Foto: Shutterstock

Kyberkriminalita v právní praxi

Trendem posledních let je přesun stále významnější části běžných činností do on-line prostředí. Tato forma jednání a komunikace ovšem vytváří ideální podhoubí pro kyberkriminalitu.

Strmý nárůst kybernetických útoků by měl přesvědčit každého, že problematiku bezpečnosti dat není radno podceňovat. V médiích se stále častěji objevují zprávy o provedených kybernetických útocích, jejich závažnosti, obsahu zasažených dat anebo výši způsobené škody. Tyto útoky se nevyhýbají ani České republice.

Jedny z nejčastějších typů kybernetických útoků se uskutečňují formou takzvaného ransomwaru, tedy jakéhosi digitálního vydírání. Tyto útoky ve většině případů nemají za cíl zneužít získaná data, ale jejich uzamknutím (znepřístupněním) přimět jejich vlastníka k zaplacení výkupného za opětovné zpřístupnění uzamknutých souborů. Nutno podotknout, že zaplacením výkupného není zaručeno obnovení přístupu k souborům nebo jejich funkčnosti.

V Česku téměř každá třetí firma

Zpráva The State of Ransomware 2021 od bezpečnostní společnosti Sophos sleduje výskyt těchto útoků ve společnostech ve třiceti zemích světa, mezi nimi i ve sto společnostech sídlících v České republice. V roce 2021 bylo v České republice podle této studie nějakou formou ransomwaru zasaženo 30 procent dotázaných společností. Výše požadovaných částek za odemčení zasažených systémů se liší v návaznosti na několik faktorů, zejména velikost zasažené společnosti a také komplexnost daného útoku. Průměrná hodnota negativního dopadu ransomwarového útoku je v České republice v přepočtu okolo sedmi milionů korun. Ač se tato částka může zdát vysoká, je s ohledem na výsledky zprávy Sophos významně pod evropským průměrem, i tak se ale jedná o významný finanční obnos.

Příslušným správním orgánem v oblasti kybernetické bezpečnosti je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Ten uvádí, že se v roce 2021 jedním z nejvyhledávanějších cílů ransomwarových útoků stali poskytovatelé právních služeb, a to v těsném závěsu za nejvíce zasaženým sektorem stavebnictví. Kyberútoky se samozřejmě nevyhýbají ani institucím veřejného sektoru, ministerstvům, významným specializovaným nebo obecním či krajským úřadům, včetně Magistrátu hlavního města Prahy. Komplexní analýza zasažených odvětví je však obtížná, a to zejména proto, že povinnost informovat o proběhnuvším kyberútoku doléhá pouze na povinné osoby dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, tedy orgány veřejné moci a subjekty poskytující pro stát zásadní služby. O zbylých incidentech víme pouze na základě dobrovolného hlášení.

Zvlášť zranitelným odvětvím je pak sektor zdravotnictví. NÚKIB ve své rubrice Kybernetické incidenty pohledem NÚKIB říjen 2021 mimo jiné uvádí, že české zdravotnictví čelí i rok a půl po vypuknutí koronavirové pandemie zvýšenému počtu útoků hackerů, který neustále narůstá, a zároveň se zvyšuje i jejich sofistikovanost. Za rok 2019 nahlásily zdravotnické organizace šest takových incidentů, v roce 2020 to bylo 16 a v letošním roce hlásí NÚKIB ke konci října již 24 notifikovaných útoků. Zde je však nutno podotknout, že s novelou vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, došlo k rozšíření kritérií, na základě nichž subjekt spadá či nespadá pod definici

Průměrná hodnota negativního dopadu ransomwarového útoku je v České republice v přepočtu okolo sedmi milionů korun.

provozovatele základních služeb. Tím pádem je i více subjektů, na něž příslušná povinnost dle zákona o kybernetické bezpečnosti notifikace o proběhnuvších útocích dopadá.

Historicky první ochranné opatření NÚKIB

V bezpečnosti, i té kybernetické, platí zlaté pravidlo, že nejúčinnější ochranou před útokem je prevence. NÚKIB v duchu tohoto pravidla vydal v říjnu tohoto roku historicky první ochranné opatření na základě § 14 zákona o kybernetické bezpečnosti. V souladu s tímto opatřením budou muset povinné subjekty adekvátně zabezpečit své e-mailové schránky. Nic však nebrání ostatním subjektům aplikovat takto nastavený standard zabezpečení i do jejich provozu a minimalizovat tak případně nedostatečně nastavené zabezpečení. Samotné ochranné opatření NÚKIB zároveň doprovází podrobná technická metodika a dále odpovědi na nejčastěji pokládané otázky, jež těm, kteří jsou k tomu povinni nebo se rozhodnou tento standard aplikovat dobrovolně, ozřejmí důvody NÚKIB, které stojí za zaváděnými pravidly, a další podrobnosti.

K vydání ochranného opatření došlo na základě analýzy kybernetického bezpečnostního incidentu, který byl způsoben útokem typu Man-in-the-Middle. Tehdy se útočník dostane do pozice prostředníka mezi komunikujícími subjekty, čímž naruší důvěrnost přenášených elektronických zpráv. Tento konkrétní útok byl veden právě prostřednictvím e-mailu.

Jak v reflexi na vydání ochranného opatření uvedl ředitel NÚKIB, Karel Řehka, *„(…) e-mail je z pochopitelných důvodů velmi rozšířený a v podstatě nezastupitelný, ale obecně nepatří k nejbezpečnější formě komunikace. Proto jsme vypracovali sérii opatření, která výrazně komplikují odposlouchávání této komunikace či její podvržení“*. Zavedení plošného ochranného opatření pro zajištění bezpečnosti elektronicky předávané komunikace bylo tak dle NÚKIB nezbytné, neboť pro zajištění dostatečné ochrany je nutné, aby měly požadované prvky ochrany zavedeny oba komunikující subjekty. V opačném případě probíhá celá komunikace v nedostatečně zabezpečeném prostředí, a ochrana přijatá pouze jednou z komunikujících stran tak zcela postrádá smysl.

Dalšími motivy NÚKIB pro zvýšení technických požadavků na úroveň zabezpečení e-mailové komunikace je kromě obecného významu komunikace soukromoprávních subjektů, a to mezi sebou, tak i směrem k orgánům veřejné moci, jakož i spíše opomíjený význam komunikace mezi orgány veřejné moci samotnými. Mimořádně významným činitelem v průběhu přípravy ochranného opatření

bylo i nadcházející předsednictví České republiky v Radě EU. Především s ohledem na hrozbu narušení bezpečnosti vzájemné komunikace orgánů veřejné moci při zajišťování úkolů v rámci předsednictví České republiky v Radě EU a s ohledem na narušení řádného průběhu našeho předsednictví a tím i snížení důvěryhodnosti České republiky v očích mezinárodní veřejnosti se NÚKIB rozhodl uvalit povinnost zavedení výše popsaného ochranného opatření na širší než minimální základnu subjektů využívajících e-mailovou komunikaci v rámci svého každodenního fungování.

Povinnými subjekty ochranného opatření jsou především orgány veřejné moci a subjekty poskytující zásadní služby. Tedy především správci a provozovatelé informačních a komunikačních systémů kritické informační infrastruktury, provozovatelé významných informačních systémů a informačních systémů základní služby, kteří jsou takto klasifikovaní přímo dle zákona o kybernetické bezpečnosti.

I přesto, že se výčet subjektů povinných zavést ochranné opatření NÚKIB zdá být velmi široký, běžní uživatelé (například občané a soukromé společnosti) se nemusí obávat jakéhokoli omezení při komunikaci se subjekty spadajícími do této kategorie. Výsledkem ochranného opatření by kromě zabezpečení komunikace mezi povinnými osobami mělo být také zvýšení ochrany i v rámci komunikace mezi nimi a veřejností samou. Tohoto efektu NÚKIB hodlá dosáhnout zavedením požadavků ochranného opatření směřujících mimo jiné k zamezení podvržení e-mailové komunikace zasílané prostřednictvím podvržené domény organizace.

Ochrana ve smluvních vztazích

Konkrétním technickým požadavkům ochranného opatření se věnuje již zmíněná technická metodika k zavedení způsobů zvýšení ochrany, podle které se ochranná opatření dají rozdělit do tří podkategorií:

- opatření pro zajištění důvěrnosti a integrity komunikace mezi poštovními servery;
- opatření pro zajištění důvěrnosti a integrity komunikace mezi klientem elektronické pošty a serverem; a
- opatření pro zajištění integrity a zamezení podvržení odesílatele elektronické poštovní zprávy.

Samotný obsah ochranných opatření, potažmo metodiky, je pak čistě v rovině technických bezpečnostních požadavků, a proto je před implementací daných pravidel nutná konzultace s odborníky v příslušné oblasti.

Účinky ochranného opatření se promítnou mimo jiné do stávajících smluvních vztahů povinných osob (či osob dobrovolně zavádějících nová pravidla NÚKIB). Citelné budou pro povinné osoby především účinky ochranného opatření na smluvní vztahy s dosavadními dodavateli jejich informačních nebo komunikačních systémů, jejichž fungování ochranné opatření upravuje. Povinné osoby budou v těchto případech muset zahrnout požadavky vyplývající z ochranného opatření do existující smluvní dokumentace tak, aby byly zohledněny v již fungujících systémech, případně nebude-li dodavatel schopen požadavkům dostát, urychleně přistoupit k výběru dodavatele nového.

Ochranné opatření samozřejmě zasáhne i do oblasti zadávání veřejných zakázek a do možné aplikace výjimky dle § 29 písm. c) zákona o zadávání veřejných zakázek, dle kterého: *„Zadavatel není povinen zadat veřejnou zakázku v zadávacím řízení, jde-li o zadávání nebo plnění veřejné zakázky v rámci zvláštních bezpečnostních opatření stanovenými jinými právními předpisy a současně nelze učinit takové opatření, které by provedení zadávacího řízení umožňovalo“*. Podle NÚKIB je na zvážení každé povinné osoby, která bude zároveň v pozici zadavatele dle zákona o zadávání veřejných zakázek, zda je institut této výjimky, s ohledem na specifické okolnosti a podmínky dané organizace, použitelný. Bude tedy zřejmě nutné, aby se současní a budoucí dodavatelé stěžejních systémů povinných osob úžeji zapojili do posouzení stavu infrastruktury příslušné povinné osoby a zda tato odpovídá požadavkům ochranného opatření.

Technická metodika pak odkazuje na několik veřejně přístupných nástrojů, v nichž si může každý jednotlivec nebo společnost v několika krátkých krocích orientačně otestovat zabezpečení své e-mailové komunikace, a to jak její příjem, tak i odesílání. Jedním z takto doporučených nástrojů je My Email Communications Security Assessment vytvořený pro tento účel přímo Evropskou komisí.

■■■

I v případě, že nejste osobou povinnou dle zákona o kybernetické bezpečnosti anebo se na vás ochranné opatření NÚKIB přímo nevztahuje, lze jen doporučit klást na otázku bezpečnosti dat ten největší důraz. Jak je patrné ze současného stavu kyberprostoru a houževnatosti jeho narušitelů, jedná se o zcela zásadní téma, jehož vývoji a důsledkům bude čelit téměř každý z nás.

E-mail je z pochopitelných důvodů velmi rozšířený a v podstatě nezastupitelný, ale obecně nepatří k nejbezpečnější formě komunikace.

Pavel Amler
senior advokát,
Havel & Partners

Matěj Kurtin
koncipient,
Havel & Partners