo bulletinu a dále budeme využívat převážně web https://security.ics.muni.cz.

V únoru 2011 byl tým CSIRT-MU vůbec jako první univerzitní bezpečnostní tým ze zemí Visegrádské čtyřky akreditován organizací Trusted Introducer, jež sdružuje důvěryhodné evropské bezpečnostní týmy. Akreditace je klíčová pro snadnější a rychlejší komunikaci s ostatními týmy, např. při reakci na vnější útoky proti síti Masarykovy univerzity. Členové týmu se také aktivně zúčastnili setkání pracovní skupiny TERENA TF-CSIRT, která slouží pro výměnu zkušeností a znalostí týkajících se problematiky reakce na bezpečnostní incidenty a síťové bezpečnosti. Tyto aktivity vyústili mj. v navázání spolupráce CSIRT-MU se zahraniční skupinou bezpečnostních profesionálů Team Cymru v podobě výměny dat o infikovaných počítačích.

CSIRT-MU v číslech roku 2011

- 1. univerzitní bezpečnostní tým ze zemí Visegrádské čtyřky, který byl akreditován organizací Trusted Introducer
- 1617 e-mailových hlášení, z toho 1091 hlášení o incidentech
- 940 poloautomaticky zpracovaných hlášení versus 151 hlášení zpracovaných ručně
- 60 řešených incidentů v týdnu na přelomu listopadu a prosince
- 39 síťových sond monitorovalo síťový provoz 15 000 aktivních strojů v síti MU
- 1 schválený návrh novely univerzitní směrnice
- 264 účastníků interaktivního školení *Phishing na vlastní kůži*
- 7121 návštěv z 3690 IP adres vzdělávacího webu https://security.ics.muni.cz
- 1191 uživatelů si nechalo ověřit 3245 hesel v aplikaci na měření síly hesel



Obrázek 3

Výzkum a vývoj v oblasti síťové bezpečnosti

Ve čtvrtém roku řešení projektu *CYBER – Bezpečnost informačních a komunikačních systémů Armády ČR* byl vytvořen koncept aktivní obrany sítě, který využívá předností hardwarově akcelerované síťové sondy. Jde o systém automatické reakce na detekované útoky a události, který má usnadnit a urychlit práci pracovníkům bezpečnostních týmů. Dále byl vytvořen softwarový nástroj pro detekci útoků odepření služby (DoS) monitorováním doby odezvy serverů na síťové požadavky. Zvýšená doba odezvy je následně korelována s dalšími síťovými charakteristikami typickými pro tyto útoky. Dále byla zkoumána detekce síťových anomálií sledováním změn profilů chování jednotlivých zařízení. Také byl proveden srovnávací test dvou různých detekčních paradigmat: detekce anomálií založená na statistických metodách a detekce pomocí komplexních vzorů chování. V neposlední řadě byla objevena a analyzována druhá, vylepšená verze botnetu Chuck Norris, jehož první verze byla objevena v roce 2010.