http://connect.zive.cz/clanky/v-brne-se-otevre-kyberneticky-polygon-pro-simulaci-utoku/sc-320-a-178082/default.aspx#utm_medium=selfpromo&utm_source=zive&utm_campaign=RSSfeed

V Brně se otevře Kybernetický polygon pro simulaci útoků

Jan Sedlák
28. dubna 2015

Masarykova univerzita spouští Kybernetický polygon. Je to výcvikové centrum pro kybernetickou bezpečnost, které využívá superpočítačový cloud.

Masarykova univerzita tento týden otevře nové výcvikové centrum pro kybernetickou bezpečnost. Jmenovat se bude Kybernetický polygon (KYPO) a jeho zprovoznění vyjde na několik milionů korun. KYPO je mimo jiné výsledek výzkumného projektu běžícího od roku 2013, který škole zadalo ministerstvo vnitra.

Kybernetický polygon má vytvořit komplexní systém pro výcvik, testování a odrazování počítačových útoků. Nejde pouze o to vyzkoušet si kritické situace mířící na zdejší kritickou či jakoukoliv jinou infrastrukturu, ale útoky bude možné také realizovat. Zkoušet bude možné všemožné scénáře, například útoky více hackerských týmů proti sobě a podobně.

Izrael, ČEZ a JIC chtějí v Česku kybervýcvikovou arénu

KYPO bude pracovat s takzvanými sandboxy, kde je možné nasimulovat kompletní síťové prostředí a v něm pak jednotlivé scénáře podrobně zkoušet, a to nezávisle na připojení k internetu. „Nový prostor a vybavení umožňuje simulovat v podstatě jakoukoliv část informatické reality. Pokud by si experti chtěli nacvičit například útok na jadernou elektrárnu nebo elektrickou síť, nepotřebují k tomu nic, co by se jednoho nebo druhého fyzicky týkalo. Všechno si dokážou vymodelovat," vzkazují tvůrci.

Na supervýkonném cloudu

Kybernetický polygon má sloužit více složkám státu i odborné veřejnosti. Trénovat zde budou například zaměstnanci Národního centra kybernetické bezpečnosti (NCKB), které funguje rovněž v Brně. Zapojí se i další části Národního bezpečnostního úřadu, policie, vojenští zpravodajci, odborníci a další akademici. Projekt budou moci využívat také studenti (pod vedením bezpečnostního týmu CSIRT-MU a lektorů) a firmy, které se zapojují do inovačních aktivit v Brně.

Pracoviště Kybernetického polygonu.

KYPO disponuje také vizualizačními nástroji a dokáže zprostředkovat bezpečnostní výstupy pro vládní složky i komerční sféru. Polygon budou moci využít i jednotlivé bezpečnostní týmy (CERT).

Kybernetický polygon vznikl na Fakultě informatiky a Ústavu výpočetní techniky na Masarykově univerzitě v Brně, konkrétně bude provozován v rámci CERIT Science Parku. Na zadaném projektu pracovalo devět lidí a další externí. Výsledkem je i několik odborných publikací.

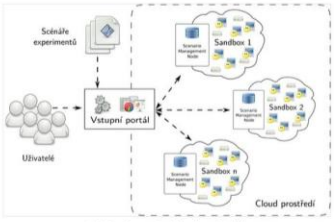

Schéma fungování simulace útoků.

Univerzita do projektu zapojuje také svůj CERIT Scientific Cloud, který vznikl přeměnou z původního Superpočítačového centra Brno. CERIT-SC je součástí národní počítačové infrastruktury a funguje po boku superpočítačového centra IT4Innovations a infrastruktury akademického CESNETu. CERIT má k dispozici přes 4800 procesorových jader a 4 PB úložného prostoru.

Tento cloud a výpočetní síla umožňují velké škálování jednotlivých simulací a experimentů. Sandboxové sítě fungují mimo internet, takže by mělo jít o bezpečné simulace. Připojení k internetu je samozřejmě možné.

Brno je obecně velkým centrem pro kybernetickou bezpečnost, které se v posledních měsících rychle rozšiřuje. Vedle zmiňovaného NCKB zde například VUT testuje DDoS útoky a některé další utajované věci (mimo jiné pro BIS a NBÚ) a zavádí samostatný výukový obor. Na Moravě vzniká také řada zajímavých nových bezpečnostních firem typu Invea-Tech. Jedná se také o tom, že by do Brna přišla mezinárodní výcviková aréna CyberGym.