Kybernetické útoky - místo výbušnin nadělá škodu pár řádků programu

13.5.2014 ct24.cz str. 0 Média/IT

izi

Brno – Internet nejsou jen e-maily, webové stránky a data. Kdo by chtěl zaútočit v kyberprostoru, má mnohem víc možných cílů: ovládnout či poškodit lze i taková zařízení jako elektrárny či vodárny. Právě na ochranu vládních institucí a tzv. kritické infrastruktury, která je pro fungování státu nezbytná, se soustředí odborníci v novém Národním centru kybernetické bezpečnosti (NCKB).

"Mnozí lidé si představují, že internet funguje pouze pro přenos dat, ale může to být také **útok** na řízení technologických procesů, protože dnes internet ovládá například vodárny, energetické subjekty a další," varoval ředitel Národního **bezpečnostního úřadu** Dušan Navrátil. Že dokáží škodlivé **počítačové programy** napáchat velmi reálné škody, pochopil svět na přelomu let 2009 až 2010. Tehdy záškodnický **počítačový program** - červ zvaný Stuxnet - výrazně zasáhl íránský jaderný program, když vyřadil z provozu tisícovku íránských centrifug na obohacování uranu. **Jednalo** se o první známý program, která dokázal poškodit cíle z reálného světa.

Aby podobný **útok** nepotkal zařízení a instituce, které jsou zásadní pro bezproblémové fungování státu, to bude mít na starost Národní centrum kybernetické bezpečnosti. "Srdcem budovy je monitorovací sál, kde se sbíhají hlášení o incidentech. Sedí zde odborníci, kteří hlášení **přijímají** a provádějí prvotní analýzu," popsal ředitel NCKB Vladimír Rohel. "Všichni zaměstnanci musí mít **bezpečnostní prověrku**, je důležité, aby byli důvěryhodní," dodal k fungování nového úřadu Rohel.

"V 21. století informační technologie tvoří nervovou páteř moderní společnosti, je proto velmi důležité, aby stát byl schopen zajistit určitý dohled, servis a možnost zásahu," řekl dnes při otevření NCKB premiér Bohuslav **Sobotka** (**ČSSD**). Centrum bude sloužit nejen **České republice**, ale i našim spojencům. "Vytvoření NCKB je součástí **strategického** plánu **NATO** v oblasti kybernetické bezpečnosti. Je to něco, co bychom chtěli na národní úrovni udělat mezi všemi spojenci. Všichni jsme propojeni, měli bychom informace sdílet," uvedl náměstek **generálního** tajemníka **NATO** Sorin Ducaru.

Hodně škody za málo peněz

Jak se používání internetu, mobilních zařízení a výpočetní techniky rozšiřuje, přibývá i kybernetických **útoků**. "Kybernetické **útoky** jsou velice levné a snadno nadělají velkou škodu. Na druhé straně je velice těžké, někdy až nemožné, vypátrat viníka. Je to skutečně reálná hrozba," varoval Navrátil. Připravit například kyberútok, který by paralyzoval **Spojené státy americké**, by podle odhadů některých odborníků trvalo dva roky a stálo méně než 50 milionů dolarů.

"Některé státy, jako například **USA**, Izrael nebo arabské státy, už jsou dnes v kybernetické **válce**, což si mnozí ještě neuvědomují. A samozřejmě že s prudce se zhoršující **bezpečnostní situací** v Evropě není vyloučeno, že taková situace nastane i v Evropě," varoval Navrátil. "Dnes už málokdo někam vyšle **bombardéry**. Například program Stuxnet nám čtyři roky doslova protékal mezi prsty. Bylo to v uvozovkách jenom pár řádku programu - žádná bomba, žádná výbušnina, žádná sabotáž v klasickém slova smyslu. A přitom zpozdil íránský jaderný program o jeden až dva roky," upřesnil odborník na kybernetickou bezpečnost Tomáš Přibyl.

Útoky, o kterých se nemluví

Některé z **útoků** běžní uživatelé internetu pociťují na vlastní kůži – když kvůli zahlcenému serveru nefungují stránky nebo když někdo pirátsky převezme jejich správu. "To jsou takzvané defacementy - někdo změní původní stránku, píše tam třeba něco hanlivého," vysvětlil Rohel.

Je ale i část **útoků**, o kterých veřejnost neví. A právě ty jsou největší hrozbou. "Jsou to cílené **útoky** na organizace, kdy je opravdu účelem zaškodit, něco zničit. Ty jsou nejzákeřnější a s těmi se

převážně potýkáme," uvedl Rohel a vzpomněl jeden nedávný případ, kdy se útočník pokusil dostat do citlivé mailové korespondence jednoho z vládních úřadů.

Centrum zahájilo svoji činnost v lednu 2012, a to v prostorách **brněnské Univerzity obrany**. Zatím v něm pracuje 22, ale časem by se měl tým rozšířit na 34 pracovníků. Dnes centrum oficiálně otevřelo nové sídlo v **brněnské** Mučednické ulici. Budovu dříve využívala **armáda**. Její oprava stála 34 milionů korun, technické zabezpečení vyšlo na 6,5 milionu a vybavení nejmodernější počítačovou technikou na přibližně 38 milionů korun.

"Vytvoření centra je významným krokem v oblasti kybernetické bezpečnosti republiky. Zároveň se pracuje na přípravě zákona o kybernetické bezpečnosti. Tyto dvě věci řadí **ČR** v ochraně proti počítačovému pirátství na přední příčky mezi státy Evropy," řekl Jan Hajný, který vede **pracovní skupinu** kybernetické bezpečnosti Vysokého učení technického (VUT) v **Brně**.

URL| http://www.ceskatelevize.cz/ct24/media...busnin-nadela-skodu-par-radku-programu/