CSIRT-MU – bezpečnostní tým Masarykovy univerzity v roce 2014

Výzkumné projekty a aktivity

Bezpečnostní tým řešil v roce 2014 celkem pět projektů bezpečnostního výzkumu a vývoje – nejen pro potřeby státu, ale i komerčního partnera (INVEA-TECH).

Kybernetický polygon (KYPO)

Velký podíl výzkumných aktivit zaujímalo v roce 2014 rozvíjení prostředí Kybernetického polygonu.

Rozšíření funkcí – vývojářům z týmu CSIRT-MU se podařilo rozšířit počet podporovaných operačních systémů, které lze provozovat ve virtuálním prostředí. Nyní lze pracovat s linuxovými systémy, MS Windows i s mobilní platformou Android.

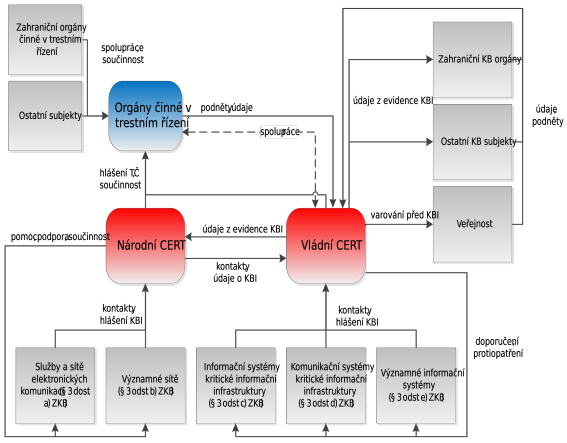
Nové ukázky využití – v průběhu roku 2014 byly v KYPO připraveny scénáře demonstrující jeho využití. Namátkou lze jmenovat školení laické veřejnosti v otázkách pokročilých hrozeb (APT), výuka specialistů v oblasti penetračního testování formou bezpečnostní hry či komplexní simulace rozsáhlých útoků proti kritické infrastruktuře a podpora forenzních analýz.

Uživatelské testování – členové týmu se v průběhu roku účastnili řady akcí, na nichž prezentovali projekt za účelem získání zpětné vazby od potenciálních uživatelů a bezpečnostní komunity na národní i mezinárodní úrovni (např. u příležitosti setkání sdružení bezpečnostních týmů TF-CSIRT). Tyto živé ukázky a cvičení byly vždy hodnoceny velmi kladně a poskytly cennou zpětnou vazbu pro další rozvoj KYPO.

Přednášky a konference – členové týmu CSIRT-MU představili projekt a dosažené výsledky na veletrhu **Future Crises 2014,** konferenci **European Grid Symposium** a dalších obdobných akcích.

České centrum excelence pro kybernetickou kriminalitu (C4e)

CSIRT-MU se podílel na formování modelu spolupráce bezpečnostních týmů a orgánů činných v trestním řízení. Navržené postupy byly konzultovány s evropskou agenturou ENISA a organizací Europol.



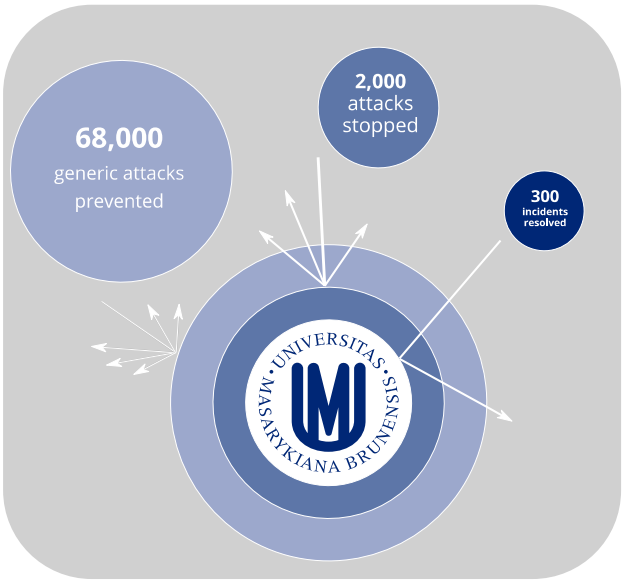
CSIRT-MU

Institute of Computer Science, Botanická 554/68a, 602 00 Brno, Czech Republic
csirt-info@muni.cz | +420 549 494 242 | www.muni.cz/csirt | Twitter: @csirtmu

CSIRT-MU – bezpečnostní tým Masarykovy univerzity v roce 2014

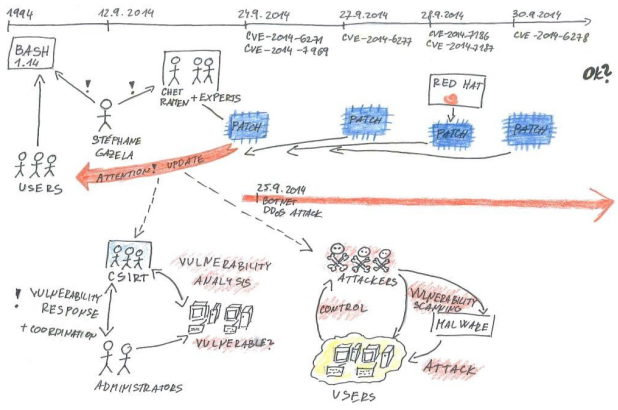
Ochrana počítačové sítě a služeb Masarykovy univerzity

Garant bezpečnosti – Tým CSIRT-MU řešil v roce 2014 více než 70.000 bezpečnostních incidentů dotýkajících se ICT infrastruktury Masarykovy univerzity.



Více než **68.000** incidentů tvořily **běžné útoky**, které tým odvracel plně automatickými metodami bez nutnosti zapojovat do řešení lokální správce IT infrastruktury.

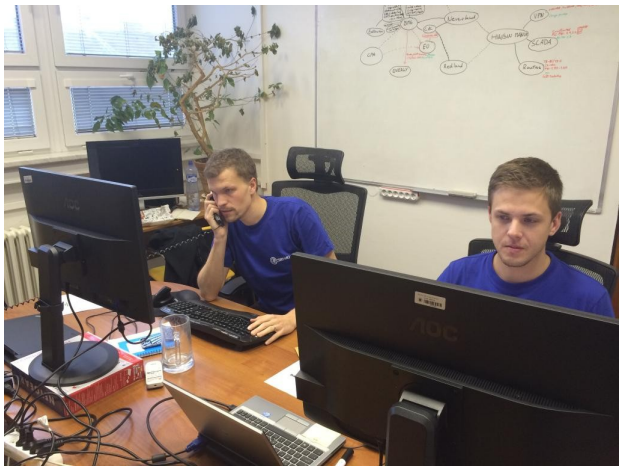
Proti síti a službám MU bylo vedeno přes **2.000 útoků**, jež vyžadovaly specifické zásahy ze strany týmu. Přes **300 útoků** bylo nutno vyřešit ve spolupráci s lokálními správci.



Upozornění na hrozby – tým CSIRT-MU monitoroval aktuální bezpečnostní hrozby, detekoval zranitelné stroje a služby v síti MU a dohlížel na jejich zabezpečení.

Sdílení zkušeností – členové týmu se aktivně zapojovali do důležitých akcí z oboru IT bezpečnosti – např. **Cyber Security Month** a setkání Pracovní skupiny CSIRT.CZ. Vedoucí týmu Jan Vykopal byl zvolen do řídícího výboru pracovní skupiny TERENA **TF-CSIRT** sdružující evropské bezpečnostní týmy.

Bezpečnostní cvičení – členové týmu se účastnili prestižních mezinárodních cvičení **Cyber Europe 2014** a **Cyber Coalition 2014** zaměřených na nácvik kooperace mezi týmy a ochranu kritické informační infrastruktury a prvního národního cvičení Cyber Czech.



Stáž pro NBÚ – tým uspořádal v pořadí již třetí školení bezpečnostních expertů Národního centra kybernetické bezpečnosti Národního bezpečnostního úřadu.

Spolupráce s Policií ČR – tým CSIRT-MU významnou měrou přispěl k odhalení a dopadení hackera, který dlouhodobě napadal a zneužíval až 1.500 počítačů.

Studijní obor – členové týmu se podíleli na přípravě nového oboru na FI MU, tak aby reflektoval současné požadavky kladené na členy bezpečnostních týmů.

CSIRT-MU
Institute of Computer Science, Botanická 554/68a, 602 00 Brno, Czech Republic
csirt-info@muni.cz | +420 549 494 242 | www.muni.cz/csirt | Twitter: @csirtmu