Výroční zpráva Bezpečnostního oddělení ÚVT MU za rok 2013

Bezpečnostní oddělení provozuje pro Masarykovu univerzitu prostřednictvím bezpečnostního týmu CSIRT-MU dohled nad zabezpečením univerzitní počítačové sítě.

Zkušenosti s provozem CSIRT týmu oddělení uplatňuje i v rámci výzkumné činnosti. V roce 2013 získalo Bezpečnostní oddělení 4 nové výzkumné projekty národního i evropského významu, jejichž řešení dále probíhá a je plánováno až do roku 2015.

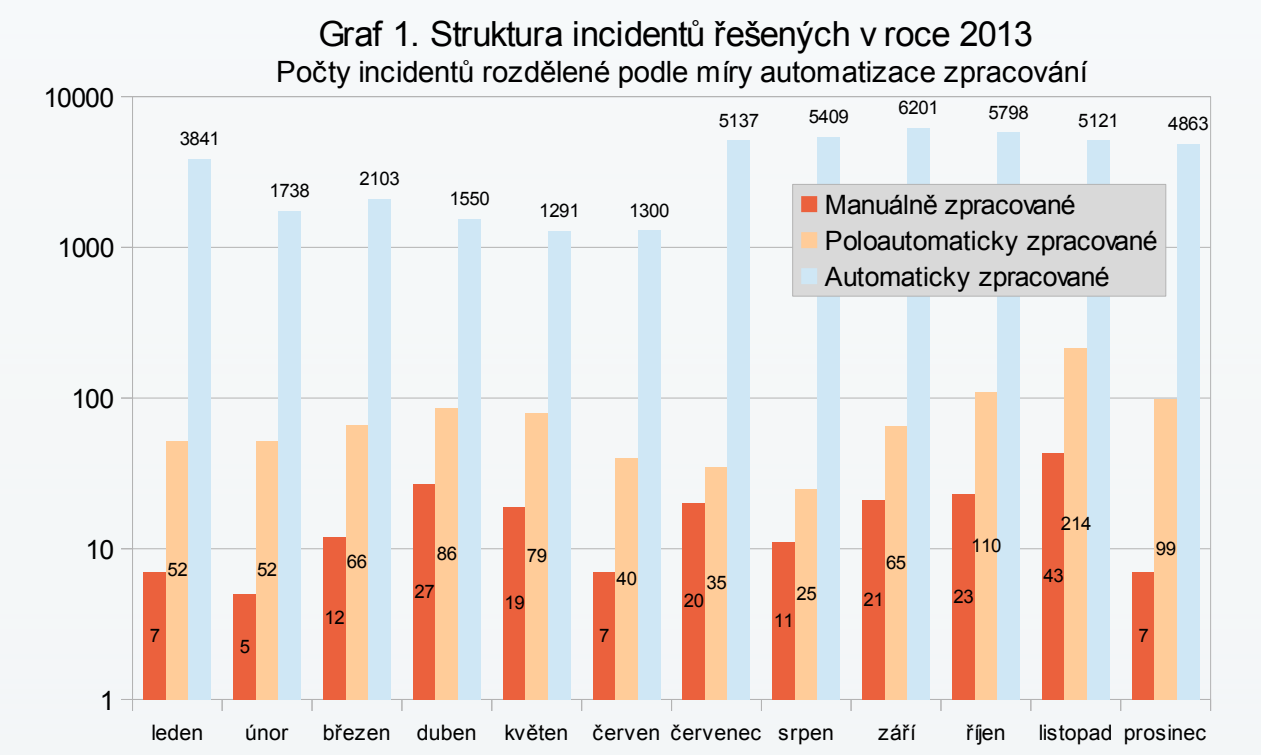
Oddělení se dále angažuje ve výuce a nastavování studijních rámců tak, aby znalosti a zkušenosti, které studenti v rámci studia získají, reflektovaly specifické potřeby bezpečnostních týmů obecně. Členové oddělení vedou bakalářské či diplomové práce a v rámci disertačních prací zkoumají možné cesty dalšího rozvoje počítačové bezpečnosti.

COMPUTER SECURITY INCIDENT RESPONSE TEAM OF MASARYK UNIVERSITY
Ústav výpočetní techniky, Masarykova univerzita, Botanická 68a, 602 00 Brno
web: http://csirt.muni.cz, tel: +420 549 49 4242, fax: +420 549 492 747

Garant bezpečnosti na MU – tým CSIRT-MU

Tým CSIRT-MU dlouhodobě vystupuje v roli centrální bezpečnostní autority sítě Masarykovy univerzity. Vystupuje jako jednotný kontaktní bod v komunikaci s "vnějším" světem, dovnitř univerzity potom jako centrální koordinátor bezpečnosti univerzitní sítě.

Tým provozuje síť tzv. síťových sond, pomocí nichž je schopen zajistit nejen detailní přehled o stavu sítě a o charakteristikách provozu v síti uskutečněného, ale umožňují týmu i nasazení automatizovaných detekčních mechanismů, které odhalují desítky tisíc bezpečnostních incidentů ročně. S důrazem na automatizaci zpracování (Graf 1) je tým schopen při relativně nízkém počtu zaměstnanců obsloužit obrovské množství událostí, které se v síti MU objevují, přičemž je schopen nadále sledovat trendy a vyvíjet či nasazovat nové detekční metody a mechanismy s ohledem na zajištění bezpečnosti univerzitní sítě.



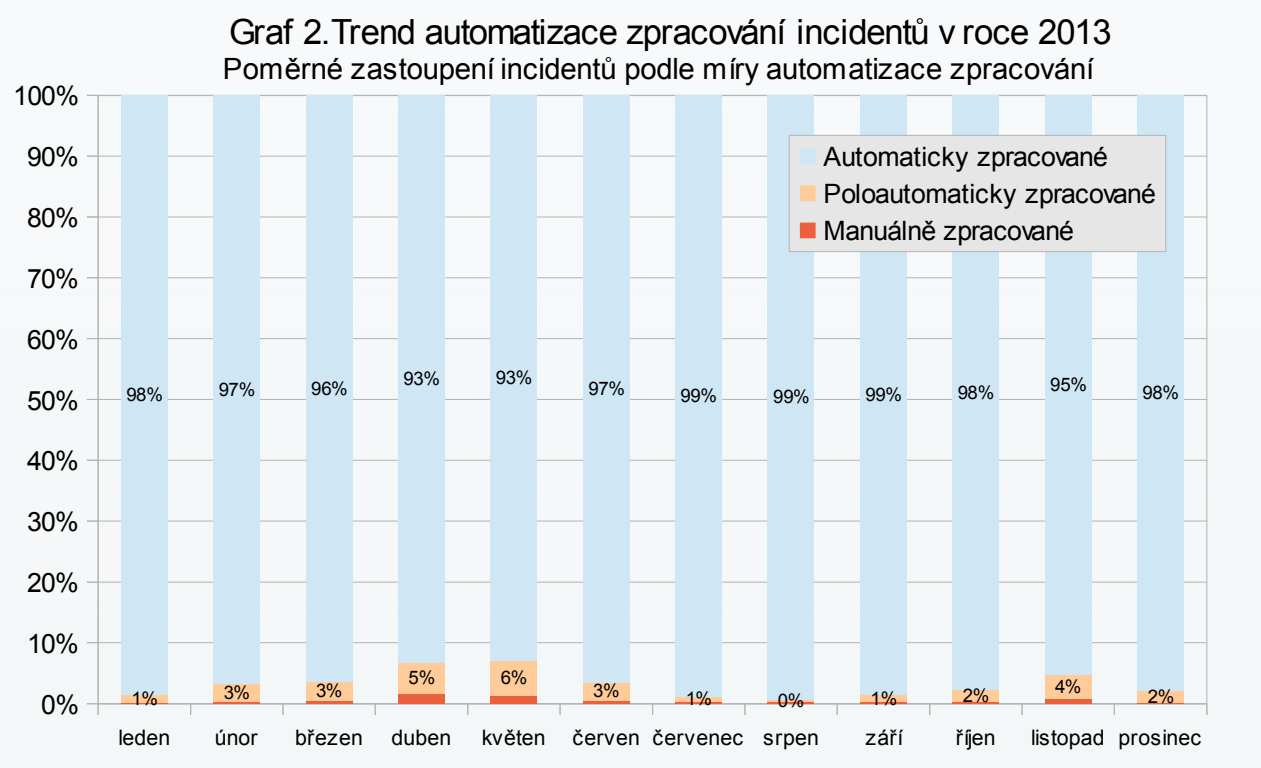
Tým CSIRT-MU se v roce 2013 podílel na řešení v českém prostředí unikátního bezpečnostního incidentu týkajícího se rozsáhlého DDoS útoku proti řadě významných internetových služeb provozovaných v ČR (Seznam.cz, mobilní operátoři, atd.) Členové

týmu se následně aktivně účastnili jednání komise NBÚ shrnující nebezpečí plynoucí z takových útoků a možnosti budoucí prevence. Členové bezpečnostního týmu CSIRT-MU se dále zúčastnili akce Communication Study II, jejímž cílem bylo otestovat připravenost bezpečnostních týmů v otázkách komunikace na nadnárodní úrovni.

Koordinace řešení bezpečnostních incidentů v síti MU

Bezpečnostní oddělení provozuje bezpečnostní tým CSIRT-MU, do jehož hlavních aktivit patří:

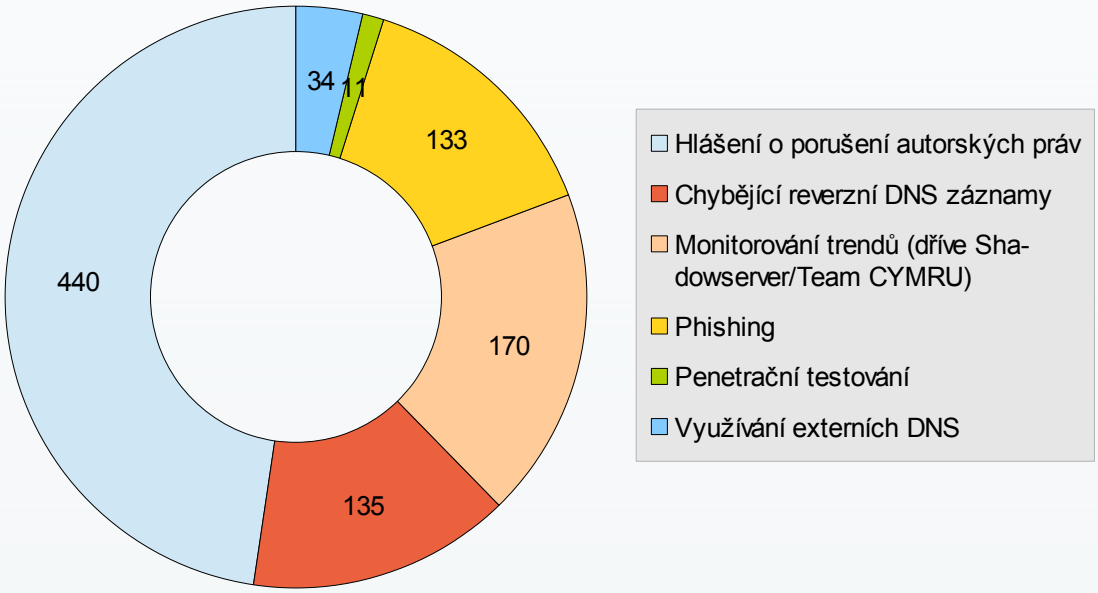
- dohled nad zabezpečením počítačové sítě MU,
- koordinace řešení identifikovaných bezpečnostních incidentů,
- zajištění jednotného komunikačního bodu v síti pro otázky spojené s bezpečností informačních technologií.



Tým klade při aplikaci bezpečnostních mechanismů důraz na co největší míru **automatizace procesů** (Graf 2), která přináší nižší personální náklady ve spojení s větším rozsahem poskytovaných služeb. Současně se snaží nastavit formu spolupráce s lokálními administrátory tak, aby byla jednoduchá, jednoznačná a nespotřebovávala nadbytečné zdroje jak týmu samotnému tak jednotlivým administrátorům.

Aktivní komunikace Bezpečnostního oddělení s administrátorskými týmy vyvrcholila v roce 2013 nasazením **nového schématu hlášení** bezpečnostních incidentů, které jednoznačně odlišuje důležité bezpečnostní incidenty, u nichž se od administrátorů očekává aktivní řešení problému a komunikace s týmem, a měsíční informativně-provozní reportování řady doplňujících informací, jež mohou administrátorům pomoci při správě svěřené sítě, avšak rozsah využití těchto informací je plně v jejich rukou.

Graf 3. Rozložení typů mezi poloautomaticky zpracovanými incidenty



Proces postupné automatizace kroků požadovaných pro úspěšné řešení bezpečnostních incidentů vedl v roce 2013 taktéž k nasazení rozhraní, které umožnilo týmu přímo kontaktovat uživatele kolejních sítí bez nutnosti předávat tyto generické úkony správcovskému oddělení spravujícímu kolejní sítě. Výrazně se tak zkrátila doba nutná k vyřešení incidentů uživatelů kolejních sítí, stejně jako se dramaticky snížila personální náročnost na straně týmu CSIRT-MU i administrátorů těchto sítí.

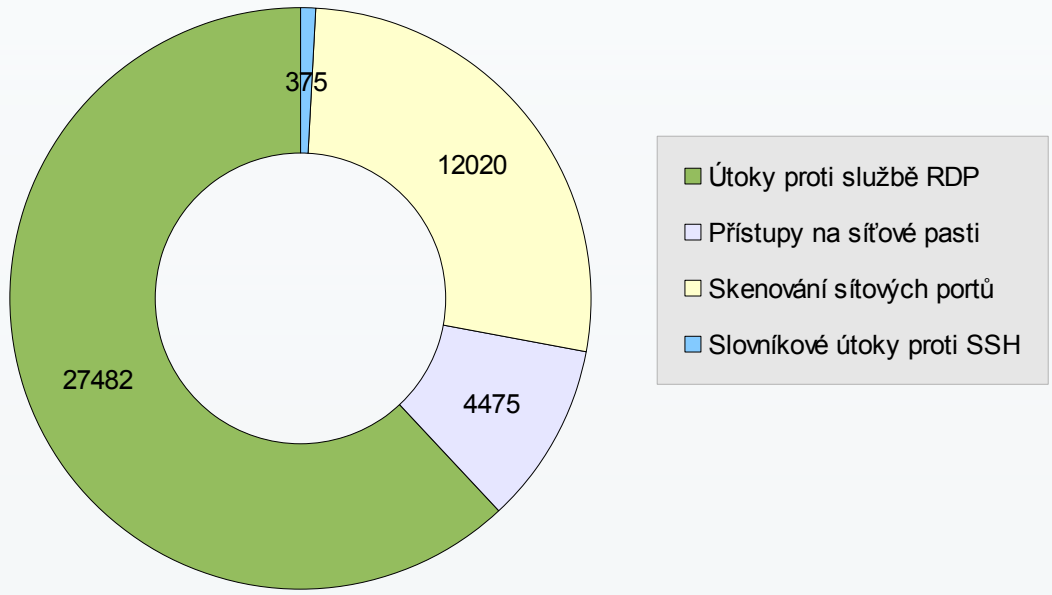
Monitorování sítě MU

Tým CSIRT-MU dohlíží na univerzitní síť prostřednictvím 24 NetFlow sond, pomocí kterých měří a analyzuje provozní charakteristiky procházející komunikace. V roce 2013 došlo k nasazení nejnovější verze síťových sond, které nově umožňují monitorovat širší spektrum potenciálních hrozeb a tím tak dostává do rukou silnější zbraně proti potenciálním útočníkům.

V roce 2013 proběhlo dále nasazení regeneračního TAPu na první ze dvou vstupních bodů do sítě MU, který rozšiřuje a zlepšuje možnosti nasazování nástrojů určených k analýze provozu a detekci bezpečnostních rizik. V závislosti na tomto kroku dojde v roce 2014 k nasazení druhého regeneračního TAPu na druhý vstupní bod.

Dalším přínosem pro tým je i nasazení nového analytického systému pro hlubší analýzu provozu a zlepšení přehled o tom, co se v sítí děje.

Graf 4. Rozložení typů mezi automaticky zpracovanými incidenty



Vzhledem k tomu, že proces detekce anomálií v síťovém provozu je pouze jedna z řady možností využití sesbíraných provozních dat, nabízí tým lokálním administrátorům specifická data týkající se jimi spravované části sítě, provozní analýzy a statistiky a v neposlední řadě připravuje i anonymizovaná data k využití při výuce. Archivovaná provozní data mohou dále, byť ve výjimečných případech, posloužit i při odhalování trestné činnosti.

Rozvoj detekčních metod

S ohledem na stále rostoucí počet potenciálních hrozeb a útoků, které cílí na univerzitní síť, se tým snaží neustále doplňovat portfolio monitorovaných služeb tak, aby maximálně reflektovalo aktuální potřeby sítě (Graf 3 a 4).

Z toho důvodu nasadil tým v úvodu roku 2013 **automatizované testování** špatně zabezpečených **síťových zařízení**, jako jsou např. síťové tiskárny, IP kamery, apod. Problematiku testování špatně konfigurovaných nebo nezabezpečených zařízení umístěných v síti MU vnímá tým jako prioritu, které se bude věnovat i nadále.

Podobně pak členové týmu pracovali i na zpřesnění detekce potenciálních obětí phishingových útoku, které se objevují stále častěji a které pro řadu běžných uživatelů MU (a tedy i pro zdroje a služby na MU) představují významné riziko.

Dále byla nasazena nová služba upozorňující administrátory na bezpečnostní rizika spojená se stroji v jejich správě, které využívající nestandardní nebo špatně nastavené DNS servery.

Vedle vylepšení detekce potenciálních obětí phishingových útoků v síti MU se tým zaměřil i na detekci anomálií v časových řadách reprezentujících síťový provoz. Pro tyto účely vyvinutý nástroj zpřesňuje současné detekční metody a umožňuje detekci nových druhů anomálií v síťovém provozu MU.

Bezpečnostní výzkum a vývoj

Členové Bezpečnostního oddělení řeší celou řadu výzkumných projektů národního a evropského významu. Cílem těchto aktivit je aktivně propojovat provozní zkušenosti nabyté praxí bezpečnostního týmu CSRIT-MU s výzkumem a vývojem v oblasti bezpečnosti informačních technologií, stejně jako zpětně aplikace a ověřování znalostí a technologií získaných v rámci výzkumu do provozních aktivit týmu. Toto rozkročení umožňuje zdaleka nejpřesněji odhadovat žádoucí směry vývoje, držet přímý kontakt s nastupujícími trendy a vyhnout se určitému odtržení od reality, které může hrozit ryze výzkumným týmům. Důkazem toho jsou čtyři aktuální projekty, kterých se členové oddělení účastní. Tým spolupracuje taky s komerční sférou formou smluvního výzkumu, v rámci nějž dostává cennou zpětnou vazbu k vyzkoumaným závěrům z produkčního nasazení v rozličných typech sítí.

Souběžně s výzkumem v rámci projektů se tým snaží rozvíjet i talentované studenty, kterým nabízí, mimo jiného, vedení bakalářských či diplomových prací. U nadějných absolventů je doporučováno (a preferováno) pokračování doktorským studiem a zapojení do výzkumných aktivit Bezpečnostního oddělení.

Kybernetický polygon (KYPO)

web

Projekt bezpečnostního výzkumu Kybernetický polygon má za cíl vytvořit unikátní prostředí pro výzkum a vývoj metod na ochranu proti útokům na kritické infrastruktury. Ve virtualizovaném prostředí bude možno provádět komplexní scénáře útoků vedených proti kritickým infrastrukturám a analyzovat jejich průběh. Prostředí

bude sloužit pro aplikovaný výzkum a ověřování nových bezpečnostních metod, nástrojů a školení členů bezpečnostních týmů. Projekt reaguje na aktuální potřeby Národního bezpečnostního úřadu (NBÚ), rezortu Ministerstva vnitra a vládních a národních bezpečnostních CSIRT týmů.

Czech CyberCrime Centre of Excellence (C4e)

web

Bezpečnostní oddělení spolupracuje s Právnickou fakultou MU, NBÚ a společností Risk Analysis Consultants s.r.o. na evropském projektu Czech Cyber Crime Centre of Excellence. Hlavním cílem projektu je vytvoření kvalitního centra pro školení a vzdělávání v oblasti prevence a represe kybernetické kriminality. Základní cílovou skupinou C4e jsou složky Policie ČR. Centrum je však budováno se záměrem poskytovat služby i pro další cílové skupiny, např. soudy, státní zastupitelstvo, advokacii, státní instituce, privátní organizace a akademickou sféru.

Bezpečnost optických prvků v datových a komunikačních sítích (BOP)

web

V projektu bezpečnostního výzkumu České republiky zadaném Ministerstvem vnitra ČR Bezpečnostní oddělení zkoumá a vyvíjí prostředky k zajištění kybernetické bezpečnosti ve vysokorychlostních sítích. Výstupy projektu budou využity bezpečnostním týmem CSIRT-MU ke zlepšení zabezpečení univerzitní sítě.

Mobilní dedikované zařízení pro naplňování schopností reakce na počítačové incidenty (CIRC)

web

Společně s Fakultou informatiky MU spolupracují členové oddělení na projektu, jehož cílem je vytvořit mobilní dedikované zařízení pro naplňování schopností reakce na počítačové incidenty (CIRC) v informačních a komunikačních systémech provozovaných v rámci operačního taktického systému velení a řízení (OTS VŘ) v polních podmínkách (v misích) a naplnění schopnosti kybernetické obrany v těchto podmínkách. Projekt spadá do jedné z hlavních tématických priorit obranného výzkumu a vývoje Ministerstva obrany ČR.

Osvěta a školení uživatelů

Bezpečnost informačních technologií začíná u samotných uživatelů. Bezpečnostní oddělení se snaží přibližovat univerzitním uživatelům zábavnou formou střípky z oblasti IT bezpečnosti. Za tímto účelem v roce 2013 uveřejnilo na webu https://security.ics.muni.cz tři interaktivní animace ilustrující aktuální problémy sužující běžné uživatele: jak fungují distribuované DoS útoky, čím jsou charakteristické

tzv. botnety a co všechno může uživateli způsobit malware. Vedle těchto animací byli uživatelé informováni o nejzávažnějších zranitelnostech prostřednictvím vývěsky IS MU. Edukačním aktivitám a zvyšování bezpečnostního povědomí vyjádřilo oddělení jednoznačnou podporu účastí v akci Den bezpečnějšího internetu 2013.

Výuka

Provozovat úspěšné a reakceschopné Bezpečnostní oddělení (CSIRT tým) vyžaduje celou řadu specifických dovedností z různých, nejen informatických, oborů. Tuto skutečnost si členové Bezpečnostního oddělení uvědomují a snaží se proto zkušenosti nabyté za 5 let fungování oddělení předávat dál. Podílí se tak například na školení bezpečnostních specialistů Národního centra kybernetické bezpečnosti provozovaného Národním bezpečnostním úřadem (NBÚ). Ve spolupráci s Fakultou informatiky připravují nový obor přímo zaměřený na výchovu specialistů plnohodnotně připravených pro specifické požadavky CSIRT týmů, jejichž důležitost a popularita v posledních letech významně roste.

Stáže pro NBÚ

V roce 2013 uspořádalo Bezpečnostní oddělení pro NBÚ dvě rozsáhlá školení bezpečnostních specialistů. Školení zahrnovalo nejen teoretické studium procesů, jak by měl bezpečnostní tým správně fungovat, ale především praktickou část, při níž účastníci školení "stínovali" pracovníky týmu CSIRT-MU a zblízka se tak seznámili s podstatou práce týmu. Paralelně řešili i úkoly napodobující skutečné problémy, které pracovníci týmu řeší - ať už ty běžné, každodenní, nebo ty výjimečné, s nimiž se oddělení setkává pouze několikrát do roka.

Výuka na FI MU

Členové oddělení se aktivně zapojují do výuky na Fakultě informatiky MU. Provozní praxe členům Bezpečnostního oddělení poskytuje jedinečný pohled na to, jaké znalosti by měli absolventi mít, aby se mohli ucházet o práci v bezpečnostním CSIRT týmu. Na základě této reflexe spolupracuje oddělení s FI MU na vytvoření nového **studijního oboru Kybernetická bezpečnost**, který by měl odrážet aktuální potřeby a trendy v otázkách kybernetické bezpečnosti, bezpečnostních politik, legislativy či manažerských dovedností. Obecně se oddělení podílí na rozšíření portfolia předmětů, které by měly být schopné pokrýt činnost standardního CSIRT týmu.

Národní a mezinárodní spolupráce

Nově se Bezpečnostnímu oddělení v oblasti spolupráce podařilo navázat kontakty s bezpečnostním týmem Ministerstva obrany ČR CIRC-MO, s nímž sdílí vybrané bezpečnostní události a přispívají tak vzájemně k vyššímu zabezpečení obou spravovaných sítí. V květnu 2013 prezentovalo oddělení úspěšný model automatizace správy bezpečnostních incidentů a detekčního nástroje na odhalování phishingových průniků na veletrhu ITTE, v závěru roku se pak podílelo na vzniku studie Detect, SHARE, Protect vznikající pod hlavičkou organizace ENISA a zaměřující se na nejvhodnější metody sdílení dat a komunikaci mezi bezpečnostními týmy.

CESNET-CERTS

Tým CSIRT-MU dlouhodobě aktivně spolupracuje s týmem CESNET-CERTS, bezpečnostním týmem dohlížejícím na akademickou síť CESNET2. Spolupráci tvoří nejen vzájemné předávání detekovaných hrozeb u druhé strany, ale i výměna postupů a zkušeností z běžné praxe bezpečnostního CSIRT týmu. V neposlední řadě společně vyvíjejí systém WARDEN, který je určen k jednoduché a rychlé výměně detekovaných hrozeb mezi zapojenými CSIRT týmy. Do projektu jsou zapojeny i další akademické bezpečnostní týmy z ČR.

Národní bezpečnostní úřad

Tým CSIRT-MU aktivně spolupracuje s Národním centrem kybernetické bezpečnosti, součástí Národního bezpečnostního úřadu, na řešení otázek kybernetické bezpečnosti a pomocí získaných zkušeností vzdělává odborníky v oblasti bezpečnosti počítačových sítí.

INVEA-TECH, a. s.

Tým úzce spolupracuje s firmou INVEA-TECH, která je univerzitním spin-offem zaměřeným na vývoj nejmodernějších řešení pro vysokorychlostní síťové aplikace, na vývoji bezpečnostních zásuvných modulů a aktivně přispíváme do INVEA-TECH Community programu. Tým CSIRT-MU používá sondy FlowMon a další nástroje k nepřetržitému monitorování sítě MU.

TEAM CYMRU

CSIRT-MU dlouhodobě spolupracuje s mezinárodní skupinou Team Cymru na identifikaci a eliminaci strojů a stanic v síti MU nakažených nejrůznějšími druhy malware. Souběžně sdílí a analyzujeme relevantní data nasbíraná z honeypotů

provozovaných týmem CSIRT-MU v rámci univerzitní sítě s jasným záměrem identifikovat a eliminovat větší množství potenciálních útočníků.

TF-CSIRT

Jakožto akreditovaný člen organizace Trusted Introducer tým CSIRT-MU trvale spolupracuje s ostatními (nejen) akreditovanými bezpečnostními CSIRT týmy sdružujícími se kolem skupiny TF-CSIRT. Tým inicioval založení pracovní skupiny Network Security Monitoring Working Group, v níž aktivně vystupuje a představuje metody a postupy využívané při detekci anomálií a monitorování sítě MU.