

<https://zpravy.aktualne.cz/zahranici/evropsky-parlament/v-kyberneticke-bezpecnosti-muze-jit-cesko-evrope-prikladem/r~45eb1c52bbd411e79603002590604f2e/?redirected=1510514694>

Kyberbezpečnost? Evropa se může od Česka učit, ve státní správě ale chybí "ajt'áci", říkají experti

9. 11. 2017



Ilustrační foto. | Foto: CyberGym Europe

Ještě před několika lety se Česko učilo od jiných evropských zemí, jaká opatření zavést v kyberbezpečnosti. Nyní pořádá školení, kde čeští experti sami radí - například svým kolegům z Balkánu. Zaznívá ale i kritika. Česku podle analytika Tomáše Rezka chybí IT odborníci ve státní správě.

Doporučujeme



[Nedaleko břehů Evropy je novodobé tržiště s otroky. V Libyi se draží migranti na aukcích](#)



[K pirátům se po volbách hrnou stovky nových členů, táhne TOP 09 i komunisté. Lidovců naopak ubývá](#)

Brusel/Praha - Evropské země by se od [Česka](#) mohly učit, jak se chránit před [kybernetickými útoky](#). Česko je totiž o krok napřed - alespoň podle expertů z [estonské](#) neziskové organizace [e-Governance Academy](#), která hodnotí, jak jsou státy připravené na útoky hackerů.



[Mají hackeři otevřené dveře do vašeho mobilu nebo počítače? Expert odpovídal k problémům s wi-fičist článkem](#)

"V našem národním indexu kybernetické bezpečnosti drží Česká republika první příčku," říká šéf organizace Raul Rikk.

Žebříček porovnává úroveň kybernetické bezpečnosti ve 38 zemích světa, mezi kterými nechybí ani [Polsko](#) nebo [Nizozemsko](#).

Do [indexu](#) se započítává například úroveň zákonů, vzdělávání v oblasti IT nebo schopnost země analyzovat kybernetické hrozby.

reklama



Body získala Česká republika taky za existenci Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Ten vznikl v roce 2014, kdy byl ve světě ještě ojedinělým.

"Česká republika se stala jakýmsi modelem pro další státy, jak legislativně upravit a podchytit povinnosti a mandáty v oblasti kybernetické bezpečnosti," uvádí Daniel Bagge, který vede odbor kybernetických bezpečnostních politik.

Od nováčka k lídrovi

Ještě v letech 2012 a 2013 Česko čerpalo ze znalostí svých mezinárodních partnerů, jako je například Evropská agentura pro bezpečnost sítí a informací (ENISA).

Ted' naopak pomáhá ostatním státům vyvíjet vlastní bezpečnostní opatření.

"Pořádáme pro ně technická cvičení na polygonu v Brně. Jako třeba počátkem letošního roku pro šest států západního Balkánu," upřesňuje Bagge, co dělá NÚKIB.

Ten se na rozdíl od podobných úřadů v jiných unijních zemích zabývá jak řešením samotných incidentů v kyberbezpečnosti, tak i právní stránkou věci, vzděláváním nebo mezinárodní spoluprací.



[PřehledPřehledně: Evropa čelí trojským koním i vyděračským virům. Hackeři mají stále rafinovanější metody](#)

Navíc státy EU, kterým takový úřad chybí, ho budou muset zavést. Ukládá jim to nová evropská směrnice.

"Je to jediné dobře, protože bude alespoň jasné, na koho se obrátit v případě mezinárodního kybernetického útoku," vysvětluje Bagge.

Podle směrnice bude muset mít každá země svůj tým expertů, kteří budou schopni reagovat 24 hodin denně na hackerské útoky. Dále bude pro státy povinné přijmout strategii pro kybernetickou bezpečnost a spolupracovat s ostatními zeměmi při řešení bezpečnostních problémů.

Máme málo odborníků

Češi ale mají pořád na čem pracovat, říká analytik Asociace pro mezinárodní otázky Tomáš Rezek. A ukazuje na malý počet schopných lidí, kteří chtějí přejít ze soukromé sféry do té státní.

"Ne vždy se nám daří získat především pro státní sektor dostatek kvalifikovaných odborníků," vysvětluje analytik.

Dalším problémem je podle něj chabé povědomí o kybernetické bezpečnosti na úrovni běžných uživatelů.



[Experti objevili závažnou chybu bezpečnosti wi-fi. Potenciálně ohrožena je každá síť, potvrdiličíst článek](#)

Největší hrozbu pro Evropu vidí Rezek v současnosti v takových útocích, které jsou vedené ve velkém rozsahu, ale na konkrétní cíl. Jen těžko se jim dá bránit.

Aby bylo Česko vůči těmto útokům odolnější, mělo by začít více spolupracovat s ostatními evropskými státy, míní Rezek.

Unie totiž podle něj pomáhá členským zemím například sdílením informací o aktuálních hrozbách.

Vzdělání je základ

Sama Evropská unie pak hodlá přitlačit na vzdělávání IT odborníků a zaměstnanců na úradech. Už v říjnu na to apeloval [Evropský parlament](#) a před dvěma týdny taky Rada EU.



[VideoÚčty na sítích řízené roboty? Další nástroj ruské hybridní války, postižené je i Česko, říká expertsledovat video](#)

O kybernetické bezpečnosti by se navíc měly v budoucnu informovat i děti. Europoslanci například vybídlí členské státy, aby tuto oblast zařadily do hodin informatiky na školách.

S potřebou zlepšit vzdělávání souhlasí i český koordinátor pro digitální agendu Ondřej Malý. Jako jednu z možností vidí právě posílení zmíněné evropské agentury ENISA.

"Vzdělávání v oblasti kyberbezpečnosti nezaznívá pouze na evropské úrovni, ale patří i mezi vládní priority v České republice," dodává Malý. O vzdělávání v tomto oboru se v Česku stará právě NÚKIB.

Ten se momentálně chystá na proškolení státních zaměstnanců o hrozbách hackerů.

Podle Daniela Baggeho z NÚKIB je pak důležité přesvědčit i samotnou veřejnost, že kybernetické útoky se mohou týkat taky obyčejných uživatelů internetu.

"Kolik z nás si uvědomuje, že mobilní telefony v našich kapsách disponují výpočetním výkonem, který by byl před mnoha lety nemyslitelný? A že jsou zároveň branou do našeho soukromí a práce?" uzavírá.