číslo 3 | ročník 2019

Právo a bezpečnost

OBSAH

PRÁVO A BEZPEČNOST, ČÍSLO 3, ROČNÍK 2019

CONTENT

LAW AND SECURITY, ISSUE 3, YEAR 2019

EDITORIAL

STÁTNÍ ZNAK NEBO LOGO

Stát je reprezentován státním znakem. Ten je v případě evropských států staletým symbolem určité země. Stát jej chrání a jeho užívání je bezplatné. Naproti tomu logo je záležitostí proměnlivé módy a jeho autoři pobírají peníze za autorská práva. Logo nemá vyšší přínos, než který má státní znak.

Přesto některé státní úřady vymýšlí různá loga a platí za ně. Jsou to vyhozené peníze. Ocenění log je subjektivní. Fakticky jde o projev špatného hospodaření a vyvedení veřejných peněz do něčí soukromé kapsy.

Proto zaráží snaha Ministerstva průmyslu a obchodu vytvořit další logo státu a vnutit jej všem vládním úřadům. Tím by tyto úřady zmarnily peníze vložené do současných log, a ještě více se omezí užívání státního znaku. Čím více úřadů bude nové logo užívat, tím více bude autor žádat za autorská práva. Bude to dražší. Hledání loga státu se tak stává tunelováním státu.

Že je takový plán ministerstva protiprávní, je pro něj asi vedlejší. Zákon o působnosti Ministerstva průmyslu a obchodu mu nedává pravomoc vymýšlet loga státu a vnucovat je jiným úřadům. Navíc ústava státní symboly zakotvuje právě za účelem užití pro prezentaci státu a jeho orgánů. Proto je činnost ministerstva nezákonná i neústavní. Je to stejně nepřípadné, jako kdyby ministerstvo chtělo nahradit státní hymnu nějakou znělkou nebo státní vlajku transparentem. Ministerstvo průmyslu a obchodu projevuje neúctu ke skutečným státním symbolům.

Státní znak byl vytvořen parlamentem s vědomím toho, že stát vznikl ze tří zemí – Čech (na červeném štítě stříbrný korunovaný lev), Moravy (na modrém štítě stříbrnočerveně šachovaná korunovaná orlice) a Slezska (na zlatém štítě černá korunovaná orlice), což je vyjádřeno ve velkém státním znaku. Existuje i malý státní znak ve formě znaku Čech (stříbrný lev), který zákon určuje především pro razítka, jež mají malou plochu, a figury čtvrceného velkého státního znaku by na nich mohly být nezřetelné. Ministerstvo však uvažuje o výlučném užití českého lva, což je pohrdáním staleté sounáležitosti obyvatel Moravy a Slezska s jejich symboly. Proto je správné, se Ministerstvu průmyslu a obchodu vzepřít a chránit skutečné státní symboly.

Zdeněk Koudelka

Předseda redakční rady

REAKCE NA KYBERNETICKÉ BEZPEČNOSTNÍ UDÁLOSTI A INCIDENTY

Lubomír Almer, Rudolf Urban

1. ÚVOD

S narůstajícím podílem informačních a komunikačních technologií v každodenním fungování společnosti dochází paralelně ke vzniku nových kybernetických bezpečnostních hrozeb. Ruku v ruce s těmito hrozbami vyvstává potřeba ochrany vůči nim. Jedním z klíčových prvků takovéto ochrany je identifikace a reakce atypických situací, kterými se dané působení hrozeb na námi chráněné prvky vyznačuje. Identifikací je v tomto kontextu myšlena zejména detekce kybernetických bezpečnostních událostí a následná práce s nimi. Detekce samotná by měla být realizována na více úrovních a pouze komplexní pokrytí všech úrovní vede k úspěšné minimalizaci kybernetického bezpečnostního dopadu na námi chráněná aktiva, a to zejména díky efektivnímu procesu řízení kybernetických bezpečnostních událostí a incidentů. Z hlediska komplexnosti kybernetické bezpečnosti však na detekci musí být navázaný další reakční kroky.

2. ŘÍZENÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

Samotná reakce na kybernetické bezpečnostní hrozby by měla být rozdělena do dvou úrovní. Rozdělení by mělo být na úrovni, zda již byl aktivován zdroj hrozby či nikoliv. Reakce na neaktivované hrozby spočívá zejména ve stanovení řídících a kontrolních opatření, a to s ohledem a ve vztahu ke kritičnosti daných aktiv na která může daná hrozba působit. Tato kontrolní a řídící opatření se doporučuje zanést do strategie rozvoje bezpečnosti s konkrétním implementačním plánem daných opatření v čase. Implementace řídících a kontrolních opatření na kybernetické hrozby je vzhledem ke komplexnosti a složitosti celého procesu velice zdrojově nákladná. Ukazuje se žádoucí tuto implementaci důkladně naplánovat, a to zejména s ohledem na vypracovanou analýzu rizik a to tak, aby v prvé řadě byla zohledněna rizika ohodnocená jako kritická, následně rizika ohodnocená jako vysoká a až poté implementovat opatření na rizika střední a nízká. Optimální se jeví implementace opatření, která pozitivně ovlivní nejširší množinu identifikovaných a hodnocených rizik

a sníží tak pravděpodobnost aktivace zdroje hrozeb. Strategie rozvoje bezpečnosti by tak měla poskytovat dostatečně detailní přehled a plán reakce na neaktivovaná rizika. Jako reakce na rizika, která byla aktivována se doporučuje vytvoření procesu řízení kybernetických bezpečnostních událostí a incidentů. Při tvorbě procesu je žádoucí dodržení šesti dílčích částí, které se neustále opakují a utváří tak cyklický proces. Jedná se o části:

- přípravy;
- detekce;
- analýzy;
- investigace;
- reakce;
- aktivit po incidentu.

Proces řízení bezpečnostních událostí a incidentů popisuje řízení životního cyklu bezpečnostních událostí a incidentů vzniklých během provozování služeb organizace, přičemž slouží jako podpůrný prostředek pro zajištění efektivní a účinné reakce na vzniklé události a incidenty. Cílem navrhovaného procesního postupu je zejména minimalizace kybernetického dopadu na aktiva či obchodní procesy organizace. Podobu procesu řízení kybernetických bezpečnostních událostí a incidentů prezentuje obrázek 1.

Obr. 1: *Proces řízení kybernetických bezpečnostních událostí a incidentů*

Zdroj: vlastní zpracování

2.1 PŘÍPRAVA

Tato část procesu řízení kybernetických bezpečnostních událostí a incidentů spočívá zejména v identifikaci chráněného prostředí a modelování hrozeb, které toto prostředí mohou ovlivnit. V rámci přípravy se rovněž doporučuje investice do vzdělání a znalostí řešitelského týmu. Do části přípravy by měly být zahrnuty veškeré činnosti uvedené v reakci na neaktivované hrozby.

2.2 DETEKCE

Detekce kybernetické bezpečnostní události je jedním z primárních vstupů do celého reakčního procesu. Detekce samotná představuje základní předpoklad pro realizaci jednotlivých kroků uvedených v procesu řízení kybernetických bezpečnostních událostí a incidentů. Bez aktivace části detekce nejsou aktivovány další kroky procesu. Detekci se doporučuje realizovat na třech úrovních, které jsou uvedeny následovně:

- **Automatizovaná detekce** prostřednictvím technických/technologických řešení. Tento typ detekce poskytuje automatizované třídění a analýzu zdrojových dat v reálném čase za účelem identifikace potenciálního průniku či narušení chráněného prostředí. Korelace událostí je prováděna dle předem stanovených scénářů. Automatizovaně jsou prováděny analýzy bezpečnostních událostí, určení jejich závažnosti a potenciálu narušit námi chráněnou část organizace, a to zejména prostřednictvím nástroje pro podporu bezpečnostního monitoringu.
- **Manuální nahlášení** události nebo incidentu uživatelem či zainteresovanou stranou nastává v případě, že je danou osobou identifikováno atypické chování aplikací a IT infrastruktury. Samotné nahlášení by dále mělo probíhat ustanoveným postupem a to tak, že je daná skutečnost nahlášena odpovědné osobě, která ji postoupí vyhodnocení v podobě analýzy.
- **Identifikace** členem či členy řešitelského týmu **v průběhu investigace** existujícího incidentu. Členové týmu mohou identifikovat podezřelé skutečnosti i z bezpečnostních technologií a analytických nástrojů, při řešení jiných incidentů a ostatních činností nesouvisejících s řešením konkrétního bezpečnostního incidentu. V případě identifikace dříve nezjištěného bezpečnostního incidentu je tento incident postoupen procesu řízení kybernetických bezpečnostních incidentů.

2.3 ANALÝZA

Jedná se o následný krok po aktivaci detekce. V tomto dílčím kroku je realizováno rozhodnutí, zda se jedná o kybernetický bezpečnostní incident či nikoliv. Pro toto rozhodnutí je v některých případech nezbytné doplnění znalostí či informací. Zde je nezbytné definovat konkrétní informační kanály, kterými může dojít k obohacení znalostí a doplnění informací nezbytných k tomuto rozhodnutí. V případě, že se nejedná o bezpečnostní incident, je vhodné realizovat změnu v detekci, zejména změnou detekčních technik a zde krok detekce končí a nejsou realizovány žádné následující aktivity. V případě, že se jedná o bezpečnostní incident, doporučuje se tento incident postoupit dalšímu kroku procesu řízení kybernetických bezpečnostních událostí a incidentů a to investigaci.

2.4 INVESTIGACE

V rámci investigace by mělo dojít ke stanovení priority kybernetického bezpečnostního incidentu a návrhu reakčních kroků. Prioritu kybernetického bezpečnostního incidentu se doporučuje stanovit zejména na základě informací získaných v předchozích krocích v kombinaci se znalostmi řešitelského či reakčního týmu. Primárním cílem investigace je však stanovení způsobu realizace reakce na kybernetický bezpečnostní incident. Sekundárním cílem je zpřesnění předchozí analýzy. Doporučuje se, aby podrobná analýza byla realizována nad informacemi z různých datových zdrojů zapojením veškerých členů řešitelského týmu s cílem odpovědět na otázky:

- kdo;
- co;
- kdy;
- kde;
- proč;
- jaký je rozsah narušení bezpečnosti;
- jak je možné omezit dopad.

V případě potřeby je žádoucí, aby tato podrobná analýza kybernetického bezpečnostního incidentu byla doplněna či rozšířena o informace od externích specialistů, jakými jsou například technologičtí partneři pro danou technologii, která kybernetický bezpečnostní

incident detekovala, či informace od poradenských a konzultačních společností, které se přímo na takovéto případy specializují.

V průběhu investigace se může ukázat žádoucí aktivace dočasného řešení ke zmírnění dopadu daného bezpečnostního incidentu. Investigace však nekončí tímto dočasným řešením. Krok investigace je realizován opakovaně až do situace, kdy je nalezeno trvalé řešení kybernetického bezpečnostního incidentu.

2.5 REAKCE

V rámci reakce se doporučuje realizovat aktivity vedoucí k neutralizaci bezpečnostního incidentu, dle postupu, který byl ustanoven v investigaci. Před aktivací reakčních kroků je nezbytné celou reakci zkoordinovat. Pro koordinaci je vhodné ustanovení koordinátora kybernetického bezpečnostního incidentu. Tento koordinátor by měl disponovat dostatečnými znalostmi a zkušenostmi v dané oblasti, které jsou pro vykonání rozhodnutí zcela nezbytné. V rámci reakce se doporučuje realizovat zejména kroky:

- Omezení rozsahu dopadu pro minimalizaci negativního dopadu daného kybernetického bezpečnostního incidentu.
- Izolaci napadených systémů či aktiv (aktivní obrana) pro minimalizaci kompromitace dalších systémů či aktiv (například v podobě logické či fyzické izolace dotčených systémů).
- Neutralizaci veškerých identifikovaných a útočníkem zanechaných artefaktů (vyčištění dotčených systémů), které by mohly v budoucnu umožnit dotčený systém opětovně diskreditovat či napadnout.
- Návrat napadeného systému či aktiva do plnohodnotného provozu (například obnovou ze zálohy).

2.6 AKTIVITY PO INCIDENTU

O každém kybernetickém bezpečnostním incidentu, který byl postoupen investigaci se doporučuje zaznamenat veškerá zjištěná fakta, a to zejména z důvodu zvýšení informovanosti řešitelského týmu, například pro případ, že by se incident opakoval. Dokumentace kybernetického bezpečnostního incidentu by tedy na základě uvedeného měla přinejmenším obsahovat:

- Shrnutí kybernetického bezpečnostního incidentu.
- Určení příčiny jeho vzniku.
- Vazbu na další kybernetické bezpečnostní události a incidenty, které k tomuto incidentu vedly.
- Výčet provedených aktivit veškerých členů reakčního či řešitelského týmu.
- Hodnocení dopadu daného kybernetického bezpečnostního incidentu.
- Kontaktní informace na veškeré zainteresované strany, které se na řešení podílely.
- Plán opatření vedoucí k zamezení opakování kybernetického bezpečnostního incidentu.
- Zajištění a zaznamenání veškerých informací nezbytných pro reporting v rámci organizace, ale i mimo ni (například národním a nadnárodním autoritám).

V rámci aktivit po incidentu se předpokládá zlepšování procesu řízení kybernetických bezpečnostních incidentů, ale i kybernetické bezpečnosti organizace jako takové.

3. ZÁVĚR

Vzhledem k narůstajícímu množství kybernetických bezpečnostních hrozeb lze předpokládat, že se kybernetická bezpečnost nejen organizací, ale i jednotlivých subjektů bude zvyšovat. Tento fakt je podpořen i integrací informačních a komunikačních technologií do každodenního života, včetně provázanosti těchto technologií a jejich použití nejen v soukromém, ale zejména v pracovním prostředí. Proces řízení kybernetických bezpečnostních událostí a incidentů je jednou ze základních částí kybernetické bezpečnosti. Díky včasnému odhalení aktivované hrozby můžeme zamezit výrazným ztrátám, a to nejen z ekonomického hlediska. V obecné rovině je možné konstatovat, že problematiky kybernetické bezpečnosti musí být neustále rozvíjena, a to zejména za účelem minimalizace hrozeb, které ze zmíněného každodenního používání informačních a komunikačních technologií vyplývají.

Literatura:

ČSÚ. *Informační technologie – Kraj*. In: Český statistický úřad | ČSÚ [online]. 2. 5. 2019. [cit. 2018-04-23]. Dostupné z: https://www.czso.cz/csu/xe/informacni_spolecnost-xe.

Průzkum SophosLabs odhaluje nárůst lokalizovaných kybernetických hrozeb. In: Sdělovací technika [online]. 11. 5 2016. [cit. 2018-04-23]. Dostupné z: http://www.stech.cz/clanky/archiv-a-clanku-a-aktualit/id/2336/pruzkum-sophoslabs-odhaluje-narust-lokalizovanych-kybernetickych-hrozeb.aspx.

STROPNICKÝ, Martin. *Válčení v kyberprostoru se nevyhneme*. In: Ministerstvo obrany [online]. 7. 11. 2016 [cit. 2019-05-10]. Dostupné z: http://www.mocr.army.cz/informacni-servis/forum/valceni-v-kyberprostoru-se-nevyhneme-128489.

ŠULC, Roman. *Evropská komise představila novou Strategii kybernetické bezpečnosti*. In: Evropský bezpečnostní žurnál [online]. 24. 9. 2017 [cit. 2018-04-23]. Dostupné z: https://www.esjnews.com/cs/evropska-unie-strategie-kyberneticka-bezpecnost.

Abstrakt:

Kybernetické bezpečnostní události, které mohou, ale i nemusí přerůst v bezpečnostní incidenty jsou nevyhnutelné a prakticky se s nimi setkáváme denně. Při potenciálním narušení bezpečnosti, tak záleží zejména na rychlosti reakce a efektivitě reakčních kroků. Článek popisuje, jaké kroky by měli být realizovány k zajištění efektivní reakce schopnosti na tyto situace.

Klíčová slova: *kybernetická bezpečnosti, bezpečnostní událost, bezpečnostní incident, hrozba, riziko, aktivum*

Abstract:

Cybersecurity Evants and Incident Reaction

The cybersecurity events they have, but also the access to an overgrowth in security incidents are at risk and can be set up daily. Thus, in the event of a potential security breach, response speed and efficiency of the reaction capabilities are of particular importance. The article describes what steps should be taken to ensure effective responsiveness to these situations.

Keywords: *cybersecurity, security event, security incident, threat, risk, asset*
JEL: H56

Ing. **Lubomír Almer**, Ph.D. – AEC a.s., bezpečnostní specialista, lubomir.almer@aec.cz.
Prof. Ing. **Rudolf Urban**, CSc. – Vysoká škola regionálního rozvoje a Bankovní institut – Ambis, Katedra bezpečnosti a práva, Lindnerova 1, 180 00 Praha, rudolf.urban@ambis.cz.

BEZPEČNOST UŽIVATELŮ E-MAILŮ – VYDĚRAČSKÉ E-MAILY

Vladimír Šulc

1. ÚVOD

V souvislosti s vývojem informačních technologií a internetových sítí se vytvořil zcela nový prostor, do kterého se přemístily nejrůznější aspekty našeho života, a to včetně kybernetických hrozeb. Ovšem vnímání těchto hrozeb se proměňuje stejným způsobem jako vnímání jiných hrozeb ve všedním životě s ohledem na aktuálnost, popřípadě hodnotu konkrétního chráněného zájmu[1].

Je ovšem třeba upozornit, že kybernetické útoky jsou čím dál tím častější a mají potenciál způsobit značnou škodu. Právem se řadí mezi nejzávažnější rizika. Jejich nebezpečnost pro společnost spočívá především v jejich asymetrii, kdy náklady na jejich realizaci jsou zanedbatelné vzhledem ke škodě, kterou mohou způsobit. Dokonce se uvádí se, že dopad kybernetických útoků může být větší než škody, které mají na svědomí přírodní katastrofy a klasické teroristické útoky, protože mohou způsobit selhání kritické infrastruktury, na které jsme čím dál závislejší, ať už chceme nebo ne[2].

Pro pochopení, jakým způsobem probíhají kybernetické útoky na jednotlivé subjekty a jak je možné tyto útoky detekovat a následně zastavit, jsou v následujících kapitolách uvedeny praktické příklady kybernetických útoků.

2. KYBERNETICKÉ ÚTOKY

Hrozba a potenciál kybernetických útoku roste s počtem zařízení připojených do internetu, která mohou být napadena a ze kterých může být veden i následný útok. Ano, řeč je o tzv. internetu věcí, s kterým se budeme setkávat stále častěji. Počet kybernetických útoků po celém světě stále roste a ztráty firem jdou do miliard dolarů. Roste počet zařízení připojených do internetu, počet potenciálních obětí, počet útočníků a logicky roste také počet útoků, protože se jedná o velice výnosný business.

Do internetu a informačního systému firmy jsou připojeni všichni zaměstnanci, někteří dokonce také ze svých soukromých zařízení. Stírá se rozdíl mezi soukromým a pracovním

[1] DOUCEK, Petr. *Řízení bezpečnosti informací*. Praha: Professional Publishing, 2011.
[2] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007.

životem. Firmy razí se slogan „anytime, anywhere, any device“, trendem je mít přístup do systému kdykoliv, odkudkoliv a z čehokoliv a tím se podstatně zvyšuje riziko. Vezměte si jen, kolik jste měli elektrických zařízení před 30 lety a kolik jich máte dnes. Většina z vás má počítač v práci a pak má ještě vlastník notebook, tablet, smartphone a někdo i chytré hodinky. Pak jsou tu ještě různá zařízení, která jsou schopna se připojit do sítě – od herních konzolí, televizí, domácích spotřebičů až po auta, která lze vzdáleně monitorovat a ovládat.

Bezpečnostní návyky těchto uživatelů jsou prakticky nulové a bezpečnost je obtěžuje. Krásně je to vidět například na heslech – přestože požadavek na jejich délku a komplexitu je uživatelům neustále vštěpován do hlavy, je z každoročních úniků databází hesel zřejmé, že uživatelé používají stále snadno prolomitelná hesla (typu 123456) a na mobilních telefonech nemají nastaven žádný zámek obrazovky, případně je odemykají tažením nebo nakreslením jednoduchého gesta. A nejinak je tomu, i co se týče sdílení informací na internetu. Tito uživatelé s tím rozhodně nemají problém, takže se informace o tom, kde se právě nacházejí, kde pracují, na čem zrovna dělají, s kým se přátelí, objevují zhusta na sociálních sítích, kde je stačí jen posbírat a zneužít.

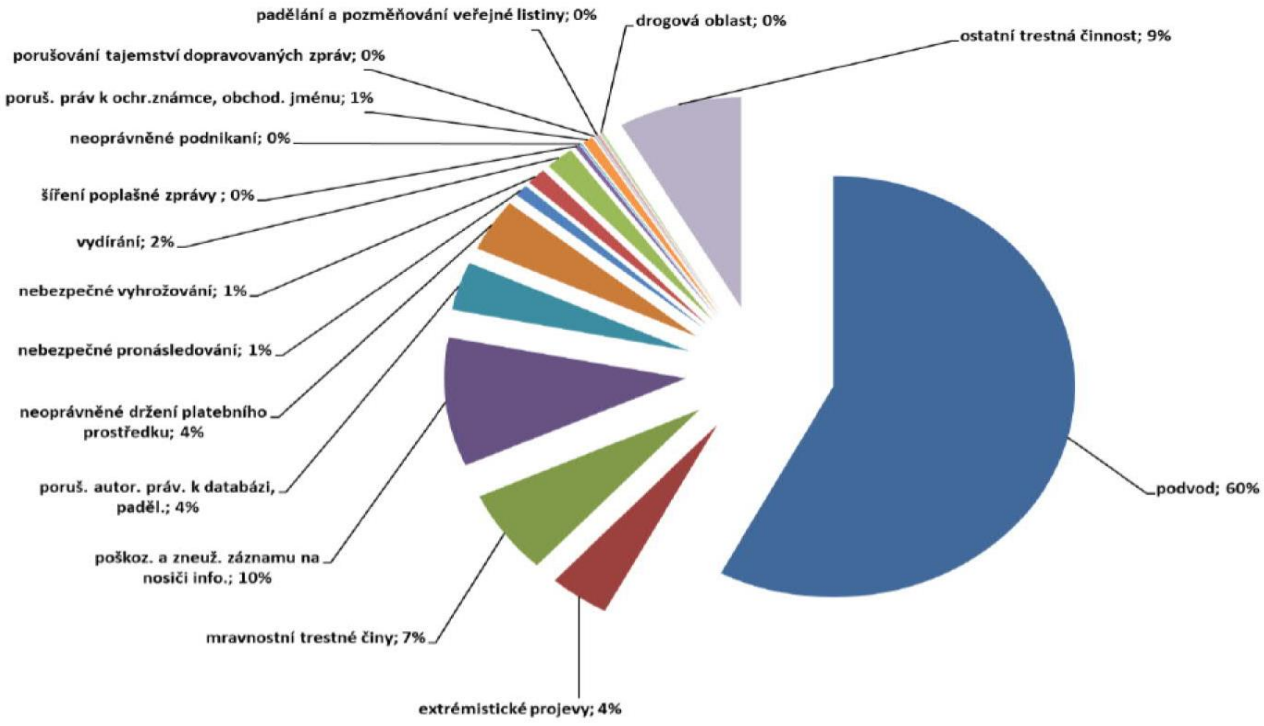
Tohle všechno nahrává útočníkům, jejichž počet také roste, protože návratnost investice je vysoká. Další skutečnost, která útokům nahrává, je otevřenost. Dříve bylo obtížné sdílet know-how, ale díky webu 2.0 to nyní není problém. Kdokoliv může vytvářet a sdílet obsah, včetně informací, jak na někoho vést kybernetický útok. Stačí zadat jen správné klíčové slovo do vyhledávače a můžete si z internetu stáhnout nástroj, pomocí kterého si můžete za pár minut napsat vlastní virus a pokud to neumíte, tak může využít již hotový anebo si dokonce útok na někoho za pár dolarů objednat. Ano, skutečně jen za pár dolarů. Náklady na realizaci útoku z výše uvedených důvodů klesají. Útok je nabízen jako služba, včetně podpory, jedná se o tzv. CaaS (Crime as a Service) a je to služba se vším všudy. Pomocí ní můžete vyhledávat nějaké systémy (které by se daly napadnout) rozesílat phishing e-maily (s odkazem na podvodné stránky nebo škodlivou přílohou) nahrát na Google Play podvodnou aplikaci nebo shodit server na druhé straně zeměkoule[3].

Většina útoků totiž probíhá tak, že útočník doslova skenuje celý internet a hledá nějakou známou slabinu na webu, které by se dalo využít anebo rozešle obrovské množství e-mailů s odkazem či přílohou a pak už jen čeká, kdo na odkaz či přílohu klikne. A je mu jedno, kdo se stane jeho další obětí a čí systém kompromituje. Zde narážíme na často diskutovaný

[3] BAGGILI, Ibrahim. *Digital Forensics and Cyber Crime*. New York: Springer, 2011.

problém, zda by se měly informace o zranitelnostech zveřejňovat anebo ne. Odborná veřejnost je rozdělena na dva přibližně stejně velké tábory, což potvrzují i výsledky nejrůznějších anket. Jeden tvrdí, že zveřejňování zranitelností nahrává útočníkům a druzí tvrdí, že nikoliv. Skutečnost je taková, že v okamžiku, kdy se objeví informace o nové zranitelnosti, tak záhy unikají exploity a zdrojové kódy, objevují se nové varianty malwaru a počet útoků zneužívajících danou zranitelnost dramaticky roste. Nejzranitelnější jsou pak právě malé a střední firmy, které bezpečnost z uvedeného důvodu podceňují, o tuto oblast se nezajímají a investice do ní považují jako naprosto zbytečný náklad. Investice do bezpečnosti je náklad, ale nikoliv zbytečný, nýbrž nezbytný, protože jedině tak se společnost může na trhu dlouhodobě udržet[4].

***Graf. č. 1**: Podrobnější rozdělení oblastí kybernetické kriminality*



Zdroj: Statistiky PČR 2018.

3. VÝHRUŽNÉ E-MAILY

V poslední době se šíří vlny výhrůžných e-mailů, jejichž obsah se nepatrně „obměňuje.“ V jednom z aktuálně nejrozšířenějších vyděračských e-mailů se podvodníci vydávají za hackery. Podvodníci příjemcům tvrdí, že se jim podařilo do jejich zařízení nainstalovat tzv.

[4] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches*. 2015.

RAT virus, který dovoluje zařízení ovládnout na dálku. Díky tomu údajně aktivovali webkameru a natočili majitele napadeného stroje, jak masturbuje při sledování lechtivého videa[5]. Pisatelé sdělují příjemci, že přes webovou kameru notebooku získali choulostivé a citlivé informace. Následuje výhrůžka zveřejnění informací o uživateli a instrukce k uhrazení částky 250 dolarů v bitcoinech (virtuální měně) ve lhůtě 48 hodin. Odesílatelé těchto e-mailů ve skutečnosti žádnými daty nedisponují. Doufají však, že adresát tomuto tvrzení uvěří a požadovanou částku uhradí. Podobné e-maily se šíří ve vlnách s nepatrnými obměnami. Jedná se o fenomén, který se vyskytuje ve větším množství států po celém světě v různých jazykových mutacích[6].

4. ŘEDITELSKÉ E-MAILY

Jedná se o internetové podvody, které souvisejí s neoprávněným přístupem k počítačovému systému a nosiči informací. Pachatel se zde vydává za jednatele (ředitele) společnosti a píše většinou asistence nebo účetní, aby urychleně provedla bankovní převod na jím určený (většinou zahraniční) bankovní účet. Útok bývá buďto veden ze skutečné „napadnuté" jednatelovy e-mailové schránky, anebo se jedná o mírně pozměněnou e-mailovou adresu. K odesílání ředitelských emailů bývají také využívány speciální aplikace, které dokáží pachatelem odesílaný e-mail zobrazit jako e-mail odesílaný z ředitelovy a-e-mailové schránky. E-mailové adresy ředitele a jeho asistentky jsou přitom často volně dostupné například na internetových stránkách dané společnosti[7].

5. PODVODY NA INTERNETU SPOJENÉ S PRODEJEM ZBOŽÍ ČI SLUŽEB

Patří mezi nejčastější podvody páchané na internetu. Podvody začínaly s nabízením výrazně levného atraktivního zboží na internetových prodejních portálech. Po objednání zboží a zaplacení požadované částky kupujícímu:

- nic nepřijde,
- přijde něco jiného, například naplněná PET lahev vodou,
- přijde padělané zboží (falešné NIKE).

[5] MCQUADE, Samuel. *Encyclopedia of Cybercrime*. Westport: Greenwood Press, 2012.
[6] REVERON, Derek. *Cyberspace and national security: threats, opportunities, and power in a virtual world*. Washington DC: Georgetown University Press, 2012.
[7] SINGER, Peter W. a Allan FRIEDMAN. *Cybersecurity: What Everyone Needs to Know*. USA: Oxford University Press, 2013.

Dalším významným trendem u podvodných prodejů zboží je zřizování celých falešných internetových obchodů, serverů, a dokonce i slevových portálů. Peníze jsou odesílány většinou na zahraniční bankovní účty, nebo i na bankovní účty v ČR, kdy se však jedná o bankovní účty vedené na tzv. bílé koně. V poslední době se setkáváme i s převodem finančních prostředku na bitcoinové účty, kde jsou tyto poškozenými převedené peníze již dále prakticky nedohledatelné.

6. PODVODY NA INTERNETU SPOJENÉ SE SEZNAMOVÁNÍM LIDÍ

Patří mezi další významné druhy podvodů vyskytující se na internetu. Pachatel se zde vydává za nějakou atraktivní osobu, například za amerického vojáka, kdy osloví většinou na sociální síti facebook ženu (zajímavé je, že většinou ve věkové skupině 50-60 let), kdy následně tuto ženu prostředky propracovaného sociálního inženýrství úplně „oblbne“ a následně pod různými záminkami, nejčastěji pod záminkou posílání zboží, tuto přinutí odeslat peníze na jím uvedený zahraniční účet[8].

7. ÚVĚROVÉ A JINÉ PODVODY NA INTERNETU

Tvoří další významnou skupinu podvodů páchaných v prostředí internetu. Zde pachatel při žádosti o půjčku na internetu většinou nepravdivě vyplní údaje o svých příjmech a dluzích. K tomuto využije i například odcizené doklady nebo běžný účet vedený na bílého koně.

Problematika „nevypátratelných“ virtuálních měn v poslední době velice usnadňuje vyděračům a hackerům jejich práci a policejnímu orgánu znemožňuje nalézt skutečnou osobu útočníka. Z adresy bitcoinové peněženky totiž na rozdíl od například čísla běžného účtu, téměř nic nezjistíte. Útočník k napadenému počítačovému systému přistupuje z anonymizované IP adresy, pro policii je tak prakticky také nezjistitelný. V prověřování této trestné činnosti se proto často spoléháme na provedenou chybu útočníka. Jedině totiž tak lze pachatele této sofistikované trestné činnosti skutečně odhalit[9].

[8] SHACKELFORD, Scott J., Scott RUSSEL a Andreas KUEHN. *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*. Chicago Journal of International Law. 2016, 17(1).
[9] SHOEMAKER, Dan a Arthur CONKLIN. *Cybersecurity: The Essential Body Of Knowledge.* USA: Cengage Learning, 2011.

Další možností páchání této trestné činnosti je to, že útočník vlastní útok neprovede a pouze jeho provedením vyhrožuje. Za nekonání kybernetického útoku poté útočník vyžaduje od správce nebo vlastníka systému kybernetické výpalné. Kybernetické výpalné může, jako například u trestného činu vydírání, spočívat v převedení určité finanční částky na bankovní účet určený útočníkem. Mnohdy by ani útočník požadující kybernetické výpalné nebyl schopen útok doopravdy uskutečnit a pouze útokem vyhrožuje[10].

8. ZÁVĚR

Je velice důležité na podobné nevyžádané e-maily nereagovat, a především nikam neposílat peníze! S největší pravděpodobností jde o výmysl. Pokud přece jen máte podezření, že by se ve vašem počítači nějaký virus mohl nacházet, kontaktujte odborníky na komunikační technologie. Policie ČR, která tyto případy registruje, v důsledku další masivní vlny varuje všechny uživatele elektronické pošty, aby podezřelé e-maily neotvírali, smazali je či označili jako spam, na uvedené ani podobné e-maily nereagovali a nic neplatili. Pokud již došlo k zaplacení, neprodleně věc nahlaste Policii ČR.

Literatura

BAGGILI, Ibrahim. *Digital Forensics and Cyber Crime*. New York: Springer, 2011.

DOUCEK, Petr. *Řízení bezpečnosti informací*. 2. rozšířené vydání. Praha: Professional Publishing, 2011.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches*. 2015.

JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1. vydání. Praha: Grada, 2007.

MCQUADE, Samuel. *Encyclopedia of Cybercrime*. Westport: Greenwood Press, 2012.

REVERON, Derek. *Cyberspace and national security: threats, opportunities, and power in a virtual world*. Washington DC: Georgetown University Press, 2012.

[10] YANNAKOGEORGOS, Panayotis. *Conflict and cooperation in cyberspace the challenge to national security*. Boca Raton: Taylor & Francis, 2013.

SINGER, Peter W. a Allan FRIEDMAN. *Cybersecurity: What Everyone Needs to Know*. USA: Oxford University Press, 2013.

SHACKELFORD, Scott J., Scott RUSSEL a Andreas KUEHN. *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*. Chicago Journal of International Law. 2016, 17(1).

SHOEMAKER, Dan a Arthur CONKLIN. *Cybersecurity: The Essential Body Of Knowledge.* USA: Cengage Learning, 2011.

YANNAKOGEORGOS, Panayotis. *Conflict and cooperation in cyberspace the challenge to national security*. Boca Raton: Taylor & Francis, 2013.

Abstrakt:

Počítačová kriminalita patří v dnešní době mezi nejzávažnější formy trestné činnosti, která se oproti ostatní kriminalitě liší především nízkým procentem její objasněnosti. Pachatelé počítačové kriminality mají oproti ostatním delikventům obrovskou výhodu v tom, že protiprávní činnost soustředí do celosvětové komunikační sítě nazývanou internet. Internet jim poskytuje určitý pocit nepolapitelnosti a nepostižitelnosti. Je proto velice důležité se blíže seznámit s možnými způsoby, jak tito pachatelé „pracují", jedině tak bude možné tyto útoky detekovat a následně zastavit.

Klíčová slova: *Bezpečnost, bitcoin, e-mail, internet, kybernetický útok.*

Abstract:

Email Users Security – Blackmail Emails

Nowadays, cybercrime is one of the most serious forms of crime, which differs in comparison with other crime mainly due to its low detection rate. Cybercriminals have a huge advantage over other offenders by concentrating their illegal activities on a global communications network called the Internet. The Internet gives them a sense of elusiveness and intangibility. It is therefore very important to learn more about the possible ways these offenders "work" in order to detect and then stop these attacks.

Key words: *Cyber attack, bitcoin, email, internet, security.*

JEL: K24

Ing. **Vladimír Šulc**, Ph.D. – Vysoká škola Ambis, Katedra bezpečnosti a práva, Lindnerova 1, 180 00 Praha. sulc@mail.ambis.cz.

JAK VZNIKÁ AGREGOVANÉ BEZPEČNOSTNÍ RIZIKO

Miroslav Čermák

1. ÚVOD

Tento příspěvek vznikl na základě dlouhodobého pozorování několika vybraných organizací v ČR, hloubkových rozhovorů s manažery informační a kybernetické bezpečnosti těchto organizací, rozborem zpráv a bezpečnostních reportů uvolňovaných v rámci bezpečnostní komunity, a na základě osobních zkušeností.

V posledních dvou dekádách došlo v oblasti informačních technologií k několika na první pohled veskrze pozitivním změnám, které by nás samy osobě nemusely vůbec znepokojovat. Společně však mohou představovat značné nezanedbatelné agregované riziko, a to pro většinu organizací v ČR, neboť ty jsou stále více závislé na informačních technologiích, prostřednictvím kterých své služby poskytují i svým zákazníkům a občanům.

Především pak organizace, které jsou součástí kritické informační infastruktury státu, by měly riziko, které je popsáno dále, kriticky zhodnotit a nebrat jej na lehkou váhu. Ono riziko pak představuje samotný přístup k datům a systémům organizací, které jsou umístěny v cloudu, a které jsou spravovány třetí stranou a ze soukromých zařízení zaměstnanců i pracovníků třetích stran přes internet z prostředí jejich domova. Tito zaměstnanci, jejich zařízení i samotná infrastruktura jsou totiž předmětem plošných i cílených kybernetických útoků[1].

Kybernetické útoky jsou rovněž sofistikovanější a nabírají na intenzitě. A nic nenasvědčuje tomu, že by se tento trend měl v dohledné době změnit. Naopak lze očekávat, že tento trend bude nadále pokračovat, neboť silně koreluje s růstem počtu uživatelů, jejich nízkým bezpečnostním povědomím, rostoucím počtem zařízení připojených do internetu, objemem zpracovávaných dat, a v neposlední řadě pak i s množstvím a velikostí aplikací a celkové komplexity systémů.

Pokud je v textu dále použit pojem organizace, tak jím jsou míněny jak firmy založené za účelem dosažení zisku, tak i podniky jednotlivce a rovněž i organizace, jejichž cílem není

[1] GENES, Raimund. *Targeted Attacks versus APTs: What's The Difference? – TrendLabs Security Intelligence Blog*. blog.trendmicro.com [online]. 14. září 2015 [vid. 12. březen 2019]. Získáno z: https://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attacks-versus-apts-whats-the-difference/

generovat zisk, ale poskytovat jen vybrané služby, jako je např. školství, zdravotnictví, policie, soudy, uzemní samospráva a vůbec veškeré organizační složky státu.

2. AGREGOVANÉ RIZIKO

Od roku 1995, kdy sleduji úroveň bezpečnosti ve vybraných organizacích, jsem identifikoval následující společné charakteristiky, a to za použití soukromých zařízení pro přístup do informačních systémů organizací, umožnění přístupu do těchto systémů z domova, přesunu těchto systémů a dat do cloudu a v neposlední řadě pak outsourcing správy těchto systémů. V následujících kapitolách jsou stručně popsány jednotlivé změny, ke kterým v minulých letech došlo a jaké představují riziko.

3. ROSTE POČET UŽIVATELŮ PŘIPOJENÝCH DO INTERNETU

Byť počet uživatelů internetu roste, tak bez ohledu na to, že se toto tempo růstu zpomaluje, a nejspíš tomu tak bude i nadále, neboť bude v zásadě kopírovat populační křivku, tak naproti tomu počet zařízení připojených do internetu roste výrazně vyšším tempem a zdaleka přesahuje aktuální počet obyvatel. Dle InternetLiveStats[2] přesáhl počet uživatelů internetu 4 miliardy a v Česku pak dle NetMonitoru[3] 7,8 miliónů uživatelů.

4. ROSTE POČET ZAŘÍZENÍ PŘIPOJENÝCH DO INTERNETU

Zpočátku byl přístup do internetu možný pouze z vyhrazených počítačů, připojených do internetu přes vytáčenou telefonní linku, které byly umístěny mimo sít a byly i pod dohledem. A jen minimum domácností mělo připojení do internetu. To bylo mimo jiné dáno i poměrně vysokými poplatky za připojení, které byly účtovány dle doby připojení. Později byly počítače připojené do internetu umístěny v samostatné síti a odděleny od zbytku sítě. V poslední fázi byl internet zpřístupněn ze všech počítačů, ale přístup byl možný pouze na vybrané stránky (white list). S růstem počtu těchto webových stránek se však stala situace neudržitelná a byl zvolený opačný přístup, kdy začal být vytvářen seznam stránek, resp. kategorií, které jsou zakázány (black list). Do internetu dnes nejsou připojeny jednotlivé

[2] Number of Internet Users (2016) – Internet Live Stats. Internet Users [online]. [vid. 16. únor 2019]. Získáno z: http://www.internetlivestats.com/internet-users/
[3] NetMonitor [online]. [vid. 16. únor 2019]. Získáno z: http://www.netmonitor.cz/

počítače, ale celé sítě. Dle iot-analytics[4] je do internetu připojeno více jak 17 miliard zařízení. To představuje cca 4 zařízení na uživatele, kterými zpravidla jsou stolní počítač, notebook, tablet a smartphone.

5. ROSTE POČET ZRANITELNÝCH ZAŘÍZENÍ

Zkracuje se vývojový cyklus, zrychluje se uvolňování nových verzí SW a HW, objevují se počítače v podobě nejrůznějších jednoúčelových zařízení připojitelných do internetu, ledničky, myčky, mikrovlnky, televize, žárovky, termostaty, zkrátka tzv. IoT (internet of things), ale i smartphonů a tabletů, které se stávající de facto spotřebním zbožím s krátkou dobou morální i fyzické životnosti. U takových zařízení se vzhledem k jejich ceně a překotnému vývoji jaksi nepočítá s nějakou dlouhou dobou životnosti a už vůbec ne s doživotním vydáváním bezpečnostních aktualizací za účelem odstranění zranitelností, kterými tato zařízení trpí už v okamžiku, kdy sjíždějí z výrobní linky, a které jsou následně zneužívány útočníky krátce po jejich připojení se do internetu. Je tomu tak proto, že většina těchto zařízení obsahuje zranitelnosti a nějaké aktualizace svého operačního systému se za doby svého života nikdy nedočká. To v konečném důsledku vede k tomu, že je do internetu připojeno velké množství zařízení, která je možno napadnout, ovládnout a vést z nich útok na další cíle. Je zde enormní tlak na co nejnižší cenu a snižování nákladů.

6. ROSTE RYCHLOST PŘIPOJENÍ

Rychlost pevného i mobilního připojení rok od roku roste, je to dáno rostoucí poptávkou a konkurencí na telekomunikačním trhu. Rychlost vzrostla z několika jednotek kilobit za sekundu až na několik megabitů za sekundu. Během dvou dekád tak vzrostla rychlost přenosu dat tisícinásobně[5], ale přitom velikost citlivých dat je pořád stejná, jinými slovy, číslo karty, účtu nebo adresa má pořád stejnou velikost, což lze vyjádřit pomocí stejného počtu bitů. To ve výsledku znamená, že zatímco v minulém období nebylo možné v případě napadení bez povšimnutí stáhnout např. celou databázi klientů o velikosti několika stovek MB anebo ji zašifrovat, protože se jednalo o výpočetně i datově velice náročnou operaci, tak

[4] LASSE LUETH, Knud. *State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating*. iot-analytics.com [online]. 8. srpen 2018 [vid. 16. únor 2019]. Získáno z: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

[5] Český statistický úřad. 061004-17_S.pdf [online]. [vid. 17. prosinec 2019]. Získáno z: https://www.czso.cz/documents/10180/46014808/061004-17_S.pdf

dnes je to otázka maximálně několika málo minut. Vyšší rychlost připojení tak umožňuje rychlejší útok, na který mnohé organizace ani nestačí zareagovat.

7. ROSTE VYUŽITÍ CLOUDŮ

Organizace přesouvají svá data a své systémy do cloudu. Cloudy prosazují nadnárodní společnosti jako je Microsoft, Google, Amazon, ale ty sledují výhradně své ekonomické zájmy a těmi je vysoká návratnost investice a dosažení zisku, takže v jejich zájmu je přesvědčit management organizací, aby k nim své systémy a data přesunuly. Jako argumenty k tomu využívají možnost dosažení nižších nákladů, realizovaných především jako úspory z rozsahu a dále vyšší úrovní bezpečnosti. A protože dávno došlo k oddělení vlastnictví od řízení a na okamžité výsledky jsou vázány i manažerské bonusy, tak k tomuto masivnímu exodu do cloudu dochází[6]. V zákoně o veřejných zakázkách pak je zohlednění ceny sice doporučováno, přesto však je toto kritérium stále mnohými manažery považováno za stěžejní a obávají se, aby neudělali chybu, a odvolávají se na problémy s tím spojené[7], a tak se nelze divit, že v okamžiku, kdy je průměrný životní cyklus manažera několik let, tak volí nejlacinější řešení v podobě cloudů. Může se však jednat o morální hazard, neboť vrcholový management může nabýt falešného dojmu, že když jeho systémy a data spravuje renomovaná společnost, takže už nemusí řešit otázky spojené s bezpečnosti. Je třeba si však uvědomit, že každý stát sleduje především své národní zájmy a podporuje své firmy, a že ten, kdo byl naším spojencem, již zítra spojencem být nemusí, takže v případě kritické informační infrastruktury státu je nutné provést výběr cloudu a analýzu rizik obzvlášť důkladně. Jistou obezřetnost doporučuje i Evropská komise, která cloud jinak doporučuje[8]. Ostatně skutečnost, že je cloud obousečná zbraň, je uvedeno i v Národní strategii kybernetické bezpečnosti České republiky na období let 2015–2020[9]. V akčním plánu k této strategii je však ambice řešit jen systémy, které spravuje stát[10], což je nedostačující, protože

[6] Český statistický úřad. ce31b358-2dca-4204-b507-c7e4656064e7.pdf [online]. [vid. 17. prosinec 2019]. Získáno z: https://www.czso.cz/documents/10180/61601888/06200518.pdf/ce31b358-2dca-4204-b507-c7e4656064e7?version=1.1

[7] K rozdělení nejnižší nabídkové ceny jako hodnotícího kritéria. EPRAVO.CZ [online]. [vid. 17. prosinec 2019]. Získáno z: https://www.epravo.cz/top/clanky/k-rozdeleni-nejnizsi-nabidkove-ceny-jako-hodnoticiho-kriteria-107907.html

[8] MICHLMAYR, Thomas. *European Commission Cloud Strategy. nedatováno*, s. 28.

[9] Národní stálá konference o bezpečnosti. nskb-150216-final.pdf [online]. [vid. 18. prosinec 2019]. Získáno z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

[10] akc48dnc3adplc3a1n-rkb-final-150408.pdf [online]. [vid. 18. prosinec 2019]. Získáno z: https://www.govcert.cz/download/gov-cert/container-nodeid-967/akc48dnc3adplc3a1n-rkb-final-150408.pdfakc48dnc3adplc3a1n-rkb-final-150408.pdf [online]. [vid. 18. prosinec 2019]. Získáno z: https://www.govcert.cz/download/gov-cert/container-nodeid-967/akc48dnc3adplc3a1n-rkb-final-150408.pdf

většinu systémů stát nespravuje a výkon národního hospodářství se odvíjí především od úrovně bezpečnosti soukromých firem, a ty jsou vedeny profesionálními manažery, kteří vidí v cloudech spíše řešení umožňující jim okamžitě snížit náklady než cokoliv jiného.

Z rozhovorů s některými manažery navíc vyplynulo, že vůbec nemají vypracován postup pro případ, kdyby cloud byl nedostupný anebo potřebovali přejít k jinému poskytovateli. A pokud organizace nebudou navrhovat a vyvíjet své systémy jako cloud-native, tak přechod od jednoho poskytovatele cloudu (Cloud Service Provider, zkr. CSP) k druhému nebude možný, a těmto organizacím bude hrozit vendor lock-in a to se všemi následky, které z tohoto problematického stavu vyplývají, a CSP ji v tom samozřejmě nijak pomáhat nebude, naopak. Snadno pak taková organizace může zaznamenat rostoucí náklady nebo bezpečnostní problémy.

Dále je třeba si uvědomit, že cloudy byly navrhnuty tak, aby byly odolné vůči hrozbám přírodního původu jako je zemětřesení, bouře, záplavy a rovněž i vůči klasickým zbraním a dokázaly nějak fungovat v případě dočasné nedostupnosti datového centra nebo i jeho kompletního zničení. Slabinou cloudů však vždy bude lidská chyba nebo kybernetický útok zneužívající SW zranitelnosti. Pokud jde o lidskou chybu, tak nezapomínejme, že když chybu udělá admin v DC, nemusí si toho nikdo ani všimnout, ale chyby v cloudu si okamžitě všimnou všichni, co ho využívají[11]. Napadnout takový cloud a požadovat výpalné, je velice lákavé a pokud k němu dojde, tak ti slabí nepřežijí, protože pojišťovna jim škodu neuhradí, neboť kybernetická válka je zahrnuta ve výlukách. Jasně se to ukázalo na případu Mondelez[12].

Problémem je dále vysoká homogenita cloudů, která vede k agregovanému riziku. A řešením, jak toto riziko snížit, je jedině zanesení určité heterogenity, což znamená opět zvýšení nákladů a tím pak tak trochu padá i onen argument ohledně nižších nákladů na straně CSP.

I přes určitý pokrok v posledních letech je zde stále patrná značná závislost na CSP co do možnosti logování událostí a jejich forenzní analýze a šetření bezpečnostních incidentů, a rovněž i co do možnosti obnovy systému po havárii.

Problém je, že CSP z principu ani moc nějaké logy poskytovat nemůže. Nezapomínejme, že v logách jsou zaznamenány informace i o jiných klientech. Je tomu tak proto, že kvůli snížení

[11] *Don't be the fool in the cloud* | Computerworld [online]. [vid. 18. prosinec 2019]. Získáno z: https://www.computerworld.com/article/3233289/don-t-be-the-fool-in-the-cloud.html

[12] *What Mondelez v. Zurich May Reveal About Cyber Insurance in the Age of Digital Conflict.* Lawfare [online]. 8. březen 2019 [vid. 18. prosinec 2019]. Získáno z: https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict

nákladů je použita sdílená infrastruktura. Náhledy na tyto logy jsou nedokonalé, a neúplné, to však zjistíte až v okamžiku, kdy začnete šetřit nějaký bezpečnostní incident. Podle některých bezpečnostních expertů je ona chybovost až 50 %. Z probíhajícího průzkumu mezi bezpečnostními experty dále vyplývá, že více jak 80 % z nich je přesvědčeno, že kritická informační infrastruktura státu by neměla být umístěna do zahraničního cloudu[13].

8. ROSTE POČET PŘÍSTUPŮ ZE SOUKROMÝCH ZAŘÍZENÍ

Organizace podporují program BYOD (z anglického bring your own device), který zvítězil nad programem COPE (Corporate Owned Personally Enabled)[14]. Jinými slovy zaměstnanci k práci používají svá vlastní soukromá zařízení, která organizace nemá vůbec pod kontrolou namísto toho, aby používali firemní zařízení i k soukromým účelům. A i když z těchto zařízení zaměstnanci přistupují k systémům organizací přes technologii VPN (virtual private network), která zajišťuje tzv. end-to-end šifrování, používají pro přihlášení dvoufaktorovou autentizaci, a na zařízeních jim běží VDE (virtual desktop environment), což je v podstatě virtuální desktop, který má organizace zpravidla pod kontrolou, a kde proběhl nějaký hardening, a jsou zde bezpečnostními politikami vynuceny určité zásady, tak přesto mohou být tato zařízení zaměstnanců resp. jejich hostitelské systémy napadeny a spuštěn v nich škodlivý kód, který může dané zařízení kompletně ovládnout, začlenit jej do botnetu a umožnit útočníkovi vzdálený přístup k datům a do systému organizace[15]. Je třeba si uvědomit, že na těchto zařízeních není často aktuální operační systém, nejsou aktualizovány veškeré aplikace, které jejich uživatel používá, neběží zde antivirus, a je z nich zcela bez omezení přistupováno do internetu. Práce ze soukromého zařízení už dávno není v mnoha organizacích benefitem, ale způsobem, jak snížit náklady na výpočetní techniku, a to i včetně příspěvku na nákup daného zařízení.

[13] ČERMÁK, Miroslav. *Ohrožuje přesun systémů do cloudu naše národní hospodářství a bezpečnost? CleverAndSmart Management Consulting* [online]. 29. listopad 2019 [vid. 18. prosinec 2019]. Získáno z: https://www.cleverandsmart.cz/ohrozuje-presun-systemu-do-cloudu-nase-narodni-hospodarstvi-a-bezpecnost
[14] ČERMÁK, Miroslav. *BYOD vs. COPE*. *CleverAndSmart* [online]. 12. duben 2012 [vid. 25. červen 2019]. Získáno z: https://www.cleverandsmart.cz/byod-vs-cope/
[15] ČERMÁK, Miroslav. *Je VDE bezpečnější? CleverAndSmart Management Consulting* [online]. 4. říjen 2017 [vid. 17. prosinec 2019]. Získáno z: https://www.cleverandsmart.cz/je-vde-bezpecnejsi/

9. ROSTE POČET ZAMĚSTNANCŮ PRACUJÍCÍCH Z DOMOVA

Zaměstnanci stále častěji využívají možnosti home office neboli práce z domova[16] a do systému svého zaměstnavatele se připojují ze svého soukromého zařízení přes internetové připojení svého poskytovatele internetu. Problém však je, že zaměstnanec přistupující do systému a k datům společnosti z domova není schopen zajistit a nemá zajištěnou stejnou úroveň fyzické bezpečnosti jako zaměstnanec, který se nachází v prostředí organizace, do které je zpravidla vstup možný pouze přes recepci, probíhá zde kontrola osob a rovněž je zde výrazně nižší riziko, že by zaměstnance bez povšimnutí někdo donutil fyzickým či jiným násilím provést neautorizovanou operaci v systému[17]. To v domácím prostředí, které není pod trvalým kamerovým dohledem a není napojeno na PCO (pult centrální ochrany) možné je. Práce z domova je trend, který už dávno není v mnoha organizacích benefitem, ale způsobem, jak ještě více snížit náklady na jedno pracovní místo.

10. ROSTE POČET OUTSOURCOVANÝCH ČINNOSTÍ

Organizace správu dat a systémů outsourcují. V praxi tak dochází k tomu, že data a systémy spravují zaměstnanci třetích stran a že tito pracovníci spravují i data jiných společností a mohou to být i systémy a data konkurence. Tito pracovníci tak mohou mít mnohem větší příležitost tato data vytěžovat a svého přístupu zneužít spíš než vlastní zaměstnanec organizace, který přístup k datům jiných organizací nemá. Vzhledem k tomu, že dost často byl outsourcing zvolen kvůli nižším nákladům, je zcela na místě se ptát, jak těchto nižších nákladů může být v praxi dosaženo, obzvlášť pokud má správu provádět kvalifikovaný zaměstnanec, disponující příslušnými certifikacemi a dodržovat přitom veškeré bezpečnostní požadavky. Z rozhovoru s příslušnými manažery vyplynulo, že náklady jsou jen zdánlivě nižší a jejich dosahováno především proto, že je rozsah dodávky oproti původním předpokladům omezen, resp. je dodáváno přesně to, co je ve smlouvě uvedeno, a za vše ostatní se musí zaplatit a rovněž je daná činnost vykonávána v zemi, kde jsou výrazně nižší mzdové náklady a vyšší fluktuace zaměstnanců.

[16] S.R.O, *VisionApps. Zaměstnanci chtějí home office. Splňte tyto 2 podmínky, aby práce z domu fungovala*. LMC [online]. [vid. 17. prosinec 2019]. Získáno z: https://www.lmc.eu/cs/magazin/data-a-pruzkumy/zamestnanci-chteji-home-office-splnte-tyto-2-podminky-aby-prace-z-domu-fungovala/

[17] ČERMÁK, Miroslav. *Práce z domova*. *CleverAndSmart Management Consulting* [online]. [vid. 17. prosinec 2019]. Získáno z: https://www.cleverandsmart.cz/tag/prace-z-domova/

11. ROSTE VZDÁLENOST MEZI ÚTOČNÍKEM A OBĚTÍ

Pro útoky v kyberprostoru je typické, že vzdálenost mezi útočníkem a obětí nehraje žádnou roli a že útočník bývá dost často také obětí, resp. systém, ze kterého je útok veden, je pod kontrolou útočníka a ten může po sobě zametat stopy anebo i vytvářet stopy falešné, aby svedl vyšetřování jiným směrem. Škodlivý kód, který je dost často v rámci těchto útoků přepoužíván různými organizovanými skupinami se nachází ve více či méně modifikované podobě v různých exploitech a je umísťován na napadené servery, sloužící jako watering hole, nebo umísťován do trojanizovaných aplikací anebo distribuovaný jako příloha v rámci nejrůznějších phishing kampaní, může být chybně na základě pojmenování jednotlivých, proměnných, funkcí, knihoven a případně i komentářů částí kódu přisouzen někomu zcela jinému. Jinými slovy ruský programátor umístí anebo prodá na darknetu svůj exploit, který se stane součástí exploitu kitu, který je následně použit v rámci phishingu na klienty ukrajinské banky, je následně přepoužit jinou organizovanou skupinou k útoku na klienty bank v ČR, může vyvolat dojem, že za útokem stojí ruská APT skupina a stejně tak skutečnost, že server, který slouží jako řídící CaC server se nachází v Číně, ještě neznamená, že za útokem stojí čínská APT skupina. Nehledě na to, že dochází k vzájemnému napadání jednotlivých mocností a součástí těchto útoků může být úmyslné podvrhnutí kódu. Z výše uvedeného důvodu by bylo nezodpovědné provést za těchto podmínek protiútok na systém, ze kterého útok probíhá, protože následkem tohoto útoku by mohla být ještě větší škoda. Je proto třeba pečlivě zvažovat, jak v případě takového útoku postupovat a věnovat dostatečnou pozornost i novele zákona o vojenském zpravodajství a vést na toto téma seriózní diskusi[18].

12. ROSTE POČET KYBERNETICKÝCH ÚTOKŮ

Počet kybernetických útoků stále roste[19]. S počtem zranitelných zařízení roste i počet zařízení, na která může být veden útok a zároveň, ze kterých může být veden útok v okamžiku, kdy dojde k jejich kompromitaci. Tato zařízení mohou být začleněna do botnetu a dále pronajímána, tomu, kdo zaplatí, jedná se o tzv. Crime as a Service, zkr. CaaS. Možnosti jejich zneužití jsou značné, mohou být zneužita pro lámání hesel, mohou být zneužita k realizaci podvodných bankovních transakcí, může z nich být veden DDoS útok

[18] ŠPIDLA, Aleš. *Novela zákona o vojenském zpravodajství – potřebujeme ji? IT SECURITY NETWORK NEWS* [online]. 26. únor 2019 [vid. 12. březen 2019]. Získáno z: https://www.itsec-nn.com/novela-zakona-o-vojenskem-zpravodajstvi-potrebujeme-ji/

[19] zprava-o-stavu-kyberneticke-bezpecnosti-cr-2018-cz.pdf [online]. [vid. 17. prosinec 2019]. Získáno z: https://www.nukib.cz/download/publikace/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2018-cz.pdf

na jinou organizaci, mohou z nich být hackovány další systémy, může z nich být rozesílán SPAM, mohou sloužit jako proxy servery, přes které je veden útok, takže identita útočníka tak zůstane skryta a co víc, může pak být na základě zdroje útoku přisouzena zcela jinému subjektu. Otázka dne už není, zda k útoku na danou organizaci dojde, ale kdy a za jak dlouho od průniku bude organizace schopna si tuto skutečnost vůbec uvědomit a reagovat na ni. Přičemž dle statistik M-Trends je to často až po několika týdnech[20]. Přesto je většina manažerů přesvědčena, že se jich útok netýká, protože jejich organizace nedisponuje žádnou převratnou technologií ani know-how, které by bylo pro útočníka bylo zajímavé. Jaksi si nechtějí připustit, že kromě cílených útoků jsou tady ještě tzv. plošné útoky, které jsou mnohem častější[21], a že se jejich organizace může stát obětí ransomwaru a její činnost může být zcela ochromena.

13. BEZPEČNOSTNÍ POVĚDOMÍ JE STÁLE NÍZKÉ

Investice do bezpečnosti a školení jsou v zásadě stále stejné, a i když se v poslední době v některých organizacích v souvislosti s GDPR zvýšily, tak nedochází k podstatné a žádoucí změně chování ze strany zaměstnanců. Pouze v organizacích, ve kterých dochází spolu s osvětou i k testování odolnosti zaměstnanců vůči těmto útokům, je možné zaznamenat výrazné zlepšení oproti předchozímu období. Meziročně pak dochází i k trvalému zlepšování, kdy zaměstnanci těchto organizací jsou schopny správně identifikovat phishing, který stále představuje nejčastější vektor útoku, a tedy i způsob jako dochází ke kompromitaci koncových zařízení zaměstnanců a proniknutí útočníka do prostředí organizace. Schází nám větší informovanost o hrozbách a probíhajících útocích v kyberprostoru. O jednotlivých útocích se z médií dozvídáme jen výjimečně, neexistuje jednotná taxonomie kybernetických hrozeb, neexistuje přehledná statistika útoků, která by uváděla vektor útoku, zasažený sektor, výši škody apod. K dispozici jsou sice nejrůznější statistiky třeba CSIRT[22] nebo policie[23], ale ty jsou samy o sobě neúplné a nevypovídající. K dispozici jsou dále bezpečnostní reporty zahraničních firem mapující situaci ve světě, ale

[20] ČERMÁK, Miroslav. *Cyber resilience: Dwell time. CleverAndSmart* [online]. 6. květen 2019 [vid. 25. červen 2019]. Získáno z: https://www.cleverandsmart.cz/cyber-resilience-dwell-time/

[21] ČERMÁK, Miroslav. *Na koho jsou vedeny kybernetické útoky a proč. CleverAndSmart Management Consulting* [online]. 23. říjen 2019 [vid. 17. prosinec 2019]. Získáno z: https://www.cleverandsmart.cz/na-koho-jsou-vedeny-kyberneticke-utoky-a-proc/

[22] *Statistiky řešených incidentů – CSIRT* [online]. [vid. 17. prosinec 2019]. Získáno z: https://csirt.cz/page/2635/statistiky-resenych-incidentu/

[23] *Kyberkriminalita – Policie České republiky* [online]. [vid. 17. prosinec 2019]. Získáno z: https://www.policie.cz/clanek/kyberkriminalita.aspx

ni ty nepřinášejí podstatné informace, a jsou mnohdy značně zavádějící[24]. To samo o sobě zhoršuje vnímání bezpečnosti ze strany vrcholového managementu, kterému není možné předložit konkrétní případy, ke kterým na území ČR došlo a jaké byly jejich následky a závažnost bezpečnostních hrozeb je tak bagatelizována.

14. ZÁVĚR

Sledované organizace vykazují určité společné charakteristiky. Alfou a omegou je pak snižování nákladů, to lze pozorovat ve všech sledovaných organizacích. Zaměstnanci se připojují z domova přes svého poskytovatele internetu a ze svých soukromých zařízení do systémů a k datům svých zaměstnavatelů, která jsou umístěna kdesi v cloudu. Fyzické prostory odkud se zaměstnanci připojují, nejsou pod kontrolou, zařízení, ze kterých se zaměstnanci připojují, nejsou pod kontrolou, datová připojení, které zaměstnanci používají, nejsou pod kontrolou a rovněž i cloudy, kde jsou data a systémy organizací umístěna, nejsou pod kontrolou, neboť vše je ošetřeno jen smluvně. Výše uvedené trendy, které zároveň představují i riziko, byly i jako riziko v mnoha případech hodnoceny, ovšem izolovaně. Je nutné provést novou analýzu rizik např. i s využitím Cybersecurity frameworku[25] a posoudit účinnost stávajících bezpečnostních opatření organizační a technické povahy. Jasné stanovisko k tomuto riziku by měly vyjádřit i příslušné orgány a reagovat na něj i aktualizací svých doporučení, vydání závazných stanovisek apod. neboť v krajním případě může dojít i k ohrožení hospodářských výsledků a zájmů České republiky.

Literatura

Český statistický úřad. 061004-17_S.pdf [online]. [vid. 17. prosinec 2019]. Získáno z: https://www.czso.cz/documents/10180/46014808/061004-17_S.pdf

Český statistický úřad. akc48dnc3adplc3a1n-rkb-final-150408.pdf [online]. [vid. 18. prosinec 2019]. Získáno z: https://www.govcert.cz/download/gov-cert/container-nodeid-967/akc48dnc3adplc3a1n-rkb-final-150408.pdf

[24] ČERMÁK, Miroslav. *Co mi vadí na nejrůznějších bezpečnostních reportech firem nabízejících bezpečnostní řešení. CleverAndSmart Management Consulting* [online]. 7. listopad 2019 [vid. 18. prosinec 2019]. Získáno z: https://www.cleverandsmart.cz/co-mi-vadi-na-nejruznejsich-bezpecnostnich-reportech-firem-nabizejicich-bezpecnostni-reseni/

[25] NICOLE.KELLER@NIST.GOV. *Cybersecurity Framework. NIST* [online]. 12. listopad 2013 [vid. 18. prosinec 2019]. Získáno z: https://www.nist.gov/cyberframework

Český statistický úřad. ce31b358-2dca-4204-b507-c7e4656064e7.pdf [online]. [vid. 17. prosinec 2019]. Získáno z: https://www.czso.cz/documents/10180/61601888/06200518.pdf/ce31b358-2dca-4204-b507-c7e4656064e7?version=1.1

ČERMÁK, Miroslav. *BYOD vs. COPE. CleverAndSmart* [online]. 12. duben 2012 [vid. 25. červen 2019]. Získáno z: https://www.cleverandsmart.cz/byod-vs-cope/

ČERMÁK, Miroslav. *Je VDE bezpečnější? CleverAndSmart Management Consulting* [online]. 4. říjen 2017 [vid. 17. prosinec 2019]. Získáno z: https://www.cleverandsmart.cz/je-vde-bezpecnejsi/

ČERMÁK, Miroslav. *Co mi vadí na nejrůznějších bezpečnostních reportech firem nabízejících bezpečnostní řešení. CleverAndSmart Management Consulting* [online]. 7. listopad 2019 [vid. 18. prosinec 2019]. Získáno z: https://www.cleverandsmart.cz/co-mi-vadi-na-nejruznejsich-bezpecnostnich-reportech-firem-nabizejicich-bezpecnostni-reseni/

ČERMÁK, Miroslav. *Cyber resilience: Dwell time. CleverAndSmart* [online]. 6. květen 2019 [vid. 25. červen 2019]. Získáno z: https://www.cleverandsmart.cz/cyber-resilience-dwell-time/

ČERMÁK, Miroslav. *Na koho jsou vedeny kybernetické útoky a proč. CleverAndSmart Management Consulting* [online]. 23. říjen 2019 [vid. 17. prosinec 2019]. Získáno z: https://www.cleverandsmart.cz/na-koho-jsou-vedeny-kyberneticke-utoky-a-proc/

ČERMÁK, Miroslav. *Ohrožuje přesun systémů do cloudu naše národní hospodářství a bezpečnost? CleverAndSmart Management Consulting* [online]. 29. listopad 2019 [vid. 18. prosinec 2019]. Získáno z: https://www.cleverandsmart.cz/ohrozuje-presun-systemu-do-cloudu-nase-narodni-hospodarstvi-a-bezpecnost/

ČERMÁK, Miroslav. *Práce z domova. CleverAndSmart Management Consulting* [online]. [vid. 17. prosinec 2019]. Získáno z: https://www.cleverandsmart.cz/tag/prace-z-domova/

Don’t be the fool in the cloud | Computerworld [online]. [vid. 18. prosinec 2019]. Získáno z: https://www.computerworld.com/article/3233289/don-t-be-the-fool-in-the-cloud.html

GENES, Raimund. *Targeted Attacks versus APTs: What’s The Difference? – TrendLabs Security Intelligence Blog.* blog.trendmicro.com [online]. 14. září 2015 [vid. 12. březen 2019]. Získáno z: https://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attacks-versus-apts-whats-the-difference/

LUKOVIČ, Radoslav, 2018. *K rozdělení nejnižší nabídkové ceny jako hodnotí. EPRAVO.CZ* [online]. [vid. 17. prosinec 2019]. Získáno z: https://www.epravo.cz/top/clanky/k-rozdeleni-nejnizsi-nabidkove-ceny-jako-hodnoticiho-kriteria-107907.html

Kyberkriminalita – Policie České republiky [online]. [vid. 17. prosinec 2019]. Získáno z: https://www.policie.cz/clanek/kyberkriminalita.aspx

LASSE LUETH, Knud. *State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. iot-analytics.com* [online]. 8. srpen 2018 [vid. 16. únor 2019]. Získáno z: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

MICHLMAYR, Thomas. *European Commission Cloud Strategy. nedatováno, s. 28.*

NetMonitor [online]. [vid. 16. únor 2019]. Získáno z: http://www.netmonitor.cz/

NICOLE.KELLER@NIST.GOV. *Cybersecurity Framework. NIST* [online]. 12. listopad 2013 [vid. 18. prosinec 2019]. Získáno z: https://www.nist.gov/cyberframework

NÁRODNÍ STÁLÁ KONFERENCE O BEZPEČNOSTI. nskb-150216-final.pdf [online]. [vid. 18. prosinec 2019]. Získáno z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

Number of Internet Users (2016) – *Internet Live Stats. Internet Users* [online]. [vid. 16. únor 2019]. Získáno z: http://www.internetlivestats.com/internet-users/

S.R.O, VisionApps. *Zaměstnanci chtějí home office. Splňte tyto 2 podmínky, aby práce z domu fungovala. LMC* [online]. [vid. 17. prosinec 2019]. Získáno z: https://www.lmc.eu/cs/magazin/data-a-pruzkumy/zamestnanci-chteji-home-office-splnte-tyto-2-podminky-aby-prace-z-domu-fungovala/

Statistiky řešených incidentů – CSIRT [online]. [vid. 17. prosinec 2019]. Získáno z: https://csirt.cz/page/2635/statistiky-resenych-incidentu/

ŠPIDLA, Aleš. *Novela zákona o vojenském zpravodajství – potřebujeme ji? IT SECURITY NETWORK NEWS* [online]. 26. únor 2019 [vid. 12. březen 2019]. Získáno z: https://www.itsec-nn.com/novela-zakona-o-vojenskem-zpravodajstvi-potrebujeme-ji/

What Mondelez v. Zurich May Reveal About Cyber Insurance in the Age of Digital Conflict. Lawfare [online]. 8. březen 2019 [vid. 18. prosinec 2019]. Získáno z: https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict

Národní úřad pro kybernetickou a informační bezpečnost. zprava-o-stavu-kyberneticke-bezpecnosti-cr-2018-cz.pdf [online]. [vid. 17. prosinec 2019]. Získáno z: https://www.nukib.cz/download/publikace/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2018-cz.pdf

Abstrakt:

V posledních dvou desetiletích jsme mohli pozorovat několik převážně pozitivních významných změn, které na druhou stranu mohou v konečném důsledku představovat pro většinu organizací v České republice závažné bezpečnostní riziko. Jedná se o možnost přístupu k informačním systémům a datům umístěným v cloudu a spravovaných třetí stranou ze soukromého osobního zařízení přes internet. Cloudy byly navrhnuty tak, aby byly odolné vůči hrozbám přírodního charakteru a dokázaly být v chodu pro případ dočasné nedostupnosti datového centra nebo i jeho kompletního zničení. Slabinou cloudů však vždy bude lidská chyba nebo kybernetický útok zneužívající SW zranitelnosti. Příspěvek se zabývá jednotlivými změnami v předmětné oblasti, které ovlivňují rostoucí počty agregovaného rizika.

Klíčová slova: *koncová zařízení, BYOD, cloud, práce z domova, outsourcing, zranitelnosti, kybernetické útoky, bezpečnostní povědomí, agregované riziko.*

Abstract:

How the Aggeged Security Risk is Arised

In the last two decades we could observe several predominantly positive significant changes, which, on the other hand, may ultimately pose a serious cumulative security risk for most organizations in the Czech Republic. Namely it is possibility to access information systems and data placed in cloud and administered by third party from private personal device via internet. Cloudy has been designed to be resilient to nature threats and proves to work in the event of a data center failure or complete destruction. The weakness of the clouds, however, will always be a human error or cyber attack exploiting SW

vulnerabilities. The paper deals with individual changes in the subject area, that affect the increasing number of aggregated risk.

Key words: *end points, BYOD, cloud, home office, outsourcing, vulnerabilities, cyber attacks, security awareness, aggregated risk.*

JEL: H56, K24

Ing. **Miroslav Čermák** – Policejní akademie, Katedra managementu a informatiky, Lhotecká 7, Praha. cermak.miroslav@pacr.eu.

PARALELNÍ TRESTNÍ STÍHÁNÍ A MAXIMÁLNÍ DÉLKA VAZBY

Zdeněk Koudelka

1. ÚVOD

Trestní řád stanoví maximální délku vazby podle závažnosti trestného činu, pro který se vede trestní stíhání. Ovšem v praxi se lze setkat s tím, že jsou proti obviněnému vedena paralelní trestní stíhání. Otázkou je, zda maximální délka vazby je omezena zákonnou délkou vazby podle nejpřísněji trestného činu pro všechna trestní stíhání, anebo se posuzuje v každém trestním stíhání délka vazby samostatně a vazby z různých trestných stíhání mohou na sebe bezprostředně navazovat.

Vazba je závažným narušením základního lidského práva na svobodu. Výslovně Listina práv a svobod stanoví, že nikdo nemůže být ve vazbě leč na dobu stanovenou zákonem.[1] Tedy v případě překročení zákonné délky vazby se nejedná jen o porušení zákonného pravidla, ale i základního práva na osobní svobodu chráněného ústavně. V oblasti základních lidských práv a svobod je z pohledu materiální ochrany těchto práv a jejich významnosti správné v případě pochybností volit ten výklad právních norem, který více chrání základní práva, před výkladem, který základní práva omezuje.

2. DŮSLEDKY SPOLEČNÉHO A ODDĚLENÉHO POSUZOVÁNÍ DÉLKY VAZBY

Uplatní-li se zásada, že se pro každé trestní stíhání posuzuje doba vazby samostatně, tak je na vůli policie a státního zastupitelství, jak bude člověk dlouho ve vazbě. Tyto orgány totiž ovládají přípravné řízení a je v jejich moci rozhodnout, že se povede jedno společné trestní stíhání pro dva skutky anebo se povedou dvě samostatná trestní stíhání pro každý skutek zvlášť. V prvním případě by byla maximálně přípustná délka vazby 1, 2, 3 nebo 4 roky a v druhém případě by se státní zastupitelství domáhalo vazby trvající až 2, 4, 6 a 8 let.

Tento výklad může mít absurdní důsledek, když pro více trestných činů lze uložit jen trest odnětí svobody dle sazby za čin nejpřísnější trestný, tedy výše trestů se nesčítá. Pokud by se posuzovala délka v těchto trestních řízeních samostatně, tak v případě maximálního

[1] Čl. 8 odst. 5 Listiny základních práv a svobod.

možného trestu 10 let by mohl někdo být ve vazbě postupně pro čtyři různá trestní stíhání v celkové délce 12 let. Tento příklad ukazuje nelogičnost takového výkladu, kdy je nesmyslné, aby vazba byla delší než samotný hrozící trest odnětí svobody.

Nelze připustit libovůli policie a státního zastupitelství tak, že by tyto orgány svévolně ovlivňovaly délku vazby v případě stíhání za více trestných činů tím, že některá spojí do společného řízení a některé naopak budou stíhat samostatně. Pokud údajné trestné činy spolu souvisí, měly by být řešeny ve společném trestním řízení. Není-li tomu tak, musí soud posuzovat maximální délku vazby s ohledem na její trvání v obou trestních řízeních.

3. LEGITIMITA DŮVODŮ NAVAZUJÍCÍCH VAZEB

V době totality byla známá praxe policejních orgánů a prokuratury, kdy maximální délka zadržení byla obcházena tím, že jedno zadržení se formálně ukončilo a ihned následovalo jiné zadržení pro jiný skutek či z jiného důvodu. Taková praxe je zneužíváním moci a není možné ji akceptovat při obcházení nejvýše přípustné zákonné délky vazby. V případě podezření na zneužití státní moci v trestním řízení je důkazní břemeno na straně státního zastupitelství, neboť to musí být schopno prokázat, že jím zvolený postup je ústavně konformní a nejedná se o obcházení zákonných limitů pro délku vazby. Je nutné obecně vyžadovat, aby každý státní orgán byl schopen prokázat legálnost i legitimnost z pohledu dodržování ústavních principů svůj postup, kterými zasahuje do ústavně zaručených práv lidí. Podezřelou indicií je kumulace chybných postupů, které samy o sobě by nezakládaly důvodné podezření na zneužití moci, ale jejich soustavné, opakované a společné působení hrubě narušuje právnost konkrétního trestního řízení.

Naše trestní právo spočívá na zásadě absorpce trestu, která rozdílně od zásady kumulace trestu, neumožňuje sčítání trestních sazeb při ukládání trestů.[2] To vede k ukládání trestu, kde je horní hranice trestu odnětí svobody dána nejpřísněji trestným činem, včetně souhrnného trestu z různých trestních řízení. Tato zásada by se měla zohlednit v posuzování délky vazby z různých trestních řízení. Lze připustit, že budou na sebe navazovat vazby z různých trestních řízení, ale v takovém případě, dojde-li k překročení vazby pro nejpřísněji trestný čin, by to měl soud zvlášť odůvodnit (např. obviněný z vraždy ke konci vazební lhůty ve vazbě spáchá čin ublížení na zdraví).

[2] § 43-45 trestního zákoníku č. 40/2009 Sb.

4. HLEDISKA POSUZOVÁNÍ

V demokratickém právním státě je nutné omezit zneužívání moci represivními orgány, kam patří i policie a státní zastupitelství. Je-li dána maximální délka vazby, není správné toto zákonné ustanovení obcházet tím, že se účelově rozdělí trestní věc do formálně samostatných trestních stíhání.

Proto by soud rozhodující o vazbě měl přihlédnout k délce vazby v součtu všech uložených vazeb v trestních řízeních, kde ze zákona při případném budoucím odsouzení obviněného dojde k uložení souhrnného trestu, především v případě útěkového důvodu vazby. Je zřejmé, že pokud se řízení vede pro trestný čin, kde je možné uložit např. trest odnětí svobody 8 let a obviněný je v tomto řízení ve vazbě 1 rok, je motivace k útěku s ohledem na hrozící délku trestu jiná, pokud již vykonal v jiném trestním řízení vazbu 3 roky, přičemž pro oba skutky v případě odsouzení dojde k započtení vazby, a tedy tak již ve vazbě obviněný fakticky vykonal polovinu maximálního trestu odnětí svobody.

V rozporu s logikou a zásadou šetření lidských práv a svobod je útěková vazba obviněného, u něhož v dříve zahájeném trestním řízení, kde je ohrožen vyšším trestem odnětí svobody, byla vazba nahrazena např. peněžitou zárukou, pakliže se o útěk nepokusil. Pakliže soud dojde k závěru, že lze obviněného ponechat na svobodě a přijme peněžitou záruku při stíhání za trestný čin např. s možností trestu 13 let, měl by se tím řídit i vazební soud rozhodující později o vazbě v trestním stíhání za čin méně trestný.[3]

Zvlášť pečlivě by soud měl zkoumat to, když obhajoba namítne, že nové trestní stíhání je snahou státního zastupitelství obejít nejvyšší zákonnou délku vazby pro předcházející trestní stíhání. Důkazní břemeno, že nejde o manipulativní rozdělení trestní věci do dvou trestních řízení za účelem obejití zákona, musí unést státní zastupitelství. Indiciemi je především to, když druhé trestní stíhání souvisí s původním např. totožností dozorového státního zastupitelství anebo tím, že obvinění bylo učiněno na základě informací, které mělo státní zastupitelství a policie k dispozici několik let a náhle je použily pro nové trestní stíhání až před vypršením maximální délky vazby v původním trestním řízení. Pak je zřejmé, že informace byly uloženy v šuplíku policie a státního zastupitelství právě proto, aby byla obejita zákonem stanovená délka vazby.

[3] Nález Ústavního soudu z 18. 6. 2014, I.ÚS 980/14: „*za situace, kdy se započítává do délky trestu doba, kterou stěžovatel strávil ve vazbě, se pokušení obviněných uprchnout či skrývat se postupně nutně snižuje, neboť se snižuje i délka možného trestu. Tyto měnící se podmínky způsobené plynutím času představují podstatný faktor při posuzování útěkové vazby, se kterým se každý soud rozhodující o pokračování vazby musí vypořádat.*“.

Abstrakt:

Článek popisuje kriticky praxi prolamování maximálních lhůt vazby v trestním řízení formou následných trestných stíháních, kdy se pro každé trestní stíhání počítá maximální doba zvlášť, byť je možné uložit jen jeden souhrnný trest. Tento postup hodnotí text kriticky s dopady na neústavní zásah do práva na svobodu.

Klíčové slovo: *vazba.*

Abstract:

Length of Remand for Related Criminal Enforcement

The article critically describes the practice of breaking the maximum time limits of custody in criminal proceedings in the form of subsequent prosecutions, where the maximum time is calculated separately for each prosecution, even if it is possible to impose only one collective punishment. This procedure evaluates the text critically, with implications for unconstitutional interference with the right to freedom.

Key words: *remand.*

JEL: N440

Doc. JUDr. **Zdeněk Koudelka**, Ph.D. – Katedra ústavního práva a politologie Právnické fakulty Masarykovy univerzity Brno. Vysoká škola Ambis, Mezírka 1, 602 00 Brno. zdenek.koudelka@mail.muni.cz.

KE DVĚMA AKTUÁLNÍM PROBLÉMŮM Z OBLASTI ÚZEMNÍ SAMOSPRÁVY

Petr Kolman

1. ÚVOD

V předloženém textu se budeme zabývat dvěma aktuálními problémy z oblasti územní samosprávy. V první části článku se zaměříme na problém související s tématikou odvolání vedoucího úředníka městského úřadu, v části druhé si rozebereme zajímavý oříšek týkající se mimořádných odměn ředitelů příspěvkových organizací. Obě tyto sporné otázky měly a mají přesah z práva veřejného (správního) i do práva soukromého.

2. ODVOLÁNÍ VEDOUCÍHO ÚŘEDNÍKA

V praxi se několikrát vyskytla otázka, zda má starosta obce povinnost před odvoláním vedoucího úředníka nebo vedoucího úřadu z funkce upozornit tohoto vedoucího úředníka nebo vedoucího úřadu na porušování povinností a stanovit lhůtu k nápravě. Existuje skutečně taková „napomínací“ povinnost anebo možno vedoucího úředníka bez jejího splnění?

Nejprve je dobré zmínit, že podle ustanovení § 12 odst. 1 zákona o úřednících územních samosprávných celků[1] (dále i jen zákon o úřednicích) vedoucího úředníka nebo vedoucího úřadu lze z funkce odvolat, pouze pozbyl-li některý z předpokladů stanovených podle § 4 zákona o úřednících, anebo porušil-li závažným způsobem některou ze svých zákonem stanovených povinností, nebo dopustil-li se nejméně dvou méně závažných porušení zákonem stanovených povinností v době posledních šesti měsíců, anebo neukončil-li vzdělávání vedoucích úředníků ve lhůtě podle § 27 odst. 1 zákona o úřednících.

Dále je dobré připomenout, že dle § 12 odst. 4 zákona o úřednících odvoláním nebo vzdáním se funkce vedoucího úředníka nebo vedoucího úřadu pracovní poměr nekončí. To ovšem neplatí, v případě že byl předmětný pracovní poměr založen jmenováním na dobu určitou.[2] Územní samosprávný celek (obec, kraj) je povinen podat vedoucímu úředníku nebo vedoucímu úřadu návrh na změnu jeho dalšího pracovního zařazení u územního

[1] Zákon č. 312/2002 Sb., o úřednících územních samosprávných celků.
[2] SVOBODA, I.: *Zákoník práce s komentářem.* Ostrava: KEY Publishing, 2008, s. 23-26, ISBN 978-80-87071-66-3.

samosprávného celku převedením na jinou práci. A to takovou, jenž koresponduje s jeho zdravotním stavem a dosaženou odbornou kvalifikací. Pakliže územní samosprávný celek nemá pro vedoucího úředníka (anebo vedoucího úřadu) takovou vhodnou práci nebo ji vedoucí úředník či vedoucí úřadu odmítne, jde o překážku v práci na straně územního samosprávného celku a současně je dán výpovědní důvod podle ustanovení § 52 písm. c) zákoníku práce. Dodejme, že odstupné poskytované vedoucímu úředníku nebo vedoucímu úřadu při organizačních změnách nenáleží v případě rozvázání pracovního poměru po odvolání nebo vzdání se funkce vedoucího úředníka či vedoucího úřadu.

V souladu s judikaturou nutno konstatovat, že ustanovení § 12 odst. 1 zákona o úřednících nestanoví starostovi povinnost upozornit vedoucího úředníka nebo vedoucího úřadu na porušování povinností a stanovit lhůtu k nápravě, neboť pouze interpretací ustanovení § 12 odst. 1 zákona o úřednících nelze dovozovat další novou povinnost, jež by musel starosta před odvoláním vedoucího úředníka nebo vedoucího úřadu z funkce splnit. Ostatně potom by mu v rozporu s článkem 4 odst. 1 Listiny základních práv a svobod, podle něhož povinnosti mohou být ukládány toliko na základě zákona a v jeho mezích a jen při zachování základních práv a svobod, byla ukládána povinnost, která nemá oporu v zákoně (ani v zákonném zmocnění).[3] Takový postup by byl protiústavní.

Na jednu stranu sice platí, že legální vymezení důvodů, pro něž možno vedoucího úředníka nebo vedoucího úřadu z funkce odvolat, obsažené především ve výše citovaném § 12 odst. 1 zákona o úřednících nelze vykládat jako pouhou deklaraci mající jen proklamativní anebo doporučující obsah. Zmíněné vymezení představuje jasné a předvídatelné stanovení podmínek, za nichž lze vedoucího úředníka (nebo vedoucího úřadu) z funkce odvolat. A je de facto i výrazem zvýšené (ne však absolutní) ochrany jejich vedoucího postavení. A z toho srozumitelně plyne, že je vyloučeno odvolat vedoucího úředníka územního samosprávného celku z funkce, v případě že nejsou splněny stanovené právní předpoklady pro tento postup, které stanoví zejména výše citovaný § 12 zákona o úřednících.

Na stranu druhou taktéž platí, že nemožno nad rámec zákona tyto zákonné parametry svévolně posilovat, a tedy žádat po starostech obcí, aby plnili podmínky jdoucí nad rámec zákona o úřednících[4]. Zde konkrétně ohledně zmíněné „napomínací a nápravné“ povinnosti.

[3] Srov. Nejvyšší soud 21 Cdo 3535/2017.
[4] Zákon č. 312/2002 Sb., o úřednících územních samosprávných celků.

3. VYPLÁCENÍ ODMĚNY ŘEDITELI PŘÍSPĚVKOVÉ ORGANIZACE

V praxi se možno setkat s otázkou, zda může starosta obce svou nečinností „zablokovat“ odměnu řediteli příspěvkové organizace, kterou zmíněnému řediteli předtím schválila rada obce za splnění mimořádných pracovních úkolů v souladu se zákoníkem práce? Zmíněná situace nastává zpravidla v případě, že starosta byl na radě obce v této věci přehlasován.

Podle § 134 zákoníku práce za úspěšné splnění mimořádného nebo zvlášť významného pracovního úkolu může zaměstnavatel poskytnout zaměstnanci odměnu. Odměna je nenárokovou složkou platu, zaměstnanci na ni vzniká nárok až na základě výjimečného (neběžného) rozhodnutí zaměstnavatele o jejím přiznání. Tímto rozhodnutím ztrácí odměna svou nenárokovou (fakultativní) povahu a zaměstnavatel je povinen tuto složku platu zaměstnanci vyplatit, neboť jsou splněny podmínky pro její poskytnutí. Rozhodnutí zaměstnavatele o přiznání odměny zaměstnanci podle § 134 zákoníku práce je právním jednáním, který je projevem vůle směřujícím zejména ke vzniku, změně nebo zániku těch práv nebo povinností, které právní předpisy s takovým projevem spojují.[5]

V našem případě stojíme před otázkou, jestliže už usnesením rady obce z právního hlediska vzniká zaměstnanci oprávněný nárok na vyplacení mimořádné odměny, a to i když zde chybí projev vůle starosty obce. Pro zodpovězení otázky je v souladu s judikaturou rozhodující, zda uvedené usnesení rady představovalo rozhodnutí o odměně ve smyslu ustanovení § 134 zákoníku práce, jímž by se předmětná odměna stala nárokovou složkou platu zmíněného ředitele příspěvkové organizace.

V souladu s judikaturou Nejvyššího soudu můžeme konstatovat, že projev vůle starosty navenek, zde představuje jen formální dovršení právního jednání, jehož absence nemá vliv na vznik nároku zaměstnance na vyplacení odměny podle § 134 zákoníku práce. Zaměstnanec získal legitimní očekávání, že mu bude odměna poskytnuta, neboť se o schválení odměny radou obce již dříve dozvěděl. Uvedený závěr chrání zaměstnance obce před situací, že by (ne)vyplacení odměny záviselo na uvážení starosty, jenž by tímto takřka svévolným způsobem mohl měnit vůli rady města, případně ji nečinností fakticky vyloučit.[6] Jednání v podobě činnosti starosty obce zde není nutné, z pohledu práva postačuje

[5] Rozsudek Nejvyššího soudu ze dne 8. 11. 2004, 21 Cdo 537/2004, uveřejněný pod č. 28 ve Sbírce soudních rozhodnutí a stanovisek, roč. 2005 a rozsudek Nejvyššího soudu ze dne 23. 2. 2016, 21 Cdo 4481/2014, R 27/2017.

[6] Rozsudek Nejvyššího soudu ze dne 15.2.2017, čj. 21 Cdo 2144/2016, www.nsoud.cz.

rozhodnutí rady obce o udělení zmíněné mimořádné odměny řediteli příspěvkové organizace. Starosta tedy nemůže zakázat vyplacení již radou obce řádně schválené odměny.

Literatura

SVOBODA, I.: *Zákoník práce s komentářem.* Ostrava: KEY Publishing, 2008, s. 23-26, ISBN 978-80-87071-66-3.

Abstrakt:

Text se zabývá dvěma problémy územní samosprávy. Nejprve otázkou, zda je nutné před odvoláním vedoucího úředníka upozornit jej na možnost odvolání. Druhý problém je o tom, zda starosta může zamezit vyplacení odměny řediteli příspěvkové organizace obce, kterou již schválila rada obce.

Klíčová slova: *územní samospráva, odvolání vedoucího úředníka.*

Abstract:

On Two Topical Problems in the Area of Territorial Self-government

The presented text deals with two topical issues in the area of territorial self-government. In the first part of the article we will focus on an interesting issue related to the topic of dismissal of a senior official of the municipal office, in the second part we will discuss a current and interesting problem concerning extraordinary remuneration of directors of contributory organizations. Both of these issues have and have an overlap between public (administrative) and private law.

Keywords: *Local government, dismissal of senior official.*

JEL: H83

JUDr. **Petr Kolman**, Ph.D. – Vysoká škola Ambis, Katedra bezpečnosti a práva, Lindnerova 1, 180 00 Praha. pkolman@post.cz.

ZÁKON O OBCÍCH (OBECNÍ ZŘÍZENÍ) – KOMENTÁŘ.

ZDENĚK KOUDELKA, PETR PRŮCHA, JANA ZWYRTEK HAMPLOVÁ:

Praha Leges 2019, 480 s., ISBN 978-80-7502-335-3, www.knihyleges.cz.

Petr Kolman

Jako učitel správního práva mám vždy radost, pokud vyjde nová publikace v našem oboru. V následující anotační recenzi se budu věnovat dílu kolektivu autorů: Zákon o obcích (obecní zřízení) – Komentář. Jak již složení autorského tria naznačuje, jde o vysoce erudovanou publikaci z pera zkušených autorů. Velice stručně si autory představme.

Doc. JUDr. ZDENĚK KOUDELKA, Ph.D. je dlouholetým advokátem a vysokoškolským docentem v oboru ústavního práva, v minulosti byl mj. i poslancem. Autor tedy v sobě spojuje jak teoretika, tak i ostříleného praktika. Zdeněk Koudelka také mimo odborného tisku rád a často publikuje v tisku denním. Jeho popularizace jsou vždy přínosné a je vidět, že autor tzv. drží prst na tepu doby a neuzavírá se ve slonovinové akademické věži a nežije minulostí.

Prof. JUDr. PETR PRŮCHA, CSc. již v roce 1976 absolvoval Právnickou fakultu Masarykovy univerzity (tehdy to byla ještě Universita Jana Evangelisty Purkyně v Brně), kde je od té doby pilířem katedry správního práva a správní vědy. Katedru také mnoho let vedl. Petr Průcha byl v letech 2003-2019 respektovaným soudcem Nejvyššího správního soudu, kde zastával pozici předsedy senátu. Je autorem desítek učebnic a odborných článků především z oblasti správního práva. Od 1. ledna 2020, po odchodu z justice, se stal členem Legislativní rady vlády.

Mgr. JANA ZWYRTEK HAMPLOVÁ je advokátka se specializací na územní samosprávu. V letech 1986–90 pracovala v samosprávě, poté jako novinářka a organizační poradkyně, od roku 1994 dodnes působí v advokacii. Tato žena z autorského kolektivu je zkušenou právní praktičkou, u protistran možná až obávanou advokátkou. Je známá zejména čtenářům časopisu Moderní obec, kam píše pravidelně více než dvacet let. Jana Zwyrtek Hamplová byla také v minulosti poslankyní.

Recenzovaná odborná publikace z oblasti územní samosprávy nabízí zejména odpovědi na pestrou škálu otázek vznikajících při aplikaci zákona č. 128/2000 Sb., o obcích (obecní

zřízení). Jde zde o literární formu komentáře, nikoliv tedy klasické učebnice, nicméně možno ji doporučit zvídavějším studentům právnických i dalších fakult se zájmem o obecní zřízení a otázky související.

Komentář zmíněného autorského tria je založen na dlouholetých zkušenostech tvůrců z oblasti teorie i praxe správního a ústavního práva. Výklad k jednotlivým ustanovením zákona o obcích je značně podrobný, avšak i srozumitelný, a to nejen právníkům, právničkám a studentům práv. Nutno uvítat, že zmíněná publikace je obohacena jednak přehledem pečlivě vybrané judikatury vztahující se k jednotlivým ustanovením, tak i seznamem souvisejících právních předpisů.

U judikatury někdy bývá metodologický problém, že reflektuje překonaný právní stav. U této knihy to však neplatí, protože v rámci zařazené judikatury jsou uvedena i rozhodnutí soudů, jenž sice vznikla za jiného právního stavu, ale pakliže jsou tato soudní rozhodnutí využitelná odbornou veřejností i dnes. Přísnější oponent by možná vytknul, že nebyla zařazena judikatura zahraniční, nicméně nejedná se o rigorózní či dizertační práci. Nadto samoúčelné citování různých exotických právních úprav by zde nebylo účelné. Je sice hezké, pokud se autor „pochlubí“, že vyhledal např. uruguayskou či mongolskou judikaturu, nicméně většinou to dílo spíše neposouvá myšlenkově kupředu, a leckdy právníky z veřejné správy zdržuje nebo dokonce odrazuje. Je dobře, že u jednotlivých komentovaných paragrafů je důsledně odkazováno i na související odbornou literaturu.

Text Komentáře je vyrovnaný, žádná z jeho částí není výrazně substandardně zpracována. Autorovi recenze se subjektivně asi nejvíce líbí pasáže věnované orgánům obcí, ale i například části ohledně pojetí samostatné a přenesené působnosti obcí jsou vysoce kvalitní. Nebudu snad daleko od pravdy, pokud budu konstatovat, že komentář zákona o obcích byl sepsán se záměrem, aby forma i smysl byly co nejpřístupnější nejen odborné právnické veřejnosti, ale především radním, zastupitelům a zaměstnancům obcí (popř. i krajů a příspěvkových organizací zřizovaných územně samosprávnými celky), jejichž každodenní práce vyžaduje znalost právních předpisů a aplikační nepochybnost při jejich užívání. Recenzovaný Komentář je zpracován na základě stavu platného k 1. prosinci 2019.

JUDr. **Petr Kolman**, Ph.D. - Vysoká škola Ambis, Katedra bezpečnosti a práva, Lindnerova 1, 180 00 Praha. pkolman@post.cz.

Redakční rada časopisu

doc. JUDr. Zdeněk Koudelka, Ph.D. ***Předseda***	*Vysoká škola Ambis, Právnická fakulta Masarykovy univerzity*
prof. Vladimír Belych, Dr.Sc.	*Právnická fakulta, Uralská státní univerzita Jekatěrinburg Rusko*
prof. JUDr. Jozef Čentéš, Ph.D.	*Generální prokuratura Slovenska Bratislava, Univerzita Komenského Bratislava*
doc. Ing. Jaroslav Dočkal, CSc.	*Střední škola informatiky, poštovnictví a bankovnictví Brno*
JUDr. Ing. Zdeněk Dufek, Ph.D.	*Fakulta stavební, Vysoké učení technické Brno*
prof. Ivan Halász, Ph.D.	*Národní univerzita veřejné služby Budapešť, Ústav práva Maďarské akademie věd Maďarsko*
JUDr. Milan Hodás, Ph.D.	*Ústav státu a práva Slovenské akademie věd Slovensko*
Ing. Radoslav Ivančík, Ph.D.	*Akademie Policejního sboru Bratislava – Slovensko*
doc. JUDr. Ing. Radek Jurčík, Ph.D.	*Mendelova univerzita Brno*
doc. Ing. Ludvík Juříček, Ph.D.	*Vysoká škola Karla Engliše Brno*
JUDr. Alena Kandalcová, Ph.D.	*Ústavní soud Brno*
Mgr. Pavel Kandalec, Ph.D.	*Právnická fakulta, Masarykova univerzita Brno*
JUDr. Petr Kolman, Ph.D.	*Vysoká škola regionálního rozvoje a bankovní institut Ambis Praha*
doc. JUDr. Jan Kolouch, Ph.D.	*Vysoká škola Ambis Praha*
prof. JUDr. Petr Průcha, Ph.D.	*Nejvyšší správní soud, Právnická fakulta, Masarykova univerzita Brno*
doc. Ing. Milan Jan Půček, Ph.D.	*Vysoká škola Ambis Praha*
JUDr. Filip Rigel, Ph.D.	*Univerzita Hradec Králové*
RSDr. Petr Rožňák, CSc.	*Vysoká škola Ambis Praha*
doc. JUDr. Jan Svatoň, CSc.	*Právnická fakulta, Masarykova univerzita Brno*
prof. Dr. Boguslaw L. Ślusarczyk	*Řešovská univerzita, Rzeszów - Polsko*
JUDr. Renata Vesecká, Ph.D.	*Vysoká škola finanční a správní Praha*

Adresa redakce

Vysoká škola Ambis

Časopis Právo a bezpečnost

Mezírka 775/1, 602 00 Brno

zdenek.koudelka@is.ambis.cz

Vydává:

Vysoká škola Ambis

Lindnerova 575/1

180 00 Praha 8 - Libeň

Tisk:

NOVPRESS s.r.o.,

Nám. Republiky 15,

614 00 Brno-Židenice

Registrováno Ministerstvem kultury pod číslem E 21228.
ISSN 2336−5323

Datum vydání: 31. 12. 2019

Objednávky předplatného přijímá vydavatel, cena předplatného je 600 Kč ročně, jednotlivé číslo stojí 200 Kč a lze jej zakoupit na adrese redakce. Vychází 3x ročně.


Ambis.