Rizika hackerských útoků jsou v Česku reálná. Určitě víc než válka, tvrdí šéf nového úřadu pro kyberbezpečnost

16.12.2016 iHNed.cz str. 0

Lukáš Prchal

Ředitel Národního **bezpečnostního úřadu** Dušan Navrátil bude nyní vést úřad pro kyberbezpečnost. **Česko** podle něj zatím nezažilo masivní kybernetické **útoky**, menší **útoky** zde však probíhají, jen nejsou pořádně vidět.
"Nejsme **Spojené státy** ani Izrael. Ve světě jsou tyto **útoky** mnohem masivnější. To se ale může během chvíle po nějakých rozhodnutích, například politických, změnit," říká.

Dušan Navrátil na začátku příštího roku odejde po více než deseti **letech** z postu ředitele Národního **bezpečnostního úřadu** (NBÚ), který vytvářel. Pod Úřadem vlády začne stavět nový úřad pro kyberbezpečnost.

"Má mít stejné postavení jako Národní **bezpečnostní úřad**, bude se **jmenovat** Národní úřad kybernetické a informační bezpečnosti. Když to projde schválením vlády a parlamentu a všechno půjde dobře, vznikne nejdříve v září v příštím roce," vysvětluje.

Co přesně bude nový úřad dělat?

Bude se zabývat bezpečností v kyberprostoru a bude mít stejnou roli jako současné Národní centrum kybernetické bezpečnosti, bude tedy řešit problematiku kybernetické bezpečnosti a zároveň bude národní autoritou pro tuto oblast.

Bude chránit systémy kritické informační infrastruktury, tedy chránit důležité funkce státu. Podle zákona nám musí být hlášeny kybernetické **útoky**, které vyhodnocujeme, a varujeme pak příslušné subjekty. Eventuálně jsme schopni a máme pravomoc jim nařídit, aby udělaly nějaká opatření, kdyby šlo do tuhého.

Národní centrum kybernetické bezpečnosti, které sídlí v **Brně**, vzniklo na NBÚ před lety. Už nějakou dobu jsme ale cítili, že se bude muset osamostatnit, protože už začalo přerůstat kapacitu NBÚ.

Pro nový útvar bychom měli dostat pozemek v **Brně**, v **kasárnách** v Černých polích, což je objekt **Univerzity obrany**, kde bychom měli po roce 2020 stavět.

Nebude se NBÚ překrývat ve svých pravomocech s novým úřadem, který vytvoříte?

Národní **bezpečnostní úřad** se bude zabývat **prověrkami**, utajovanými informacemi. Nový úřad se bude zabývat kybernetickou bezpečností, ochranou utajovaných informací v komunikačních a informačních systémech, včetně kryptografické ochrany.

Kolik by měl mít nový úřad při plné síle lidí?

Hrubým odhadem až 400, ale to je zatím předčasné.

Nebude problém sehnat tolik počítačových **specialistů**? Už nyní jich je málo a do státní správy se ajťáci špatně získávají.

To jste uhodil hřebíček na hlavičku. Ajťáků je málo všude ve světě, ale v novém úřadu nebudeme mít jen samé ajťáky.

Navíc bude velká výhoda, že budeme mít sídlo v **Brně**, což je v uvozovkách **české** "Silicon Valley". A už nyní spolupracujeme s univerzitami, vedeme diplomky... Vyplácí se nám to a pak si dobře vybíráme.

Berete jako povýšení, že máte vytvářet nový úřad, když máte za sebou dekádu na postu šéfa NBÚ?

Je to pro mě velká výzva, kybernetická rizika narůstají geometrickou řadou.

Měli bychom se kybernetických **útoků** obávat více než pušek?

Rizika jsou v **České republice** značná a reálná, určitě reálnější než faktická **válka**.

V čem jsou reálná?

Česko zatím nezažilo masivní kybernetické **útoky**. S jednou výjimkou - to bylo v roce 2013, kdy po čtyři dny docházelo k zahlcení komunikace některých webů. Tehdy to bylo hodně medializované. **Útoky** u nás ale probíhají, jen nejsou pořádně vidět a nejsou v takovém rozsahu, aby nadělaly příliš velké škody. Nejsme **USA** ani Izrael. Ve světě jsou tyto **útoky** mnohem masivnější. To se ale může během chvíle po nějakých rozhodnutích, například politických, změnit.

A to je důvod, aby se vytvořil nový úřad?

Musíme na to být nachystáni. Máme **armádu**, protože konvenční **válka** je možná, a musíme být připraveni i na **útoky** z kyberprostoru.

Můžeme mluvit i o nějakých příkladech?

V Estonsku došlo před lety, kdy byl přemístěn pomník sovětského **vojáka**, k **útokům** z ničeho nic. A k tomu může dojít i u nás a může pro to být důvod, který nyní samozřejmě neznáme, nenapadá nás. Ale může to nastat. V **USA** jsou kyberútoky na denní bázi, v Jižní Koreji jsou časté **útoky** od jejich severních sousedů. Podobně je na tom Izrael. A všichni jsou na to připraveni a připravují se na další možnosti.

Do jaké kategorie a stupně nebezpečí by se řadilo loňské nabourání e-mailu premiéra **Sobotky**?

Nedošlo tam k žádným závažným škodám, kromě medializace. Ale pan premiér není první, stalo se to více lidem - i nejvyšším funkcionářům **americké** CIA. Také v **sociální demokracii** měli hackeři vyhlédnuto více lidí a záměrně se nabourávali do více schránek. Pan premiér měl v tu chvíli smůlu, že byl pan premiér.

Jak přimět státníky či instituce, aby například používali šifrované telefony?

Bude to znít úsměvně, ale osvětou. Bohužel. Není to jednoduchá věc, ale bojují s tím i všechny nám podobné organizace ve světě. Úkolem nového úřadu tak bude mimo jiné osvěta.

Máme ale i právo kontrolovat a udělit pokutu, když některá instituce neplní standardy svých systémů, které jsou předepsané.

Ale pokuty jsou to poslední, co chceme dělat. Důležité je komunikovat a pomáhat jim a vysvětlovat jim, co by měli dělat.

Jak si vysvětlujete, že kyberbezpečnost a vůbec internet se začaly řešit nyní v tak rozsáhlé míře?

Protože je tam reálné nebezpečí. Společnost je čím dál více závislá na fungování v informačních systémech. A to se každým rokem silně prohlubuje.

Navíc se **bezpečnostní rizika** po roce 2014 prudce zvýšila po celém světě – migrační krize, **válka** na Ukrajině, Islámský stát. Do té doby byl svět více méně stabilní, ale svět se mění a **bezpečnostní rizika** prudce stoupla. Do roku 2014 jsme si mysleli, že ani **armádu** nepotřebujeme, ale přišla Ukrajina a ukázalo se, že **armáda** by se měla posílit.

A nyní se ukazuje, že bude potřeba větší bezpečnost v kyberprostoru.

Proč jste se ale až nyní začali zajímat o internet?

Podívejte, rizika si uvědomujeme, vnímáme je, říkáme "Ano, má se to řešit". Ale dokud nepřijde nějaký průšvih, tak to není tak intenzivní a jde to pomalu. A když se něco stane, všichni se semknou a začne

se to řešit daleko intenzivněji. Kdyby se něco stalo, lidé se budou ptát, proč na to nejsme připraveni. Nyní děláme kroky, abychom připraveni byli.

Pro to všechno, co chcete dělat i v novém úřadě, budete vy i **Vojenské zpravodajství** potřebovat velkou důvěru lidí. Protože jako obyčejný člověk si budu říkat, že tady je Velký bratr, který sleduje moje fungování na síti.

Od začátku působení jsme z toho jako NBÚ byli obviňováni, ale myslím si, že jsme dokázali, že žádným Velkým bratrem nejsme. Nás nezajímá obsah internetu. A máme důvěru odborné veřejnosti, kterou jsme si vybudovali.

Jaké jsou nyní fenomény kybernetického nebezpečí, kterým bude nový úřad muset čelit?

Hlavně jsou to stále DDoS **útoky**, kdy dojde k takzvanému zahlcení komunikace, což je stará záležitost. Je to jako silnice přeplněná auty, která se stane neprůjezdnou. Ale nedávno proběhly tyto **útoky** na DNS servery soukromých IT společností. Při nich byla zapojena zařízení, která se při těchto **útocích** ještě neobjevovala, jako například kamery. Ovládli procesory asi dvaceti tisíc kamer a došlo k tomu, že všechny kamery útočily a zahlcovaly provoz.

Jeden IT manažer mi vyprávěl, že budou čipovány stromy v Amazonii a dovede si představit, že ty stromy také budou zvládat útočit DDoS **útokem**. Takže i přesto, že je to starý **útok**, stále je hojně využíván. **Obrana** proti tomu je v robustnosti systému a je to velmi nákladná záležitost.

Existují také **útoky** na technologické procesy. Například v Německu se kybernetickým **útokem** podařilo zablokovat vysokou pec, kde zatuhlo železo, což způsobilo velkou škodu. Spadá sem i **útok** na petrolejářskou společnost v Saúdské Arábii, kde zaútočili na síť počítačů a zničili je.

Další fenomén je normální malware, který krade nebo mění vaše data, či ransomware, který vám zašifruje data, a když nemáte zálohy, nedostanete se k nim. Ti, co to udělají, pak žádají výkupné, aby vám data vrátili. To je v současnosti běžný **útok** na **americké nemocnice** a jejich databáze – ti zaplatí velmi rychle. Drobné **útoky**, kdy útočníci žádají výkupné, probíhají i v **Česku**.

Dá se tomu bránit?

Když už to dojde do situace, kdy útočník požaduje výkupné, často nezbývá nic jiného než zaplatit. Ale prostě je nutné dávat pozor, na co klikáte na internetu nebo ve svém e-mailu. Něco takového rozšifrovat je na roky a je na to potřeba superpočítač.

Řadu věcí se daří rozšifrovat, ale jakmile něco prokoukneme, hackeři vymyslí něco nového, jsou velmi dynamičtí.

A proti tomu se nedá bojovat?

Samozřejmě dá, ale to neděláme a nebudeme dělat my. Když jste na internetu zručný, dostanete se do míst, kde si můžete nějaký škodlivý malware koupit, dokonce k tomu dostanete i upgrade. Dá se objednat i hackerský **útok** a je smutné, že je to vlastně velmi jednoduše dostupné.

Je to stále boj s útočníky, kteří jsou vždy o krok napřed, a nyní je pro nás důležité, aby **Česká republika** měla prostředky, jak tomu čelit. Nikdo jiný to za nás neudělá.

Kdo by měl tedy i útočit, když ne vy?

To by mělo nově dělat **Vojenské zpravodajství**. Nyní se to řeší, ale měli by mít tyto schopnosti. Protože v budoucnosti nastane situace, kdy nebudou mít jinou možnost než zaútočit.

Novým ředitelem **bezpečnostního úřadu** se má stát Jiří Lang, který třináct let šéfoval BIS - čtěte ZDE

NBÚ vybuduje v **Brně** nové centrum kybernetické bezpečnosti. Pojme téměř desetkrát více pracovníků než v současnosti - čtěte ZDE

Vládou prošla novela posilující kybernetickou bezpečnost. **Útoky** mají nově hlásit třeba i vyhledávače či e-shopy - čtěte ZDE

Kreml ovlivňoval **americké** volby, říká CIA. Stojí i za e-maily zveřejňovanými přes WikiLeaks - čtěte ZDE

URL| http://domaci.ihned.cz/c1-65560020-riz...di-sef-noveho-uradu-pro-kyberbezpecnost