

Češi vyvíjejí přelomovou technologii k zabezpečení počítačových sítí

V Praze dne 5. března 2019

Bezpečnost počítačových sítí a obranu proti internetovým útokům má zvýšit nový projekt českých specialistů z elektrotechnické fakulty ČVUT. Pokročilá technologie je založena na strojovém učení a teorii her a ocení ji zejména větší organizace, jejichž sítě jsou pod neustálým útokem. Projekt podpořila Technologická agentura ČR (TA ČR) a vložila do něj přes 10 milionů korun z Programu EPSILON. Účastní se jej i odborníci ze sdružení CZ.NIC.

Unikátním projektem s názvem Ludus chtějí vývojáři využít pokročilou technologii k chytrému zabezpečení velkých počítačových sítí, a sice vytvořením kooperativní a snadno přizpůsobitelné obranné strategie. Tyto nové metody mají zvýšit bezpečnost kritických počítačových infrastruktur a komunikačních sítí podléhajících častým útokům.

„Vzhledem k tomu, že se čím dál tím více lidských činností přesouvá do kyberprostoru, může být tento český projekt jedním z nejpokrokovějších výzkumů v dané oblasti na světě. Vývojáři v něm navrhují využití strojového učení a herně teoretických přístupů k nalezení obranných strategií. Ani největší světové společnosti v současné době nevyužívají herně teoretické přístupy v takto rozsáhlém měřítku. Projekt ČVUT má rozhodně smysl a zaslouží si naši podporu,“ uvedl předseda TA ČR Petr Konvalinka s tím, že hrozby a přímé útoky na internetu stále přibývají, vyvíjejí se a adaptují měnícímu se prostředí. Přestože jsou některé programy automatizovány, stojí za nimi především lidé. *„Velmi proto vítáme nová protipatření a projekty, které se snaží analyzovat rizikové situace a tyto škodlivé aktivity ztlumit nebo dokonce zcela zastavit,“* dodal Konvalinka.

Podle specialistů z ČVUT lze pomocí teorie her modelovat interakci mezi útočníky a obránci. *„Obránce si volí, které protipatření použít ve své síti, a útočník si vybírá, na který cíl zaútočit. Náš projekt se snaží zvýšit bezpečnost pomocí tří etap. Nejprve vyhodnotíme kvalitu zabezpečení stávající sítě, pak vyvineme herně-teoretické modely pro výpočet strategií, které proti útočníkům rozmístují falešné cíle, jako například honeypots a honeytokens. Tyto technologie mají útočníky nalákat a zmařit jejich snahy dřív, než se jim podaří napadnout skutečnou síť. A poslední etapou je vývoj nové komplexnější metody, která se přizpůsobí novým trendům útoků, a bude tak maximalizovat počet odhalených hrozeb a zlepšovat bezpečnost organizace,“* vysvětlil Sebastián García, hlavní řešitel projektu Ludus z ČVUT.

Finanční podporou přesahující deset milionů korun pomůže TA ČR vývojářům z ČVUT pokračovat a zlepšit výzkum v dalších směrech, sestavit tým ze studentů a vyvinout software, který budou moci volně využívat nejrůznější organizace a společnosti. Projekt Ludus včetně nového softwaru plánuje ČVUT dokončit na podzim letošního roku.

Kontakt:
Ing. Ivana Drábková, tisková mluvčí TA ČR
 E: drabkova@tacr.cz
 T: 777 016 525