Karel Řehka (NÚKIB)

Zcela v bezpečí nebudete nikdy

MICHALA BENEŠOVSKÁ

Kybernetická bezpečnost je bezesporu nejdůležitější oblast dnešního digitálního světa. Karel Řehka, ředitel Národního úřadu kybernetické a informační bezpečnosti, nám poskytl rozhovor o tom, čím se úřad zabývá a jak pomáhá se vzděláváním a osvětou, řeč byla také o ransomwaru, podpoře mladých talentů a způsobech, jak minimalizovat rizika kybernetického útoku.

Můžete ve stručnosti shrnout, co je NÚKIB a co je jeho úkolem?
Máme tři hlavní oblasti činnosti: kybernetická bezpečnost, bezpečnost utajovaných informací v informačních a komunikačních systémech a veřejně regulovaná služba navigačního systému Galileo. V oblasti kybernetické bezpečnosti regulujeme systémy, které jsou nezbytné pro chod státu a bezpečí jeho obyvatel. Prostřednictvím zákonů a vyhlášek stanovujeme, jak mají být tyto systémy zabezpečeny, toto zabezpečení kontrolujeme a pomáháme se zvládáním případných incidentů. Také máme koordinační úlohu v kybernetické bezpečnosti, neboť tu nemůže zajišťovat jeden úřad, ale musí jít o kolektivní úsilí.

V oblasti ochrany utajovaných informací certifikujeme systémy pro nakládaní s těmito informacemi, vyvíjíme a testujeme národní šifry a celkově se staráme o to, aby nejcitlivější informace státu byly v informačních systémech v bezpečí. U veřejně regulované služby Galileo je všechno teprve na začátku, ale postupem času půjde o další velkou agendu, neboť tato část služby Galileo bude mít velký význam pro bezpečnostní složky, integrovaný záchranný systém a další oblasti. V zásadě ale i zde naše role spočívá především zajištění kybernetické a informační bezpečnosti s ohledem na požadavky bezpečnosti přenosu a distribuce signálu této služby.

Máte obsáhlou agendu, spolupracujete i s podobnými organizacemi z jiných zemí. Jak tato spolupráce probíhá?
Mezinárodní spolupráce probíhá ve všech oblastech naší činnosti. V rámci kybernetické bezpečnosti provozujeme například tzv. vládní CERT (Computer Emergency Response Team), který má na starosti technickou část této problematiky. Podobné týmy působí v řadě dalších zemí a vzájemně si vyměňují informace o aktuálních hrozbách. Zároveň máme několik tzv. cyber attaché, kteří působí na našich ambasádách v zahraničí, konkrétně jde o dva lidi v Bruselu (jeden zaměřený na EU, druhý na NATO), dalšího člověka v USA a dalšího v Izraeli.

Snažíme se maximálně spolupracovat se svými spojenci v NATO a EU a také se zeměmi, které mají se zajišťováním kybernetické bezpečnosti největší zkušenosti, což je bezpochyby například Izrael. Kromě výměny informací o aktuálních hrozbách si vyměňujeme i zkušenosti s jejich řešením. Česko například uspořádalo již dvakrát Prague 5G Security Conference, která slouží k mezinárodní výměně zkušeností s bezpečným budováním sítí 5G. Vedle toho se také účastníme programů, které mají naopak za cíl pomáhat s budováním schopností v kybernetické bezpečnosti v zemích, které jsou v této oblasti méně zkušené.

Jak je na tom podle NÚKIB Česká republika s ochranou proti kybernetickým hrozbám v porovnání s ostatními evropskými zeměmi?
Kybernetická bezpečnost je stále ještě velmi nový obor a k jejímu zajišťování přistupují různé státy různě, což je vidět i na příkladu nových technologií, jako jsou třeba sítě páté generace. Je těžké úroveň kybernetické bezpečnosti v České republice nějak zobecnit. V některých oblastech si ve srovnání vedeme velmi dobře, někde nás ale naopak čeká ještě spousta práce. Na jedné straně máme systémy regulované naším zákonem o kybernetické bezpečnosti. Ty musejí plnit velmi striktní podmínky na zabezpečení po technické i netechnické stránce. A pak jsou tu všechny ostatní systémy, které nijak regulované nejsou, nespadají pod náš dohled a jejich zabezpečení se pohybuje někde na škále špičkové–tragické. Trochu bližší vhled mohou poskytnout naše Zprávy o stavu kybernetické bezpečnosti, které každoročně vydáváme. Z těch je dobře patrné, že třeba bankovní sektor je zabezpečen velmi dobře, ale ve zdravotnictví přetrvává řada problémů. Podotýkám, že některá zařízení z těchto odvětví pod náš zákon spadají, ale zdaleka ne všechna.

Kdo je dnes nejvíc ohrožen kybernetickým útokem?
Ohroženi jsou v podstatě všichni. Když pomineme sofistikované cílené útoky, je většina útoků necílená. Na zavirovanou přílohu e-mailu nebo na odkaz vedoucí na zavirovanou stránku může kliknout kdokoli. Tyhle běžné lidské chyby jsou přitom nejčastějším způsobem, jak se útočníci dostanou do zařízení obětí i do celých systémů v případě velkých organizací.

Zvláště na pozoru by se ale měli mít ti, kteří uchovávají nějaká citlivá data. Nemusí jít zdaleka jen o nějaké státní strategické informace. Velmi cenné jsou interní firemní údaje, velké databáze klientů a další data, která by neměla nikdy uniknout. Takovéto databáze se stávají častým terčem kyberzločinců, kteří pak požadují výkupné za jejich rozšifrování, případně nezveřejnění.

Jak důkladně je chráněna kritická infrastruktura?
Kritická infrastruktura je dost široký pojem. Pod naši regulaci spadá kritická informační infrastruktura, což jsou komunikační a informační systémy provozované některým prvkem kritické infrastruktury, jak ji definují jiné zákony. Každopádně tyto systémy podléhají nejvyšším požadavkům na zabezpečení.

Různé organizace i firmy se v minulosti staly cílem ransomwarového útoku. Jak se dá účinně proti těmto útokům bránit? Jak se NÚKIB staví k vyplácení výkupného útočníkům?
Ransomware je dlouhodobě na vzestupu. Provozuje jej řada zločineckých skupin a dá se pořídit i jako služba, kterou si prostě pronajmete. Pro předcházení těmto útokům jsme vydali kompletní manuál, který je k nalezení na našem webu. Základem je proškolit zaměstnance, jak s počítačem a telefonem zacházet bezpečně. Dále je klíčové zálohování, a to podle pravidla 3-2-1, tj. tři kopie dat, na dvou různých typech médií, z toho jedno mimo pracoviště. Důležitá je také segmentace sítě, aby se nákaza nemohla šířit. A potom mít zpracované a procvičené krizové plány pro případ, že budete přes všechno úsilí zasaženi. Další opatření jsou ve zmíněném manuálu.

Pokud jde o placení výkupného, doporučujeme nikdy neplatit. Neexistuje žádná záruka, že pak útočník data odemkne, a navíc to podporuje kriminální činnost. Nehledě na to, že i z právního hlediska to může být dost komplikované, ale to už bychom zabíhali do podrobností.

Které kybernetické hrozby kromě zmíněného ransomwaru považujete v současné době za nejzávažnější a jaké mohou být jejich důsledky?
Kybernetické hrozby nebývají toho charakteru, že přijde jedna, nebo druhá. Spíše se vzájemně doplňují. Základem bývá phishing, tj. podvržený mail, u něhož uživatel na něco klikne a do zařízení se mu dostane škodlivý kód nebo třeba přijde o své přihlašovací údaje. Následovat může třeba ransomware nebo nějaký špionážní software, který krade data a je těžké jeho činnost detekovat. Běžný uživatel se však nejčastěji setká s phishingem, který je bohužel čím dál tím sofistikovanější. Pořád se ještě můžeme setkat s legendárními strýčky z Ameriky a podobnými věcmi, ale jinak už jsou phishingové maily psané čím dál lepší češtinou a je čím dál obtížnější je odhalit. Obvykle se snaží uživatele přesvědčit, aby někam poslal peníze. Ale hrozí i zmíněné krádeže přihlašovacích údajů nebo infikování zařízení škodlivým kódem.

Existuje v dnešní digitální době, kdy jsou prakticky všichni potenciálními cíli útoku, možnost, jak se účinně chránit?
Bezpečnost nefunguje binárně, že buď jste v bezpečí, nebo nejste. Cílem je útočníkům maximálně ztížit úspěšné provedení útoku

a v případě jejich úspěchu zmírnit dopady. Zcela v bezpečí tak nebudete nikdy, ale můžete žít s vědomím, že děláte všechno, co se dělat má. Na individuální úrovni jde o poměrně známé poučky týkající se kvalitních hesel, různých hesel pro různé účty, vícefaktorového ověřování identity, pravidelného zálohování dat, kontroly došlých zpráv na různých platformách (e-mail, sociální sítě atd.), zda jsem je opravdu dostat měl a zda nejsou podvržené, pravidelných aktualizací všech zařízení a tak dále. Doporučit mohu naše osvětové kurzy. Dají se najít na našem webu a jsou volně přístupné veřejnosti. Kdo takovým kurzem projde, získá základní návyky, jak se v kyberprostoru chovat bezpečně.

Na úrovni instituce jde například o segmentaci sítě, systém řízení přístupů, aby neměli všichni všude přístup, opět důsledné zálohování a také pravidelné školení zaměstnanců a obecně uživatelů. NÚKIB před časem ve spolupráci s MV a NAKIT vydal tzv. Minimální bezpečnostní standard. Jde o sérii doporučení, která může aplikovat v podstatě jakákoli organizace, a výrazně tak posílit svoji odolnost vůči kybernetickým hrozbám.

Často slýcháme, obzvláště ve firemním segmentu, že dnes už nejde o to, jestli k nějakému incidentu dojde, ale kdy se tak stane. V souvislosti s tím se často zmiňuje, že už nejde jen o to chránit se před útoky, ale umět se co nejrychleji a nejlépe vyrovnat s jejich následky. Jak se s tímto postojem ztotožňujete?

To všechno je součástí kybernetické bezpečnosti. Na jednu stranu se samozřejmě snažím, abych měl ošetřená všechna problematická místa. To znamená správné technické nastavení systémů, proškolené uživatele, zálohovaná data a tak dále. Ale také mám plány, co budu dělat v případě incidentu. A ideálně budu takové incidenty i cvičit, aby všichni tušili, jak takový incident může vypadat.

Všechno vychází z analýzy rizik. Měl bych vědět, jak cenná data mám ve správě, jaká rizika mi hrozí, jak se proti nim můžu bránit. A na jednotlivá rizika bych měl být schopen najít přiměřená opatření. V okamžiku, kdy má opatření nezafungují, musím mít plán, jak minimalizovat škody a co nejrychleji obnovit fungování organizace, počínaje kritickými funkcemi s postupnou obnovou těch méně důležitých.

Jste garantem akce European Cyber Security Challenge 2021, která je určena mladým talentům v oblasti kybernetické bezpečnosti. Proč jsou takové akce důležité a jak je na tom Česká republika s (ne)dostatkem bezpečnostních expertů?

Česká republika stejně jako celý svět čelí nedostatku expertů na tuto oblast. Kdo dnes studuje kybernetickou bezpečnost, nemusí se rozhodně bát, že by o něj na trhu práce nebyl zájem. Proto je pro nás tak důležité podporovat soutěž, jako je tato. Díky podobným akcím je možné nalézt mladé talenty, dále je podporovat v rozvoji a navázat potřebné kontakty. Jako organizace podporujeme rozvoj budoucích odborníků také spoluprací se školami a prostřednictvím studijních stáží u různých organizačních součástí NÚKIB.

Mimo to máme i řadu vlastních vzdělávacích aktivit a snažíme se maximálně šířit osvětu. Klíčové je, aby vedle dostatečného počtu odborníků mělo co možná největší množství lidí alespoň základní návyky z oblasti kybernetické bezpečnosti. Jen tak se nám podaří vybudovat odolnou společnost, která je jedním ze tří pilířů Národní strategie kybernetické bezpečnosti.

Zabýváte se také osvětou a vzděláváním v oblasti kybernetické bezpečnosti, což potvrzuje i vaše spoluúčast na ECSC. Které další vaše aktivity byste zmínil jako důležité pro zvyšování povědomí o kybernetické bezpečnosti?

Většinu jsem už letmo zmínil, ale zaslouží si trochu bližší popis. Vzdělávací a osvětové aktivity máme rozdělené podle cílových skupin. Pro malé děti máme kurzy formou komiksů, například Vanda a Eda v online světě, případně interaktivní komiks Digitální stopa. Kurzy jsou zaměřené na to, co by žáci prvních stupňů základních škol měli vědět o bezpečném pohybu na síti. Pro druhý stupeň základních škol máme kurz Jsem netvor – tvor, který žije na netu. V něm rizika internetu dětem vysvětlují známí youtubeři, kteří oslovují právě tuto cílovou skupinu a kteří byli ochotní nám pomoct se šířením osvěty. Dále máme e-learningové kurzy základů kybernetické bezpečnosti, například kurzy Dávej kyber, případně kurz Šéfuj kyber, který je věnovaný manažerům kybernetické bezpečnosti. Mimo to máme také specializované kurzy pro zdravotníky, neboť zdravotnictví považujeme za jednu ze svých priorit.

Kromě těchto kurzů je u nás na webu ke stažení i spousta návodů, manuálů a příruček. Kromě zmíněného Minimálního bezpečnostního standardu jsme vydali také Bezpečnostní standard pro videokonference, Příručku kybernetické bezpečnosti pro top management, návod, jak se bránit útokům ransomwarem, a řadu dalších materiálů.