

Za útoky přestávají být zodpovědní lidé. Místo nich za nimi stojí počítačové programy. Nelze je nahmatat, těžko se proti nim brání a často není možné je odsoudit. Jak současným kyberhrozbám čelit, zkoumají odborníci z **Fakulty informatiky**, Právnické fakulty matiky, a Ústavu výpočetní techniky Masarykovy univerzity v Brně v centru excelence. Jejich práci podpořila i EU více než 190 milionů korun z evropských fondů.

Brno – Centrum excelence pro kyberkriminalitu, **kyberbezpečnost** a ochranu kritických informačních infrastruktur vzniklo v Brně zhruba před deseti lety. Tvoří unikátní spojení odborníků z Masarykovy univerzity, kteří vynikají v informačních technologiích a právu. Jejich cílem je vytvářet základní poznatky o bezpečném pohybu na internetové síti, které následně v praxi využijí například zaměstnanci Národního úřadu pro kybernetickou a informační bezpečnost.

SPOJENÍ NĚKOLIKA RŮZNÝCH OBORŮ

Centrum, zkratkou nazývané také jako C4e, tvoří tři základní pilíře. Jedná se o **kyberbezpečnost**, ochranu kritických informačních infrastruktur a právo. Všechny dohromady má na starost Roman Čermák.

„Mým úkolem je vytvářet prostředí pro excelentní výzkumníky, kteří propojují jednotlivá témata, čímž vznikne hodnotnější výsledek. Síla centra spočívá ve schopnosti kombinovat teoretické poznatky z více oblastí a poté je předávat těm, kteří je užijí v praxi,“ vysvětluje ředitel.

V loňském roce získali vědci téměř 198milionovou dotaci od Evropské unie. Díky ní se mohou problematice věnovat ještě hlouběji. „Uspěli jsme jako jedni z mála v nabitě konkurenci. Díky penězům můžeme zapojit i mezinárodní výzkumníky a také nám to pomáhá ty dosavadní udržet.

Čerpání peněz je pětileté, což pro vědce znamená jistotu, že mohou bádát. V Brně je konkurence **IT** firem obrovská,“ poznamenává Čermák.

Souhlasí s ním také Pavel Čeleda, který má na starost pilíř kyberbezpečnosti. „Brno je městem informačních technologií. Je těžké ve výzkumu udržet lidi, kteří mají vidinu rychlého zisku ve firmě,“ říká.

Podle Čermáka jsou přítomni pro výzkumníky odměnou nejen peníze, ale i vědomí, že pracují na něčem společensky přínosném.

Právě **kyberbezpečnost** ale patří mezi jedny z nejatraktivnějších oborů, který hraje v čím dál tím více digitalizovaném světě významnou roli.

„Kyberútoky už neznamenají jenom to, že lidem někdo přečte e-maily. Může to být třeba zašifrování dat nemocnice, kdy pak jde o život. Virtuální počítačový svět se navíc stává arénou mocenských bojů. Kybernetická válka nemá hranice, útočník může projít několika státy. Těmto rizikům se snažíme čelit,“ přibližuje Čeleda.

OBRANA PRO BLÍZKOU BUDOUCNOST

Výzkumník Martin Drašar doplňuje, že za útoky brzy nebudou stát jednotlivci, ale automatizované nástroje. „Jedná se o relativně blízkou budoucnost.

Člověka nahradí programy, které se budou samy vyvíjet a přizpůsobovat podle toho, co se děje na druhé straně. Tyto programy pak ale nelze ani odsoudit,“ přiznává Drašar.

Právě na tento problém naráží se svým týmem právník a vedoucí jednoho z pilířů Radim Polčák.

„Jednou z oblastí kyberobrany jsou vztahy mezi státy. Je jasné, že když země hodí bomby na jinou, je to užití síly. Co je ale vloupání do systému jiné země? My zkoumáme, jak legálně získat důkazy, které potom můžeme použít u soudu,“ uvádí.

Polčák poznamenává, že když někdo ovlivňuje volby, tak je to zásah do suverenity, těžko ale dokážou, že to zorganizovala konkrétní země.

„Česká republika naštěstí není v první linii těchto útoků. To platí například pro Spojené státy americké,“ uklidňuje.

Odborníci z Brna školí i zaměstnance NATO. Slouží jim k tomu kybernetický polygon, tedy aréna, která vytváří prostředí simulovaných útoků.

„Hledáme cestu, jak lidi vzdělávat, aby porozuměli složitým technickým dějům. K běžným útokům dochází denně. Ty, za kterými stojí národní stát, jsou méně časté, ale o to větší mají dopad. Trvat mohou navíc i měsíce,“ konstatuje Čeleda.

Česká republika je podle vědců zvýhodněná v tom, že má mezi sebou špičky ve svém oboru, které například stály u jednoho z prvních zákonů o kybernetické bezpečnosti v Evropě.

„Brno je městem informačních technologií. Je těžké ve výzkumu udržet lidi, kteří mají vidinu rychlého zisku ve firmě.“ Pavel Čeleda, expert na **kyberbezpečnost**

PROJEKT V ČÍSLECH

Příjemce: Masarykova univerzita

Cíl projektu: Výzkum kybernetické bezpečnosti pro ochranu kritických infrastruktur.

Zahájení projektu: 1. 4. 2018

Ukončení projektu: 31. 12. 2022

Celková částka: 197 459 332 Kč

Veřejné zdroje ČR: 29 618 900 Kč

Výše dotace EU: 167 840 432 Kč

ZDROJ: MMR

Foto popis| ARÉNA ÚTOKU. V kybernetickém polygonu neboli místnosti, ve které se odehrávají simulované kybernetické boje, školí brněnští experti zaměstnance Národního úřadu pro kybernetickou a informační bezpečnost i Severoatlantické aliance. Studenti se tam také zúčastňují soutěží.

Foto autor| Foto: Masarykova univerzita

Foto popis| STOVKY DAT. Informatici musí využívat technologie, díky kterým mohou naráz pracovat s velkým objemem dat.

Foto autor| Foto: Deník/Klára Vašíčková

Region| Jižní Morava

Publikováno| Brněnský deník; ; 12

Publikováno| Vyškovský deník; ; 12

Publikováno| Břeclavský deník; ; 12

Publikováno| Blanenský deník; ; 12

Publikováno| Hodonínský deník; ; 12

Publikováno| Znojenský deník; ; 12

ID| 4d254f3c-8f19-4275-a0a5-a947a8407b05