Lukáš Kintr

V roce 2015 působil jako auditor kybernetické bezpečnosti Národního centra kybernetické bezpečnosti, které bylo do roku 2017 součástí NBÚ, a později na NÚKIB působil jako vedoucí oddělení kontroly. Od září 2019 se stal náměstkem ředitele NÚKIB pro řízení NCKB. Od 1. července 2022 je Lukáš Kintr ředitelem Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

Marika Vitnerová

Lukáš Kintr: **Největším problémem je nedostatečné povědomí uživatelů o kybernetické bezpečnosti**

Kybernetická bezpečnost patří v poslední době mezi nejdiskutovanější bezpečnostní témata. Je to přirozená reakce na kyberkriminalitu a kyberhrozby. Podle Lukáše Kintra, ředitele Národního úřadu pro kybernetickou a informační bezpečnost, lze ochránit data samosprávy, školy i nemocnice tím, že na bezpečné uložiště budou pravidelně zálohovat svá data a konzistenci zálohovaných dat testovat.

Úřad se v létě stal vnitrostátním orgánem certifikace kybernetické bezpečnosti. Co to pro služby na našem trhu znamená a jaký význam mají ověřené konkrétní produkty?

Určením NÚKIB jako vnitrostátního orgánu certifikace kybernetické bezpečnosti splnila Česká republika svoji povinnost vůči Evropské unii. Smyslem certifikace je zvyšování důvěry veřejnosti v produkty, služby a procesy v oblasti informačních a komunikačních technologií skrze jejich bezpečnost. Pokud obdrží certifikaci, bude zřejmé, že splňují stanovené bezpečnostní požadavky. Výhodou bude především uznávání certifikátů v celé EU. Takže pokud bude mít výrobce certifikaci v ČR, může prokázat bezpečnost svých výrobků i v kterékoliv jiné unijní zemi.

Válka na Ukrajině se promítla i do online světa. Z pohledu množství DDoS útoků byl podle statistik rekordní březen a duben, kdy se na české instituce a firmy útočilo nejčastěji z Ruska. Z toho vyplývá, že útoky lze očekávat při podobných událostech. Co dalšího může vést k útokům?

Je to poprvé, co můžeme spojit válečný konflikt s vlnou kyberútoků na Českou republiku. Podle posledních dostupných informací DDoS byly útoky převážně hacktivistického rázu. Skupiny upozorňovaly na svou existenci a snažily se především vystrašit své oběti. Tato kampaň tak byla součástí hybridní války vedené proti nám. Vlny incidentů jinak všeobecně nejčastěji sledujeme při zjištění nových zranitelností, což je označení pro chybu, která v softwaru nebo v hardwaru způsobuje bezpečnostní problém.

Vydali jste přehled Kybernetických incidentů. Jaké jsou aktuální trendy zaznamenaných útoků?

Mezi trvalé trendy patří útoky, které narušují dostupnost služeb. K tomu dochází v důsledku například DDoS útoků, technických chyb nebo ransomwarových útoků. Dalším trendem jsou takzvané průniky, což může být například kompromitace aplikace nebo uživatelského účtu. Nelze opomenout také phishing a vishing, tedy podvodné zprávy a telefonáty. Uvedenou formu útoků se snaží útočníci neustále zdokonalovat. Například podvodné e-maily dříve bylo možné rozeznat na první pohled díky nekvalitní češtině. Stejně tak podvodné telefonáty často nevedli příliš dobře česky mluvící jedinci. Dnes je to jinak. Své metody podvodníci skutečně zlepšují, a pokud oběť není pozorná, může lidově řečeno snadno naletět.

> „Je nezbytné si uvědomit, že kybernetická bezpečnost je nedílnou součástí světa kolem nás.

Kyberútokům už čelily i některé úřady, které musely odstavit agendy a po této zkušenosti začaly prostřednictvím dotačních programů investovat do kyberbezpečnosti. V čem jsou samosprávy zranitelné, které oblasti podceňují?

Obecně lze podceňované oblasti, a to nejen u samospráv, rozdělit do dvou rovin – technické a organizační. Mezi technické nedostatky často patří zastaralé nebo ne-

aktualizované systémy, u kterých jsou pak známé zranitelnosti jednoduše zneužitelné. A právě aktualizace, případně obnova, zranitelnosti odstraňují. Dalším technickým problémem je nevhodné rozdělení sítě, která není například dostatečně rozčleněná do více částí a není řízena komunikace mezi těmito částmi. Pokud takovou síť napadne škodlivý kód, například ransomware, dojde k jeho rozšíření do celé sítě a dokáže způsobit rozsáhlé škody. Jako další příklad lze uvést nedostatečné zálohování dat či nedostatečně zabezpečený VPN přístup. Na organizační úrovni se pak jedná například o nedostatečně nebo nevhodně stanovená pravidla v oblasti kybernetické bezpečnosti či nedostatečné proškolení uživatelů i administrátorů. Stále totiž platí, že většina útoků je zapříčiněna lidskou chybou. Pomoci s osvětou v různých oblastech se snažíme formou volně dostupných e-learningových kurzů na našem webu osveta.nukib.cz.

Digitalizace služeb úřadů je jistě cesta správná, ale ruku v ruce v ní vidím i rostoucí nebezpečí. Co je nyní největším strašákem v oblasti informačních systémů?

Největším problémem je obecně nedostatečné povědomí uživatelů o kybernetické bezpečnosti. Další hrozbou rovněž může být zanedbání principu secure-by-design, tedy že při pořizování informačních systémů nejsou dostatečně stanoveny požadavky na jejich bezpečnost. Zavádět bezpečnostní opatření až při ostrém provozu je často nákladnější a složitější vzhledem k tomu, že daný systém je již využíván. Je nezbytné si uvědomit, že kybernetická bezpečnost je nedílnou součástí světa kolem nás. Stejně jako se pravidelně školíme třeba v oblasti bezpečnosti práce, je potřeba věnovat dostatečnou pozornost i kyberbezpečnosti.

Mohou instituce snížit hrozbu kybernetických útoků i tím, že nebudou využívat zbytečné množství různých technologií, které je třeba individuálně spravovat a chránit?

Je to situace „něco za něco“. Pokud bude infrastruktura monolitická, je výhodou, že aktualizace a další správa takové infrastruktury je mnohem jednodušší. Zároveň je však pro útočníka snadno čitelná a ten tak může jednodušeji vyřadit její velkou část. Při větším množství různých technologií je pro útočníka složitější se v takové infrastruktuře pohybovat a zmapovat ji. Na druhou stranu je zde vyšší pravděpodobnost „zapomenutých“ neaktualizovaných nástrojů. Správa takové infrastruktury je samozřejmě pro vlastníka mnohem složitější.

Je možným řešením, jak ochránit data pro místní samosprávy, školy nebo nemocnice, vlastnit bezpečné úložiště?

Ano, pokud budou na bezpečné úložiště pravidelně zálohovat svá data a konzistenci zálohovaných dat testovat. V případě ztráty dat je pak důležité mít funkční a v praxi otestovaný proces zpětné obnovy. Pokud jsou

> Univerzální postup, který by fungoval pro všechny, existovat nemůže. Proto by subjekty měly mít vlastní plán, který je tvořen na míru přímo jim a obsahuje postupy, jak v případě napadení jednat.

úložiště v cloudu, doporučuji mít data šifrovaná. Pokud je v lokální infrastruktuře, je důležité zajistit, aby byl zálohovací server mimo produkční infrastrukturu.

Existuje vůbec nějaké komplexní řešení na stanovení optimálního bezpečnostního opatření?

Ti, co spadají pod regulaci zákona o kybernetické bezpečnosti, se musí řídit zákonem a mají mnoho věcí jasně stanoveno. Subjekty, které pod regulaci nespadají, mohou využít Minimálního bezpečnostního standardu, který náš úřad připravil ve spolupráci s partnery. Zvýší se tak úroveň kybernetické bezpečnosti vlastní organizace. V tom může pomoci i Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti, kterou jsme připravili také společně s partnery.

Máte pro města a obce doporučení, co mají dělat, když dojde k napadení informačního systému?

Existují samozřejmě základní rady a postupy, jak se chovat při kybernetických incidentech. Problémem je ovšem jedinečnost jednotlivých organizací, jejich systémů a sítí a také rizik, která dané organizace ohrožují. Univerzální postup, který by fungoval pro všechny, existovat nemůže. Proto by subjekty měly mít vlastní plán, který je tvořen na míru přímo jim a obsahuje postupy, jak v případě napadení jednat. Případný incident je potřeba hlásit na Národní nebo Vládní CERT, kde jsou schopni pomoci s analýzou a dalšími kroky. Zjednodušeně, subjekty regulované zákonem o kybernetické bezpečnosti spadají pod Vládní CERT, ostatní subjekty mohou hlásit takovou událost na Národní CERT. Oba týmy ale spolu úzce spolupracují.

Upozorňujete na phishingové kampaně s cílem zneužít bankovní identitu a máte k tomu doporučení. Kyberbezpečnost tedy není věc jen ajťáků, ale zodpovědnost nás všech. Mám v tu chvíli pocit, když se to týká i mě, že se raději chci odpojit od internetu úplně. Je ostražitost na místě?

Kyberbezpečnost se opravdu týká každého z nás a bohužel nelze jednoznačně říct, zda jste v bezpečí, nebo ne. Na druhou stranu toho můžeme pro svou bezpečnost na internetu spoustu udělat. Jednou z věcí je vzdělávat se. Například v našich kurzech se můžete seznámit s různými typy útoků, na co si dát v kyberprostoru pozor a čemu se vyvarovat. Není potřeba se bát, jen je potřeba zůstat ostražitý a myslet na to, že každý klik může být nebezpečný. Když si budeme hlídat, na co se díváme, co otevíráme, co kam píšeme, jaké stránky navštěvujeme nebo co stahujeme, významně snížíme riziko, že se staneme obětí kyberútoku.

Když zjistíme, že jde o podvodnou zprávu, kam ji můžeme hlásit?

V případě, že se setkáte jako organizace nebo úřad s podvodnou zprávou (phishing) nebo podvodným telefonátem (vishing), informujte Národní nebo Vládní CERT. Pokud se vám něco takového stane jako občanovi, obraťte se na Policii ČR.

Dokážete vyjmenovat tři věci, které je schopen starosta, zastupitel, úředník nebo i já udělat hned, aby posílil svoje bezpečí v kyberprostoru?

Je těžké jmenovat jen tři věci. Pokud se bavíme o jednotlivci, který chce navýšit svou bezpečnost, tak to jsou základní návyky, které si lze osvojit – zálohovat data, mít kvalitní a pro každou službu unikátní hesla, vícefaktorové ověřování identity, pravidelné aktualizace nebo si kontrolovat došlé zprávy. O obezřetnosti jako takové jsem již mluvil. Základem je prostě osobní zodpovědnost každého z nás. Důležité je pravidelně investovat do kvalitních školení týkajících se kybernetické bezpečnosti. Jako základ doporučuji zmíněné vzdělávací kurzy na našem webu. V neposlední řadě je také dobré si u svých „IT bezpečáků“ ověřit, zda všechna technika a sítě vaší organizace splňují minimální bezpečnostní standardy, které NÚKIB v minulosti vydal.

Jaké online komunikační formy doporučujete používat pro veřejnost i pro instituce?

Náš úřad přímo nedoporučuje konkrétní formy či aplikace pro komunikaci. Vydali jsme ale analýzu komunikačních aplikací s end-to-end šifrováním. V ní poskytujeme informace, které by měly posloužit jak veřejnosti, tak regulovaným subjektům k tomu, aby udělaly informované rozhodnutí, který nástroj budou pro komunikaci používat. Také jsme vydali bezpečnostní standard pro videokonference. Kromě uvedených materiálů jsme v únoru 2022 zveřejnili doporučení, jak bezpečně používat aplikaci Signal. Všechny informace se dají najít u nás na webu.

Dojde u něčeho z toho, co jsme si řekli, v budoucnu ke změně na legislativní úrovni? Mají obce a další organizace čekat velké změny?

Ke konci tohoto roku dojde na úrovni EU k přijetí nové směrnice o kybernetické bezpečnosti – takzvaná NIS2. Směrnice přináší mnoho změn v oblasti kybernetické bezpečnosti a bude se týkat velkého množství organizací, které zatím pod regulaci NÚKIB nespadaly, a tudíž nemusely plnit žádné povinnosti. Hovoříme tu o více než 6 000 subjektech, které budou rozděleny do dvou režimů povinných osob – „important“ a „essential“. Režim „important“ se bude řídit současnou vyhláškou o kybernetické bezpečnosti a subjekty v „essential“ režimu budou plnit povinnosti na základě nové vyhlášky, která bude obsahově od vyhlášky o kybernetické bezpečnosti odvozena. ČR však může nyní těžit z kvalitně zpracovaného zákona o kybernetické bezpečnosti, protože velká část změn, které přijdou se směrnicí NIS2, míří směrem k současné české regulaci. Pro subjekty, kterých se týkala původní směrnice NIS, se toho v praxi příliš měnit nebude. ■

foto: archiv NÚKIB