data security management®

ČASOPIS O BEZPEČNOSTI, SPRÁVĚ A ŘÍZENÍ
RIZIK INFORMAČNÍCH SYSTÉMŮ

Ročník XXIV
Číslo 1| 2020

INFORMATION SECURITY SUMMIT

IS2 – KYBERPROSTOR V NAŠEM ŽIVOTĚ

...hrozby a rozmazané hranice

Budeme se věnovat tématům:

- hybridní útoky na finanční průmysl a KI
- bankovní identita
- cloudová bezpečnost
- dezinformace a dezinformační kampaně
- privacy by design a další...

Jedinečná příležitost setkat se v Praze s mnoha osobnostmi.

XXI. ročník
mezinárodní konference
o informační bezpečnosti

Praha

www.is2.cz

Záštitu nad IS2 2020 přijali

Tomáš Petříček, Ph.D., Ministr zahraničních věcí
Ing. Jan Bartošek, Předseda poslaneckého klubu KDU-ČSL
Brigádní generál Ing. Jan Beroun, Ředitel Vojenského zpravodajství
Ing. Vladimír Dzurilla, Vládní zmocněnec pro IT a digitalizaci
RNDr. Josef Postránecký, Náměstek Ministerstva vnitra pro státní službu
Ing. Jaroslav Šmíd, Náměstek ředitele NÚKIB
JUDr. Ivana Janů, Předsedkyně Úřadu pro ochranu osobních údajů
Ing. Vladimír Dlouhý, CSc., Prezident Hospodářské komory ČR
Ing. Pavel Štěpánek, Výkonný ředitel ČBA

Na tomto ročníku vystoupí i tyto osobnosti

JEFFREY BARDIN

- CIO v Treadstone 71, zakládající člen Cloud Security Alliance, své dlouholeté zkušenosti z tajných služeb zúročil jako šéf bezpečnosti pro Fortune 100 korporace.

MICHAEL A. GOEDEKER

- V přednášce vysvětluje různé typy hybridních útoků na finanční průmysl a kritickou infrastrukturu, které využívají kybernetické zbraně a špionážní a zpravodajské taktiky.

JAKUB KALENSKÝ

- Soustředí se na zvyšování povědomí o pro-kremelské dezinformační kampani a vedl kampaň EUvsDisinfo.

NAMRATA GOSWAMI

- Je nezávislá strategická analytička v oblastích boje proti povstalcům a terorismu, alternativních budoucností a velkomocenské politiky.

JOSEF DONÁT

- Ve své přednášce se zaměří na bankovni identitu v souvislosti s nově schválenou legislativou.

DENNIS MOREAU

- Hlavní architekt v Office of the CTO ve společnosti VMware, kde pracuje na bezpečnostních inovacích.

JAN BLAŽEK

- Programový manažer v ČSOB promluví o bankovní identitě.

TOP partner: Deloitte.
PLATINOVÝ partner: ICZ
ZLATÍ partneři: insighti
STŘÍBRNÝ partner: pwc
Partner Síně slávy Cybersecurity: CETIN
Partneři: NG Národní galerie Praha, OneTrust Privacy
Technický partner konference: STREAM CIRCLE

Programový výbor

Lukáš Klášterský – Erste Group (předseda PV)
Radek Komanický – MALLGroup
Radim Kolář – DHL IT Services
Eva Racková – RVDA
Pavel Východský – TOP Consulting CZ
Michal Wojnar – PwC

Čestní členové programového výboru

Jeffrey Bardin – Treadstone 71
Sean S. Costigan – IllustroTech/George C. Marshall Center
Vashek Matyáš – MU Brno
Zdeněk Říha – MU Brno

Poradci programového výboru

Peter Chrenko – PWC
Tomáš Jabůrek – E.ON
Richard Kadlčák – MZV
Petr Kučera – Power Patterns
Vladimír Matouš – Raiffeisen Bank
Jiří Mifek – Komerční banka Slovensko
Daniel Rous – ČEZ
David Šetina – Ideal IT
Miroslav Uřičař – Legalité
Daniel Votápek – ČSOB
Marcel Zanechal – Slovak Telekom & T-Mobile CZ

Komise Síně slávy

Michal Frankl – CETIN
Ondřej Filip – CZ.NIC
Richard Kadlčák – MZV
Lukáš Klášterský – Erste Group (předseda PV)
Martin Maisner – advokát a rozhodce
Vladimíra Mandulová – TATE International
Jaroslav Šmíd – NÚKIB

www.is2.cz

Organizátor: Tate International

OBSAH

Články označené prošly odborným recenzním řízením.
Články označené firemním logem jsou komerčními prezentacemi.

Rozhovor s Jeffreym Bardinem — strana 7

Adam Lamser

Jeffrey Bardin je výkonným ředitelem a zároveň hlavním zpravodajcem ve firmě Treadstone 71. Jako předního odborníka jak na zpravodajství, tak i na kyberprostor jsme se ho v tomto díle ptali na Cyber Threat Intelligence, co to vlastně znamená být zpravodajcem v soukromém sektoru a jak vnímá pokroky kybernetické bezpečnosti od jejího zrodu.

Povinnost Data Retention v judikatuře Soudního dvora EU a Ústavního soudu ČR — strana 17

Miroslav Uřičař

Povinnost uchovávat provozní a lokalizační údaje (Data Retention) byla od svého přijetí kritizována kvůli zásahům do práva na soukromí. Povinnost Data Retention již byla předmětem tří rozhodnutí Soudního dvora EU a tří rozhodnutí Ústavního soudu ČR, nejvýznamnějším z nich byl rozsudek Soudního dvora EU o prohlášení Data Retention Směrnice za neplatnou. V probíhající věci francouzský, belgický a britský soud požádaly Soudní dvůr EU, aby posoudil, zda jejich národní povinnosti Data Retention jsou v souladu s unijním právem. Generální advokát Soudního dvora přednesl své stanovisko v těchto věcech 15. ledna 2020. Podle jeho názoru musejí být prostředky a metody boje proti terorismu v souladu s požadavky právního státu. Proto konstatuje, že ePrivacy směrnice brání takové právní úpravě, která ukládá povinnost plošně a nerozlišujícím způsobem uchovávat provozní a lokalizační údaje všech účastníků, jako je tomu u francouzské, belgické a britské právní úpravy. Rozhodnutí Soudního dvora může být očekáváno v nadcházejících měsících.

DevOps – část VII. — strana 30

Vladimír Kufner

Předposlední díl série článků o DevOps shrnuje dosažené výsledky transformace na DevOps po cca 10letém období a zamýšlí se nad odhadem budoucího vývoje DevOps. Článek probírá nejčastější mýty a typické problémy při transformaci na DevOps.

Soukromí uživatelů v prostředí internetové reklamy na českém webu — strana 11

Libor Polčák

Pro zobrazení co nejrelevantnější internetové reklamy jsou využívané aukční servery, které šíří nabídky prozrazující velké detaily o uživateli, jeho vlastnostech, prohlížeči, poloze apod. Proto jsou v poslední době podávány četné stížnosti k dohledovým orgánům. Tento článek ukazuje, že i v ČR jsou zpracovávána citlivá osobní data bez odpovídajících souhlasů.

Průzkum stavu digitalizace — strana 23

Peter Chrenko

Ze slovních spojení obsahujících slova Digitalizace a Digitální transformace se postupně stává klišé, případně každý si pod ní představuje něco úplně jiného. Ukazuje se, že nejobvyklejší představa souvisí se zaváděním nových technologií a aplikací, které nám usnadňují práci a zákazníkům zpříjemňují život. Čím víc firma do těchto technologií investuje, tím se považuje za digitálnější. Realita je však taková, že tyto investice nepřináší očekávaný efekt, protože se v tomto „digitálním“ snažení zapomíná na to nejdůležitější – zákazníka (interního a externího). Cílem článku je s využitím nedávných miniprůzkumů poodhalit, jaká je digitální skutečnost ve velkých firmách a naznačit, jak k této komplexní problematice prakticky přistupovat v organizacích a začít vytvářet povědomí pro veřejný sektor, aby to dělal správně hned na první pokus, protože to má dopad na všechny občany a celou společnost.

Dvě dekády snah OSN o stabilizaci kybernetického prostoru — strana 36

Richard Kadlčák

Článek pojednává o historickém vývoji snah OSN o stabilizaci kybernetického prostoru od devadesátých let do současnosti. Zároveň identifikuje hlavní třecí plochy mezi státy hájícími svobodný, otevřený a bezpečný kyberprostor na straně jedné, a státy, které usilují o omezení svobody na internetu pod záminkou zajištění kyberbezpečnosti, na straně druhé. V neposlední řadě článek přibližuje roli České republiky v mezinárodních jednáních OSN a zamýšlí se nad praktickými způsoby stabilizace kybernetického prostoru na globální úrovni.

OBSAH

Malware Emotet – Trickbot – Ryuk v benešovské nemocnici strana 39

Adam Kučínský, Vojtěch Sikora

Článek se zabývá kybernetickým útokem na nemocnici v Benešově, který proběhl v prosinci 2019. V článku je popsán útok, malware, který byl v tomto případě použit, postup po detekci útoku a opatření, která je třeba uplatnit k prevenci a reakci na tyto typy útoků.

Recenze knihy strana 50

Miroslav Uřičař

Recenze knihy Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti (Smejkal Vladimír, Sokol Tomáš, Kodl Jindřich)

Skutečnost může být horší než očekávání strana 44

Martin Hlaváč

Koncem roku 2019 narazili IT administrátoři významné finanční instituce v České republice na neobvyklé aktivity v IT infrastruktuře firmy. V průběhu ověřování dospěli k závěru, že společnost byla napadena hackery, a pokusili se problém vyřešit vlastními silami. Po několika týdnech neúspěšných snah byl o pomoc požádán tým ze společnosti AEC. Expertům na kybernetickou bezpečnost se záhy podařilo rozkrýt nebývalý rozsah incidentu, odhalit vstupní vektor útočníků do systému a následně útok za pomoci přesně koordinovaných kroků zastavit. Finální eliminaci útočníků v infrastruktuře instituce umožnilo nasazení EPP/EDR řešení a následné manuální ukončení zbývajících aktivit hackerů. Ti byli v průběhu vyšetřování incidentu identifikováni jako členové celosvětově aktivní skupiny Cobalt Group, která se specializuje na nezákonné vyvádění finančních prostředků z firem a institucí.

RUBRIKY

Virová stránka	52
Normy a publikace	54
Metamorfosa: Ohlédnutí za Svatomartinskou husou	55
Informace z partnerských společností	56
Metamorfosa: Zabijačka anebo workshop	57
Právní rubrika	58
Management summary	60
Tiráž	62

„Žádnou hru, žádný souboj nikdy nevyhrajete, pokud hrajete pouze na své polovině hřiště. Vždy prohrajete, protože nikdy neútočíte. Takže jestli jsem pro hackback? Rozhodně. Měl by se ho snažit dělat každý? Rozhodně ne. Mělo by to být povoleno? Do určité míry.“

...Rozhovor s Jeffreym Bardinem najdete na str. 7.

Jak uchránit český kyberprostor? Musíme táhnout za jeden provaz

V souvislosti s narůstajícími kybernetickými útoky se čím dál více objevuje otázka – jak uchránit český kyberprostor? Je to vůbec možné? Odpověď zní, že stejně jako ve všech jiných oblastech bezpečnosti těmto útokům nikdy nelze stoprocentně předejít. Nejzávažnější kybernetické útoky jsou v podstatě stejné, jako ty teroristické. Jejich projevem je vyvolání paniky, chaosu a šoku. Přicházejí neočekávaně a míří na kritická místa infrastruktury. Pokud ale vytvoříme účinný systém ochrany kybernetického prostoru, můžeme jejich číslo a dopady výrazně snížit. Klíčové slovo přitom zní: spolupráce.

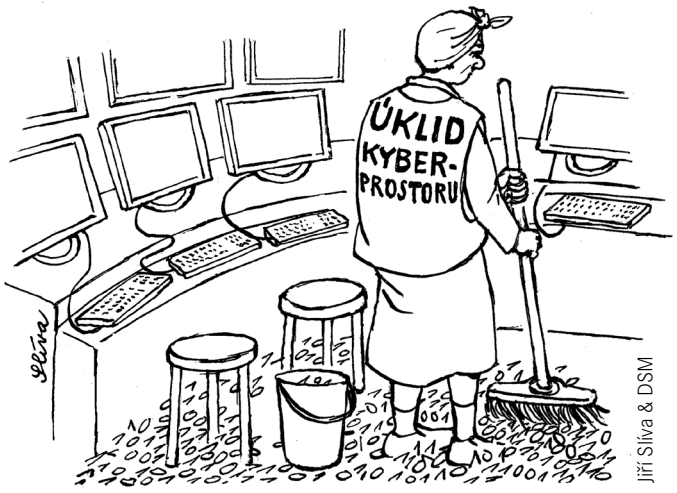
Představit si to můžeme na integrovaném záchranném systému. Ten je tvořen několika subjekty, od hasičů až po policisty. Všechny tyto subjekty v něm mají svou danou úlohu. Navzájem si nekonkurují. Naopak spolupracují a jeden bez druhého by se v krizových situacích neobešly. Stejně tak je to při ochraně českého kybernetického prostoru.

V oblasti kybernetické bezpečnosti je nutné neustále vzdělávat českou společnost, upozorňovat na kybernetické hrozby a všeobecně se zabývat vším, co do online světa patří. To u nás zastává Národní úřad pro kybernetickou a informační bezpečnost. Dále musíme neustále poznávat kybernetický prostor, studovat a zkoumat jeho jednotlivé anomálie, abychom je dokázali identifikovat, pojmenovat a tím uměli rozpoznat případný chystaný útok, který musíme být schopni následně i odvrátit. To je úkol Vojenského zpravodajství, samozřejmě ve spolupráci s dalšími složkami.

Potřebujeme ale také vyvíjet a aplikovat kvalitní řešení systémů kybernetické bezpečnosti. České ICT společnosti a místní pobočky nadnárodních firem přitom díky své tvořivosti a schopnosti improvizovat vyvíjí jedny z nejlepších takových systémů. S nimi musíme tuto problematiku diskutovat, spolupracovat jak na vzájemném vzdělávání, tak na řešení krizových situací, ale i nabídnout jim jejich osobní podíl na zajišťování kybernetické obrany. To jim umožní například zapojení do chystaných aktivních záloh Vojenského zpravodajství. Tito „ajťáci" nejen že jsou špičky ve svém oboru, ale jsou to také vlastenci, kteří mají rádi svoji zem, čehož si velmi vážím.

V neposlední řadě pak potřebujeme někoho, kdo dokáže případné útočníky chytit a postavit před soud – tedy Policii České republiky. Problematika kybernetických hrozeb je přitom stále tak nová, že se v ní pořád učíme, takže počet těchto subjektů se může i nadále zvyšovat dle aktuálního vývoje.

Vše uvedené je třeba spojit do jednoho funkčního systému, ve kterém musíme všichni společně spolupracovat.



Není to jednoduchý úkol, naopak stojíme před velkou výzvou. Zůstávám ale optimistický, v bezpečnostní komunitě se pohybuji v podstatě celý život a za tu dobu jsem na české společnosti vypozoroval jednu věc – když jde do tuhého, umí se spojit a táhnout za jeden provaz. Soustřeďme se tedy společně na vytvoření co nekvalitnějšího komplexního systému, který bude chránit náš kyberprostor. Štěstí přeje připraveným.

Jan Beroun
ředitel Vojenského zpravodajství

Kybernetické zpravodajství

Jeffrey Bardin

Jeffrey Bardin je výkonným ředitelem a zároveň hlavním zpravodajcem ve společnosti Treadstone 71. Pracoval např. v organizacích General Electric nebo Lockheed Martin. Předtím sloužil v Letectvu Spojených států amerických jako kryptologický lingvista, kde v mnoha jazycích a pod mnoha kybernetickými identitami pronikal do nepřátelských skupin. V minulém dílu jsme se ho jako předního odborníka na zpravodajství i na kyberprostor ptali na Cyber Threat Intelligence a jak vnímá pokroky kybernetické bezpečnosti od jejího zrodu. Nyní nám mimo jiné prozradí, co si myslí o potenciálu a úskalí umělé inteligence ve službě kyberbezpečnosti a jaký je jeho názor na fenomén „hackback“.

Jaký vidíte význam nástupu umělé inteligence pro kybernetické zpravodajství a kybernetickou bezpečnost obecně?

Dnes je to pouze takový buzzword, což ale neznamená, že by AI neměla do budoucna potenciál. Kam až ten potenciál sahá? Tím si nejsem zcela jistý. Jako vše ostatní to začíná v rovině konceptů a akademických studií. Můžete si být jistý, že vlády a organizace jako IARPA nebo DARPA se tomuto tématu věnují intenzivně. Komerční sektor je většinou za těmito organizacemi pozadu minimálně 10–15 let, takže kdo ví, jaké všechny schopnosti už jejich „umělá inteligence“ má. Já ale vidím problém někde jinde. Nejde ani tak o to, co všechno může umělá inteligence udělat pro bezpečnost, jako spíš o to, že se její bezpečností a tím, jak do ní bezpečnost začlenit ve vývoji jejích dnešních schopností a funkčností, průběžně nikdo nezabývá. Zrovna nedávno jsem jako subkontraktor pro Ministerstvo vnitřní bezpečnosti (DHS)

dokončil 10měsíční studii, kde jsem dělal sběr a analýzu dat v oblasti autonomních vozidel a umělé inteligence. Bylo zjevné, že tam měli vzhledem k výsledkům této analýzy určitá očekávání. Ve skutečnosti jim nešlo ani tak o to, co naznačují dnešní data, chtěli hlavně zjistit, „jak a kdo nám to hackne“. To se ale ze současných dat nepozná, protože tu ještě nemáme statický model. Proto je potřeba to řešit průběžně ve vývoji. Podobně jako se vším ostatním tu něco budujeme a řešit zabezpečení budeme až zpětně.

Jelikož jde o něco nového, bude také zajímavé sledovat závod o vlastnictví těchto modelů umělé inteligence. Ten, kdo tento závod vyhraje a bude na pomyslné pásce první, získá totiž AI i z pohledu duševního vlastnictví. Kdokoli bude vlastnit či skoupí strategické části dodavatelského řetězce určitého modelu umělé inteligence, ať už autonomních vozidel nebo lékařských zařízení, stane se vlastníkem celého tohoto prostředí, protože bude vlastnit komponenty, které zpracovávají nebo jimi putují data – všechny ty bity a bajty. A pokud to vlastním, nemusím to hackovat. Je to podobné jako s Huawei a 5G a celkově se síťovým prostředím, které tradičně vlastnilo Cisco. Spojené státy jsou v 5G pozadu a nemohou si dovolit, aby v něm mělo Huawei nadvládu. Něco na tom, že do těchto produktů Čína schovává backdoory, určitě bude. Stejně tak je tam bez pochyb mají i Spojené státy a všichni ostatní. A i kdyby je tam neměli teď, není problém je tam dostat později. Tady to trochu zoptimalizuji, sem dodám aktualizaci firmwaru – to je přece imperativ výrobce. Jak jsem říkal, technologie, u kterých jde vývoj dopředu takhle rychle, nechci muset hackovat, chci je vlastnit. A pak kdokoli je bude vlastnit, toho se budou snažit hacknout všichni ostatní.

Je známo, že lidé jsou výteční na řešení problémů, ale poměrně mizerní analytici psychologických jevů, jako je kognitivní disonance a konfirmační zkreslení.

...technologie, u kterých jde vývoj dopředu takhle rychle, nechci muset hackovat, chci je vlastnit. A pak kdokoli je bude vlastnit, toho se budou snažit hacknout všichni ostatní.

Co kdybych Vám řekl, že můžete mít analytika, který nejenže není poznamenán těmito jevy, ale je navíc schopen zpracovat v podstatě neomezené množství informací? Není to jeden z možných přínosů umělé inteligence?

Řekl bych super, pojďme do toho. Nic takového ale nemáte a ještě dlouho mít nebudete. Umělá inteligence bude napsána lidmi, kteří do ní svůj způsob myšlení chtě nechtě promítnou. Takže tyto analytické defekty, které jste zmínil, se jí minimálně ze začátku budou týkat také. I tak by to samozřejmě bylo o několik řádů lepší, než co máme k dispozici dnes, už jenom díky schopnosti pracovat s tolika daty. Kdybych si měl tipnout, jak to bude probíhat, tak lidé vždy nějakou „lidskost“ do umělé inteligence zabudují, ať už záměrně nebo nevědomky. Ta pak ale bude sama na sobě pracovat a od těchto lidských předpojatostí se postupně oprostí. Dříve či později to určitě nastane, ale myslím, že schopnost naprosto čistého kalkulu, vyhodnocení něčeho bez jakékoli předpojatosti, zaujatosti a v naprosté objektivitě je skutečně hodně daleko za horizontem.

Podívejte se třeba na West World. I tam umělé inteligence měly své vlastní emoce, přestože je původně mít neměly. Je to ve skutečnosti jediný způsob, jak je lidé mohou interpretovat, jak se s nimi ztotožnit, takže to automaticky komponujeme do našeho modelu. Jako se vším ostatním, jinak by se to neprodávalo. Těžko si představit, že vybudujeme podobný model bez něčeho, o čem si ani neuvědomujeme, že to tam přidáváme. Otázkou druhou je, jak by taková čistě objektivní umělá inteligence bez lidskosti vypadala. Obávám se, že by nám nebyla příliš sympatická a ani závěry, se kterými by tato umělá inteligence přicházela, by se nám lidem nemusely moc líbit.

Jaký je váš názor na hackback a „ofenzivní bezpečnost“ celkově?

Já osobně jsem byl zastáncem hackbacku od samého začátku, co se tato myšlenka objevila. Na internetu žádná policie není. Pokud se k vám nabourávám ze svého prostředí, je mi úplně jedno, jestli jste chráněn nějakým zákonem nebo regulací. Jediné, co máte, je jakýsi obranný postoj. Žádnou hru, žádný souboj ale nikdy nevyhrajete, pokud hrajete pouze na své polovině hřiště. Vždy prohrajete, protože nikdy neútočíte. Takže jestli jsem pro hackback? Rozhodně. Měl by se ho snažit dělat každý? Rozhodně ne. Mělo by to být povoleno? Do určité míry. Do jaké? Těžko říct. NATO Cyber Command se tímto zabývá od roku 2008. Panovaly okolo toho velké diskuze zejména právnického charakteru, co by se mělo, co by se nemělo. Diskutovali o tom pořád dokola tak dlouho, až z toho nakonec vypadl Tallinnský manuál. Což je v podstatě taková kuchařka v židovsko-křesťanském podání, co si ještě můžete dovolit, aby vás Západ hackl nebo nehackl. Jenže pokud nejsem ze Západu, když se Západem nesouhlasím nebo jsem jiného náboženského vyznání, je mi to úplně jedno. Děkuji vám, že jste mi popsal,

jak přesně se budete za jaké situace chovat. Je to kompilát precedentů a judikatury mezinárodního práva z fyzického světa ohnutý do kybernetického prostoru. Neříkám, že je to zcela k ničemu, ale ukažte to třeba Rusům nebo Číňanům, co si o tom myslí. Nikdo přece nemůže očekávat, že se podle toho snad budou řídit.

Vezměte si třeba, jak to je v Americe s policií a principem naléhavé okolnosti. Například představte si, že vlastníte vilu a horní patro někomu pronajímáte. Ten se jednoho dne rozhodne, že vykrade banku a pak se schová u vás v tom patře, které mu v dobré víře pronajímáte. Někdo ho zahlédne, jak vstupuje do domu, zavolá policii, která hned přijede. Pár výstřelů z okna a policie to začne naplno kropit do vaší vily. Vyrazí dveře, vtrhne dovnitř, něco převrhne a omylem způsobí požár, načež začne pronásledovat lupiče, který mezitím vyběhl zadními dveřmi na zahradu, pak k sousedům a tak dále. Tam pošlapou kytky, rozbijí sochy, prostřelí bazén, až nakonec lupiče chytí. A všechna ta destrukce okolo, vaše vila, která mezitím lehla popelem – tomu se říká naléhavá okolnost. Je nám to líto, ale museli jsme pronásledovat a zneškodnit tuto hrozbu veřejné bezpečnosti. To se ve fyzickém světě děje neustále, a přesto si myslíme, že v kyberprostoru je hackback špatný, protože bychom snad mohli nějak postihnout

něčí server. Ten samý server, který je pod kontrolou útočníků a slouží jako řídící server pro útok na vaši organizaci. Neříkám, že je potřeba sestřelit celé IT prostředí dané organizace. Už jen z toho důvodu, že jde často o státní aktéry. Není to o tom spustit kybernetickou válku, ale zasáhnout a zbavit se té hrozby je na místě. Musíte mít samozřejmě ty správné lidi, kteří jsou schopni něco takového precizně uskutečnit. V praxi právníci a korporace svým lidem nikdy nic takového nedovolí, protože by tím riskovali právní mrzutosti. Což ale neznamená, že si na to nemůžou najmout někoho jiného. Existují společnosti, které takové služby poskytují. Některé to zvládají hůře, některé tak dobře, že je vláda Spojených států několikrát klepla přes prsty, jako třeba CrowdStrike. A tak si na to začali najímat třetí strany.

Je to podobné jako na základní škole, když na vás někdo větší doráží. Dokud mu jednu nevlepíte, bude na vás dorážet neustále. Jakmile se mu postavíte, nechá vás na pokoji a půjde otravovat někoho jiného. To je přesně to, co bychom měli dělat i v kyberprostoru, dokud tu nebudeme mít onu internetovou policii nebo to prostředí přirozeně nedospěje do bodu, kdy bude poskytovat jakousi inherentní ochranu. Jinak jenom stojíte na brankové čáře a snažíte se vykrýt jednu ránu za druhou, které na vás útočníci z různých stran pálí. To pak přirozeně můžete jenom prohrát. Je to o tom zaujmout skutečný obranný postoj a vyslat signál, že pokud si na vás někdo dovolí, budete se bránit a situaci útočníkům výrazně komplikovat. Na to většinou všichni říkají: Pokud to uděláte, budou na vás útočit ještě víc. Ale nic takového se nikdy nestalo, žádná data ničemu takovému nenasvědčují.

Takže ano, jsem pro hackback. I z toho důvodu, že vynutí určité změny, protože právně jsme se v této věci nikam neposunuli. Frameworky? Problém není v nedostatku kvalitních rámců, těch máme spíše až příliš mnoho. Je jedno, kolik

po mně hodíte frameworků, stále budete trčet v tom samém křečovitém postoji, který zjevně nefunguje.

Z hlediska mezinárodního práva jsou problémem otázky suverenity a atribuce. Na základě precedentů, které jste zmiňoval, není hackback považován za adekvátní odpověď. Přestože s Vámi souhlasím, těžko si představit, že by něčí oficiální politika byla v rozporu s mezinárodním právem.

Máte pravdu, že to nejspíš vždycky bude normou. Ale ruku na srdce, drží se v dnešní době někdo mezinárodních norem? Drží se jich Spojené státy? Podívejte se třeba na Irák, tam dodnes zuří válka založená na čistě vykonstruovaných zpravodajských informacích. Afghánistán, to byla jedna věc. Těžko si ale představit někoho sekulárnějšího a chamtivějšího, než byl Saddám Husajn – naprostý opak bin Ládina, neměli spolu nic společného. Takže jakéže normy se tedy snažíme neporušit? Jsou porušovány každý den. Stuxnet byl naprostým narušením íránské suverenity. Kdyby něco takového udělali oni nám, okamžitě bychom jim vyhlásili válku. To oni udělat nemohli, prostě protože jsou menší. A to je samozřejmě jen špička ledovce. Každý den v médiích obviňujeme Rusko, Čínu, Severní Koreu a další z kybernetických útoků. Nikde se ale nedočteme o útocích, které provádíme my na ně. To ale neznamená, že se nedějí – naopak. Je to proto, že diktatury a autokracie si nemohou dovolit být viděny jako slabé a zveřejňovat, že jsou každý den hacknuty.

A ohledně atribuce, ta mě ve skutečnosti vůbec nezajímá, jde mi o zneškodnění hrozby. Budu prostě postupně sledovat stopu útočníka, stejně jako to dělá policie. Nijak nadšený z toho nejsem, ale myslím, že je změna přístupu nutná. Bavíme se o tom od roku 2008, tedy už 11 let, a od té doby jsme se nikam neposunuli. Máme tu skvělý dokument, výborně. No a co?

Je hackback tím nejlepším řešením? Nevím. Rozhodně je to ale lepší než se snažit něco vyřešit právně, když právo v této aréně stejně nikoho nezajímá. Je potřeba si uvědomit, že nové technologie, které se vyvíjejí stále rychleji, budou tento problém umocňovat, zvláště za situace, kdy si stále více zemí buduje své vlastní kybernetické síly. Kyberprostor je více než pouze pátá doména. Prostupuje ostatními doménami, všechno propojuje. Máme tu drony a protiletecké systémy, ale nakonec budou všechny zbraně závislé na kyberprostoru. A dříve nebo později někdo přijde s kybernetickou zbraní hromadného ničení. I když to zatím zní poněkud úsměvně, je to pouze otázka času. Proč by někdo něco takového chtěl mít? Stejně jako jaderné zbraně – k odstrašení. Více zbraní pro zaručenou vzájemnou hromadnou destrukci.

Tím jste se lehce dotkl mé další otázky, a to jak vidíte budoucí vývoj v prostoru kybernetična?

Moc optimistický ohledně toho, kam míříme, nejsem. Mám takový dojem, že před sebou máme ještě hodně tvrdý boj, než i jenom zahlédneme světlo na konci tunelu. A vůbec nevím, jak se postavit tomu, co tam na nás číhá. Honba za ziskem je dnes základní hnací silou všeho a zároveň jednou z hlavních příčin problémů, kterým čelíme. Většina z nich je spojena s nástupem internetu a sociálních sítí. Je opravdu dokázáno, že lidé jsou všeobecně hloupí a uvěří víceméně čemukoli, co je v souladu s tím, čemu už věří. A nevykážou žádnou snahu si ověřit fakta nebo jen přečíst a zvážit něco, co jejich víře neodpovídá. Všechny sociální sítě jsou postaveny přesně na tomto principu. Jejich cílem je, aby uživatelé klikali na obsah a reklamy. Spadáte do skupiny, které by se mohlo něco na základě jejich profilu líbit? Budu vám to servírovat všude, kam se na internetu podíváte. Nelíbí se vám něco nebo s něčím máte pravděpodobnost nesouhlasit? Tak se ujistím, že už to nikdy neuvidíte. Čistý marketing. V tomto ohledu opravdu nebylo to, co se stalo během amerických voleb v roce 2016, překvapením. Zamyslete se, že tímto jednoduchým principem bylo možné výrazně zasáhnout do voleb největší světové mocnosti. Mocnosti, která udává směr, kam se svět několik dalších let bude ubírat. Je to děsivé. A obávám se, že jsme se dna v tomto ohledu ještě nedotkli.

Měl byste ještě nějaký vzkaz našim čtenářům?

Já osobně mám v určitých ohledech poměrně idealistický pohled na věci, ale všechno vyhodnocujte. Dobírejte se pravdy, neakceptujte jenom tak něco, co je vám prezentováno. Obávám se, že jsme trochu zapomněli učit se kriticky myslet, vyhodnocovat data a na základě toho tvořit hypotézy. Jaké je mé doporučení čtenářům? Začněte myslet. Přestaňte jednat na základě pocitů.

Děkujeme za rozhovor.

Za DSM se ptal Adam Lamser.

> ...dříve nebo později někdo přijde s kybernetickou zbraní hromadného ničení. I když to zatím zní poněkud úsměvně, je to pouze otázka času.

Soukromí uživatelů v prostředí internetové reklamy na českém webu

Reklama zajišťuje chod celé řady webových serverů, pro které často bývá hlavním zdrojem příjmů. V dnešním marketingu se používá celá řada způsobů cílení reklamy včetně cílení na dřívější zákazníky identifikované e-mailem nebo telefonním číslem. Pro zobrazení co nejrelevantnější reklamy se využívají aukční servery, které šíří nabídky prozrazující velké detaily o uživateli, jeho vlastnostech, prohlížeči, poloze apod. Proto jsou v poslední době podávány četné stížnosti k dohledovým orgánům. Jaký je stav v ČR? Tento článek ukazuje, že neradostný.

internetová reklama Real Time Bidding soukromí GDPR Transparency and Consent Framework

Služby, které jsou na internetu dostupné zdarma, musí někdo financovat. Byla vybudována data centra, nakoupena technika, je nutné platit účty za elektřinu a platy zaměstnanců. Odkud berou provozovatelé peníze? Z obchodu s reklamou založenou na předávání osobních údajů. Dnešní trh s internetovou reklamou lze charakterizovat jako malou vesnici [3], ve které si reklamní společnosti vyměňují detailní informace o drtivé většině internetové populace na planetě [8, 5, 6]. *Real Time Bidding* (RTB) umožňuje v desítkách až jednotkách stovek milisekund distribuovat mezi desítky i stovky společností informace o navštívených stránkách (URL) společně s dalšími informacemi (jednoznačný identifikátor uživatele, IP adresa nebo její podstatná část, poloha uživatele, informace o prohlížeči, operačním systému, velikosti obrazovky atd.) [5].

Pokud budeme vycházet z rozhodnutí Soudního dvoru EU C-210/16 [9], jsou za to, co se s daty děje v rámci reklamního systému, spoluzodpovědní provozovatelé služeb, kteří si partnery nasmlouvali, včetně českých novin a dalších stránek zobrazujících reklamu pomocí RTB nebo poskytujících služby a inzerujících v RTB, takže dodávají informace svým partnerům, kteří je následně šíří desítkám až stovkám společností.

Již v roce 2018 byla podána dosud neuzavřená stížnost na fungování RTB k dohledovým úřadům v Irsku a Velké Británii, která se později rozšířila do dalších zemí včetně ČR [8]. Ve Francii byla vyšetřovaná firma Vectaury, které dohledový úřad CNIL nezakázal využívání RTB [4]. CNIL však nevyšetřoval podstatu systému RTB. Britský dohledový úřad ICO současné reklamní systémy charakterizuje jako *vytváření a sdílení osobních profilů osob v míře, která působí nepřiměřeně, vlezle a neférově obzvláště při uvažení, že se týká osob, které nevědí, že se takové aktivity dějí* [6, str. 4]. Norská asociace ochrany spotřebitelů Forbrukerrådet provedla výzkum mobilních aplikací a reklamní systém považuje za utržený ze řetězu a nabádá společnosti finančně závislé na příjmech z reklamy, aby si našly jiné zdroje příjmů[1].

[1] https://www.forbrukerradet.no/out-of-control/

Možnosti cílení internetové reklamy

V současnosti existuje několik možností, podle kterých si může inzerent vybírat, kde a komu chce zobrazovat reklamu. Následující výčet se zaměřuje na ty nejobvyklejší:

- *Kontextová reklama:* Inzerent specifikuje např. domény, části URL, kategorie webu, na kterých by chtěl inzerovat. Reklama tedy není cílená na specifické uživatele, ale zobrazuje se podle kontextu stránky. Dnes se však spíše používají techniky popsané níže.

- *Behaviorální reklama:* Reklamní společnosti budují profily pro uživatele prohlížečů. Obsahují atributy popisující vlastnosti uživatelů, jeho domovskou polohu apod. Inzerenti si vybírají kombinaci atributů, na které reklamu cílí – atributy, které by uživatelé měli a neměli mít. Yuan a kol. [12] píše, že společnost evidující nejvíce atributů jich uživateli přiřazuje více než 3 000. U Facebooku bylo nalezeno celkem téměř 240 000 atributů, které přiřazuje uživatelům [10]. Uživatel si pak na Facebooku průměrně nese 523,7 atributů, zatímco BluKai eviduje průměrně 422,4 atributů a Google 42,3 atributů pro uživatele [2]. Účastníci výzkumu Bashira a kol. však považovali jen 27% atributů za velmi relevantní údaj [2].

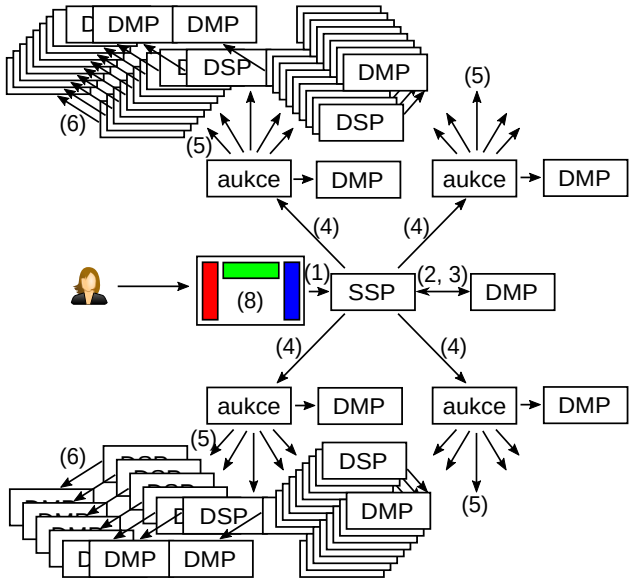
- *Retargeting:* Obvykle využívaný provozovateli e-shopů a poskytovateli placených služeb. Cílem je přesvědčit k návratu uživatele, kteří navštívili inzerentův web a neuskutečnili nákup. Inzerenti si však možná neuvědomují, že spolu s možností retargetingu dávají reklamním společnostem příležitost ke tvorbě profilů pro behaviorální reklamu. Je dobré si pečlivě zkontrolovat uzavřenou smlouvu, jestli obsahuje požadavek na reklamní společnost, aby na základě inzerentových dat nebudovala profily, ze kterých by mohla těžit konkurence. Obr. 1 ukazuje příklad komunikace návštěvníka webu České spořitelny, která instruuje prohlížeč ke kontaktování smluvních reklamních společností nazývaných také jako *data management platform* (DMP). Nasbíraná data může Česká spořitelna později využít k retargetingu.

- *Vlastní výběr osob (custom audience nebo customer match)*[2]*:* Používají obvykle obchodníci, kteří chtějí oslovit své dřívější zákazníky, např. po uvedení nového produktu na trh, při slevových akcích apod. Takový obchodník zná telefonní čísla a e-mailové adresy svých zákazníků. Tyto identifikační údaje tedy může nahrát do reklamního systému a kampaň nakonfigurovat tak, aby se reklama zobrazovala právě zákazníkům uvedeným v seznamu.

[2] https://about.ads.microsoft.com/en-gb/solutions/audience-targeting/custom-audiences,
https://www.godatafeed.com/blog/google-customer-match,
https://www.businesswire.com/news/home/20110626005114/en/ChoiceStream%C2%AE-Launches-CRUNCH%E2%84%A0-Advertising%E2%80%99s-Custom-Audience-Targeting

Status	Met...	Domain	File	Cause
200	GET	www.google.com	conversion_async.js	script
200	GET	c.imedia.cz	retargeting?id=25316&category=&itemId=&url=https://www.csas.cz/cs/osobni-finance	img
304	GET	www.google-analytics.com	analytics.js	script
200	GET	track.adform.net	/Serving/Cookie/?adfaction=getjs;adfcookname=uid	script
200	GET	googleads.g.doubleclick.net	/pagead/viewthroughconversion/980831788/?random=1579257959998&cv=9&fst=1579257959998&num=1&bg...	script
200	GET	track.adform.net	/serving/scripts/trackpoint/async/	script
200	GET	www.google-analytics.com	js?id=GTM-KZT6KWR&cid=2143872554.1579257874	script
200	GET	www.google.com	/pagead/1p-user-list/980831788/?random=1579257959998&cv=9&fst=1579255200000&num=1&bg=ffffff&guid...	img
200	GET	www.google.cz	/pagead/1p-user-list/980831788/?random=1579257959998&cv=9&fst=1579255200000&num=1&bg=ffffff&guid...	img
200	GET	track.adform.net	/Serving/TrackPoint/?pm=1369211&ADFPageName=path_/cs/osobni-finance&ADFdivider=|&ord=908967354767...	script
200	GET	googleads.g.doubleclick.net	/pagead/viewthroughconversion/980831788/?random=1579257961735&cv=9&fst=1579257961735&num=1&gu...	script

Obr. 1: Vybraná komunikace probíhající při návštěvě stránek České spořitelny. Sledující skripty a pixely.



Obr. 2: Ilustrativní schéma šíření informací v rámci RTB. Ve skutečnosti nemusí každá zapojená společnost spolupracovat s DMP nebo může spolupracovat s více DMP. Podobně každá DMP může spolupracovat s více SSP, DSP a aukčními společnostmi.
Pozn.: Šíření nabídek od DSP k aukcím a SSP (7) není zakresleno.

- *Inzerce osobám podobným mému výběru (look-alike audience nebo similar audience)*[3]*:* Nevýhodou vlastního výběru oslovených osob je, že tito zákazníci již nakoupili. Nevýhodou behaviorálního cílení je, že inzerent musí vědět, jaké atributy potenciální zákazník nejspíše má. Inzerce osobám podobným mému výběru sestaví automaticky behaviorální profil, který mají osoby uvedené na dodaném seznamu, a cílí na neuvedené osoby mající odvozené vlastnosti.

Real Time Bidding — aukce o zobrazení reklamy

Pro zajištění zobrazení reklamy za co nejlepší cenu pořádají reklamní společnosti aukce RTB. Aukce probíhá samostatně pro každé místo zobrazení reklamy na stránce, kterou uživatel navštívil. Obr. 2 ukazuje šíření informace o návštěvě stránky uživatele k předem neznámému množství společností.

1. Provozovatel stránky má uzavřenou smlouvu s jednou nebo několika společnostmi zabývajícími se prodejem reklamy (*Supply-Side Platform* – SSP).

2. Každé SSP může spolupracovat s jednou nebo několika společnostmi zabývajícími se získáváním informací o internetových uživatelích (DMP).

3. DMP identifikují uživatele pomocí skriptu vykonaného v uživatelově prohlížeči a dodají SSP informace o uživateli (typicky profil včetně retargetingových informací).

4. Každé SSP předá požadavek na zobrazení reklamy aukčním serverům, které mohou informace o uživateli dále obohatit daty svých DMP. DMP může identifikovat uživatele pomocí skriptu vykonaného v uživatelově prohlížeči.

5. Aukční servery rozešlou požadavek na nabídku v aukci (*Bid Request*) společnostem zabývajícím se vytvářením reklamních kampaní a stykem s inzerenty (*Demand Side Platform* – DSP).

6. V rámci požadavku na nabídku v aukci je uživatel identifikován identifikátorem (pseudonymem) aukčního serveru. Pro ten může mít dodatečné informace některá z DMP spolupracujících s DSP.

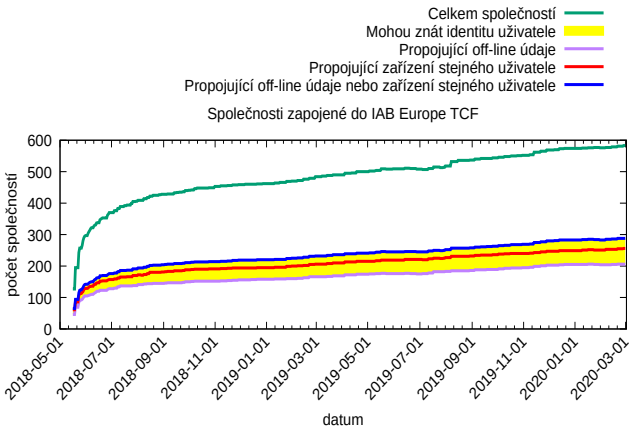
7. DSP předávají aukčnímu serveru své nabídky na zobrazení reklamy včetně ceny, kterou jsou ochotni zaplatit. Nejlepší nabídky se dostanou k SSP.

8. DSP s nejlepší nabídkou může zobrazit uživateli reklamu a také distribuovat vlastní JavaScriptový kód směrem k uživateli a může provést tzv. *Cookie Matching* (CM)[4], tedy propojení vlastního identifikátoru pro uživatele s pseudonymem používaným aukčním serverem. CM dovoluje DSP a partnerským DMP depseudonymizovat nejen všechny budoucí nabídky aukčního serveru, ale také všechny uložené dřívější nabídky týkající se tohoto uživatele.

Ne vždy jsou role DSP, DMP, SSP a aukčního serveru odděleny. Např. stejný subjekt může plnit roli DSP a SSP.

Transparency and Consent Framework

GDPR přineslo požadavek na transparentnost zpracování osobních dat. *Interactive Advertising Bureau Europe* vytvořila pro zajištění transparentnosti a získávání souhlasů se zpracováním osobních údajů *Transparency and Consent Framework* (TCF). V rámci něj reklamní společnosti oznamují své účely zpracování a právní důvod pro toto zpracování – oprávněné zájmy nebo souhlas subjektu údajů. Tento seznam je volně dostupný na Internetu[5]. V rámci analýzy TCF jsme na FIT VUT vytvořili dlouhodobé statistiky[6].



Obr. 3: Počet společností zapojených do TCF a těch v pozici zjistit skutečnou identitu uživatele

Obr. 3 ukazuje počet společností zapojených do TCF a jejich zjišťování skutečné identity uživatele (identifikátor z reálného světa). Společnosti inzerující párování offline údajů musejí k propojení online a offline dat znát identifikátory používané v reálném světě, např. zjistit uživatelovu e-mailovou adresu nebo telefonní číslo. Znalost identifikátorů z reálného světa umožňuje provádět propojování zařízení stejného uživatele, avšak není pro toto propojování nutná [1]. Proto společnosti schopné zjistit skutečnou identitu uživatele zahrnují společnosti inzerující spojování offline údajů a část společností inzerujících propojování zařízení stejného uživatele.

[3] https://support.google.com/google-ads/answer/7151628?hl=en
[4] https://developers.google.com/authorized-buyers/rtb/cookie-guide
[5] https://vendorlist.consensu.org/vendorlist.json
[6] https://www.fit.vutbr.cz/~polcak/tcf/

Analýza českého webu

Další výzkumnou otázkou je, jak moc jsou české weby zapojené do globálního reklamního systému pomocí RTB a jestli jsou o tomto předávání dat uživatelé informováni.

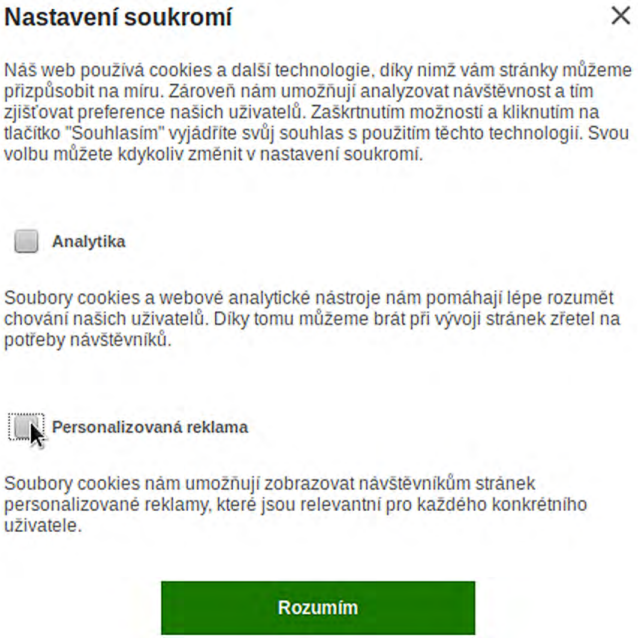
Z dat publikovaných Matte a kol. [7] vyplývá, že na českém webu není TCF běžně nasazené. Jediná zmíněná doména je livesport.cz. Při návštěvě tohoto webu jsme se pokusili nesouhlasit se zpracováním dat v rámci reklamních systémů (viz Obr. 4). Použitím nástroje *Cookie Glasses* [7] jsme však zjistili, že ve skutečnosti si stránka uložila souhlas se všemi pěti účely zpracování definovanými TCF pro 544 firem zapojených do TCF (viz Obr. 5).

Hlavní analýzu českého webu[7] jsme provedli následovně:

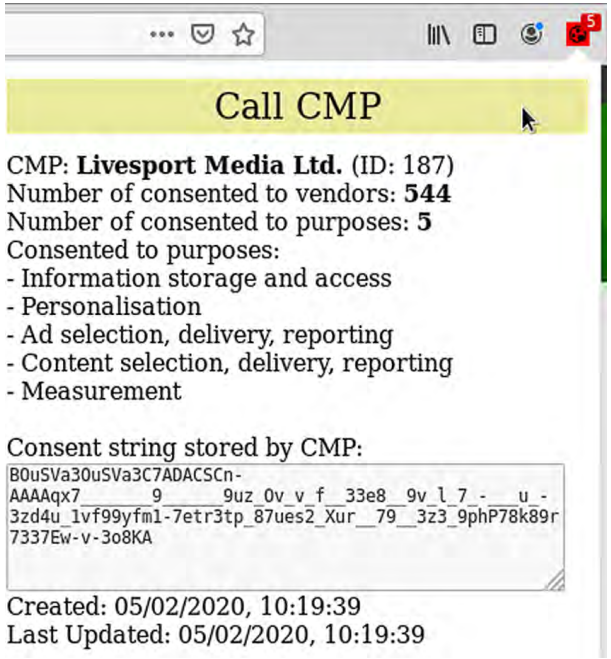
1. V datech zveřejněných 16. ledna 2020 službou netmonitor.cz jsme identifikovali 464 domén druhého řádu.

2. Z uvedených 464 domén jsme stáhli 367 souborů ads.txt[8]. Soubory ads.txt slouží nakupujícím v rámci RTB k ověření, že reklamu nakupují od subjektu, který má právo prodávat reklamní prostor na daném serveru. Umístění tohoto souboru je dobrovolné, takže se dá usuzovat, že nejméně 79 % nejnavštěvovanějších českých webů prodává svůj reklamní prostor v rámci RTB.

3. Ze stažených souborů jsme extrahovali počty stránek prodávajících na nám známých tržištích. Počty jsou uvedené v Tab. 1.[9, 10]



Obr. 4: Okno pro získání souhlasu se zpracováním osobních dat při prohlížení stránky livesport.cz. Okno může uživatel zobrazit až po načtení stránky, tedy až po komunikaci v rámci RTB.



Obr. 5: livesport.cz nerespektuje volbu uživatele a ukládá falešné souhlasy se zpracováním

Název tržiště	Počet webů	Právní základ pro výběr reklamy (TCF)
Oath/AOL (aol.com)[9]	101	Oprávněné zájmy
openx.com[9]	277	Souhlas
ibillboard.com[10]	297	Oprávněné zájmy
rubiconproject.com[9]	299	Oprávněné zájmy
indexexchange.com[9]	300	Oprávněné zájmy
appnexus.com[9]	335	Oprávněné zájmy
pubmatic.com[9]	336	Oprávněné zájmy
Doubleclick (google.com)[9]	337	Není zapojený do TCF

Tab. 1: Počet stránek předávajících osobní data jednotlivým tržištím a právní základ zpracování

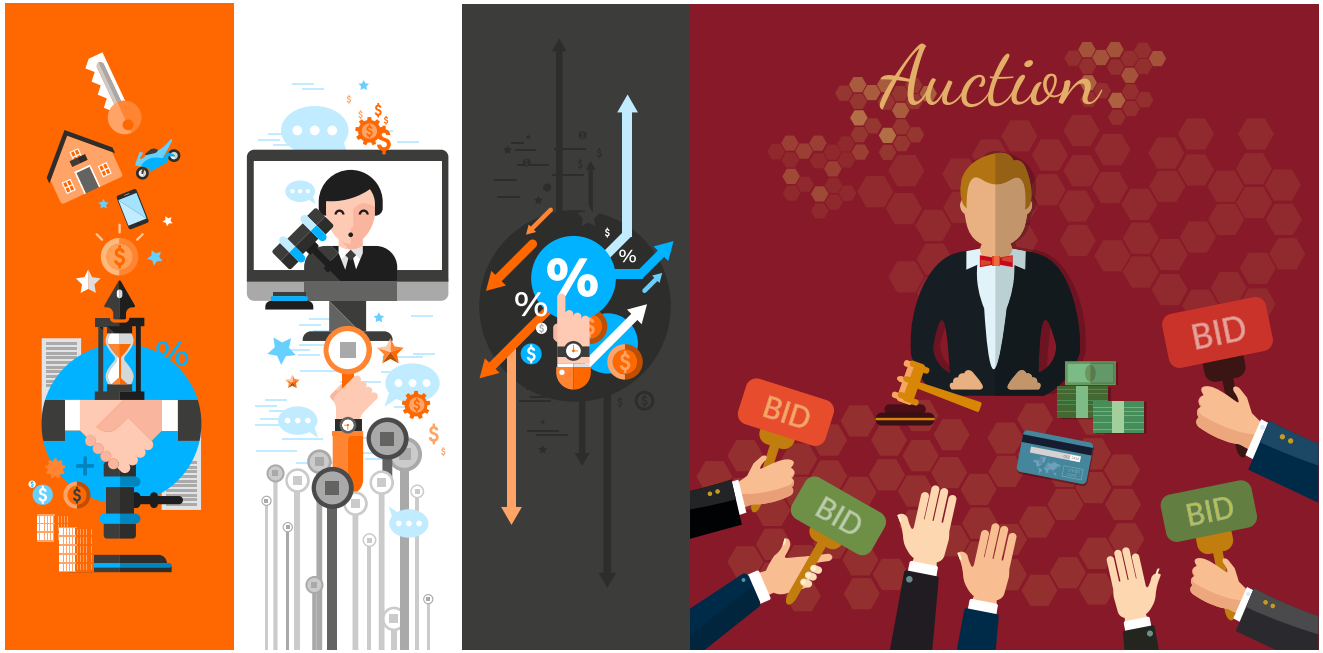
[7] Data jsou dostupná na https://www.fit.vutbr.cz/~polcak/czech_rtb.zip
[8] https://iabtechlab.com/ads-txt/
[9] https://brave.com/wp-content/uploads/2019/07/Scale-billions-of--bid-requests-per-day-RAN2019061811075588.pdf
[10] Např. https://www.slideshare.net/iBILLBOARD/future-with-ibillboard--january-2013

Po právní stránce je velkou otázkou, zda tržiště uvedená v Tab. 1 mohou předávat osobní data společnostem bez souhlasu subjektu údajů. Jsou oprávněné zájmy tržišť RTB pubmatic.com, appnexus.com, indexexchange.com, rubiconproject.com, ibillboard.com a Oath/AOL v souladu s očekáváním subjektů údajů ohledně zpracování pro účely výběru reklamy, a prošly tedy balančním testem oprávněných zájmů GDPR? Podle ICO by zpracování v rámci RTB mělo být založeno na souhlasu [6, str. 18].

Jakým způsobem se společnosti vypořádaly s přenosem citlivých dat a osobních údajů dětí? Např. společnost PubMatic ve svých podmínkách užívání služeb žádá, aby se skrze jeho služby nezasílaly citlivé osobní údaje, a dětem zakazuje užívání svých služeb. Opravdu platí, že si jsou uživatelé internetu vědomi zpracování citlivých dat [6]? Jsou uživatelé před takovýmto zpracováním varováni?

Z analyzovaných webů jsme vybrali ty, u nichž existuje předpoklad předávání citlivých údajů:

- *abctehotenstvi.cz* nezobrazuje uživateli žádné varování týkající se předávání osobních údajů, přitom využívá AppNexus a PubMatic,
- *ceskozdrave.cz* nezobrazuje uživateli žádné varování týkající se předávání osobních údajů, přitom využívá všechna tržiště z Tab. 1,
- *detsky-web.cz* nezobrazuje uživateli žádné varování týkající se předávání osobních údajů, přitom využívá všechna tržiště uvedená v Tab. 1,



- *naseporodnice.cz* nezobrazuje uživateli žádné varování týkající se předávání osobních údajů, přitom využívá všechna tržiště z Tab. 1 kromě Oath/AOL,
- *seznamka.cz* získává souhlas setrváním na stránkách, přitom využívá Google Doubleclick,
- *vitalia.cz* nezobrazuje uživateli žádné varování týkající se předávání osobních údajů, přitom využívá všechna tržiště z Tab. 1 kromě Oath/AOL,
- *ulekare.cz* získává souhlas setrváním na stránkách, zobrazená lišta obsahuje souhlasné tlačítko, ale data se do RTB dostávají i bez kliknutí na toto tlačítko. Web využívá všechna tržiště uvedená v Tab. 1,

- *zdrave.cz* získává souhlas setrváním na stránkách, zobrazená lišta obsahuje tlačítko rozumím, ale data se do RTB dostávají i bez kliknutí na toto tlačítko. Web využívá všechna tržiště z Tab. 1 kromě Oath/AOL,

- *zdraveomlazeni.cz* získává souhlas setrváním na stránkách, zobrazená lišta obsahuje tlačítko v pořádku, ale data se do RTB dostávají i bez kliknutí na toto tlačítko. Web využívá všechna tržiště z Tab. 1 kromě Oath/AOL.

K výše uvedenému seznamu stránek je potřeba poznamenat, že získání souhlasu setrváním na stránkách neumožňuje vyjádřit souhlas svobodný (není jasné, jak vyjádřit nesouhlas), konkrétní ke specifickému zpracování či správci dat, ani jednoznačný (GDPR, čl. 4, odst. 11). Souhlas se zpracováním zvláštních kategorií osobních údajů má být výslovný (GDPR, čl. 9).

Závěr

Jak ukazuje analýza českých webů a společností zapojených do TCF, v celé řadě případů dochází ke zpracování osobních údajů, včetně citlivých, bez udělení odpovídajících souhlasů. To vzbuzuje otázku, zda opravdu platí, že je zajištěná vysoká úroveň ochrany osobních údajů, kterou zmiňuje nařízení GDPR. Pochyby přidávají i četné stížnosti podané k dohledovým úřadům zmíněné v úvodu článku. Z celoevropského pohledu je zajímavá studie nasazení TCF [7], která reportovala celou řadu pochybení v získávání souhlasů.

Závěrem je potřeba upozornit, že souhlasy s personalizací reklamy a dalšími účely zpracování je možné získávat i nerušivými prostředky [11] jako distribucí rozšíření prohlížečů, které budou uživatele transparentně informovat o účelech zpracování. Na stránky lze také vhodně umístit tlačítka, která v případě zájmů otevřou dialog pro udělení informovaných souhlasů se zpracováním.

Poděkování
Tento příspěvek vznikl za podpory projektu VI20172020062 financovaného Ministerstvem vnitra ČR.

Libor Polčák
polcak@fit.vutbr.cz

Ing. Libor Polčák, Ph.D.

Působí na Fakultě informačních technologií Vysokého učení technického v Brně, kde také vystudoval. V rámci výzkumné skupiny počítačových sítí se dlouhodobě zabývá bezpečnostním výzkumem.

POUŽITÉ ZDROJE

[1] Adbrain: Demystifying Cross-Device. 2015. URL https://www.iabuk.com/sites/default/files/public_files/Adbrain_Demystifying_Cross_Device.pdf
[2] BASHIR, M. A.; FAROOQ, U.; SHAHID, M.; aj.: Quantity vs. Quality: Evaluating User Interest Profiles Using Ad Preference Managers. In Network and Distributed Systems Security (NDSS) Symposium 2019, 2019, ISBN 1-891562-55-X.
[3] BASHIR, M. A.; WILSON, C.: Diffusion of User Tracking Data in the Online Advertising Ecosystem. Proceedings on Privacy Enhancing Technologies, ročník 2018, č. 4, 2018: s. 85–103, ISSN 2299-0984.
[4] CNIL – Commission Nationale de l'Informatique et des Libertés: APPLICATIONS MOBILES: clôture de la mise en demeure à l'encontre de la société VECTAURY. 2019. URL https://www.cnil.fr/fr/applications-mobiles-cloture-de-la-mise-en-demeure-lencontre-de-la-societe-vectaury
[5] IAB Tech Lab: AdCOM Specification v1.0. 2018. URL https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM
[6] ICO – Information Commissioner's Office: Update report into adtech and real time bidding. 2019. URL https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf
[7] MATTE, C.; BIELOVA, N.; SANTOS, C.: Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. 2019. URL https://arxiv.org/abs/1911.09964v1
[8] RYAN, J.: Behavioural advertising and personal data. 2018. URL https://brave.com/wp-content/uploads/2018/09/Behavioural-advertising-and-personal-data.pdf
[9] Soudní dvůr Evropské unie: Rozsudek Soudního dvora (velkého senátu), věc C 210/16. 2018.
[10] SPEICHER, T.; Ali, M.; Venkatadri, G.; aj.: Potential for Discrimination in Online Targeted Advertising. In FAT 2018 – Conference on Fairness, Accountability, and Transparency, ročník 81, New-York, United States, 2018, s. 1–15.
[11] WP29 – Article 29 Data Protection Working Party: Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising. 2011, WP188, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf.
[12] YUAN, Y.; WANG, F.; LI, J.; aj.: A survey on real time bidding advertising. In Proceedings of 2014 IEEE International Conference on Service Operations and Logistics, and Informatics, 2014, s. 418–423.

Povinnost Data Retention v judikatuře Soudního dvora EU a Ústavního soudu ČR

Povinnost uchovávat provozní a lokalizační údaje již počtvrté přezkoumává Soudní dvůr EU. Na základě žádostí francouzského, britského a belgického soudu posuzuje, zda vnitrostátní právní úprava, která ukládá povinnost plošného uchování údajů všech účastníků, je v rozporu s unijním právem. Generální advokát Soudního dvora v těchto třech věcech přednesl své stanovisko 15. ledna 2020. Autor popisuje vývoj povinnosti Data Retention a zkoumá hlavní body aktuálního případu posuzovaného Soudním dvorem EU, včetně potenciálního vlivu rozsudku v této věci na aktuální úpravu Data Retention v právním řádu ČR.

Data Retention elektronické komunikace provozní a lokalizační údaje
Soudní dvůr EU Ústavní soud ČR

Povinnost uchovávat provozní a lokalizační údaje

V rámci povinnosti Data Retention uchovávají poskytovatelé služeb a provozovatelé sítí elektronických komunikací rozsáhlé kategorie provozních a lokalizačních údajů účastníků a uživatelů pro účely jejich možného vyžádání oprávněnými orgány. Povinnost má svůj základ v již neplatné Data Retention Směrnici[1] (dále jen „Směrnice“) a v národních právních úpravách členských států EU přijatých k jejímu provedení. Národní úpravy vymezují kategorie údajů, dobu jejich uchovávání, oprávněné orgány a další podrobnosti. V právním řádu ČR je povinnost Data Retention zakotvena v zákoně č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů (dále jen „ZoEK“), a v navazující úpravě zákona č. 141/1961 Sb. o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů (dále jen „Trestní řád“).

Povinnost Data Retention vzbuzovala od počátku značné kontroverze. Pracovní skupina WP 29[2], složená ze zástupců národních orgánů dozoru nad ochranou osobních údajů členských států EU a zástupců Evropské komise, vyslovila již před přijetím Směrnice v několika kritických hodnoceních a stanoviscích pochyby o odůvodněnosti povinného

[1] Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES; směrnice je často zkráceně označována jako Data Retention Směrnice.

[2] Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováváním osobních údajů zřízená na základě článku 29 směrnice 95/46/ES, tzv. Article 29 Working Party – Pracovní skupina podle článku 29, nejčastěji označována jako Pracovní skupina WP 29 či jen WP 29., k Data Retention se vyjadřovala především ve stanoviscích Opinion 10/2001 on the need for a balanced approach in the fight against terrorism (adopted on 14 December 2001), Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21. 09. 2005) a Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the Retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

všeobecného uchovávání údajů. WP 29 varovala před snahou označovat ochranu osobních údajů za překážku účinného boje proti terorismu, opatření v rámci boje proti terorismu by dle WP 29 neměla snižovat standardy ochrany základních lidských práv, upozorňovala také na alternativní přístupy, nesrovnatelně šetrnější vůči soukromí, např. tzv. quick-freeze procedura[3].

Navzdory tomu byla Směrnice přijata[4], a to nikoli jako prostředek boje proti terorismu či závažné trestné činnosti, nýbrž jako *„opatření ke sbližování ustanovení právních a správních předpisů členských států, jejichž účelem je vytvoření a fungování vnitřního trhu“*[5]. Některé členské státy EU (vč. České republiky[6]) totiž již dříve ve svých právních řádech uložily obdobnou povinnost. Evropská komise vyhodnotila právní a technické odlišnosti mezi těmito předpisy (odlišné požadavky na druhy uchovávaných údajů, lhůty a další) jako překážku na vnitřním trhu elektronických komunikací. Směrnice uložila členským státům EU povinnost přijmout do 15. září 2007 národní úpravu ukládající poskytovatelům služeb elektronických komunikací povinnost uchovávat veškeré provozní a lokalizační údaje všech účastníků a uživatelů po dobu min. 6 a max. 24 měsíců.

Dosavadní judikatura Soudního dvora EU

Po přijetí Směrnice a odpovídajících národních právních úprav v jednotlivých členských státech byla tato povinnost, resp. právní úpravy, v nichž byla obsažena, předmětem řady rozhodnutí soudů členských států EU včetně Ústavního soudu ČR i Soudního dvora EU, který se touto povinností zabýval dosud celkem třikrát.

Irsko podporované Slovenskou republikou se již 6. července 2006 žalobou u Soudního dvora domáhalo zrušení Směrnice kvůli jejímu nesprávnému přijetí jako *„opatření k odstranění překážek na vnitřním trhu EU“*, přestože ve skutečnosti má usnadnit vyšetřování trestných činů, zejména v souvislosti s hrozbou terorismu. Dle argumentace Slovenské republiky navíc uchovávání údajů dle Směrnice významně zasahuje do práva jednotlivců na respektování soukromého života, takovýto zásah proto nemůže být odůvodněn odstraněním překážek na vnitřním trhu. Soudní dvůr EU žalobu zamítl[7] s tím, že Směrnice byla přijata na náležitém právním základě, jelikož *„rozdíly mezi jednotlivými vnitrostátními právními předpisy přijatými v oblasti uchovávání údajů... mohly mít přímý dopad na fungování vnitřního trhu a... bylo možné očekávat, že se tento dopad bude zhoršovat“*.

Podruhé Soudní dvůr EU posuzoval Směrnici k žádostem irského High Court (věc C-293/12) a rakouského Verfassungsgerichtshof (věc C-594/12) o rozhodnutí o předběžné otázce podaným v roce 2012; v řízení se zaměřil primárně na slučitelnost Směrnice s Listinou základních práv EU, především s právem na respektování soukromého života a právem na ochranu osobních údajů. Rozsudkem z 8. dubna 2014 Soudní dvůr EU prohlásil Směrnici za neplatnou[8]. Úprava totiž dle závěrů Soudního dvora umožňovala *„vyvodit velmi přesné závěry o soukromém životě osob, jejichž údaje byly uchovány, tedy o každodenních zvyklostech, o místech, kde trvale či přechodně pobývají, o denních či jiných přesunech, o jejich aktivitách, společenských vztazích těchto osob a o společenských kruzích, s kterými se stýkají“*. Směrnice se navíc *„vztahuje na všechny účastníky a registrované uživatele“* a *„představuje tedy zásah do základních práv téměř celé evropské populace“*, přitom *„nestanoví jasná a přesná pravidla pro rozsah zásahu do základních práv zakotvených v článcích 7 a 8 Listiny“*, a nelze tak zaručit, že je tento zásah omezen na nezbytné minimum.

Prohlášení Směrnice za neplatnou však nemělo právní ani faktický dopad na národní právní úpravy přijaté do té doby v jednotlivých členských státech EU k transpozici povinností ze Směrnice. V pořadí třetí případ, v němž se Soudní dvůr EU zabýval povinností Data Retention, iniciovaly dvě žádosti o rozhodnutí o předběžné otázce podané v roce 2015 Odvolacím správním soudem ve Stockholmu (věc C-203/15[9]) a Odvolacím soudem pro Anglii a Wales (věc C-698/15[10]) a týkající se švédské a britské právní úpravy Data Retention. Jelikož Směrnice byla již v té době neplatná, posuzoval Soudní dvůr soulad povinnosti uchovávat provozní a lokalizační údaje s ustanovením

[3] Definice obsažená v Memorandu Evropské komise European Commision. Memo Frequently Asked Qestions: The Data Retention Questions, datovaném 8. dubna 2014 vymezuje „Data retention quick freeze“ jako uchovávání provozních a lokalizačních údajů pouze ve vztahu ke konkrétní osobě, od okamžiku vzniku konkrétního podezření vůči této osobě.

[4] Na zasedání Rady EU dne 21. února 2006 hlasovaly proti přijetí pouze delegace Slovenska a Irska (viz Press Release, 2709th Council Meeting, Justice and Home Affairs), 15. března 2006 Směrnici schválil Evropský parlament.

[5] Takovéto opatření vymezuje článek 95 Smlouvy o založení Evropského společenství.

[6] Zákon č. 127/2005 Sb. o elektronických komunikacích účinný od 1. května 2005 zakotvil v § 97 odst. 3 základ povinnosti Data Retention.

[7] Rozhodnutí Soudního dvora EU C-301/06 Ireland v European Parliament and Council ze dne 10. února 2009

[8] Rozsudek soudního dvora EU (velkého senátu) z 8. dubna 2014 ve spojených věcech C-293/12 a C 594/12

[9] Žádost o rozhodnutí o předběžné otázce podané Kammarrätten i Stockholm (Švédsko) dne 4. května 2015 ve věci sporu mezi společností Tele2 Sverige AB a švédským sektorovým regulačním úřadem pro pošty a telekomunikace Post- och telestyrelsen.

[10] Žádost o rozhodnutí o předběžné otázce podaná Court of Appeal (England & Wales) (Civil Division) – občanskoprávním úsekem odvolacího soudu (pro Anglii a Wales) v kauze sporu mezi Secretary of State for the Home Department proti Tomu Watsonovi, Peteru Briceovi, Geoffreymu Lewisovi za účasti Open Rights Group, Privacy International, Law Society of England and Wales, vedená Soudním dvorem EU jako věc C-698/15.

čl. 15 odst. 1 ePrivacy směrnice[11] s ohledem na Listinu základních práv EU a zabýval se též otázkou, zda předchozí rozsudek Soudního dvora stanoví závazné požadavky unijního práva pro vnitrostátní režim přístupu k uchovávaným údajům.

V rozsudku z 21. prosince 2016[12] Soudní dvůr konstatoval, že článek 15 odst. 1 ePrivacy směrnice ve spojení s články 7, 8, 11 a čl. 52 odst. 1 Listiny základních práv EU, *„musí být vykládán v tom smyslu, že brání vnitrostátní právní úpravě, která za účelem boje proti trestné činnosti stanoví plošné a nerozlišující uchovávání veškerých provozních a lokalizačních údajů všech účastníků a registrovaných uživatelů, které se vztahují na veškeré prostředky elektronické komunikace"* a také brání vnitrostátní právní úpravě, která neomezuje přístup příslušných orgánů k uchovávaným údajům výlučně pro účely boje proti závažné trestné činnosti, která nepodmiňuje tento přístup předchozím přezkumem ze strany soudu nebo nezávislého správního orgánu a která nevyžaduje, aby tyto údaje byly uchovávány na území EU. Soudní dvůr se v odůvodnění rozsudku odvolal na své závěry vyslovené v předchozím rozsudku, kterým prohlásil Směrnici za neplatnou, a tyto závěry dále rozvinul[13].

Povinnost Data Retention v právním řádu ČR

Povinnost provozovatelů sítí a poskytovatelů služeb elektronických komunikací plošně uchovávat provozní a lokalizační údaje veškerých účastníků či uživatelů zakotvil ZoEK s účinností od 22. února 2005. V některých podstatných otázkách, včetně rozsahu provozních a lokalizačních údajů, ZoEK odkázal na prováděcí právní předpis[14], kterým byla až s účinností od 15. prosince 2005 vyhláška č. 485/2005 Sb.[15] Ta stanovila dobu uchovávání údajů na 6 měsíců, resp. 3 měsíce pro některé údaje datové komunikace. Novela ZoEK provedená zákonem č. 247/2008 Sb. do právního řádu ČR transponovala Směrnici a dosavadní právní úpravu doplnila. Na úpravu Data Retention v ZoEK navazovala úprava obsažená v Trestním řádu[16].

Tuto právní úpravu celkem třikrát posuzoval Ústavní soud ČR. Nálezem sp. zn. Pl. ÚS 24/10 ze 22. března 2011 rozhodl o zrušení právní úpravy Data Retention obsažené v ZoEK a v prováděcí vyhlášce č. 485/2005 Sb., a to ke dni vyhlášení nálezu ve Sbírce zákonů, tedy k 12. dubnu 2011. Následně nálezem sp. zn. Pl. ÚS 24/11 Ústavní soud ČR s účinností od 30. září 2012 zrušil také ustanovení § 88a Trestního řádu.

Ústavní soud ČR se v obou nálezech zabýval především právem na respekt k soukromému životu a právem na informační sebeurčení, vycházel přitom ze své ustálené rozhodovací praxe i z četných judikátů Evropského soudu pro lidská práva[17], včetně judikatury týkající se užití odposlechů telekomunikačního provozu[18]. Ústavní soud ČR totiž konstatoval značnou podobnost mezi odposlechem telekomunikačního provozu a uchováváním a vyžádáním provozních a lokalizačních údajů z hlediska zásahu do soukromí. Hlavním důvodem pro zrušení právní úpravy Data Retention bylo pro Ústavní soud ČR zejména vágní a neurčité vymezení orgánů oprávněných k vyžádání uchovávaných údajů, ne zcela jasně a přesně vymezený účel poskytování těchto údajů oprávněným orgánům a také nedostatečné požadavky na jejich zabezpečení. Jelikož povinnost dle Směrnice v té době přetrvávala, zákonodárce do právního řádu ČR opět zavedl povinnost Data Retention zákonem č. 273/2012 Sb.[19], kterým s účinností od 1. října 2012 novelizoval ZoEK i Trestní řád. Tato novelizace respektovala většinu výtek Ústavního soudu ČR obsažených v obou výše uváděných nálezech.

Skupina 58 poslanců Poslanecké sněmovny PČR se 20. prosince 2017 obrátila na Ústavní soud ČR s návrhem na zrušení ustanovení upravujících povinnost Data Retention v ZoEK, v Trestním řádu a v zákoně o Policii ČR[20] spolu

[11] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).
[12] Rozsudek Soudního dvora EU (velkého senátu) ze dne 21. prosince 2016. Tele2 Sverige AB a Secretary of State for the Home Department v. Post- och telestyrelsen a další, Žádosti o rozhodnutí o předběžné otázce Podané Kammarrätten i Stockholm a Court of Appeal (England & Wales) (Civil Division) ve spojených věcech C-203/15 a C-698/15.
[13] Podrobně viz např. UŘIČAŘ, M. Data Retention v právním řádu ČR po rozsudcích Soudního dvora EU. In: PORADA, Viktor a Eduard BRUNA (eds.) Bezpečná Evropa 2018. Sborník sdělení z IX. ročníku mezinárodní vědecké konference. Praha: VŠFS, 2019, 546 s. ISBN 978-80-7408-185-9.
[14] Zákon o elektronických komunikacích v § 97 odst. 3 stanovil, že *„rozsah provozních a lokalizačních údajů, dobu jejich uchovávání, která nesmí být delší než 12 měsíců, a formu a způsob jejich předávání orgánům oprávněným k jejich využívání, stanoví prováděcí právní předpis"*.
[15] Vyhláška Ministerstva informatiky č. 485/2005 Sb. o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání.
[16] Trestní řád v § 88a vymezil způsob, kterým bylo možno *„zjistit údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat"*.
[17] Např. rozhodnutí Evropského soudu pro lidská práva č. 8691/79 ze dne 2. srpna 1984 ve věci Malone proti Spojenému království, rozhodnutí č. 5029/71 ze dne 6.září 1978 ve věci Klaas a další proti Německu, rozhodnutí č. 9248/81 ze dne 26. března 1987 ve věci Leander proti Švédsku, rozhodnutí č. 11801/85 ze dne 24. dubna 1990 ve věci Kruslin proti Francii, rozhodnutí č. 44787/98 ze dne 25. září 2001 ve věci P.G. a J.H. proti UK, rozhodnutí č. 28341/95 ze dne 4. května 2000 ve věci Rotaru proti Rumunsku.
[18] Nálezy Ústavního soudu ČR sp. zn. II. ÚS 502/2000, sp. zn. IV. ÚS 78/01, sp. zn. I. ÚS 191/05, či sp. zn. I. ÚS 3038/07 (N 46/48 SbNU 549).
[19] Zákon č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích, a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony.
[20] Zákon č. 273/2008 Sb. o Policii ČR, ve znění pozdějších předpisů.

s prováděcí vyhláškou k ZoEK[21]. Dle navrhovatelů napadená úprava neústavně zasahuje do práva na soukromí zaručeného čl. 7 odst. 1 Listiny základních práv a svobod (dále jen „Listina"), práva na ochranu před neoprávněným zasahováním do soukromého a rodinného života podle čl. 10 odst. 2 Listiny, práva na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě podle čl. 10 odst. 3 Listiny a práva na zachování tajemství zpráv podávaných telefonem či jiným podobným zařízením podle čl. 13 Listiny.

Napadená úprava navíc dle navrhovatelů není způsobilá naplnit legitimní cíl – snížení trestné činnosti a zvýšení její objasněnosti. Z dostupných statistik kriminality policie za období 2011–2013 totiž vyplývá, že možnost použití provozních a lokalizačních údajů nemá vliv na četnost trestné činnosti ani na její objasněnost, což dokládají i zahraniční studie. Sledování provozních a lokalizačních údajů je také možno jednoduše obejít pomocí různých nástrojů, např. použitím anonymní předplacené SIM karty, čehož si jsou dobře vědomi právě pachatelé závažné trestné činnosti. Výsledkem je sledování komunikace celé společnosti, která se trestné činnosti nedopouští, na ochranu před pachateli, kteří dobře vědí, jak se sledování technicky vyhnout – opatření je v rámci testu proporcionality nevhodné k naplnění legitimního cíle. Navíc je zřejmé, že tyto údaje jsou nadužívány, neboť nejsou vyžadovány jen k objasnění zvlášť závažného zločinu, ale často slouží jako důkaz v běžných trestních řízeních.

Ústavní soud ČR nálezem ze 14. května 2019[22] návrh zamítl a napadenou právní úpravu ponechal beze změny[23]. Ve stručném odůvodnění dovodil, že *„se napadená právní úprava nevymyká evropskému standardu"* a lze ji aplikovat ústavně konformním způsobem tak, aby byla maximálně šetřena práva jednotlivců garantovaná Listinou základních práv a svobod.

Zajímavé srovnání nabízí v tomto směru již dřívější rozhodnutí Ústavního soudu Slovenské republiky, který k návrhu 31 poslanců Národní rady Slovenské republiky z 10. října 2012 pozastavil účinnost národní právní úpravy přijaté k provedení Směrnice[24] a následně nálezem z 29. dubna 2015 příslušná ustanovení slovenských zákonů zrušil[25]. V odůvodnění nálezu konstatoval, že *„napadená ustanovení... nevyžadují žádnou souvislost mezi údaji, jejichž uchovávání stanoví, a hrozbou pro veřejnou bezpečnost"*, navíc se uchovávání *„neomezuje ani na údaje z určitého časového období a/nebo z určité zeměpisné oblasti či na okruh osob, které by jakýmkoli způsobem bylo možno spojovat se závažnými trestnými činy, ani na osoby, jejichž uchovávané údaje by z jiných důvodů mohly přispět k předcházení, odhalování nebo stíhání trestných činů"*, a dodal, že *„cíle sledovaného napadenou právní úpravou... je možno dosáhnout i jinými prostředky, které představují méně intenzivní zásah do práva na soukromí, nežli je nástroj v podobě plošného a preventivního uchovávání předmětných údajů"*, jako např. tzv. data freezing.

[21] Vyhláška č. 357/2012 Sb. ze dne 17. října 2012 o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.
[22] Nález Ústavního soudu ČR sp. zn. PL. ÚS 45/17 ze 14. května 2019.
[23] Ústavní soudkyně Kateřina Šimáčková zaujala k výroku i k odůvodnění nálezu odlišné stanovisko, dle kterého napadená právní úprava z ústavněprávního pohledu neobstojí z důvodů, které ve svém stanovisku rozvíjí. Poukazuje také na odlišné úpravy v jiných evropských zemích, které přesto „plní kýžený cíl s obdobnou efektivitou".
[24] Usnesení Ústavního soudu SR sp. zn. PL. ÚS 10/2014 ze 23. dubna 2014.
[25] Nález Ústavního soudu SR sp. zn. PL. ÚS 10/2014 ze 29. dubna 2015.

Vláda Slovenské republiky v reakci na to připravila novelu příslušných právních předpisů, která s účinností od 1. ledna 2016 namísto plošného preventivního uchovávání provozních a lokalizačních údajů zavedla dvojí režim zahrnující jednak povinnost povinného subjektu předat oprávněným orgánům k jejich žádosti provozní a lokalizační údaje, avšak pouze takové, které má povinný subjekt z jiných, zákonem uznaných, důvodů (typicky pro účely vyúčtování ceny služeb účastníkovi, pro následné vymáhání její úhrady apod.) k dispozici, tedy aniž by tyto údaje povinný subjekt uchovával pouze pro potřeby jejich možného následného vyžádání oprávněnými orgány, a vedle toho též tzv. data freezing, tedy povinnost povinného subjektu uchovávat do budoucna po stanovenou dobu údaje pouze u konkrétní, v žádosti oprávněného orgánu označené osoby.

Ve shodě s výše zmiňovaným odlišným stanoviskem soudkyně Kateřiny Šimáčkové považuje autor v této souvislosti za velmi překvapivé, že se Ústavní soud ČR ve svém posledním nálezu prakticky vůbec nevypořádal s existencí odlišných právních úprav v jiných členských státech EU. Zejména slovenská úprava představuje bezesporu šetrnější zásah do práva na ochranu soukromí, přitom je na Slovensku účinná již několik let, a lze tedy posoudit, nakolik je ve vztahu ke sledovanému účelu – boji proti závažné trestné činnosti a terorismu – efektivní, navíc v zemi, která je České republice blízká nejen kulturně a geograficky, ale velmi pravděpodobně vykazuje také srovnatelnou míru kriminality. Též v Německu byla již na konci roku 2015 přijata nová úprava Data Retention[26] zakotvující velmi krátkou dobu uchovávání údajů, rozlišenou navíc podle typu údajů – 10 týdnů pro vymezené kategorie provozních údajů a pouze 4 týdny pro lokalizační údaje.

Aktuální přezkum francouzské, britské a belgické právní úpravy Soudním dvorem EU a jeho možný vliv na právní úpravu ČR

Soudní dvůr EU se aktuálně již počtvrté zabývá povinností Data Retention k žádostem francouzského (ve spojených věcech C-511/18 a C-512/18), britského (ve věci C-623/17) a belgického soudu (ve věci C-520/18). Na jejich základě posuzuje, zda vnitrostátní právní úprava může ukládat povinnost plošného uchování provozních a lokalizačních údajů všech účastníků, aniž by byla v rozporu s unijním právem. Generální advokát Soudního dvora Manuel Campos Sánchez-Bordony v těchto věcech přednesl své stanovisko 15. ledna 2020.

Posuzované národní právní úpravy dle generálního advokáta zakládají povinnost plošného a nerozlišujícího uchovávání údajů a představují tak rozsáhlý a zvlášť závažný zásah do základních práv zakotvených v článcích 7 a 8 Listiny. V návaznosti na tento dílčí závěr poté, vycházeje mj. i z dosavadní rozhodovací praxe Soudního dvora v otázkách Data Retention, generální advokát upozorňuje, že se *„právní úprava dotčená v projednávaných věcech vztahuje obecně na všechny účastníky a registrované uživatele a týká se všech prostředků elektronické komunikace a veškerých provozních údajů, [přičemž] neupravuje žádné rozlišení, omezení nebo výjimky činěné v závislosti na sledovaném cíli“* a vztahuje se *„i na osoby, v jejichž případě neexistuje důvod se domnívat, že by jejich chování mohlo, byť nepřímo nebo vzdáleně, souviset se závažnou trestnou činností“*.

Napadené právní úpravy navíc dle hodnocení generálního advokáta nevyžadují *„souvislost mezi údaji, jejichž uchovávání je stanoveno, a ohrožením veřejné bezpečnosti“* a neomezují se *„na uchovávání údajů vztahujících se buď k určitému časovému období či určité zeměpisné oblasti či okruhu určitých osob, které mohou být jakýmkoli způsobem zapojeny do závažné trestné činnosti, anebo k osobám, které by prostřednictvím uchovávání jejich údajů mohly z jiných důvodů přispívat k boji proti trestné činnosti“*. Campos Sánchez-Bordona poté analyzuje otázku, zda lze dosavadní *„judikaturu Soudního dvora v oblasti uchovávání osobních údajů ne-li změnit, tak alespoň zmírnit, když účelem tohoto ‚plošného a nerozlišujícího‘ uchovávání je boj proti terorismu“*, přičemž dospívá k závěru, že Soudní dvůr při formulaci své dosavadní judikatury v oblasti Data Retention neuvažoval o tom, že by boj proti terorismu *„mohl někdy vyžadovat změnu jeho judikatury“*.

Na základě těchto úvah pak generální advokát navrhuje, aby Soudní dvůr na hlavní položenou předběžnou otázku odpověděl tak, že ePrivacy směrnice ve spojení s Listinou základních práv EU musí být vykládána v tom smyslu, že *„brání takové vnitrostátní právní úpravě, která v kontextu vážného a trvajícího ohrožení národní bezpečnosti, a zejména rizika terorismu ukládá provozovatelům a poskytovatelům služeb elektronických komunikací povinnost plošně a nerozlišujícím způsobem uchovávat provozní a lokalizační údaje všech účastníků, jakož i údaje umožňující zjistit totožnost tvůrců obsahu nabízeného poskytovateli uvedených služeb“*. Dle závěrů generálního advokáta musejí být prostředky a metody boje proti terorismu kompatibilní s požadavky právního státu, což platí i v situaci hrozby pro národní bezpečnost, zvláště hrozby terorismu, jaká existuje u posuzované francouzské úpravy. Závěrečné návrhy generálního advokáta se týkají všech tří posuzovaných národních úprav – francouzské, belgické i britské. Tyto úpravy dle hodnocení generálního advokáta překračují *„meze toho, co je naprosto*

[26] Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (VerkDSpG k.a.Abk.) vom 10. Dezember 2015.

nezbytné“ a nelze je v demokratické společnosti považovat za odůvodněné. Generální advokát s odkazem na požadavky efektivního boje proti terorismu uzavírá, že pokud by se právní stát *„oddal bez dalšího pouhé efektivitě, ztratil by svou charakteristickou vlastnost a sám by se v krajních případech mohl stát hrozbou pro občana“*.

Soudní dvůr zpravidla rozhoduje v horizontu několika měsíců po stanovisku generálního advokáta; k datu dokončení tohoto textu Soudní dvůr nerozhodl ani neoznámil plánovaný termín rozhodnutí. Rozsudky Soudního dvora EU se obvykle opírají o závěry ve stanovisku generálního advokáta, nejedná se však o pevné pravidlo a Soudní dvůr se od návrhů generálního advokáta může odchýlit. Nelze tedy předvídat, jak Soudní dvůr rozhodne v této věci, navíc většina členských států EU, které předložily v posuzovaných věcech svá vyjádření[27], žádá Soudní dvůr, aby přehodnotil některé aspekty své dosavadní judikatury v této oblasti, vůči kterým mají výhrady.

I v případě, že Soudní dvůr rozhodne dle výše popsaných návrhů generálního advokáta, tedy tak, že unijní právo brání takové vnitrostátní právní úpravě, která ukládá povinnost plošně a nerozlišujícím způsobem uchovávat provozní a lokalizační údaje všech účastníků, nebude mít takové rozhodnutí bezprostřední dopad na právní úpravu Data Retention platnou v ČR, která je právě na principu plošného uchovávání údajů všech účastníků založena. S ohledem na nedávný nález Ústavního soudu ČR z roku 2019 uváděný výše nelze také patrně očekávat, že by Ústavní soud ČR zásadně změnil svůj názor, pokud by měl posuzovat nový návrh na zrušení povinnosti Data Retention. Změna v právním řádu ČR by tedy mohla vyplynout pouze z rozhodnutí, v němž by Soudní dvůr posuzoval českou právní úpravu Data Retention, která je založena na principu plošného shromažďování údajů všech účastníků. Autorovi však není známo, že by kterýkoli soud v ČR zamýšlel obrátit se na Soudní dvůr s podobnou žádostí o rozhodnutí o předběžné otázce, a úvahy na toto téma by tedy byly pouhou spekulací.

Shrnutí

Povinnost uchovávat provozní a lokalizační údaje (Data Retention) byla od svého přijetí kritizována kvůli zásahům do práva na soukromí. Povinnost Data Retention již byla předmětem tří rozhodnutí Soudního dvora EU a tří rozhodnutí Ústavního soudu ČR, nejvýznamnějším z nich byl rozsudek Soudního dvora EU o prohlášení Data Retention Směrnice za neplatnou. V probíhající věci francouzský, belgický a britský soud požádaly Soudní dvůr EU, aby posoudil, zda jsou jejich národní povinnosti Data Retention v souladu s unijním právem. Generální advokát Soudního dvora přednesl své stanovisko v těchto věcech 15. ledna 2020. Podle jeho názoru musejí být prostředky a metody boje proti terorismu v souladu s požadavky právního státu. Proto konstatuje, že ePrivacy směrnice brání takové právní úpravě, která ukládá povinnost plošně a nerozlišujícím způsobem uchovávat provozní a lokalizační údaje všech účastníků, jako je tomu u francouzské, belgické a britské právní úpravy. Rozhodnutí Soudního dvora může být očekáváno v nadcházejících měsících.

Miroslav Uřičař
miroslav.uricar@legalite.cz

[27] Ve spojených věcech C-511/18 a C-512/18, v nichž Soudní dvůr posuzuje žádost francouzského soudu, předložily svá vyjádření belgická, česká, dánská, německá, estonská, irská, španělská, francouzská, kyperská, maďarská, polská a švédská vláda a vláda Spojeného království.

JUDr. Miroslav Uřičař

Působí v LEGALITÉ advokátní kancelář, s. r. o. a jako jednatel LEGALITÉ Data Protection Services s.r.o. Je mj. členem Komise pro veřejné právo I – komise pro správní právo č. 1 Legislativní rady vlády ČR, členem Rozkladové komise a rozhodcem Rozhodčího soudu při HK ČR a AK ČR a Mezinárodního rozhodčího soudu při Českomoravské komoditní burze. V letech 1999–2016 působil v manažerských pozicích u jednoho z největších poskytovatelů služeb elektronických komunikací, od roku 2004 jako ředitel útvaru práva, regulace, bezpečnosti a vnějších vztahů.

Průzkum stavu digitalizace

Z pojmů Digitalizace a Digitální transformace se postupně stává klišé, případně si pod nimi každý představuje něco úplně jiného. Ukazuje se, že nejobvyklejší představa souvisí se zaváděním nových technologií a aplikací, které nám usnadňují práci a zákazníkům zpříjemňují život. Čím víc firma do těchto technologií investuje, tím se považuje za vyspělejší. Realita je však taková, že tyto investice nepřináší očekávaný efekt, protože se v tomto „digitálním“ snažení zapomíná na to nejdůležitější – zákazníka. Cílem článku je analyzovat skutečnou situaci ve velkých firmách a zamyslet se nad příčinami a možnými zlepšeními.

digitalizace upskilling analýza průzkumu leadership

IT oddělení často stojí před dvojím úkolem, a to jak co nejefektivněji zajistit IT infrastrukturu, integraci nových řešení, bezpečnost, provoz a podporu organizaci a jejím zákazníkům, tak současně zvýšit povědomí o tom, co to digitalizace vlastně je a jaká rizika i možnosti přináší. V ideálním případě pomůže nastartovat a vést postupnou transformaci a nezbytné vzdělávání zaměstnanců, aby došlo k co nejefektivnějšímu využití nově používaných technologií. Cílem celého snažení je, aby se celková digitální gramotnost napříč organizací mohla zvyšovat, IT odborníci měli časovou kapacitu na méně „běžné“ IT práce a ostatní jejich podporu zase tolik nepotřebovali.

Pro IT se tedy stává asi nejdůležitějším porozumění rychle se měnícím požadavkům businessu a rychlý a levný vývoj, integrace a provozování nových technologií.

Na posledním letním Soirée jsme tradiční průzkum zaměřili na stav digitální transformace v českých organizacích a výsledky průzkumu byly prezentovány při příležitosti Svatomartinského setkání. Zajímalo nás, jaká je realita a kde jsou rezervy a výzvy, abychom mohli účastníkům setkání dát prostor k zamyšlení i možnosti srovnání, kde se nacházejí oproti ostatním organizacím.

Průzkumu se zúčastnilo 88 respondentů napříč sektory a také z různých pozic v managementu organizací, které zastupovali. Pouze 7% respondentů bylo přesvědčeno, že digitální éra znamená jen technologickou obměnu a využití modernějších a dostupnějších technologií. Velká většina se domnívá, že se jedná o celkovou transformaci společnosti, která významným způsobem mění svět kolem nás, a my jsme nuceni se zorientovat a přizpůsobovat na osobní i organizační úrovni, abychom využili příležitosti a pomohli řešit výzvy, které tato éra přináší. A to nejen na technologické úrovni, ale také na úrovni společenské, etické, bezpečnostní a celkového způsobu života, hlavně forem a obsahu práce.

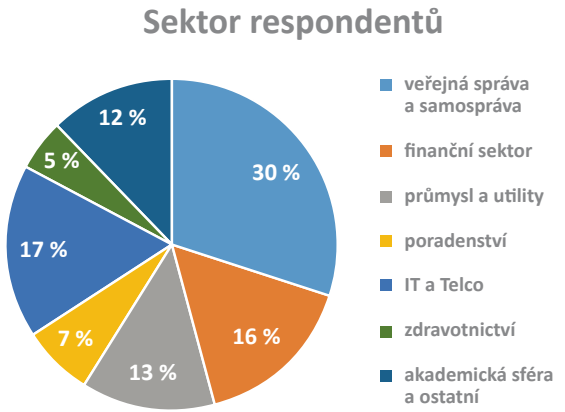
Celospolečenská změna je formována globálními megatrendy, jako je rychlá urbanizace, změna klimatu, nedostatek zdrojů, posun světové ekonomické síly, demografické a sociální změny či technologická revoluce. Tyto probíhající změny postavily civilizaci před komplexní problémy, které jsou jen stěží řešitelné tradičními cestami a bez změny paradigmatu. Dochází také k významnému posunu v potřebách, hodnotách a vnímání světa dnešní mladou generací, která již vyrůstá v relativním ekonomickém blahobytu, obklopena technologiemi a se samozřejmým přístupem k internetu a všem informacím. Typická je pro ně potřeba být

v neustálém kontaktu s kýmkoli a sdílet všechno a hned. Je proto na rozhodnutí každé organizace, jak chce na tyto změny v potřebách a preferencích stávajících i potenciálních zákazníků reagovat z pohledu nabízených produktů i služeb a jak je poskytuje (tzv. zákaznická zkušenost).

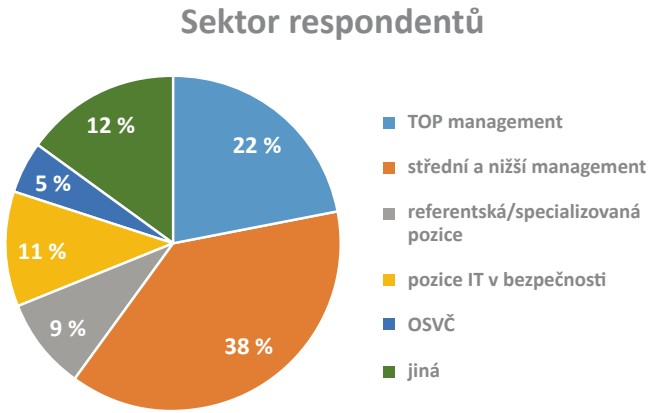
Jak vyplývá z grafu 3, většina investic a aktivit jednoznačně směřuje do infrastruktury, Cloudu a zavádění moderních technologií a aplikací pro interní nebo zákaznické využití.

Pouze třetina respondentů uvedla, že jejich organizace má propracovanou digitální vizi a strategii napříč celou organizací a zhruba třetina organizací se zatím nedokázala zorientovat a stanovit si, co to pro jejich organizaci a zaměstnance znamená a co je potřeba případně dělat jinak. Vyplývá to z toho, že v takových firmách většina aktivit v této oblasti probíhá převážně v IT oddělení. I když digitalizace není jenom o IT, většina organizací očekává, že tuto transformaci nastartuje a povede. IT však často není vybaveno dostatečnými pravomocemi, aby dokázalo rozhýbat a zapojit ostatní zaměstnance, části organizace a jejich liniové řízení. Řízení této oblasti patří na úroveň CEO a ideálně úzké spolupráce všech členů vedení organizace, tedy napříč jednotlivými funkcemi, jelikož se týká fungování, tedy řízení všech částí organizace na strategické, provozní, ale hlavně zaměstnanecké úrovni.

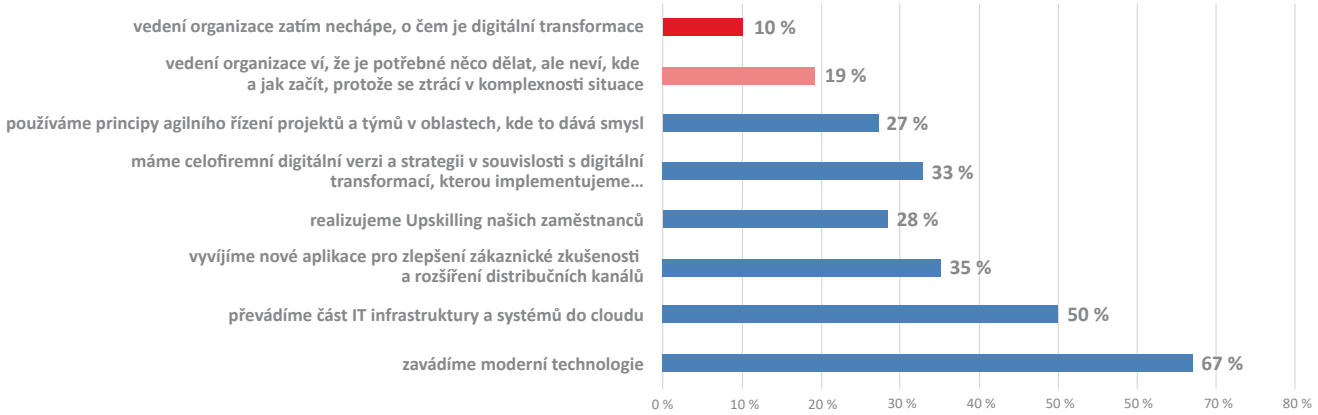
Pro zajímavost, v letním průzkumu prováděném Svazem průmyslu ČR při příležitosti MSV (Mezinárodní strojírenský veletrh) v Brně, zaměřeném na průmyslové firmy, a tedy Průmysl 4.0, se zdála situace o něco lepší. Většina ze 105 respondentů napříč průmyslovými firmami má nebo připravuje svou digitální strategii a 36% dle ní již postupuje. Některé z nich mají také zřízenou roli šéfa digitální agendy (tzv. CDO – Chief Digital Officer). Zkratka CDO se používá také pro Chief Data Officer. Jedna se o exekutivní roli, která se začíná objevovat ve větších organizacích, které již disponují, dále získávají a pracují s velkým množstvím dat o svých zákaznících, zaměstnancích a trhu obecně (banky, telekomunikace a do budoucna určitě i státní instituce). Data Officer dohlíží na sběr, správu a ukládání dat v celé organizaci. Je odpovědný za analýzu a hledání souvislostí z dat, aby tvořil informovanou obchodní strategii a hodnotu pro zákazníka, firmu a ostatní aktéry. Myslím, že jsou to právě tyto dvě role, které budou představovat významné „ohrožení“ a nadbytečnost role CEOs v jeho současném vnímání a budoucím uspořádání firem, pokud se tato role nebude postupně měnit na Chief Experience Officera, který mimochodem již v mnoha organizacích hlavně v USA existuje.



Graf 1: Struktura respondentů letního průzkumu



Graf 2: Struktura dle rolí v organizaci



Graf 3: Hodnocení stavu digitalizace v organizacích zastoupených respondenty Soirée průzkumu

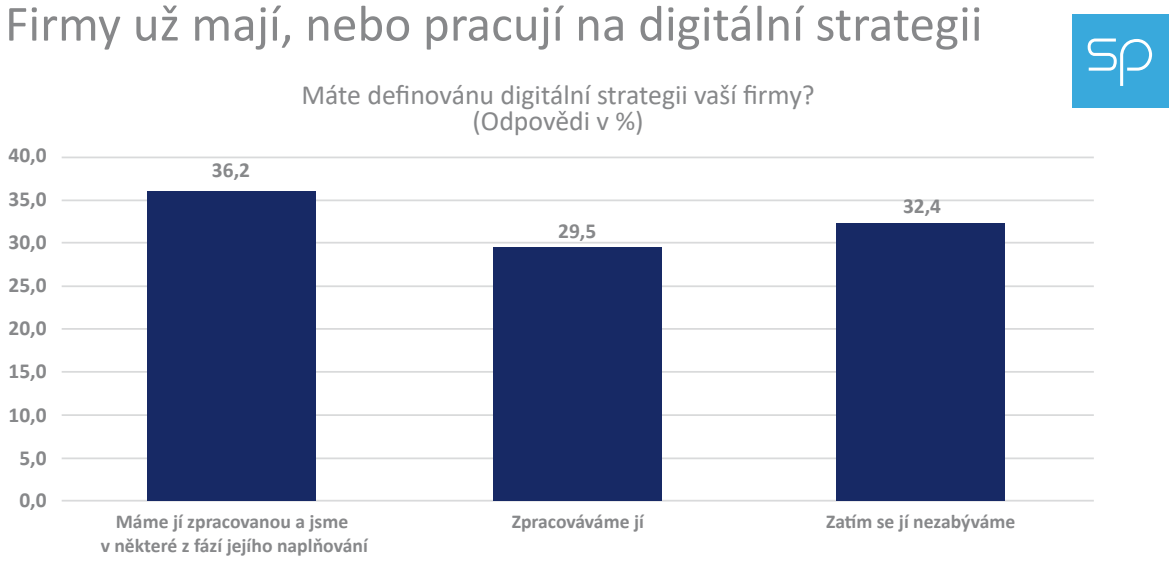
Co je tedy digitalizace?

Digitální éru je vhodné vnímat v širším kontextu jako hledání nových způsobů řešení problémů, zlepšování zákaznické a zaměstnanecké zkušenosti a zvyšování výkonnosti organizací. Technologie samotná nedosáhne pozitivního dopadu, ale přináší nové možnosti, které dříve nebyly k dispozici. Její přijetí, zavádění, ale hlavně správné využití v provázanosti na provozní model, procesy, schopnosti a chování lidí (zaměstnanců i manažerů) je proto naprosto klíčové, pokud nechcete ztrácet čas, peníze a nadšení pro dobré věci.

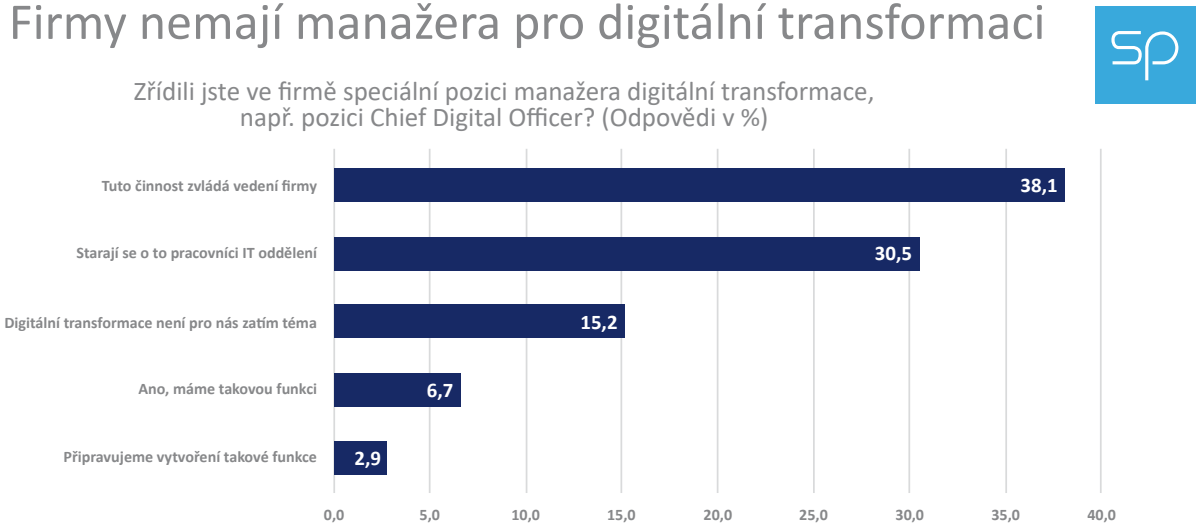
Vedení organizace může tedy digitalizací dosáhnout buď optimalizace podnikání využíváním digitální technologie, nebo se může dosavadní model podnikání transformovat směrem k digitálnímu podnikání. Digitální transformací se rozumí přehodnocení původního způsobu podnikání dané firmy s cílem nalezení nového podnikatelského modelu s exponenciálním růstem (např. Netflix). Naprostá většina firem se digitalizací snaží získat hlavně větší efektivitu nebo modernizovat a hledat nové způsoby organizace práce a zlepšování zákaznické zkušenosti.

Na základě výsledků průzkumu mají organizace největší nevyužitý potenciál v lepším nastavení provozního modelu a procesů, tedy i náplně práce jednotlivých týmů a zaměstnanců. Je tedy potřeba zapracovat na organizaci práce a jejího řízení na jednotlivých úrovních. Proto se v některých firmách již odhodlali zavést agilní struktury a metody práce, které urychlují realizaci vývoje produktů a služeb.

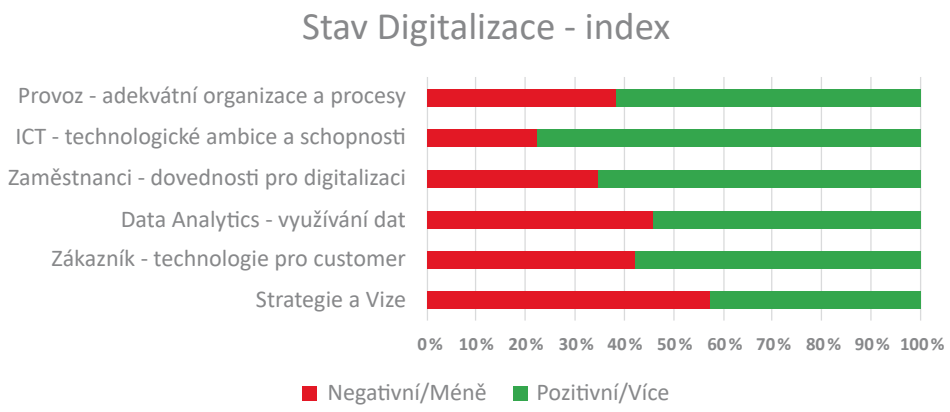
Zdá se, že většina firem si již uvědomuje důležitost zákaznických a zaměstnaneckých dat, kterými disponuje. Jejich využívání a hledání cenných informací nám zatím ovšem tolik nejde. Pokud máme licence k nástrojům, jako je třeba



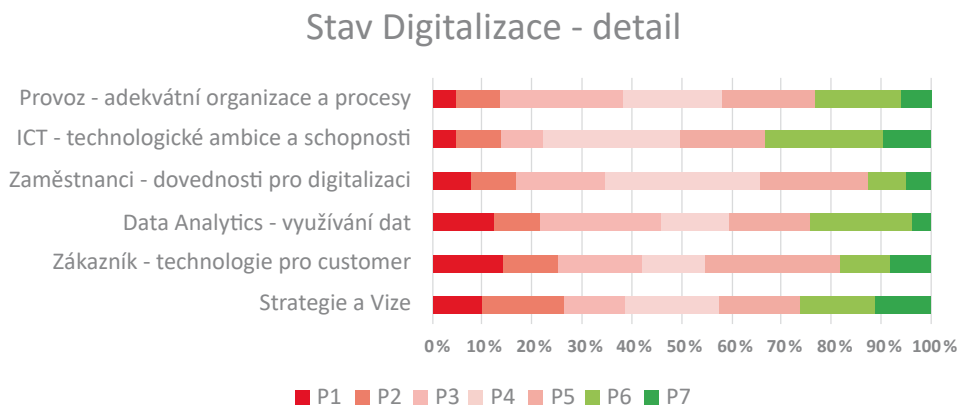
Graf 4: Průzkum SPČR ze září 2019 o stavu digitalizace a připravenosti na Průmysl 4.0



Graf 5: Průzkum SPČR - kdo řídí digitální transformaci organizace



Graf 6: Poměrný ukazatal stavu digitalizace dle respondentů Soirée



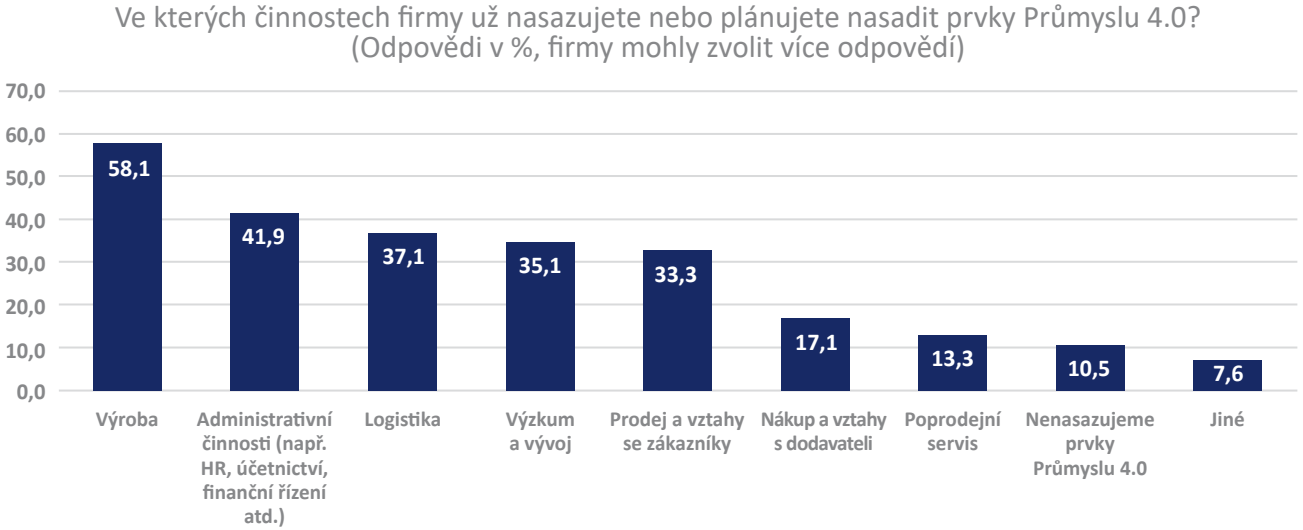
Graf 7: Detailní pohled stavu digitalizace dle respondentů Soirée

Alteryx, PowerBI nebo UiPath, využívá je malá skupinka nadšenců, zatímco širší využití pro automatizaci procesů a lepší a rychlejší rozhodování ještě chvilku potrvá.

Zaměstnanci

Většina organizací si stěžuje na nedostatek zaměstnanců s požadovanými dovednostmi, kteří by pracovali novým způsobem. Neuvědomujeme si ale, že i zaměstnanci potřebují významně pomoci s nasměrováním a nastartováním při získávání nových dovedností, které by mohli využít právě pro pozměněnou pracovní náplň. Cílený a řízený systém upskillingu konkrétních zaměstnanců na konkrétní pozice je spíše raritou, většinou se firmy nadále věnují plošnému vzdělávání digitálních dovedností, pokud vůbec. Upskillingem rozumíme získávání nových technických, odborných, a hlavně komunikačních dovedností vyžadovaných na pozměněné a nově tvořené pozice. V českých podmínkách je situace o to složitější, že máme nejnižší nezaměstnanost v EU a už není kde brát ani nekvalifikované pracovníky.

Nejčastěji se Průmysl 4.0 uplatní ve výrobě



Graf 8: Průzkum SPČR - nejčastější oblasti nasazení digitálních technologií v průmyslu

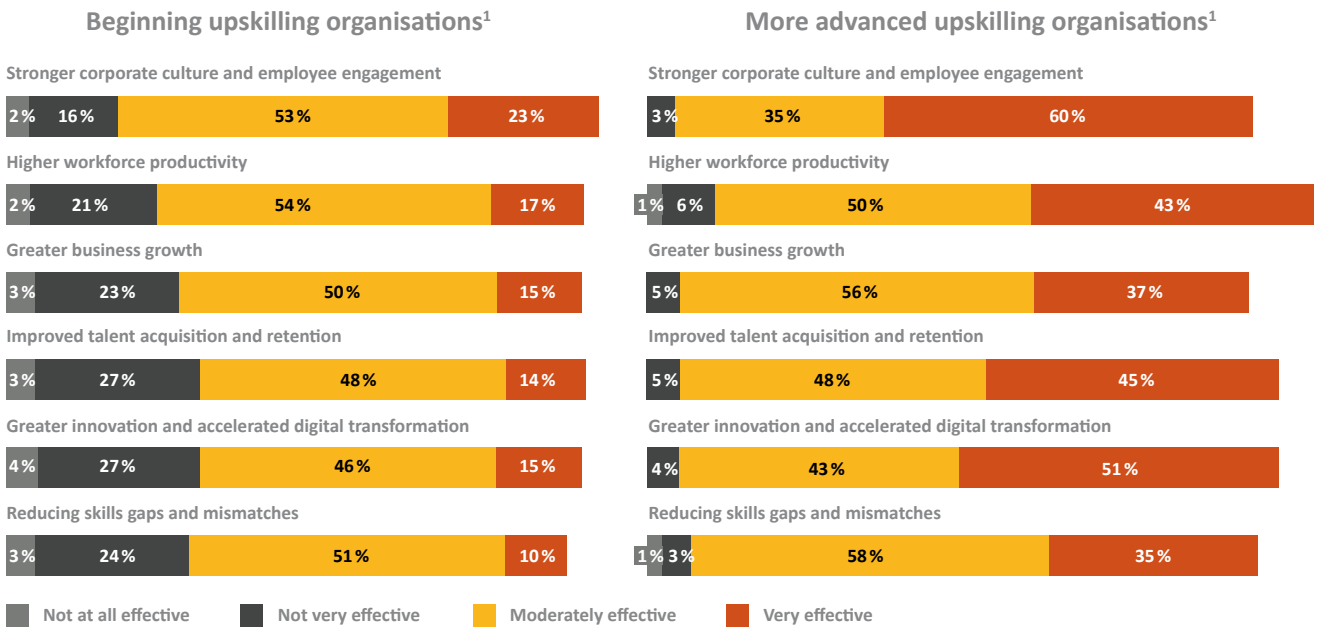
Z průzkumu Soirée vyplynulo, že přibližně jedna třetina respondentů již systematicky poskytuje vzdělávání zaměřené na zvyšování dovedností. Ve výsledcích průzkumu SPČR je tento podíl srovnatelný – přibližně 22% firem již upskilling realizovalo a 20% loni připravilo alespoň koncepci. Lze tedy předpokládat, že letos bude upskilling realizován u 40% respondentů obou průzkumů.

Z globálního, již 23. CEO Survey zveřejněného v lednu v Davosu vyplynulo, že právě správné dovednosti zaměstnanců pro budoucnost představují jeden ze tří největších problémů firem. Mnoho firem proto nastartovalo programy na upskilling, tedy rozšiřování dovedností pro lepší uplatnění, nicméně pouze 18% respondentů je spokojených s výsledky, které tyto iniciativy přinášejí, a zamýšlejí se, jak vynakládané investice do této oblasti optimalizovat. Současně si začínají uvědomovat, že se zaměstnanci po absolvování těchto programů stávají atraktivním cílem pro konkurenci.

Nicméně firmy, kterým se daří takovéto programy řídit, přiznávají, že kromě snižování mezery v požadovaných dovednostech to má mnohem hmatatelnější přínosy pro celou firmu. Z průzkumu vyplynulo, že firmy s rozvinutým upskilling programem pro své zaměstnance dosahují lepší firemní kultury pro zvyšování angažovanosti zaměstnanců, zlepšení výkonu a produktivity, a tím celkového růstu. Dále se jim daří lépe získávat, rozvíjet a udržovat talentované zaměstnance a také mají mnohem lepší výsledky v inovacích a využívání digitálních technologií.

Provoz

Samotný provoz představuje zřejmě největší prostor ke zlepšení, a to jak v hlavních, tak v podpůrných procesech. Vyžaduje to však komplexní přístup a zamyšlení se nad jednotlivými aspekty zákaznické zkušenosti, proč a jakým způsobem jsou jednotlivé agendy vykonávány a zda existuje prostor pro



Graf 9: Pozitivní dopady zavedení upskillingového programu dle 23d Global Annual CEO Survey

jejich „překopání“ právě díky možnostem nových technologií. Technologii lze pořídit a integrovat relativně rychle, ale opět budeme narážet na nepřipravenost a setrvačnost lidí fungovat tak, jak byli zvyklí. Bez pomoci a motivace učit se dělat nové věci novým způsobem to bude trvat dlouho.

Co brání efektivnějšímu zavádění digitalizace?

Z každoročního PwC Digital IQ průzkumu opakovaně vyplývá, že hlavní bariérou při snahách organizací řídit posun k větší digitalizaci není překvapivě nedostatek peněz, času a technologií, ale hlavně „tradiční“ zakořeněný způsob myšlení, návyků a dovedností vedoucích pracovníků i zaměstnanců. Když už se odhodláme, máme komplikace s nedostatkem

Bez kvalifikovaných lidí to nejde – firmy už vzdělávají zaměstnance v digitálních technologiích

21,9 %	firem už investuje do vzdělávání a rozvoje zaměstnanců v oblasti digitálních technologií
20 %	firem už připravuje koncepci vzdělávání zaměstnanců pro práci v digitálním prostředí
8,6 %	firem uvádí, že jejich zaměstnanci už mají všechny potřebné dovednosti pro zavádění Průmyslu 4.0

Obr. 1: Průzkum SPČR – stav dovedností pro Průmysl 4.0

požadovaných dovedností (37 %). Opakované průzkumy také ukazují, že se moc nezlepšuje situace na úrovni vedení, kde chybí nadšení a digitální důvtip (43 %), který by dodal víc odvahy ke kreativitě a experimentování na nižších pozicích. Jádrem problému pak je, že firmy nemají digitální strategii zahrnutou do organizační strategie (63 %) a spoléhají se na jednotlivé nekoordinované iniciativy.

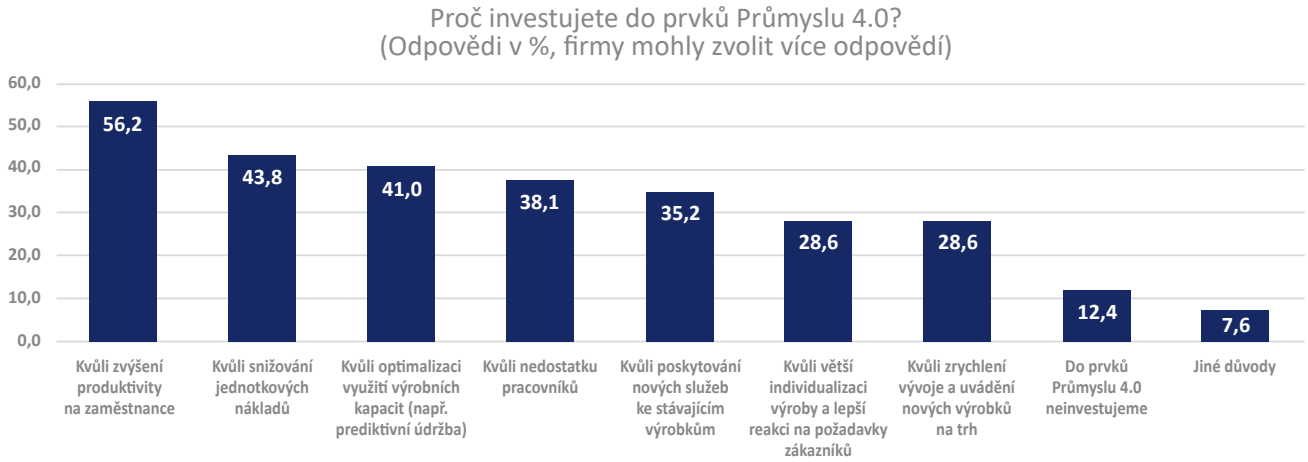
Jaké jsou elementy úspěšného postupu?

Opakované vytváření ideální zákaznické zkušenosti pro zákazníky – značka už nestačí. Obchodní značky, které jsme obdivovali před pár lety, vybledly. Některá odvětví byla překopána nebo posunula hranice svého působení. To je ale nezvratný proces a je dost nepravděpodobné, že se vrátí na výsluní ekonomické prosperity.

S přístupem k mnohem většímu množství informací prostřednictvím internetu nároky zákazníků stoupají jako nikdy předtím. Zákazníky nezajímá, kdo jste byli loni (možná vyjma státního sektoru). Většina transakcí probíhá v reálném čase a zákaznické dojmy se spontánně šíří na sociálních sítích, a to globálně. Zákazník si vaši nabídku může lehce srovnat s těmi nejlepšími v oboru. Zůstat v businessu a držet krok znamená, že musíte nabízet a skutečně dodat hodnotu pro zaměstnance i zákazníky a navíc smysluplný, opakovaný a všestranný zážitek. Máte možnost vyčkávat, co se ukáže jako funkční, a doufat, že pak nebudete poslední. Nebo můžete sami neustále zkoušet, vylepšovat a zajímat se o to, na čem skutečně záleží vašim zaměstnancům a zákazníkům.

Firmy, které si uvědomují, že jejich konkurence může přijít kdykoli a odkudkoli, místo zlepšování svého fungování přijímají nový druh myšlení, které je připravuje na další kroky. Je to o tom, jak dělat organizaci adaptabilnější a agilnější, jak se

Firmy nejčastěji investují do Průmyslu 4.0, aby zvyšovaly produktivitu



Graf 10: Průzkum SPČR - důvody investic do digitálních technologií a Průmyslu 4.0

zamýšlet a přehodnocovat co, jak a proč děláme. Nechávat větší samostatnost zaměstnancům a usnadňovat vzájemnou spolupráci. Pokud se neustále zajímáte, co se děje ve vašem okolí, a neuvízli jste ve své vlastní bublině, pokud neustále vymýšlíte koncepty, které uvádíte do reality, a zkoušíte, testujete a dále vylepšujete, pokud děláte z digitálních možností součást svého myšlení a uvažování při řešení problémů, znamená to, že již tvoříte a žijete s digitálním vědomím, které se určitě promítá do vašeho jednání ve společnosti.

Řízení digitální transformace

Vzhledem k tomu, že digitální transformace je týmovým sportem, který vyžaduje spolupráci napříč celým vedením organizace a jednotlivými funkcemi pod taktovkou digitálně zdatného kapitána/trenéra, lze doporučit několik osvědčených postupů, které používají firmy, jimž se daří růst rychleji než konkurenci právě díky řízení tohoto procesu.

U většiny lídrů existuje přirozená potřeba se zlepšovat ve svých digitálních dovednostech a toto podporovat napříč celou organizací na všech úrovních řízení i u samotných zaměstnanců. Pro překlenutí existující mezery se některé společnosti dívají mimo svá odvětví a snaží se přilákat další lídry, kteří mají nadhled a schopnost pomoci se změnou myšlení v dané organizaci a nastartování její změny. Zákaznická zkušenost je jednou z oblastí, ve které to vidíme nejčastěji.

Z průzkumu PwC Digital IQ vyplynulo, že 91 % firem patřících k nejrychleji rostoucím má výkonného ředitele, který má na starosti zaměstnaneckou zkušenost, a přibližně stejný počet má výkonného ředitele pro zlepšení zákaznické zkušenosti.

Obr. 2: Jak vnímat digitalizaci z pohledu změny způsobu práce

77% těchto firem tvrdí, že vedoucí pracovníci společně tvoří digitální strategii a také ji společně realizují a pravidelně přehodnocují. Není tedy nařízena shora ani není tvořena a řízena v jednom oddělení. Tyto firmy také věnují významné úsilí zvyšování kvalifikace a modelování nových způsobů práce místo neustálých stížností na nedostatek kvalitních uchazečů na trhu práce. Používají také více iteračních a kolaborativních přístupů a aktivně pracují na tom, aby se vyhnuly praktikám a chování, které ničí skvělé nápady. To neznamená, že všechno dělají správně, ale záleží jim na tom, aby pořád šly touto cestou.

Pokud se od vás a vašeho oddělení očekává, že tento proces nastartujete, případně již vedete, je vhodné řešit paralelně tyto čtyři oblasti, a to napříč organizací:

- *Transformace*. Je nesmírně složitá, protože se jedná o změnu, jak lidé dělají svoji práci a jak se při tom chovají k sobě navzájem, k zákazníkům i dalším aktérům. Změna se nedá vynutit, ale je nutné pomoci pochopit její přínosy pro jednotlivce a poskytnout veškerou opakovanou pomoc při dosahování změny návyků.
- *Vedení společnosti*. Je objektivně známo, že zaměstnanci (kolektivně) mají více digitálního know-how než vedení společnosti. A to je kámen úrazu. Lídři by si to měli nejenom uvědomit a otevřeně přiznat, ale také pracovat na jeho rozvoji a nových metodách řízení včetně umožnění větší autonomie a rozhodování na úrovni týmů.
- *Pracovní síla*. Dochází ke zvětšování propasti mezi dovednostmi lidí a možnostmi, které zaváděné technologie a nástroje nabízejí, ale de facto nevyužívají. Přitom firmy neustále investují do nových nástrojů, ale neadekvátně do dovedností lidí a jejich způsobů práce, návyků a osobnostního rozvoje a vědomí.
- *Disruption*. Zatím nemá český překlad, ale příhodné by bylo třeba Zruinování. Z globálního průzkumu PwC ve vyspělých ekonomikách vyplynulo, že jenom 31 % lídrů má reálnou obavu, že někdo může zruinovat jejich tradiční business novým modelem, a snaží se s tím skutečně něco dělat. Pokud si myslíte, že váš business není ohrožen, a nepatříte do státního sektoru, zatím není pozdě.

V této poslední oblasti má prozatím veřejný sektor časovou výhodu. U nás se čeká na novou legislativu, která by měla tento proces nastartovat. Určité propady jsme však měli možnost zaznamenat i zde, když byl tradiční proces soutěže na nový e-shop dálničních známek nabídnut státu zdarma ve formě Hackatonu, kterého se zúčastnili dobrovolníci. Nelze očekávat, že všechnu technologii státu budou teď tvořit dobrovolníci, lze však očekávat významný posun ve způsobu vývoje nové technologie i pro stát – tedy konečně jakýsi DevOpps a Agile ve státě. To je výborný začátek před nastartováním digitálního Česka.

Peter Chrenko
peter.chrenko@pwc.com

Peter Chrenko

Je partnerem firmy PwC, kde vede poradenský tým Lidé & Organizace, který pomáhá firmám s transformací HR funkce a agend a jejich souladu s korporátní vizí a strategiemi. Je přesvědčený o tom, že technologie nepředstavuje hrozbu pro člověka, ale příležitost pro jeho rozvoj prostřednictvím smysluplné práce, kterou nám umožňuje právě AI, automatizace a robotizace. To se neobejde bez dalšího vzdělávání a rozšíření smysluplného kontinuálního rozvoje zaměstnanců, manažerů a lídrů, orientujících se v komplexnosti současné doby a jsou připraveni na budoucnost. V současné době se proto věnuje propojení relevantních aktérů a vybudování funkčního ekosystému, který bude schopen zajistit škálovatelný systém upskillingu a reskillingu zaměstnanců v soukromé i veřejné sféře pro udržení zaměstnanosti a konkurenceschopnosti ČR v digitální éře a průmyslu 4.0.

ZDROJE

[1] Web Svazu průmyslu průzkum 2019
[2] PwC Global CEO survey 2019
[3] Průzkum TATE Soirée 2019

DevOps

část VII.

Shrnutí současného stavu, mýty a problémy

Co přinesl DevOps v současné době? Nahradí či vytlačí ostatní standardy a metodiky pro řízení IT, jako je CobIT či ITIL? „Nedojede“ DevOps na nedostatečnou bezpečnost? Co můžeme čekat do budoucna? Bude DevOps někdy standardizován? Jaké jsou s DevOps často spojované mýty a problémy?

DevOps ITIL DevSecOps State of DevOps

V předposledním dílu celého seriálu si představíme současný stav transformace na DevOps, dopady na řízení firem, časté mýty a typické problémy, se kterými se při implementaci nejčastěji potkáváme.

Současný stav DevOps aneb dosažené výsledky

Zde si stručně shrneme dosavadní výsledky včetně dopadu na business firem.

Co přináší DevOps nového vůči tradičním metodám řízení IT?

Jednoduchá otázka, ale složitá odpověď. Na tu jsme se snažili odpovědět již v předchozích dílech tohoto seriálu. Pokud bychom měli shrnout ty největší rozdíly, ale zároveň i výzvy:

- jednoznačná orientace na zákazníka (value),
- zkracování dob realizace (současně se snižováním nákladů a zajištěním vyšší kvality),
- důraz na inovace a automatizaci (robotizaci),
- nasazení nových modelů businessu, financí a zajišťování podpory IT,
- uplatnění nových typů rolí, procesů, organizačních struktur a stylů řízení,
- uplatnění nových typů alokací lidských zdrojů a procesních/projektových/produktových přístupů,
- nasazení nových typů podpůrných softwarových nástrojů,
- změna některých zažitých návyků při řízení IT (IaC, CI, CD, CT, CS, *pets/snowflakes vs. cattle*, cloud, neměnná infrastruktura atd.),
- změna kultury (od sil k spolupráci, komunikaci a sdílení) a další lidské *„soft“* i *„hard“* dovednosti,
- uplatnění agilních, interaktivních a iterativních přístupů jak ve vývoji, tak i v provozu,
- využití posledních technických a technologických řešení a inovací – cloud, kontejnery, IaaS, SDN,
- nové výzvy, zranitelnosti, ale i metody v oblasti informační bezpečnosti.

Ten seznam samozřejmě není konečný.

Jaký dopad má fakticky transformace na DevOps?

DevOps znamená určitou transformaci firmy v šesti oblastech:

- vytváří zpětnovazební smyčky v pracovním prostředí v oblasti vývoje i provozu; klíčová je komunikace a sdílení znalostí,
- považuje všechny systémy a infrastrukturu za kód (IaC) a zachází s nimi stejně jako se softwarem,
- posouvá kulturu doposud čistě technicky fungující organizace směrem vůči totální dodávce a zkušenosti uživatele (value stream mapping, customer experience) se silným zapojením útvarů businessu,
- zajišťuje daleko rychlejší kadenci rozmisťování softwaru do produkčního prostředí a redukuje změny v dodávkách,
- mění kulturu firmy, organizační a kompetenční struktury a styl práce včetně celkové governance,
- napomáhá digitální transformaci celé firmy a v dlouhodobém kontextu umožňuje přežití na trhu.

Mýty u DevOps

DevOps je stejně jako celá řada dalších nejlepších praktik předmětem častých mýtů. Protože DevOps není nijak standardizován či normalizován jako v případě dalších metodik a standardů (ITIL, CobIT atd.), je tato problematika daleko více ohrožující a může mít velmi významné

[1] Dodávejte často.

Mýtus	Realita
DevOps je řešením problému IT	Ve skutečnosti je DevOps řešením problému businessu.
DevOps se rovná implementaci softwarových nástrojů	DevOps vyžaduje spíše kulturní změnu.
DevOps a *Continuous Delivery/CD* je totéž	Každopádně to není binární vztah, jsou to související pojmy, ale určitě ne stejný obsah.
Role vývojáře, provozáka a DevOps splyne do jedné	Jsou to odlišné aspekty práce – vývoj kódu, testování, udržování infrastruktury pro tento kód a optimalizace procesů.
Provozní týmy (Ops) už nebudou potřeba (NoOps), protože všechno bude uloženo v cloudu	Ve skutečnosti i v případě veřejných cloudů pořád zbývá nutnost provozní podpory.
DevOps je jen o lepší komunikaci	To není pravda, komunikace je hodně důležitá, ale nestačí, je jen prostředkem dosahování cílů DevOps
CD znamená uvolňovat software každých pět minut	Software potřebujete uvolňovat podle reálné potřeby businessu, ale relativně rychle (několikrát denně až jednou za týden). Ani největší hvězdy *(Unicorns)* – Amazon, Netflix a Etsy – to nedělají nepřetržitě. Např. motto Facebooku je *„Ship often"*.
Na DevOps se můžete certifikovat	Certifikovat se můžete, ale dost dobře není na co (neexistuje standard). Ve skutečnosti je DevOps nikoli o nástrojích a procesech, ale spíše o komunikaci, spolupráci a empatii.
Adopce DevOps nevyžaduje *„buy-in"* na úrovni CxO	Ve skutečnosti je podpora z nejvyšších míst naprosto klíčová. A to nikoli pouze na úrovni IT, ale také businessu.
DevOps je jen nové jméno pro něco, co se v IT už dělalo	Částečně ano, ale ve skutečnosti je to o úplně jiném přístupu k práci a odlišné motivaci.
Bez cloudu nelze DevOps implementovat	Cloud pouze znamená zkratku pro rychlou a dynamickou alokaci infrastrukturních zdrojů, toho ale lze dosáhnout i automatizací tradičního IT či využitím technik, jako je virtualizace či kontejnerizace, nikoli však v tom rozsahu jako cloud.
DevOps naučí provozáky kódovat	I když Ops občas píše skripty a uplatňuje některé metody vývoje, jako je třeba verzování, pořád platí, že zůstává určitá míra specializace – vývoj, test, provoz atd.
DevOps v titulku vaší osoby znamená, že děláte DevOps	Ve skutečnosti to neznamená ještě vůbec nic, jde o změnu myšlení organizace a jednotlivců.
DevOps nelze použít pro firmy typu *Enterprise*, ale pouze pro tzv. firmy typu *„Unicorn"*	Není důvod, proč by DevOps nemohl fungovat i pro Enterprise firmy. Podle firmy Forrester je to dokonce poslední trend doby (viz [4]).
DevOps/CD je pouze pro firmy zabývající se vývojem webových nebo mobilních aplikací	Ve skutečnosti lze DevOps použít pro jakýkoli vývoj aplikací.
DevOps je pouze pro vývojáře a provozáky	Je to daleko obsáhleji definovaná množina zahrnující testery, dodavatele třetích stran, business a zákazníky. Patří sem také prodej, marketing i liniový management na úrovni CxO.
DevOps se nehodí pro firmy uplatňující ITIL	DevOps je spíše komplementární k ITIL; stále pro něj i většina definic a principů ITIL. Na druhou stranu některé konkrétní metody či praktiky ITIL V2/V3/2011 jsou v DevOps nepoužitelné. Místo toho ale můžete použít novinky z ITIL 4.
DevOps se nehodí pro firmy, které jsou předmětem regulací	DevOps ve skutečnosti zlepšuje shodu (compliance) – role automatizace, která zaručuje minimálně odchylek.
DevOps se nehodí pro firmy, které mají outsourcovaný softwarový vývoj	DevOps nemusí být kompletně zajišťován interně, můžete outsourcovat jak vývoj, tak i třeba testování, důležité je zajistit, aby procesy byly konzistentní a dobře fungovala komunikace.
DevOps se nehodí pro velké a komplexní systémy IT	I tyto systémy se dají v rámci DevOps spravovat, vždy však s ohledem na odlišné životní cykly jednotlivých částí systémů.

Tab. 1: Typické mýty DevOps

dopady na rozhodování managementu a v konečném důsledku na úspěch nasazení DevOps ve firmě.

V každém případě je potřeba tyto mýty identifikovat a vysvětlovat zaměstnancům i managementu. Asi nejúčinnějšími nástroji v téhle problematice jsou návštěvy konferencí DevOps či ITSM, školení pro zaměstnance, sebevzdělávání formou studia materiálů na internetu a knížek kolem DevOps (viz poslední díl tohoto seriálu).

Typické problémy a výzvy při implementace

Kromě mýtů si ještě proberme typické problémy, se kterými se v DevOps potkáváme. Některé z nich mohou plynout z mýtů popsaných v předchozím textu, jiné jsou prostě přirozenou věcí, kterou DevOps jakožto instrument měnící kulturu, procesy, governance a podpůrné nástroje nevyhnutelně přináší. Tím se dostáváme k největší výzvě DevOps – jak to udělat, aby se to povedlo? Toto jsme již částečně probírali v dílu IV. (DSM 2/2019) v rámci implementace, zde to však proberme z pohledu celkové governance.

Stakeholder management (aneb správa zúčastněných stran)

Tohle je velmi důležitá stránka věci. DevOps je multidisciplinární a multitýmová disciplína, která vyžaduje spolupráci, komunikaci a sdílení společného cíle. Pokud budou KPI u jednotlivých osob či celých týmů DevOps stanovena odlišně či budou tito lidé/týmy placeni z různých rozpočtů nebo bude odlišně zajišťována a řízena správa lidských zdrojů (resource management), pak celý koncept DevOps nebude korektně fungovat. Typickými skupinami v tomto kontextu jsou vývojáři, provoz, testeři, zástupci za bezpečnost a za business potažmo za zákazníky.

Důraz na aktivity (sila)	Důraz na produkt (tým)
Orientace na specializaci, formální liniová struktura	Orientace na výstupy, plochá/neformální struktura
Funkčně řízená organizace	Organizace na úrovni autonomních týmů
Důraz na projekty	Důraz na produkty
Práce na úrovni jedinců	Práce v týmu (autonomní týmy)
Optimalizováno na využití zdrojů	Optimalizováno na rychlost
Spíše formální governance, explicitní schvalování na úrovni procesních nebo liniových struktur	Neformální governance, implicitní schvalování na úrovni týmu

Tab. 2: Změny stylu práce a stylu řízení

Důležitou úlohu hraje nejvyšší vedení, a to jak IT, tak i businessu. Nemáme-li jejich podporu, vše je dopředu rovnou ztraceno. Nezapomínejme, že právě seniorní management by měl činit klíčová rozhodnutí, zajistit dostatečný rozpočet a schválit program či jednotlivé projekty realizované v rámci transformace na DevOps.

Vlastnictví, nejasné odpovědnosti

U velkých firem se hodně často potkáváme s určitým alibismem a překryvem či naopak nedostatkem kompetencí a hlavně nejasnou či nestanovenou odpovědností. Opačným problémem také bývá „všelidové“ vlastnictví, tedy situace, kdy při nějakém selhání obviníte celou firmu, Dev i Ops a jakékoli poučení z toho jde zpravidla do ztracena (viz [5]). Co zde určitě potřebujete, je jasné vlastnictví (leader pro DevOps na úrovni minimálně člena boardu, nestačí úroveň CIO), osobní angažovanost jak na straně manažerů, tak i řadových pracovníků. Další „spolehlivou“ cestou do pekel je externí implementace DevOps třetí stranou – to prostě v principu nemůže fungovat (pokud tedy nehodláte outsourcovat celé IT včetně businessu).

Realistické cíle

Velkou výzvou při aplikaci DevOps je nastavení realistických cílů (rozsah, očekávané výstupy a přínosy, finanční prostředky, čas). Častým problémem jsou totálně podstřelené časové a finanční odhady transformace na DevOps. Zde si prosím uvědomme, že se jedná spíše o cestu (journey) než o jednorázovou aktivitu či projekt. DevOps je o změně fungování IT, kultury organizace, stylu práce, a proto vyžaduje u velké firmy spíše několik let k získání zralosti. DevOps značí primárně kulturní změnu a změnu pracovního stylu. Čím větší organizace je, tím déle to bude trvat, protože to vyžaduje vysvětlování, školení a řešení otevřených bodů. Někdy to obnáší i obměnu personálu (ale i části managementu) podle známého hesla „starého psa novým kouskům nenaučíš“.

Nejasné řídící a organizační struktury

DevOps s sebou často přináší nutnost změnit jak styl řízení (přechod od liniového/procesního/projektového řízení na autonomní týmy a produktové řízení), tak i organizační a kompetenční struktury (např. *squads* – viz DSM 2/2019). Adekvátně se také mění požadavky na členy týmů i jejich manažery (nebo spíše leadery). Změnu poměrně dobře vystihuje Tab. 2.

Nevhodný výběr lidí

Jako u všech zlepšovacích iniciativ úspěch transformace na DevOps spočívá ve výběru vhodných leaderů (úmyslně nepíši manažerů), ale i členů jednotlivých týmů. O nutnosti se s některými zaměstnanci rozloučit už jsme psali. V každém případě u členů jednotlivých týmů potřebujeme diskutovat o změně jejich profilu (*T-shape* – viz díl IV., DSM 2/2019), u leaderů je zase nutné určité vůdcovství (Leadership). Direktivní a autoritativní liniový manažer je pro DevOps nepoužitelný.

Interpretace DevOps a agilních metodik jako něco, co nemá jasná pravidla

Agilní metodiky a přístupy se někdy (určitě neprávem) pojímají jako „chaos“, neexistují pevná pravidla, odpovědnosti, nedělá se dokumentace atd. Není to ale úplně pravda. Např. pokud chcete automatizovat některé procesní činnosti v rámci DevOps, musíte pravidla stanovit daleko rigidněji než třeba podle ITIL.

DevOps jako iniciativa IT

Někdy bereme start a rozvoj DevOps spíše pouze jako potřebu útvaru IT, aniž bychom reflektovali reálné potřeby businessu. Takto lze dosáhnout pouze dílčích úspěchů, např. můžeme úspěšně vybudovat agilní SW vývoj, ale nikoli celý rozsah DevOps. Způsobem, jak toho nejlépe docílit, je sdílení společných hodnot a cílů. Toho nejlépe dosáhneme díky společnému (business a IT) plánování a alokaci zdrojů, společné strategii a v neposlední řadě ve společně nastaveném financování.

Bezpečnost a governance

Poměrně často se vyskytujícím problémem je přehlížení bezpečnosti a chybějící nebo nedostatečná governance nad řízením lidí a dodávkami v rámci DevOps. Ačkoli má být DevOps rychlý a agilní, neznamená to běh bez pravidel, ale naopak více pravidel, která jsou ovšem stále více a více vynucována na úrovni podpůrných nástrojů (automatizace).

Nedostatečné testování /špatná kvalita kódu

Testování je oblast, která na jednu stranu velmi značně zrychluje release vyvinutého softwaru (za předpokladu automatizace testů), ale na druhou stranu vytváří celou řadu výzev, jak pokrýt všechny typy testů, kde vzít zkušené a levné testery, jak pokrýt oblasti, které nejdou automatizovat, atd. Řešením je zapojit vývojáře více do testování a nasadit nástroje, které umožní hlídat kvalitu vyvíjeného softwaru, upozorňovat na „škodlivý" nebo nebezpečný kód a k samotnému vývoji používat příslušné agilní metodiky, jako je např. Test Driven Development/TDD. V oblasti vývoje se pak doporučuje organizovat procedury, jak optimalizovat kód a zvyšovat jeho kvalitu (c*ontinuous refactoring, peer review* apod.).

Nedostatečná nebo chybějící dokumentace

Toto je téměř klasické téma. Většinový přístup k agilním metodikám je takový, že se podle agilního Manifesta dokumentace prostě nevytvářejí, nebo jen okrajově. Časté je to v případech startupů, kde doposud platilo, že si to prostě lidé pamatují, takže dokumentace není zapotřebí. V momentě, kdy ale startup začíná růst a nabírat nové zaměstnance, se toto stává velkou brzdou. Je to podobné téma jako testování. Naopak u firem typu Enterprise, které doposud aplikovaly nejlepší praktiky à la ITIL (s vytvářením rozsáhlé a často i zbytečné dokumentace), se zase objevuje obrácený postup, že s nasazením agilních metod (a DevOps) se od dokumentace kompletně upouští (často i v oblastech, kde je to nutné, např. Enterprise Architektura). Zradou je, že se neaktuálnost dokumentace zpravidla projeví se zpožděním několik měsíců až let. Řešením je definovat postupy a odpovědnosti, omezit tvorbu dokumentace na nejmenší možnou míru a alespoň částečně automatizovat její vytváření.

[2] Termín společnosti Gartner rozdělující aplikační portfolio na mód 1 (*systems of records*) a mód 2 (*systems of innovations*).

[3] Např. podporující chat a *instant messaging*.

Školení na DevOps BOX 1

Existuje celá řada certifikovaných i necertifikovaných kurzů na DevOps stejně jako školení na různé technologie a nástroje, neměli bychom však zapomínat na školení v oblasti kulturních aspektů (soft skills). Doporučuji všem zajistit si kvalitní kurzy a hlavně ověřené lektory. Uvědomme si, že DevOps je fenomén, který existuje pouhých deset let, takže nějakou rozsáhlou a léty ověřenou praxi nemůžeme úplně čekat. Principy a hlavně praktiky a metody používané v DevOps se neustále vyvíjejí a rozšiřují. Další věcí je závislost DevOps na technologiích a nástrojích. O tom už jsme psali, ale ještě ne v souvislosti s přímo raketovým nástupem softwarových nástrojů pro DevOps, které podle firmy XebiaLabs už tvoří tolik nástrojů, že pokryly pomyslnou periodickou tabulku prvků [1].

Velmi pečlivě si rozmyslete dvě věci: v jaké formě chcete školení absolvovat a na co se při něm chcete zaměřit. V tom prvním případě máte tři možnosti: s lektorem na místě, virtuální kurz s lektorem či tzv. E-learning (samostudium na počítači, vesměs pouze v anglickém jazyce). Zde bych asi doporučil školení s lektorem, hlavně kvůli nedostatečné úrovni angličtiny. V tom druhém případě si musíte rozmyslet, zda chcete školení zaměřené spíše na motivaci (vhodné pro větší organizace, které doposud fungují „vodopádovým" způsobem) či školení zaměřené na kulturu a tzv. soft skills, případně školení zaměřené na technologie (cloud, kontejnery) či podpůrné softwarové nástroje pro DevOps.

Komunikace a spolupráce BOX 2

Jestli něco v DevOps totálně nefunguje, tak je to formální komunikace (např. formou e-mailů, korporátních spamů) či komunikace formou vertikálních eskalací k stále vyšším manažerům na straně mé organizační entity přes manažery spolupracující entity až po jejich podřízené (komunikace typu „A"). U DevOps platí, že úspěšná je komunikace pouze tehdy, pokud je věcná, obousměrná, neformální, adresná, neobviňující a hlavně včasná a přesná. Pokud tohoto dosáhneme, jsme na nejlepší cestě k zajištění spolupráce mezi různými týmy *(collaboration)*. Tomu je potřeba přizpůsobit kulturu organizace, zavést dostatečně flexibilní nástroje[3] a motivovat zaměstnance. Samozřejmě zde totálně platí, že efektivní komunikace a spolupráce je výzvou hlavně u velkých organizací, u těch malých se to zpravidla neřeší. Pokud ve vaší organizaci platí, že standardní reakcí na adresný e-mail je žádná odpověď, a čeká se, až to budete urgovat (ať už dalším e-mailem, nebo telefonicky), asi sami dobře odhadnete, kam budete s touto praktikou v rámci DevOps směřovat.

Integrace DevOps a ITIL /změna stylu řízení

Další velmi častou výzvou jsou tzv. hybridní týmy (ITIL V3 a DevOps), které fungují odlišným způsobem pro tzv. Bi-Modální IT[2] či vícerychlostní správu aplikací (*pace-layered application management*). Ta první část funguje postaru podle ITIL V2/3 a ta druhá podle DevOps, resp. spíše její vývojová a testovací část podle agilních přístupů a část Operations podle ITIL. Tedy zkoušíme něco jako „kočkopsa" – snaha zachovat tradiční separované Dev a Ops organizační sila a přitom se pokoušet je řídit agilně. Tady se dá získat pár bodů v oblasti rychlejšího vývoje a automatizovaného testování, možná i rychlejšího vývoje kódu, ale nikoli u provozu. Vzhledem k faktu, že se tyto týmy/skupiny potkávají nad sdílenou infrastrukturou a velmi často i používají stejný podpůrný nástroj, je častou výzvou obě alternativy skloubit [2]. Moje vlastní zkušenost s použitím hybridních přístupů je spíše negativní; většinou to nefunguje.

Podniková architektura a standardizace

Dalším potenciálním problémem je chybějící podniková architektura (*Enterprise Architecture/EA*), konkrétně v kontextu budování nativních aplikací pro cloud (cloud native applications), znovu využívání částí kódu (*Microservices*) a určité standardizace, kterou DevOps určitě přináší. Všechny tyto věci vyžadují dost vysokou zralost, čehož nejde bez EA adekvátně dosáhnout.

Vzdělávání, školení na DevOps

Důležitou součástí transformace firem na DevOps je vzdělávání zaměstnanců. Řešíme tak mnohdy chybějící expertízu, přehledové znalosti v oblasti CI/CD (*T-shape*), nedostatečné zkušenosti a znalosti, ale také budování systému zajišťujícího motivaci zaměstnanců viz [1].

Kulturní aspekty

Toto je aspekt, který je snad nejvíce ignorován (specificky na úrovni nejvyššího managementu) a zanedbáván; aspekt, kde se asi dělá nejvyšší počet chyb a kvůli kterému celá řada pokusů o zvládnuté DevOps buďto úplně selže, nebo nepřináší plné výsledky. Některé poradenské firmy (viz [2]) vypichují důležitost řešení kultury ve firmách, ITIL 4 na toto téma zavádí novou praktiku zvanou *Organizational Change Management*. Velmi častým problémem v kontextu kultury organizace je prostě neochota se změnit. Potkáváme se s tím ve všech větších a historicky déle existujících organizacích – *„resistance to change"* je prostě typická forma obrany před čímkoli novým, neznámým. Toto specificky platí pro provoz IT.

Komunikace a spolupráce

Hodně důležitou a ožehavou věcí je komunikace – alfa-omega úspěchu DevOps (viz Box 2). Týká se to spolupráce týmů a organizačních jednotek, lokalit, zemí či kontinentů, používání referenčního jazyka (zpravidla angličtina), kulturních a národních rozdílů, používání společného podpůrného nástroje (chat, Skype, Webex), formy a frekvence komunikace, ochoty dávat a reagovat na zpětnou vazbu a dalších faktorů.

Podpůrné nástroje pro DevOps

A konečně posledním (nikoli však významem) bodem je úloha podpůrných SW nástrojů, na které se „implementace DevOps" někdy zvrhne. Vy tyto nástroje určitě potřebujete, o tom není pochyb, ale není to ten nejdůležitější faktor – tím hlavním jsou určitě lidé (viz [3]). U nástrojů se soustřeďte na automatizaci (včetně integrací), uživatelskou přívětivost, žádnou customizaci, zjednodušování procesů a eliminaci duplicitních nástrojů.

Automatizace pro automatizaci

Někdy máme tendenci hledat automatizovaná řešení i pro případy, které provádíme v jednotkách aktivit za rok. To není efektivní – vždy zvažujme náklady vs. reálné přínosy. Nesnažte se automatizovat aktivity, které provádíte zřídkakdy. Dávejme si pozor na „automatizovaná sila" – uspořádání podpůrných softwarových nástrojů, které zná jen dodavatel, popř. úzký okruh vašich expertů.

Závěr

V posledním, osmém díle si všechny předchozí díly shrneme, uvedeme si další zdroje a literaturu a celý seriál zakončíme závěrečnými doporučeními.

Vladimír Kufner
vladimir.kufner@t-mobile.cz

Ing. Vladimír Kufner

Vystudoval Elektrotechnickou fakultu ČVUT v Praze, kde později absolvoval i postgraduální studium. Poté působil postupně ve firmách Výzkumný ústav telekomunikací, DeTeWe, Philips, Logica (dnes CGI) a Hewlett-Packard. Poté nastoupil v roli procesního designera do společnosti T-Systems Czech Republic, která byla později zakoupena firmou T-Mobile Czech Republic. Zde nyní působí v divizi strategie a architektury jako procesní architekt a aplikační architekt v oblasti OSS. Kromě této činnosti se podílí na školeních ITIL/ITSM a DevOps v rámci tzv. T-Mobile Univerzity. Je čestným členem itSMF CZ, kde pravidelně přednáší na konferencích a tzv. mini-workshopech.

POUŽITÉ ZDROJE

[1] Periodická tabulka nástrojů DevOps, XebiaLabs, dostupné online na https://xebialabs.com/periodic-table-of-devops-tools/
[2] Axelos, dostupné z https://www.axelos.com/news/blogs/february-2017/bi-modal-two-speed-it-chaos-with-agile-projects či https://www.axelos.com/news/blogs/june-2016/integrating-devops-into-the-itil-orthodoxy
[3] The secrets of DevOps success, Gartner, dostupné z https://www.gartner.com/smarterwithgartner/the-secret-to-devops-success/
[4] Forrester, 2018: The Year Of Enterprise DevOps, dostupné z https://go.forrester.com/blogs/2018-the-year-of-enterprise-devops/
[5] Dev vs. Ops: The State of Accountability, dostupné z https://devops.com/wp-content/uploads/2019/04/dev-vs-ops-state-of-accountability-pdf-original.original.pdf

Dvě dekády snah OSN o stabilizaci kybernetického prostoru

Rostoucí počet kybernetických útoků ze strany státních aktérů podrývá vzájemnou důvěru a zvyšuje možnost eskalace, která by mohla vyústit až v kybernetickou válku. Snaha o stabilizaci kybernetického prostoru se tak rychle dostává do popředí jednání na půdě OSN. Za tímto účelem ustavilo Valné shromáždění OSN dvě pracovní skupiny, jejichž cílem je obnovit vzájemnou důvěru formulací a implementací norem zodpovědného chování států v kyberprostoru. Jednání se nyní nacházejí v klíčové fázi, přičemž vývoj příštích měsíců bude pro úspěch těchto snah kritický.

kybernetická bezpečnost OSN mezinárodní právo IS2 lidská práva online

Problematika kybernetické bezpečnosti prochází dynamickým vývojem, který má stále větší dopady na mezinárodní vztahy. S tím, jak přibývá kybernetických operací, za kterými stojí státní aktér, nabývá na intenzitě i diskuse o tom, zda je možné kybernetický prostor nějakým způsobem stabilizovat. Klíčovým a zároveň značně komplikovaným prvkem v této diskusi je hledání dohody o zásadách zodpovědného chování států v kyberprostoru, které by bylo nějakým způsobem kontrolovatelné, nebo dokonce vynutitelné.

Zvyšující se počet kybernetických hrozeb nutí Českou republiku spolupracovat se stejně smýšlejícími zeměmi, v prvé řadě v rámci EU a NATO. Kybernetická bezpečnost je však především globální problém a jako takový vyžaduje globální řešení. V tomto ohledu se zájem ČR upírá na jednání OSN, která v oblasti kybernetické bezpečnosti gradují v posledních letech. V prosinci 2018 byly ustaveny dvě pracovní skupiny OSN, které zkoumají možnosti stabilizace kybernetického prostoru a které v současnosti intenzivně jednají. Ve dnech 10.–14. února 2020 se v New Yorku uskutečnilo druhé substantivní jednání Otevřené pracovní skupiny OSN za účasti zástupců všech členských zemí OSN. Ve dnech 24.–28. února 2020 se uskutečnilo druhé substantivní jednání Skupiny vládních expertů OSN za účasti zástupců 25 zemí. ČR se aktivně účastní práce prvně jmenované skupiny.

Od obav z ICT technologií k zodpovědnému chování států v kyberprostoru

Diskuse o hrozbách vyplývajících z ICT technologií probíhá v OSN již dlouho. V roce 1998 Valné shromáždění OSN jednomyslně přijalo vůbec první rezoluci k ICTs v kontextu mezinárodní bezpečnosti.[1] V ní vyjádřilo mezinárodní společenství „obavu ze zneužití těchto technologií k účelům neslučitelným s udržováním mezinárodního míru a bezpečnosti a z negativních dopadů ICTs na bezpečnost států“. OSN tak začala poprvé uvažovat o rozvoji specifických principů a norem, které by přispěly ke snížení rizika kyberválky mezi státy a zefektivnily boj s kyberkriminalitou a kyberterorismem. Zajímavé ve světle současného vývoje je, že iniciátorem této diskuse bylo především Rusko. Následně začaly být přijímány rezoluce k ICT v kontextu mezinárodní bezpečnosti každoročně.

V roce 2004 mezinárodní společenství usoudilo, že konsekutivní rezoluce vyjadřující pokračující obavy nad zneužitím ICT systémů jsou nedostatečné. Z rozhodnutí 1. výboru Valného shromáždění proto vznikla Skupina vládních expertů (tzv. GGE)[2] se členstvím omezeným na stálé členy Rady bezpečnosti a cca 15–20 dalších států vybraných Generálním

[1] A/RES/53/70 z roku 1991.
[2] Group of Governmental Experts (pozn. autora).

tajemníkem OSN na základě principu rovnoměrného regionálního zastoupení. Skupina dostala za úkol studovat mezinárodní hrozby plynoucí z rozvoje a používání ICTs a identifikovat vhodná opatření k řešení současných a budoucích kybernetických hrozeb. Od roku 2004 proběhlo celkem pět jednacích kol skupiny GGE, přičemž tři kola vyústila v přijetí závěrečných zpráv GGE, které následně jednomyslně schválilo i Valné shromáždění OSN. Stojí za zmínku, že v letech 2004–2005 nepřijala skupina závěrečnou zprávu v důsledku rozcházejících se názorů členů na oprávněnost vojenského využití ICT systémů. Členské státy GGE se rovněž nedokázaly shodnout, zda by se další diskuze měly zaměřit pouze na bezpečnost ICT infrastruktury (názor západních států) či zahrnout i otázku regulace obsahu internetu (postup prosazovaný Ruskem a Čínou).

GGE nicméně dosáhla konsenzu v letech 2010, 2013 a 2015 a publikovala tři klíčové zprávy, které dodnes udávají směr mezinárodních diskuzí o stabilizaci kybernetického prostoru. V roce 2010 definovala GGE strategický rámec pro další snahy mezinárodního společenství o stabilizaci kybernetického prostoru. Konkrétně zpráva GGE navrhla vytvoření norem zodpovědného chování států v kyberprostoru, které by měly být doplněny o budování kyberodolnosti rozvojových států a opatření na budování důvěry (tzv. Confidence-Building Measures, CBMs). V roce 2013 přijala GGE zprávu, která s definitivní platností potvrdila, že mezinárodní právo, Charta OSN (potažmo i zákaz útočné války) stejně jako princip státní svrchovanosti se uplatní i v kybernetickém prostoru. Zpráva tak odmítla do té doby často opakovanou, byť fakticky mylnou definici internetu jakožto „volného statku-dědictví" všeho lidstva (tzv. Global Commons). Zpráva fakticky potvrdila, že i internet má státní hranice, neboť závisí na fyzické infrastruktuře pod svrchovanou kontrolou států.

[3] A/RES/70/237

Normy zodpovědného chování států

Významným dopadem uznání státní suverenity v kyberprostoru bylo nasměrování diskuzí OSN o bezpečnosti ICT k právům a povinnostem států v kyberprostoru. Výsledky těchto diskuzí jsou zohledněné ve zprávě GGE z roku 2015, která se často skloňuje jakožto nejvýznamnější dosavadní výstup z práce skupiny GGE. Konkrétně zpráva definuje 11 norem zodpovědného chování států v kyberprostoru, které určují nejen, co mají státy v kyberprostoru činit, nýbrž i jakých aktivit se mají v kyberprostoru vystříhat. Valné shromáždění OSN jednomyslně přivítalo zprávu GGE v roce 2016 a vyzvalo státy, aby se ve svém používání ICTs řídily jejími závěry.[3]

Shrnutí doporučení Skupiny vládních expertů (GGE) k normám zodpovědného chování států v kyberprostoru (zpráva UN GGE A/70/174):

Státy by neměly:

- vědomě připustit používání svého území k provádění mezinárodně protiprávních činů skrze ICTs,
- provádět či vědomě podporovat ICT aktivity cíleně poškozující kritickou infrastrukturu,
- provádět či vědomě podporovat aktivity poškozující informační systémy skupin pro reakci na počítačové hrozby (CERT/CSIRTS) ostatních států a neměly by využívat vlastní skupiny plnící tuto funkci k nepřátelským přeshraničním aktivitám.

Státy by měly:

- podniknout kroky k zajištění bezpečnosti dodavatelských řetězců a předcházet šíření škodlivých ICTs včetně jejich škodlivých skrytých funkcí,
- garantovat plné dodržování lidských práv online včetně práva na svobodu projevu,
- spolupracovat v zajištění stability a bezpečnosti ICTs a zabránit škodlivým praktikám,
- vzít v potaz veškeré relevantní informace v případě ICT incidentů,
- zvážit vhodné formy spolupráce v oblastech výměny informací, vzájemné pomoci a v potírání kriminálních a teroristických kybernetických aktivit,
- podniknout patřičné kroky k ochraně vlastní kritické infrastruktury,
- reagovat na opodstatněné žádosti o pomoc ostatních států, jejichž kritická infrastruktura je poškozována aktivitami ICT,
- podpořit zodpovědné ohlašování zranitelností v oblasti ICT a sdílet ověřené nápravné postupy.

Konkrétně normy GGE státům např. ukládají povinnost nedopustit vědomě zneužití vlastního území ke zneužívání ICT či provádět nebo podporovat aktivity na svém území, které by měly za cíl poškodit kritickou infrastrukturu ostatních států. V kontextu pokračujících mezinárodních diskuzí o bezpečnosti sítí 5G je relevantní i norma GGE, která státům ukládá povinnost podniknout konkrétní kroky k zajištění bezpečnosti dodavatelských řetězců ICT a zamezit šíření škodlivých skrytých funkcí těchto systémů. Zpráva GGE volá i po větší mezinárodní spolupráci v oblasti vzájemné výměny informací a pomoci při boji s kyberkriminalitou a kyberterorismem. Neméně důležitá je i norma GGE, která státy nabádá k dodržování základních práv a svobod na internetu včetně práva na soukromí a práva na svobodu projevu.

Tříštění mezinárodního konsensu o ICT – konec jedné éry

Další iterace skupiny GGE proběhla v letech 2016–2017 a podruhé v historii skončila nedohodou na podobě závěrečné zprávy. Vůbec nejožehavější otázku diskuzí GGE představovala aplikace mezinárodního práva v kyberprostoru, především pak uplatnění mezinárodního humanitárního práva (MHP) či

práva válečného. Uplatnění MHP v kyberprostoru ze zásady podporovaly USA, Francie, Velká Británie a další západní státy. Některé státy se však diskuzí o aplikaci MHP odmítly zabývat. Nejvýrazněji se proti uplatnění MHP v kyberprostoru postavila Čína, která argumentovala tím, že uznání aplikovatelnosti MHP by prakticky legitimizovalo militarizaci ICT, a tím zvýšilo riziko války v kyberprostoru. Státy se nicméně rozcházely i v názoru na to, zda vytvořit novou mezinárodní smlouvu, která by regulovala technologie ICT i obsah internetu (Rusko a Čína) či zda jít cestou ujasnění aplikace stávajícího mezinárodního práva na specifika kyberprostoru (západní státy).

Neshody hlavních hráčů GGE o dalším směřování skupiny se následně promítly i do jednání 1. výboru Valného shromáždění na podzim 2018, kdy Ruská federace neočekávaně předložila návrh rezoluce k bezpečnosti ICT, která namísto prodloužení mandátu expertní skupiny GGE předpokládala vytvoření nové Otevřené pracovní skupiny OSN pro ICT (tzv. OEWG). Oproti GGE je OEWG přístupná všem členským státům OSN a jedním z jejich cílů je podle potřeby formulovat nová závazná pravidla chování v kyberprostoru. Ruský návrh podpořený Čínou byl však pro západní státy nepřijatelný, neboť zahrnoval snahu schválit skrze rezoluci 1. výboru OSN Šanghajská pravidla chování pro informační bezpečnost, která na rozdíl od norem GGE kladou nepřiměřený důraz na prosazování státní suverenity v kyberprostoru na úkor dodržování lidských práv online.

USA kontrovaly vlastní rezolucí, která počítala se znovuustavením tradiční skupiny GGE. Zatímco státy EU a další podobně smýšlející země podpořily americký návrh, většina zemí světa podpořila ve snaze vyhnout se střetům při hlasování oba návrhy. Výsledkem tření na půdě Valného shromáždění bylo tedy přijetí obou rezolucí a ustavení dvou pracovních skupin k problematice informační bezpečnosti s překrývajícími se mandáty.

Cesta vpřed: dosažení komplementarity mezi GGE a OEWG

I přes komplikovaná jednání na půdě OSN představují ustavení GGE a OEWG pro státy OSN příležitost překlenout stávající patovou situaci. Faktem totiž zůstává, že přes původní skepsi západních států k ustavení OEWG nabízí její otevřený charakter v několika ohledech oproti GGE nespornou výhodu. Na rozdíl od GGE, jejíž omezený expertní formát nahrává možnosti dalšího rozpracování již přijatých norem zodpovědného chování ve zprávě GGE z roku 2015, je OEWG ideální platformou pro šíření povědomí o kyberbezpečnosti, zintenzivnění širší mezinárodní spolupráce v této oblasti a budování důvěry mezi státy. Pro mnohé státy je participace v OEWG zároveň jedinou příležitostí k výměně informací o osvědčených postupech při implementaci norem GGE a budování kapacit v oblasti kyberodolnosti.

Univerzalizace norem GGE by dozajista zásadně přispěla ke stabilizaci kybernetického prostoru. Implementace těchto norem si však vyžádá přijetí konkrétních politických, právních a technických opatření k jejich provádění. Otevřený formát OEWG je v tomto ohledu ideálním nástrojem ke sdílení praktických zkušeností s implementací na národní úrovni. Tímto směrem se ostatně ubírala i překvapivě věcná diskuze během prvního a druhého substantivního zasedání OEWG ze září 2019 a února 2020.

Česká republika v kontextu jednání OSN

Česká republika v tuto chvíli považuje jednání OEWG za příležitost a vystupuje velmi aktivně. Společně se západními partnery jasně podpořila vizi otevřeného, stabilního, bezpečného a mírového kybernetického prostoru založeného na dodržování multilaterálních pravidel a lidských práv. V této souvislosti vyjádřila i obavu ze zneužití technologií ICT autoritativními režimy k potlačování základních práv a svobod včetně práva na soukromí a svobodu projevu v digitálním prostoru. ČR připomněla důležitost zajištění bezpečnosti dodavatelských řetězců technologií ICT a deklarovala připravenost pomoci partnerům s budováním odolnosti vůči kybernetickým hrozbám. O tom, že ČR chce do budoucna hrát aktivní a konstruktivní roli v diskuzi o zajištění bezpečnosti dodavatelských řetězců ICT technologií, svědčí i intenzivní úsilí Národního úřadu pro kybernetickou a informační bezpečnost k zajištění bezpečnosti 5G mobilních sítí.

Zároveň je zjevné, že efektivní zajištění kybernetické bezpečnosti vyžaduje nejen součinnost států, ale rovněž soukromého sektoru a občanské společnosti. Ministr zahraničních věcí proto v rámci snahy diskutovat tuto problematiku co nejšířeji opakovaně udělil záštitu prestižní konferenci Information Security Summit (IS2). Na jejím okraji uspořádá Ministerstvo zahraničních věcí seminář k mezinárodně-politickým aspektům kybernetické bezpečnosti a konkrétně se zaměří vedle problematiky lidských práv a umělé inteligence právě jednání o stabilizaci kybernetického prostoru v rámci OSN.

Richard Kadlčák
okb@mzv.cz

Mgr. Richard Kadlčák

Působí na Ministerstvu zahraničních věcí ČR jako zvláštní zmocněnec pro kybernetický prostor a ředitel odboru kybernetické bezpečnosti. Jeho role zahrnuje koordinaci vnitrostátní a mezinárodní spolupráce v oblasti kybernetické bezpečnosti a reprezentování ČR na mezinárodních jednáních s tématikou kybernetické bezpečnosti. Na Ministerstvu zahraničních věcí ČR působí jako diplomat více než 20 let a v minulosti vykonával mimo jiné funkci mimořádného a zplnomocněného velvyslance ČR v Estonsku.

Malware Emotet – Trickbot – Ryuk v benešovské nemocnici

V prosinci 2019 se staly terčem kybernetického útoku dvě organizace. Nemocnice Rudolfa a Stefanie Benešov a těžební společnost OKD. Obě organizace byly úspěšně napadeny trojicí malwarů[1] Emotet – Trickbot – Ryuk. Obě organizace byly v důsledku útoku nuceny zastavit provoz a poskytování svých služeb. Nemocnice v Benešově nefungovala téměř tři týdny a škody incidentu předběžně vyčíslila na cca 30 mil. Kč. Společnost OKD pozastavila těžbu na čtyři dny a výši škod zatím nesdělila. Lze však očekávat, že i v případě OKD půjdou škody do miliónů a ani částka sdělená nemocnicí není konečná.

nemocnice malware Emotet – Trickbot – Ryuk prevence zdravotnictví

V průběhu prosince 2019 byly ransomwarem zasaženy a paralyzovány dvě organizace. Nemocnice v Benešově s 411 lůžky a cca 760 zaměstnanci, která je spádová až pro 400 000 lidí[2], a těžební společnost OKD, jediný producent uhlí v České republice se ziskem téměř 1,3 mld., vlastněný skrze společnost Prisko státem.[3] Obě společnosti byly v důsledku incidentu nuceny přerušit provoz. V ČR i ve světě se s ransomwarovými útoky každodenně potýká množství organizací, nicméně tyto konkrétní incidenty neunikly pozornosti veřejnosti a médií a otevřela se otázka kybernetické bezpečnosti podobných organizací. Média věnovala hodně pozornosti zejména benešovské nemocnici, protože se útok dotkl množství občanů a ukázal reálné dopady narušení kybernetické bezpečnosti na život společnosti. Nešlo tedy o abstraktní kybernetický útok, ale o skutečné zastavení chodu organizace, což řada pacientů reálně pocítila. Incidenty se podařilo zvládnout a skutečně vážné dopady (kromě finančních) se nerealizovaly, hlavně díky tomu, že za napadenou nemocnici zastoupily jiné nemocnice a uhlí je na trhu dost, takže těžba byla před Vánoci omezena. Incidenty se podařilo zvládnout a skutečně vážné dopady (kromě finančních) se nerealizovaly, hlavně díky tomu, že za napadenou nemocnici zastoupily jiné nemocnice a uhlí je na trhu dostatek, a navíc byla těžba před Vánoci omezena. Obě organizace byly zasaženy ransomwarem Ryuk, pro který se stal vstupní branou botnet Emotet a trojský kůň Trickbot. Data podle všeho odcizena nebyla, ale jak již bylo řečeno, obě organizace to na několik dní či týdnů odstavilo z provozu.

Popis Emotet – Trickbot – Ryuk

Zvýšenou aktivitu botnetu Emotet jsme evidovali na konci října 2019 na základě vyhodnocování logů z honeypotů a sinkhole serverů našich zahraničních partnerů. Docházelo k mnohonásobně vyššímu počtu záchytů, než je obvyklé. Zároveň se objevovaly první zprávy o obnovení aktivit dříve dopadených a vypnutých C&C serverů. Výkyv v aktivitě je u botnetů běžným jevem a často je provázen paralelními

[1] Pro účely tohoto článku bereme pojem malware jako široký zastřešující termín pro všechny možné typy škodlivých kódů (např. trojan, worn, dialer, spyware, ransomware atd.)
[2] Výroční zpráva Nemocnice Rudolfa a Stefanie Benešov, a.s. https://www.hospital-bn.cz/o-nas/vyrocni-zpravy/
[3] Výroční zpráva OKD, a.s. za rok 2018 https://www.okd.cz/cs/o-nas/vyrocni-zpravy

událostmi, jako je např. masivní phishingová kampaň. Právě Emotet takové kampaně využívá ke svému dalšímu šíření. Zatímco dříve se phishing vyznačoval špatnou češtinou, nyní to již neplatí. Čeština se časem v těchto kampaních zlepšovala až na dnešní úroveň, kdy narážíme na e-maily psané velmi dobrou obecnou nebo spisovnou češtinou. Novým trendem, který sofistikovanost phishingových e-mailů dále zvyšuje, je využívání kompromitovaných schránek k odesílání nakažené přílohy v odpovědi na dřívější legitimní komunikaci oběti.

Phishing je jako vektor útoku dlouhodobě nejvyužívanější, v závěsu lze jmenovat ukradená či slabá hesla, zranitelné a neaktualizované služby dostupné z internetu apod. Oblíbenost phishingu má bohužel základ v neznalosti a nepozornosti uživatelů, čehož útočníci úspěšně a vytrvale využívají.

Ostatním vektorům útoku lze technicky předcházet, což markantně snižuje počet kompromitovatelných strojů. To samozřejmě neplatí pro zranitelnosti typu 0-day. Ohledně způsobu průniku Emotetu do nemocnice v Benešově nelze být v tuto chvíli konkrétnější, neboť do uzávěrky tohoto článku nebyl mechanismus průniku spolehlivě prokázán.

Emotet byl původně vytvořen jako bankovní trojan ke krádeži citlivých údajů, čísel karet nebo hesel.[4] Dnes slouží primárně jako vstupní malware, který útočníkovi zajistí přístup do napadené sítě. Až ve druhé fázi dochází ke stažení trojanu Trickbot, který se postará o sběr citlivých údajů. V této druhé fázi útoku rozšiřuje Trickbot portfolio dat k exfiltraci o položky typu peněženek kryptoměn, což také koresponduje s trendy v době jeho vzniku v roce 2016.[5] Jeho zdrojový kód je neustále zdokonalován, např. po zveřejnění zranitelnosti EternalBlue byl schopen vlastního laterálního pohybu, a i nadále mu přibývají nové funkce. Útočník s takto širokou paletou dat může jednoduše zničit reputaci instituce nebo jí způsobit vážné finanční potíže.

Pro běžného uživatele je v případě nákazy Trickbotem obtížné vypozorovat nezvyklé chování počítače. Je pravděpodobnější, že nákazu zaznamená síťový administrátor v momentě, kdy počítač kontaktuje podezřelou adresu C&C serveru při exfiltraci dat či při dotazu na další instrukce. Jen málokterý uživatel je schopen škodlivou aktivitu detekovat přímo na nakaženém stroji. V tento moment už ale často dochází k velmi rozšířené a v některých případech úplné kompromitaci sítě. Malware totiž dokáže v produkční síti strávit bez detekce až několik měsíců a při tom kontinuálně sbírat informace. Po exfiltraci dat a kompromitaci důležitého prvku sítě útočníci přistoupí k poslednímu a z jejich pohledu i logickému kroku, kterým je spuštění ransomwaru.

V Benešovské nemocnici došlo ke stažení ransomwaru Ryuk[6], který postupně mapuje všechna možná síťová úložiště na privátních adresách a šifruje na nich silnými klíči RSA-4096 a AES-256. Šifrují se buď všechna data, nebo pouze výběr souborů s předem definovanými příponami. Takto zašifrované soubory není v dnešní době možné v reálném čase bez znalosti klíčů dešifrovat. Ryuk je poměrně mladý malware, který byl poprvé zaznamenán přibližně v polovině roku 2018. Antivirové společnosti ale zjistily, že jeho zdrojový kód vychází z dřívějšího ransomwaru Hermes a považují jej za další iteraci kódu. V raných verzích Ryuk zanechal – nejčastěji na ploše – soubor s kontaktem, instrukcemi k platbě, bitcoin peněženkou a dalším textem. Tím bylo možné vysledovat, že ransomware Ryuk díky své činnosti vydělal útočníkům až 4 mil. $. V reakci začali útočníci na zašifrovaných strojích zanechávat pouze kontaktní e-mailovou adresu, kam se má vydíraný ozvat. V rámci konverzace byly oběti zaslány ukázky dešifrovaných souborů a po platbě i dešifrovací nástroj. S nástrojem pro dešifrování však často nastával problém a soubory zůstaly oběti nečitelné. Zde se již můžeme jen domnívat, zda byla v dešifrovacím programu pouze obyčejná chyba nebo zda útočníci zaslali pouze ukázku exfiltrovaných dat a záměrně po platbě předali nefunkční nástroj. I z tohoto důvodu se nedoporučuje útočníkům jakékoli výkupné platit. Dalším důvodem je nepřímá podpora útočníka a jeho finančních možností při rozšiřování infrastruktury.

Na základě rychlé komunikace zejména ze strany DPO (data protection officer) benešovské nemocnice se podařilo poměrně rychle získat základní informace o incidentu a situaci na místě. Díky tomuto podnětu Národní úřad pro kybernetickou a informační bezpečnost do řešení incidentu v benešovské nemocnici zapojil analytiky, kteří svými schopnostmi pokrývali oblasti Windows domény, Windows stanic, forenzní analýzy Windows a Linux, síťového provozu a monitoringu a virtualizace infrastruktury. V rámci incident response týmů, které jsou vysílány na místo útoku, je standardně zastoupen vedle jiných analytiků také forenzní specialista, neboť většinou na počátku řešení incidentu není dostatek informací o situaci, typu útoku či rozsahu zasažení.

Forenzní specialista se zaměřuje na zajištění důkazů, zejména aby byly použitelné v dalším vyšetřování, případně v trestním řízení. Při zajišťování je potřeba dodržet postupy, které zajistí důvěryhodnost a integritu dat. Forenzní speci-

[4] The Evolution of Emotet: From Banking Trojan to Threat Distributor https://www.symantec.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor
[5] Trickbot, Technical Analysis of a Banking Trojan Malware https://www.sentinelone.com/blog/trickbot-technical-analysis-banking-trojan-malware/
[6] Threat spotlight: the curious case of Ryuk ransomware https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/

alista má mimo jiné za úkol pomoci s čištěním infikovaných strojů, hledáním persistencí malwaru a analýzou prostředí. Svůj tým malware analytiků vyslal i dodavatel antivirového řešení a jeho členové na místě analyzovali infrastrukturu a vzorky malwaru. Po počáteční analýze situace, prostředí a rozsahu škod byl společně s dodavateli infrastruktury a zaměstnanci nemocnice vytvořen plán na postupnou obnovu infrastruktury. Paralelně s tím na pracovišti NÚKIB probíhala síťová a forenzní analýza, díky které se dokázala určit šíře nákazy, persistence malwaru a indikátory kompromitace. Zejména díky indikátorům kompromitace, které se v co nejkratší době distribuovaly organizacím v kompetenci NÚKIB, se zamezilo podobné nákaze u jiné organizace. Mezi indikátory kompromitace patří nejčastěji IP adresy, domény a hashe nástrojů malwaru.

Kromě indikátorů kompromitace se zjišťovala zejména doba, po jakou byly systémy infikovány. Obvyklou chybou bývá, že správci obnoví infikované zálohy, a pokud nedojde k úpravám sítě, tak se po připojení infrastruktury k internetu nákaza opět stává aktivní a může znovu vyeskalovat v šifrování dat. Demotivační účinek takové události bývá drastický, pokud vezmeme v potaz, že obnova infrastruktury může zabrat měsíce. To se v případě benešovské nemocnice naštěstí nestalo.

Incident response tým opustil nemocnici až poté, když si byl jist, že jsou nastaveny bezpečné procesy na obnovu stanic, serverů a dat. Po celou dobu konzultoval s administrátory budoucí bezpečnostní politiky, segmentaci, problémy systémů, které nelze aktualizovat, a mnoho dalších témat bezpečnosti a IT obecně. Analýzou dostupných a zajištěných dat nebylo prokázáno narušení důvěrnosti či integrity informací zpracovávaných v zasažených systémech nemocnice.

Doporučení k prevenci a řešení těchto typů incidentů

Vzhledem k výše popsané jednoduchosti šíření těchto typů incidentu a jejich dopadům je velmi důležitá prevence a ochrana. U toho je třeba myslet na dvě základní oblasti. První z nich cílí na to, aby se incident vůbec nestal. Druhá oblast řeší otázku co dělat, až se to stane. Tato oblast by měla být pojata komplexně a neměla by se omezovat pouze na IT procesy.

Preventivní opatření

Základním opatřením při zavádění bezpečnosti je zejména vůle vedení. Pokud taková podpora chybí, je zavádění bezpečnostních opatření velmi složité.

- **Zálohování**
  Je třeba vytvářet pravidelné zálohy, které budou odděleny od provozních systémů a nebudou připojeny do sítě (offline zálohy). Tyto zálohy by měly být ukládány na geograficky oddělených lokalitách. Samotné zálohování však nestačí, zálohy musí být pravidelně testovány. Situaci, kdy při incidentu zálohy nejdou obnovit, nechce zažít asi nikdo.

- **Monitoring**
  Napadení systému nemusí být hned zřejmé, protože útočníci často v síti nějakou dobu vyčkávají. Proto je třeba detekovat a vyhodnocovat činnosti uživatelů a provoz v síti. Vzhledem k tomu, že útočníci jsou schopni nepozorovaně v systému vyčkávat, může dojít i ke kompromitaci záloh. Pokud se organizace o svém napadení nedozví včas, nemusí zálohy vždy pomoci.

- **Segmentace sítě**
  Síť by měla být segmentovaná a kancelářská (internetová) síť by měla být oddělena od ostatních (produkčních) sítí. Měly by být vytvořeny různé segmenty sítě s různými bezpečnostními pravidly a omezeními.

- **Aktualizace softwaru**
  Používání neaktuálního či nelegálního softwaru je poměrně rozšířené a velmi nebezpečné. Bezpečnostní aktualizace je třeba instalovat co nejdříve po jejich vydání. V určitých specifických systémech může být aktualizace složitá či nemožná (technická zdravotnická zařízení jsou často v provozu mnohem déle, než je životní cyklus běžného IT). V takovém případě je třeba mít tato zařízení v separátní síti bez vnějšího připojení a věnovat těmto zařízením zvýšenou pozornost.

- **Odstranění nezabezpečených přístupů**
  Nepotřebné nebo nezabezpečené přístupy by měly být odstraněny a zakázány. Pro vzdálený přístup do systému by měla být používána VPN přiřazená konkrétnímu uživateli. To platí zejména pro dodavatele.

- **Školení uživatelů**
  Obecná pravda, že největší hrozbou jsou uživatelé, stále platí. I nejlepší technické opatření tak může být neúčinné, pokud se střetne s uživateli. Jsou často první, kdo se s útokem setká, a je třeba, aby v takovém případě věděli, jak útok poznat a jak se v takovém případě správně zachovat. Proto je třeba uživatele proškolit alespoň tak, aby si byli vědomi základních rizik v kyberprostoru, základních bezpečnostních zásad, jak vypadá nestandardní chování systému a kam se mají obracet v případě takové situace.

- **Makra v MS Office**
  Makra v MS Office jsou velmi často vektorem útoku. Pokud s nimi uživatelé nemusí pracovat, je vhodné makra úplně zakázat.

Reakce

V případě přípravy reakce na incident je třeba myslet na celou řadu oblastí a každá organizace by primárně měla mít zavedeny plány a opatření pro zajištění kontinuity činností. Vedle plánů a postupů obnovy služeb je třeba mít stanovené správné postupy také v oblasti komunikace. V případě realizace incidentu je třeba komunikovat se zákazníky, dodavateli, médii a v některých případech také policií a regulátory.

- **Kontinuita činností**
  V rámci přípravy na incidenty je nezbytné mít zpracovaný plán kontinuity činností, který poskytne odpověď na otázky týkající se obnovy systému a fungování organizace. Minimální požadavky na řízení kontinuity činností poskytuje např. §15 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. Organizace musí stanovit práva a povinnosti jednotlivých rolí (administrátoři, bezpečnostní role, management), vyhodnotit dopady incidentů v systémech a tyto systémy prioritizovat. Dále je třeba určit minimální úrovně poskytovaných služeb, které jsou přijatelné pro užívání, provoz a správu informačního a komunikačního systému, dobu obnovení chodu, během níž bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního a komunikačního systému, a bodu obnovení dat jako časového období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání. Tato oblast je velmi důležitá. Mnohé organizace se nikdy nezabývaly důležitostí informačních systémů pro jejich činnost, a tak někdy ani neví, jak jsou pro ně důležité.

- **Komunikační strategie**
  Pokud nastane incident, je třeba jej vhodně komunikovat, a to nejen vně, ale také uvnitř organizace. V rámci komunikační strategie je třeba stanovit zejména kdo, o čem, kdy a s kým bude komunikovat.

  - **Kdo** – Je třeba stanovit, kdo bude za organizaci komunikovat. Pokud půjde o více osob, je třeba zajistit jejich koordinaci a sjednotit informace. Zaměstnanci by měli vědět, kdo za organizaci komunikuje s jednotlivými zainteresovanými stranami. Informace, které jednotliví aktéři dostávají, nesmějí být v rozporu. Jediný rozdíl by měl být v úrovni detailu. Pokud lze předpokládat, že o incidentu bude komunikovat také osoba mimo organizaci (např. zástupce zřizovatele), je nezbytné zajistit jejich koordinaci.

  - **O čem** – Každý, kdo má pravomoc za organizaci komunikovat, by měl vědět, o jakých oblastech může hovořit a do jakých detailů. Mělo by být zajištěné pravidelné reportování, které bude dodáno všem ve stejný čas. Ideálním řešením je jednotný kontaktní bod, u kterého se budou informace scházet a který je bude dále předávat např. tiskovému oddělení, vedení společnosti, zaměstnancům a dalším zainteresovaným stranám.

  - **Kdy** – Kritická část celé komunikace tkví zejména v jejím spuštění. Dojde-li k podobnému incidentu s viditelným dopadem (tady zastavení služeb), je více než vhodné o tom ze strany organizace informovat co nejdříve. Pokud organizace promeškává možnost o incidentu informovat jako první, dostává se do nevýhodné pozice, kdy na ni začínají dopadat dotazy médií, veřejnosti a dalších subjektů a ona přestane řídit situaci. Pokud o incidentu bude informovat dostatečně, bude demonstrovat, že o incidentu ví a že jej dokáže vyřešit.

  - **S kým** – Každý zaměstnanec by měl vědět, zda a s kým může o incidentu komunikovat a do jakého detailu.

Komunikace s úřady

Specifickou oblastí je komunikace s úřady. Určité kybernetické incidenty je totiž třeba hlásit relevantním úřadům. Téměř jistá je v případě tohoto typu kybernetického incidentu v nemocnici komunikace s Úřadem pro ochranu osobních údajů. Další organizací, kterou je v takovém případě vhodné oslovit, je Policie ČR. Pravděpodobně se totiž bude jednat o trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 trestního zákoníku.

Pokud je incidentem zasažena organizace, která je zařazena do kritické informační infrastruktury, správce významného informačního systému nebo mezi provozovatele základních služeb podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen zákon), musí být incident oznámen Národnímu úřadu pro kybernetickou a informační bezpečnost. Pokud organizace pod zákon nespadá, povinnost hlásit incident nemá, ale ohlásit jej může. Vládní CERT, specializované pracoviště NÚKIB s technickými kapacitami k řešení incidentů v souladu s písm. l) § 20 b) zákona, přijímá hlášení o kybernetickém bezpečnostním incidentu od orgánů a osob, které pod zákon nespadají, a tato hlášení zpracovává, pokud to jeho kapacity umožňují. Jedná-li se o kybernetický bezpečnostní incident s významným dopadem, poskytuje organizacím dotčeným kybernetickým bezpečnostním incidentem metodickou podporu, pomoc a součinnost. Pokud to tedy kapacity Vládního CERT dovolí, bude se incidentem zabývat a může jej pomoci vyřešit, jako se tomu stalo v případě incidentů v benešovské nemocnici a OKD. Je však třeba dodat, že Vládní CERT není dodavatelem IT systémů, a tedy nenahradí samotné techniky dotčené organizace nebo její dodavatele.

[7] https://csirt.cz/cs/

Incidenty lze také hlásit Národnímu CERTu, který provozuje sdružení CZ.NIC a který má možnost přijímat hlášení kybernetických bezpečnostních incidentů upravenou obdobně jako Vládní CERT (§ 17 písm. l zákona).[7]

Závěr

Podobný incident může zasáhnout prakticky každou organizaci. Ten prosincový v benešovské nemocnici ukázal, že kyberprostor, resp. jeho narušení, může mít vážné dopady na reálný svět, a to i v odvětví, kde je vysoký podíl lidské práce a poměrně nízká automatizace, jako např. zdravotnictví. Význam kyberprostoru a dopady jeho narušení se i díky otevřenému přístupu nemocnice a medializaci dostaly do širšího povědomí veřejnosti. Uvidíme, zda se z incidentu ostatní organizace poučí a zda nakonec dojde ke zvýšení kybernetické bezpečnosti zdravotnických i jiných zařízení.

Adam Kučínský
Vojtěch Sikora

Adam Kučínský

Vede tým specialistů, jejichž hlavní činností je implementace zákona o kybernetické bezpečnosti, nastavení regulatorních požadavků, příprava legislativy a bezpečnostních standardů v oblasti kybernetické bezpečnosti.

Vojtěch Sikora

Člen Vládního CERTu České republiky GovCERT.cz, mezi jehož hlavní úkoly patří řešení kybernetické bezpečnostní incidenty regulovaných subjektů, analýza bezpečnostních opatření nebo hodnocení zranitelností v oblasti kybernetické bezpečnosti.

POUŽITÉ ZDROJE

[1] The Evolution of Emotet: From Banking Trojan to Threat Distributor https://www.symantec.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor
[2] Trickbot | Technical Analysis of a Banking Trojan Malware https://www.sentinelone.com/blog/trickbot-technical-analysis-banking-trojan-malware/
[3] Threat spotlight: the curious case of Ryuk ransomware https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/
[4] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
[5] Vyhláška č. 82/2018 Sb., vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
[6] ISO 22301 – Systém managementu kontinuity podnikání (BCM)
[7] Bezpečnostní doporučení NÚKIB pro administrátory 3.0, https://www.govcert.cz/download/doporuceni/NUKIB_doporuceni_admin_3.0_CB.pdf
[8] Doporučení pro mediální komunikaci, verze 2.0 https://www.govcert.cz/cs/informacni-servis/doporuceni/2699-doporuceni-pro-medialni-komunikaci-verze-2-0/
[9] Contingency Planning Guide for Federal Information Systems https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final
[10] Výroční zpráva OKD, a.s. za rok 2018 https://www.okd.cz/cs/o-nas/vyrocni-zpravy
[11] Výroční zpráva Nemocnice Rudolfa a Stefanie Benešov, a.s. https://www.hospital-bn.cz/o-nas/vyrocni-zpravy/

Skutečnost může být horší než očekávání

Společnost AEC úspěšně eliminovala rozsáhlý phishingový útok na tuzemskou finanční instituci

Finanční instituce napadená mezinárodní hackerskou skupinou se pokoušela vyřešit problém vlastními silami. Nakonec však byla nucena požádat o pomoc tým expertů na kybernetickou bezpečnost. Lidé z AEC dokázali do dvou hodin od seznámení se s případem odhalit nebývalý rozsah incidentu. Útok trval několik týdnů a útočník ovládl značné množství serverů, pracovních stanic i privilegovaných účtů.

zločinecká skupina Cobalt Group **finanční instituce** **zastavení útoku**
ochrana koncových zařízení

Je konec roku 2019. Pro IT administrátora jedné z tuzemských finančních institucí jen další den běžné rutiny. Jako obvykle v tuto dobu monitoruje cvrkot na síti, ale náhle zpozorní.

„Děláš teď něco s doménou?“ obrátí se na kolegu.
„Ne.“
„Tak proč náš admin účet přistupuje k datům na půlce všech firemních serverů?“

Co může stát za nestandardní aktivitou účtu doménového administrátora Active Directory domény? Jedná se o „klíč ke království“ – tenhle účet poskytuje vlastníkovi ve většině případů „absolutní moc“, ať už přímou, či nepřímou, nad celou IT infrastrukturou. Tedy i nad daty a business aplikacemi, které instituce provozuje. Následuje několik dnů interního vyšetřování. Jako nejpravděpodobnější se zpočátku jeví zneužití přístupu třetí smluvní stranou. Ale všichni z outsourcerů, kteří spravují jeden z interních systémů společnosti, na zdvořilý dotaz okamžitě a důrazně odmítají jakoukoli práci mimo sjednaný rozsah. Takže útok? Na nás? Je to vůbec možné?

Když vlastní síly nestačí

Uvedená společnost, která nepatří na tuzemské finanční scéně ke zcela marginálním hráčům, používá pro účely bezpečnostního monitoringu nástroje SIEM (Security Incident and Event Management). Ty jsou z pohledu „log managementu“, tj. sběru a uchovávaní logů, ve výrazně lepší kondici, než je tomu v případě běžného českého průměru. Jen sbírat logy však pro detekci útoku nestačí. Některé z monitorovacích pravidel alertují nestandardní aktivity, ale tyto alerty se ztrácejí mezi množstvím jiných, méně významných upozornění.

Dobře posbírané logy v SIEM systému mohou posloužit k manuálnímu vyšetření incidentu. Oddělení bezpečnosti dané instituce tento systém využívá a nachází podezřelé aktivity v auditních záznamech Active Directory pro jeden účet na serveru, na kterém pracovala třetí strana.

I když společnost není schopná identifikovat vstupní vektor útoku ani jeho rozsah či způsob vzdálené komunikace útočníka, padne rozhodnutí čelit protivníkovi vlastními silami. Pracovníci IT oddělení firmy začínají postupně měnit hesla k vybraným privilegovaným účtům, dočasně vypínají dotčený server a zahajují masivní záplatování zranitelností. Intenzita nestandardních aktivit privilegovaných účtů v prostředí však i přes všechna tato opatření roste. Management finanční instituce je konfrontován se stávající situací a na doporučení rozhoduje bez prodlení

oslovit společnost AEC, která se specializuje na poskytování služeb v oblasti kybernetické bezpečnosti.

A na počátku byl phishing

Přestože uvedená finanční instituce nebyla klientem AEC a bezpečnostní firma nedisponuje nadbytečnými kapacitami, uvolní dočasně několik analytiků svého Cyber Defense Centra. Prvotní seznámení se se situací a s podezřeními na probíhající útok trvá expertům centra zhruba hodinu. Dosavadní opatření proti útoku jsou shledána jako zcela nedostatečná – reset hesel vybraných účtů zkušeného útočníka nemůže zastavit. Rovněž dosud nebyly identifikovány persistenční mechanismy (zadní vrátka), které útočník do prostředí během své déletrvající aktivity umístil.

Vzhledem k tomu, že není jasné ani to, zda útočník aktivně exploatoval (zneužil) zranitelnosti, nemusí být pro danou situaci relevantní ani jejich záplatování. Lidé z AEC přistupují k detailnímu náhledu do SIEM systému. K ověření probíhajícího útoku a k odhalení většiny klíčových podrobností potřebují další dvě hodiny. Zjištění se v mnohém výrazně liší od původních odhadů finanční instituce:

1. Útok začal v tichosti o několik týdnů dříve, než jej instituce zaregistrovala.
2. Útok začal kompromitací pracovní stanice jednoho z uživatelů businessu, nikoli serveru spravovaného třetí stranou. Tento uživatel totiž otevřel phishingový e-mail.
3. Útočník ovládl v prostředí značné množství serverů a pracovních stanic, nikoli jen jeden server.
4. Útočník ovládl v prostředí mnoho účtů (včetně privilegovaných), nikoli jen domnělé účty, u kterých proběhly změny hesel.
5. Mnohé z infikovaných serverů a stanic aktivně komunikují do internetu na CnC (Command and Control). Jedná se o infrastrukturu, která je dle zdrojů používaná skupinou Cobalt Group.

[1] https://www.itp.net/617212-billion-euro-cybercrime-group-strikes-again

Za vším hledej peníze

Hackerská skupina Cobalt Group je známá svými aktivitami po celém světě. Nejčastěji však útočí na finanční instituce ve východní Evropě a Asii. Její sofistikované útoky jsou finančně motivované, specializují se na vyvedení finančních prostředků prostřednictvím napadení ATM (bankomatových) systémů a systému SWIFT. Dle některých odhadů[1] se skupině podařilo tímto způsobem dosud ukrást řádově až 1 mld. $. Používá ke svým útokům mimo jiné i běžně dostupné prostředky, jako např. útočný framework Cobalt Strike, zneužití PowerShell nebo Mimikatz pro extraci hesel (či hashů hesel) v prostředí Windows.

Veškeré tyto nástroje detekovali experti AEC i během stávajícího útoku. Jejich podezření ukazující správným směrem potvrzovala i komunikace s CnC infrastrukturou (DNS doménami a IP adresami) přisuzovaná právě hackerské skupině Cobalt Group. Poté, co se definitivně potvrdilo, že se instituce nachází pod aktivním APT (Advanced Persistent Threat) útokem finančně motivovaného a velmi zkušeného útočníka, byly společně stanoveny tři primární cíle:

1. zastavení útoku,
2. identifikace vstupního vektoru,
3. analýza rozsahu kompromitovaných dat a systémů.

Zastavení útoku

Vraťme se na začátek. Instituce zaregistrovala nestandardní chování ve svém systému. Po nějaké době jej vyhodnotila jako pokus o útok a následně se pokoušela útočníka zastavit vlastními kapacitami. Protože odpovědní pracovníci společnosti neměli v té době představu o celkovém rozsahu útoku, nemohla být jejich snaha o vyřešení incidentu úspěšná.

Útočník velmi záhy jejich nesystematické pokusy zaznamenal a obratem začal používat jiné privilegované účty, pohotově vytvořil nové persistenční mechanismy (viz Obr. 1) a také jinou CnC infrastrukturu na internetu.

Poté už ale převzal taktovku tým z AEC. Základem úspěšného zastavení útoku bylo současné a koordinované provedení několika kroků. Zaprvé byla opakovaně změněna hesla všech (nikoli jen privilegovaných) účtů v Active Directory doméně. Zadruhé byly vypnuty koncové stanice a servery s prokazatelnou komunikací na CnC infrastrukturu útočníka. Zatřetí byly zásadním způsobem upraveny politiky přístupu na internet na webové proxy. Bod čtyři je nejdůležitější – byl nasazen nástroj EPP/EDR (Endpoint Protection Platform/Endpoint Detection and Response), který části útoku zastavil automaticky a části útoku detekoval pro manuální ukončení týmem AEC.

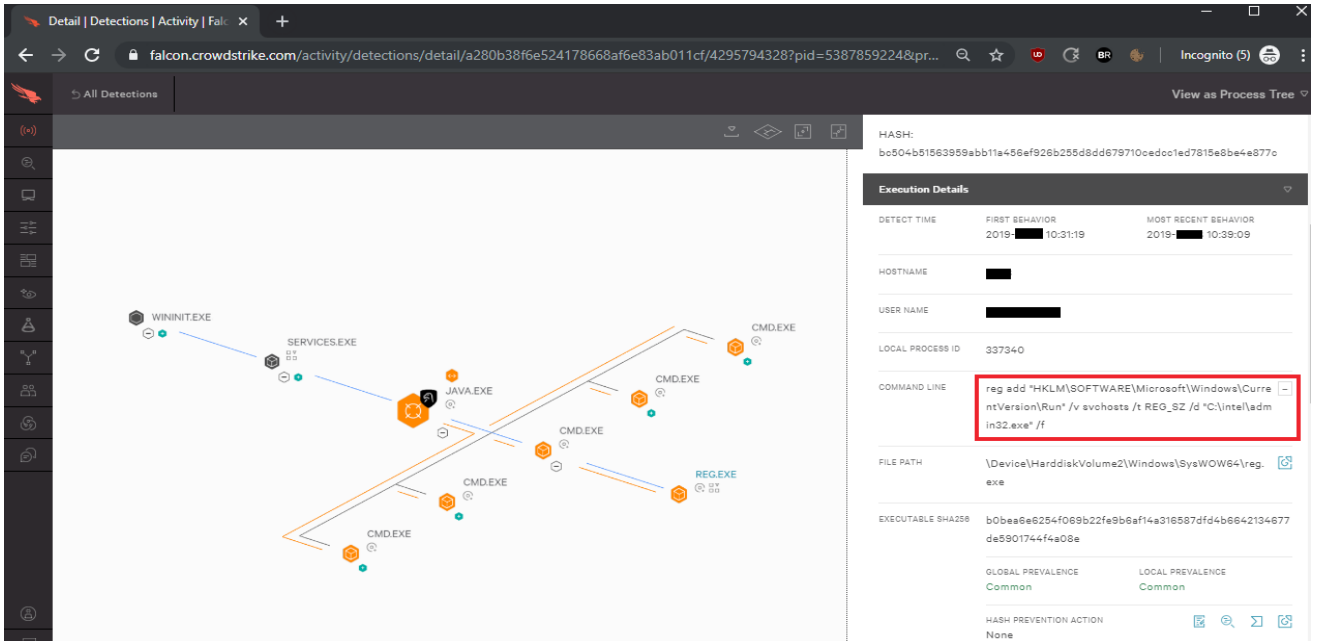
V ideálním případě je při nasazení EPP/EDR proveden restart serveru či koncové stanice. Po restartu má EPP/EDR agent možnost sledovat útočné aktivity při jejich startu, a díky tomu disponuje klíčovou výhodou v podobě výrazně zvýšené schopnosti jejich detekce. Hromadný restart serverů ale neproběhl, proto byly některé persistentní mechanismy, které útočník do prostředí umístil, aktivovány poměrně záhy. Jednalo se o automatický start škodlivého programu po přihlášení konkrétního IT zaměstnance na konkrétním počítači nebo o automatický start při startu serveru.

V době, kdy bylo EPP/EDR řešení nasazeno teprve pár dnů, nebyla jeho schopnost prevence ještě nastavena na stupeň agresivní. Některé kroky útočníka tak dosud nemohly být automaticky zablokované. V rámci agresivní detekce proto bylo nutné útočníka zastavit manuálně. Právě tato fáze byla pro specialisty, kteří se zabývají kybernetickou ochranou, mimořádně zajímavá. Umožnila jim studovat takřka v přímém přenosu kroky a chování útočníka, který si již musel být vědom toho, že se blíží konec jeho „dobrodružství" v prostředí napadené instituce.

Jedním z prvních kroků se útočník pokusil spustit nástroj Mimikatz (pro extrakci hesel a hashů hesel) k jiným účtům. Tento nástroj je natolik známý, že byl zablokován automaticky. Tato aktivita částečně potvrdila účinnost změny všech hesel, protože útočník se usilovně, ale neúspěšně snažil získat přístup k heslům novým. Následně se pokusil vytvořit další zadní vrátka na jednom ze serverů, konkrétně vytvořil nový privilegovaný účet (viz Obr. 2). Je pravděpodobné, že v této fázi byl už pod značným tlakem, protože spěchal a udělal mnoho překlepů.

Velmi zajímavé byly rovněž útočníkovy pokusy odinstalovat EPP/EDR nástroj (viz Obr. 3), což se mu nakonec kvůli neznalosti odinstalačního tokenu nepovedlo. I tyto poslední „záchvěvy" byly zastaveny a zbývající aktivní přístupy útočníka do systému ukončeny.

Po několika týdnech minimálních zásahů do konfigurace (zejména kvůli oprávněně podezřelým aplikacím využívaných IT týmem), byla i prevence nastavena do agresivního režimu. Útok APT probíhající po dobu mnoha týdnů zastavil tým specialistů z AEC během několika dnů. Kompletně eliminována byla činnost útočníka v systému napadené finanční instituce do dvou týdnů od okamžiku, kdy se tým AEC vložil do hry.



Obr. 1: Útočník vytvářející persistenci pomocí jednorázové a vzdálené služby java.exe: automatický start malwaru admin32.exe pomocí klíče v registrech `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` *maskující se za standardní process svchost*

Identifikace vstupního vektoru

Útok byl zastaven, útočník eliminován. Ale co když se pokusí do téhož prostředí vrátit? Je třeba mít naprosto přesnou představu o tom, jak se do systému dostal. Při detailní analýze byly identifikované phishingové e-maily doručené do e-mailových schránek několika zaměstnanců (viz Obr. 5).

Odesílatelem byla věrohodná (a nepodvržená) e-mailová adresa českého telekomunikačního operátora. Adresátem e-mailů pak bylo vždy několik zaměstnanců (současných, ale i bývalých) většiny finančních institucí v České republice. Úspěšně napadená instituce tedy nebyla jediným výlučným cílem útočníka, což je vždy dobrá zpráva. Útočníkovi šlo o peníze, ne o konkrétní instituci, a pravděpodobnost jeho návratu je tedy nižší.

```
net  localgroup Administraotrs guest /add
net  user Guest fXXXXXXX1
net  user Guest /active:yes
net  user Guest
net  localgroup GUests guest /del
net  localgroup GUests guestt /del
net  localgroup Administrators guest /add
```

Obr. 2: Jedny z posledních aktivit útočníka v prostředí. Pokouší se vytvořit zadní vrátka pomocí účtu Guest, který aktivuje a poskytuje práva administrátora. Má naspěch a dělá chyby (viz překlepy).

Odesílatel zprávy žádal příjemce lámanou češtinou o zaplacení faktury připojené údajně v příloze. Text byl zjevně strojově překládán z cizího jazyka, přičemž některé jeho části (např. 18.10.2019r) naznačují, ze kterého. Součástí e-mailu byla i excelová příloha. Po jejím otevření se však žádná avizovaná faktura neobjevila. Naopak se spustil škodlivý Visual Basic script, který začal okamžitě komunikovat na CnC server útočníka na internetu. Obr. 4 ukazuje, jak taková komunikace vypadá v případě, kdy ji webová proxy blokuje, a v případě, kdy ji neblokuje.

Postupně se ukázalo, že několik zaměstnanců instituce přílohu otevřelo, zachránila je však webová proxy. Ale u jednoho z uživatelů byla aplikována výjimka v nastavení proxy a komunikace na CnC server na internetu byla povolena. Poté, co útočník rozeslal stovky phishingových e-mailů, mu tato jediná skulinka umožnila vkročit do prostředí. Jeho následné kroky zanechaly množství stop: nestandardní komunikace do podezřelých států, blokace některých kroků antivirem nebo přihlášení na vysoce privilegovaný účet Active Directory. To vše během pár desítek minut od úvodní infekce. Některé z těchto stop byly dostupné v bezpečnostním monitoringu SIEM, ale v závalu dalších alertů zůstaly nepovšimnuty.

Jedním z protiopatření zabraňujících útočníkovi použít uvedený vektor k opakovanému vstupu do prostředí je zmiňovaný nástroj EPP/EDR. Jeho účinnost byla ověřena i při masivních phishingových kampaních na české finanční instituce v prosinci 2019. Navzdory intenzivní osvětě se mezi zaměstnanci zde pojednávané finanční instituce objevují i nadále tací, kteří otevírají škodlivé přílohy podvržených e-mailů. Veškeré tyto pokusy jsou však naštěstí včas zablokovány EPP/EDR řešením bez postranních false positive hlášení.

- File Name: \Device\HarddiskVolume2\ProgramData\Package Cache\{0d38521f-fdee-4bf0-a283-e8f74b153fe8}\WindowsSensor.x64.exe
- CommandLine: "C:\ProgramData\Package Cache\{0d38521f-fdee-4bf0-a283-e8f74b153fe8}\WindowsSensor.x64.exe" -burn.clean.room="C:\ProgramData\Package Cache\{0d38521f-fdee-4bf0-a283-e8f74b153fe8}**WindowsSensor.x64.exe**" -burn.filehandle.attached=328 -burn.filehandle.self=336 **/uninstall**
- SHA256: d81da6de19f0dd5bcdcaeffb760facbb2186138aa1988806292dd45ccf2ee681
- MD5: 4584c277cc9331d9097c199f2dddfa5e
- PID: 5972
- Parent ProcessId: 110552480858

Obr. 3: Útočník zaregistroval běžícího EPP/EDR agenta a neúspěšně se ho snaží odinstalovat

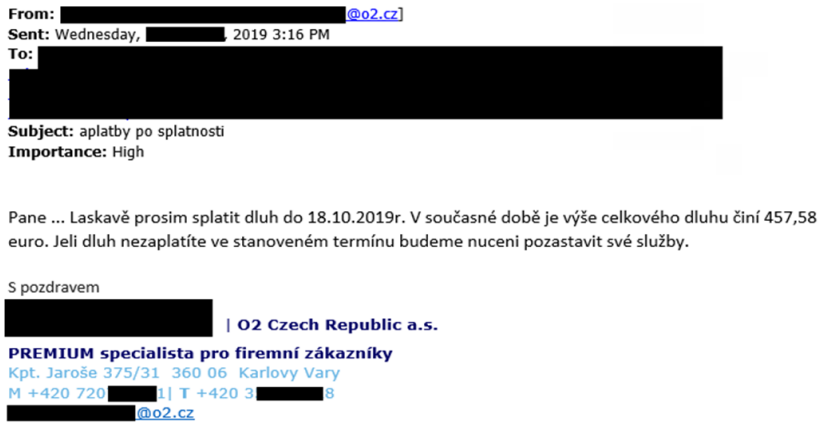
```
<30>XXX XX XX:18:16 XXX-XX mwg: LEEF:1.0|XXXXXX|Web
Gateway|7.8.2.11.0|22|devTime=15XX022296000|src=XXX.XX.X.133|usrName=XXXXXXXX|httpStatus=403|
dst=XX.XX.12.4|urlCategories=Business|blockReason=Media type
blocked|url=https://www.octetfruitsllc.com/vendor/phpunit/phpunit/src/Util/PHP/avatar.hlpv

<30>XXX XX XX:18:30 XXX-XX mwg: LEEF:1.0| XXXXXX |Web
Gateway|7.8.2.11.0|0|devTime=15XX022310000|src=XXX.XX.X.27|usrName=|httpStatus=200|dst
=X.X.X.X|urlCategories=|blockReason=|url=https://www.octetfruitsllc.com

<30>XXX XX XX:20:36 XXX-XX mwg: LEEF:1.0| XXXXXX |Web
Gateway|7.8.2.11.0|0|devTime=15XX022436000|src=XXX.XX.X.27|usrName=|httpStatus=200|dst
=X.X.X.X|urlCategories=|blockReason=|url=https://0345432456.info
```

Obr. 4: Pro většinu uživatelů, kteří otevřeli phishingovou přílohu, je komunikace s CnC infrastrukturou zablokovaná. Jeden uživatel má ale nezdokumentovanou výjimku, takže jeho PC může neautentizovaně komunikovat s proxy a proxy nedešifruje HTTPS komunikaci.

Bez ohledu na přetrvávající potíže týkající se přístupu některých zaměstnanců k podezřelým e-mailům lze ve věci identifikace vstupního vektoru do prostředí napadené instituce konstatovat, že tým AEC expertů kompletně identifikoval průběh útoku a detailně popsal přesný způsob vniknutí do systému a rozsah aktivit, které v něm útočník prováděl.


From: [redacted]@o2.cz]
Sent: Wednesday, [redacted], 2019 3:16 PM
To: [redacted]
Subject: aplatby po splatnosti
Importance: High

Pane ... Laskavě prosim splatit dluh do 18.10.2019r. V současné době je výše celkového dluhu činí 457,58 euro. Jeli dluh nezaplatíte ve stanoveném termínu budeme nuceni pozastavit své služby.

S pozdravem
[redacted] | O2 Czech Republic a.s.
PREMIUM specialista pro firemní zákazníky
Kpt. Jaroše 375/31 360 06 Karlovy Vary
M +420 720[redacted]1| T +420 3[redacted]8
[redacted]@o2.cz

Obr. 5: Phishingový e-mail, který obdrželi zaměstnanci finanční instituce

Analýza rozsahu kompromitovaných dat

Jednou z důležitých otázek bylo, jaká data byla kompromitována. Mohlo se jednat o neoprávněnou modifikaci (tj. narušení integrity) nebo o neoprávněný náhled (tj. narušení důvěrnosti). Jakkoli je tato otázka zajímavá a důležitá, není na ni možné ani s odstupem podat jednoznačnou a důkazy podloženou odpověď. Mezi úvodní kompromitací prostředí a zastavením útoku uběhly řádově týdny. Útočník přistoupil k mnohým interním systémům, např. e-mailovým systémům a sdíleným složkám s pracovními dokumenty některých oddělení společnosti. Pro pohyb v prostředí využíval standardních služeb Microsoft prostředí, např. administrátorské shary IPC$, vzdálené plánování služeb nebo obfuskované Powershell skripty. Útočník využíval privilegované účty, které byly (oproti best-practice) používané pro rutinní práci IT týmu a některých IT systémů. Odlišení aktivit útočníka od standardního chodu IT proto bylo složité, někdy dokonce zcela nemožné.

Na otázku, jaká data byla kompromitována, můžeme odpovědět následovně: z auditních stop dostupných v rámci vyšetřování nebyly nalezeny důkazy o narušení integrity dat v databázích a aplikacích. Rovněž nebyly nalezeny důkazy o extrakci dat z důvěrných systémů mimo instituci.

Jak problémům předcházet aneb zašněrujte si tkaničky u bot

Ochrana koncových stanic je často opomíjená, protože při analýzách rizik toto aktivum buď zcela chybí, nebo jsou jeho business dopady (a potažmo související rizika) hodnocené jako nízké. Jsou to ale právě koncová zařízení, která mnohdy útočníkovi umožní prvotní vstup do prostředí, např. formou phishingu. Nelze se spoléhat na to, že bezpečnostní opatření budou plně funkční vždy a za každých okolností.

- Mnoho phishingových e-mailů bylo zastaveno na vstupní e-mailové bráně, ale ne všechny.
- Většina zaměstnanců v tematizovaném případě e-mail neotevřela, ale našli se tací, kteří ano.
- Většina úvodních pokusů o komunikaci s CnC serverem byla zablokovaná, pro jednoho uživatele však nikoli.
- Některé pokusy ze strany útočníka byly zablokovány lokálním antivirem, ale ne všechny.
- Bezpečnostní dohledový systém SIEM některé části útoku detekoval v reálném čase, ale tyto důležité alerty zanikly v běžném provozním šumu.

IT hygiena při využívání privilegovaných účtů je důležitá nejen pro provoz, ale také pro bezpečnost. Práce s těmito účty (administrátorské, servisní, aplikační atd.) by měla mít jasná pravidla s nastavenou kontrolou jejich dodržování. Předešlo by se tak problémům při investigaci, kdy byl v jednom čase na stejném serveru využíván tentýž účet jak útočníkem, tak interním IT zaměstnancem (nejednalo se samozřejmě o tu samou personu).

Při segmentaci sítě je vhodné rozlišovat nejen servery od koncových zařízení, ale také jednotlivé aplikace, prostředí (produkční, testovací, vývojové), organizační strukturu (IT a non-IT) atd. Útočník měl v tomto případě příliš jednoduchou cestu – mohl se vydat libovolným směrem, kterým se mu zachtělo. Ale možná to úplně nejdůležitější doporučení se týká kontinuálního vzdělávání zaměstnanců. Ti by měli být mimo jiné schopni odlišit podvržený e-mail, neotevírat ho, resp. nebát se ohlásit otevření podezřelé přílohy bezpečnostnímu týmu.

Závěrem je třeba konstatovat jeden nezpochybnitelný fakt. Pro běžnou firmu či instituci bez ohledu na její velikost či obor zájmu je velmi obtížné odolat motivovanému útočníkovi, který má pro financování svých aktivit k dispozici ukradenou miliardu dolarů.

Ale i přes veškeré komplikace, nejasnosti a nástrahy nakonec pro každou společnost existuje jeden úplně poslední a poněkud drsný důvod, proč se řídit poznatky vyplývajícími z našeho textu a ostatními best-practise doporučeními. Pojednává o tom moc hezký příběh. Dva poutníci jdou po poušti, když tu spatří, jak se k nim z dáli řítí hladový lev. Jeden z nich se bleskurychle sehne a začne si co nejpevněji utahovat tkaničky u bot. *„Myslíš, že ti pomůže utéct mu?“* ptá se ho ten druhý. *„Asi ne. Ale mně stačí, když budu rychlejší než ty.“*

Martin Hlaváč
martin.hlavac@aec.cz

Martin Hlaváč

Pracuje v oblasti informační bezpečnosti od roku 2006. Věnoval se celému spektru témat počínaje tvorbou bezpečnostních politik a standardů přes zabezpečení integrity kritických finančních toků až po bezpečnostní monitoring a reakci na incidenty. V posledních letech se zaměřuje především na návrh, implementaci a provoz služeb souvisejících se SOC (Security Operations Center) a IR (Incident Response). V současné době působí jako technický garant služeb CDC (Cyber Defense Center) ve společnosti AEC a.s.

akademie ICT managementu

Tate International

TATE International, s.r.o.,
vydavatel časopisu DSM – data security management

p o ř á d á

Systém vzdělávacích kurzů usnadní současnému CIO plnění jeho dvojrole. Na jedné straně se od CIO očekává schopnost komunikovat s vrcholovým managementem a obchodními jednotkami o podpoře a realizaci strategických cílů (ICT enablement and alignment), na druhé straně statutární orgány předpokládají, že CIO je manažer orientovaný na efektivní řízení ICT provozní továrny (ICT management and control). Kombinace těchto dvou požadavků klade na CIO v moderní společnosti nebývalé nároky.

10. 3. – 11. 3. 2020 – Strategie ICT v 21. století I.
31. 3. – 1. 4. 2020 – Digitalizace
21. 4. – 22. 4. 2020 – Strategie ICT v 21. století III.
12. 5. 2020 – SLA v praxi
4. 6. 2020 – Právo a IT

Š k o l e n í n a a k t u á l n í t é m a t a :

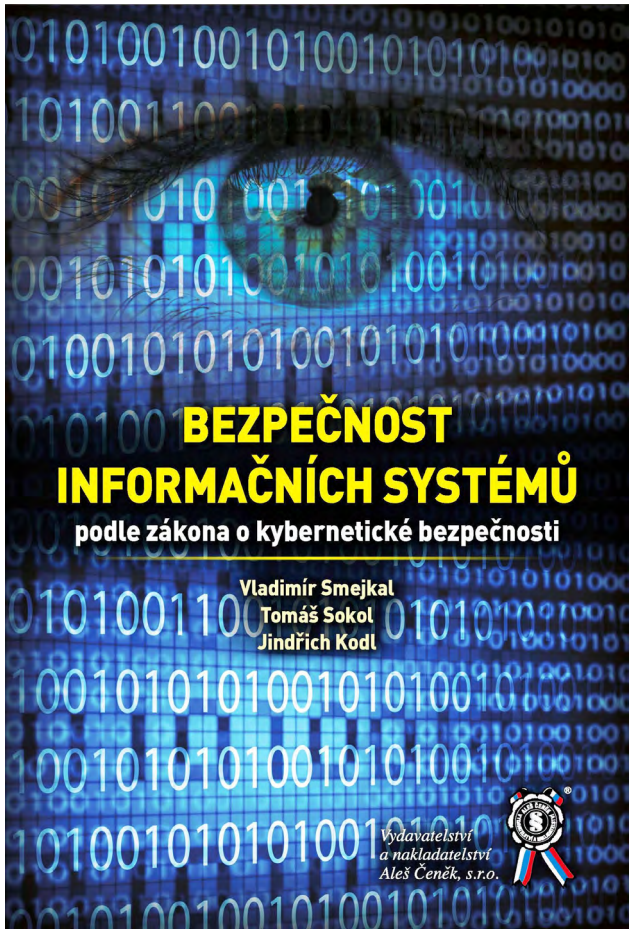
Kyberbezpečnost, Strategie ICT v 21. století II., Právo IT, Umění řízení služeb aneb SLA v praxi, Datová centra, DevOps, Business Continuity Management, Trendy koncových zařízení, Právnické minimum pro IT – eIDAS, Kvalita dat a její řízení, Strategie ICT v 21. století III B (Podniková architektura), Akceptace SW (právní servis včetně), Digitální transformace apod.

Sledujte www.tate.cz

Tel.: +420 737 215 220 • **www.tate.cz** • e-mail: aict@tate.cz

Bezpečnost informačních systémů
podle zákona o kybernetické bezpečnosti

Vladimír Smejkal, Tomáš Sokol, Jindřich Kodl



Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „ZKB“) byl schválen 23. července 2014 a nabyl účinnosti dnem 1. ledna 2015, tedy před pěti lety. Od té doby byl již šestkrát novelizován a jeho klíčový prováděcí předpis, vyhláška o kybernetické bezpečnosti z roku 2014, byla v roce 2018 nahrazena zcela novým zněním č. 82/2018 Sb. Již tyto skutečnosti by byly dostatečným důvodem pro vydání recenzovaného díla. Neméně zásadním důvodem je však skutečnost, že praxe po celou dobu účinnosti ZKB pociťovala absenci skutečně prakticky orientovaného pojednání, které by naplnilo mezeru mezi suchou literou zákona a vyhlášky a často vyzývanými normami řady 27000. Třetím důvodem pak jsou stále naléhavější otázky týkající se právní odpovědnosti za porušování povinností uložených ZKB.

Všechny tyto tři důvody se promítly do koncepce knihy, která sestává z několika tematických oblastí. V prvé řadě je to podrobný výklad jednotlivých ustanovení ZKB a na ně navazujících prováděcích předpisů, zejména nové vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb., v kapitole čtvrté. Jde o výklad komplexní, podrobný a prakticky orientovaný. Příkladem může být kapitola 4.5.3, kterou lze využít např. ve velmi aktuální (a často problematické) oblasti, jakou je bezesporu zadávání veřejných zakázek, neboť autoři v této kapitole upozorňují na novelu ZKB provedenou zákonem č. 205/2017 Sb. jakožto nepřímou novelu zákona o veřejných zakázkách obsaženou v § 4 odst. 4 a odst. 7 ZKB.

Další část knihy obsahuje v kapitole 5. neméně důležitý text pojednávající o normách a metodikách pro bezpečnost IS/IT. Autoři zde popisují mezinárodní i národní organizace pro standardizaci, velmi podrobně rekapitulují vývoj mezinárodních standardů a poté věnují pozornost především normám ČSN ISO/IEC řady 27000, jež jsou dnes považovány za hlavní, byť nikoliv jediný, normativní zdroj informací pro budování bezpečnosti IS/IT. Uvedeny jsou rovněž metodiky jako COBIT, ITIL a další, které mají přesah k manažerským a organizačním aspektům zajišťování kybernetické bezpečnosti. Navazující kapitola 6. popisuje řízení bezpečnosti informací a návrh systému řízení bezpečnosti informací (ISMS).

Třetím hlavním tématem tohoto díla je právní analýza důsledků vyplývajících ze ZKB, jež se nachází v posledních dvou kapitolách. Ty pojednávají o trestní a přestupkové odpovědnosti fyzických i právnických osob pro případ nesplnění povinností vyplývajících ze ZKB a o občanskoprávních aspektech bezpečnosti IS/IT z hlediska odpovědnosti za škody způsobené porušením ZKB.

Aby byl výklad komplexní a dostatečně srozumitelný, je kniha doplněna kapitolami obsahujícími seznam zkratek, jichž je v oblasti kybernetické bezpečnosti velké množství. Teoretiky i praktiky jistě zaujme část, v níž jsou definovány základní pojmy související s danou problematikou, jakými jsou „bezpečnost“, „kybernetická bezpečnost“, či „prvky kritické infrastruktury“. Následuje vymezení právního rámce kybernetické bezpečnosti, počínaje ZKB a souvisejícími předpisy, krizovým zákonem, zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti, jakož i dalšími právními předpisy, které mají souvislost s problematikou kyberbezpečnosti. Velmi zajímavá je kapitola třetí popisující trestné činy, jež je možné spáchat v kyberprostoru, neboť pouze tehdy, pokud víme, před čím se máme chránit, může být naše obrana úspěšná.

Výklad knihy je doplněn samostatnou kapitolou sedmou, pojednávající o řízení rizik, což je alfa a omega při zajišťování kybernetické bezpečnosti. Výklad logicky vychází z požadavků ZKB a vyhlášky o kybernetické bezpečnosti, ale zohledňuje i další normy a metodiky, které jsou v praxi používány. Nechybí ani obsáhlý seznam použité literatury, jako cenný zdroj dalších informací.

Na rozdíl od častého provedení „zákonů s komentářem“ v podobě doslovné citace zákona a (v lepším případě parafráze) důvodové zprávy je recenzovaná kniha skutečným výkladem dané problematiky, založeným na rozsáhlých zkušenostech autorů – známých odborníků s dlouholetou praxí. Toto je patrné i na místy značně hutném stylu podání rozebírané problematiky, kdy v některých kapitolách – zejména 4. až 6. – by bylo možno doporučit ještě podrobnější výklad pro ty, kdo jsou v dané oblasti spíše začátečníky. Naopak je třeba ocenit, že autoři nepodlehli současnému trendu hypertrofického zařazování problematiky GDPR prakticky do všech odborných publikací z nejrůznějších oborů.

Kniha je po odborné i jazykové stránce na vysoké úrovni a poznatky v ní uvedené odpovídají současnému stavu poznání v této oblasti, jakkoliv – vzhledem k tématu – nelze pochybovat o tom, že v dalším vydání bude třeba zohlednit novinky z legislativy (např. Nařízení Evropského parlamentu a Rady (EU) 2019/881 o agentuře ENISA, Evropské agentuře pro kybernetickou bezpečnost a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií, tzv. „akt o kybernetické bezpečnosti“, nejnovější novela ZKB provedená zákonem č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů) i z praxe (zejména nové poznatky a zkušenosti s dalším vývojem kybernetické kriminality a kyberterorismu).

Všichni, kdo se jako správci, či zpracovatelé (poskytovatelé služeb, dodavatelé atd.) podílejí na zajišťování bezpečnosti IS/IT, zejména pak těch IS, které spadají do působnosti ZKB, by knihu měli nejen mít ve svých knihovnách, ale především na svých nočních stolcích i pracovních stolech – měli by ji totiž skutečně jednak pečlivě prostudovat a zejména ji používat v každodenní praxi. Potenciálně nebezpečnými však pro tyto osoby mohou být kapitoly o právní odpovědnosti. Zjistí z nich totiž, že důvodů pro praktickou aplikaci trestní odpovědnosti fyzických i právnických osob pro porušení povinností uložených ZKB je skutečně mnoho, k čemuž bohužel přispívá i (z tohoto hlediska nikoliv zcela ideální) dikce některých ustanovení ZKB.

Je třeba zdůraznit, že dílo není zdaleka určeno pouze pro povinné osoby podle ZKB, tedy pro správce a provozovatele informačních a komunikačních systémů kritické informační infrastruktury, správce a provozovatele významných informačních systémů a informačních systémů základní služby, případně další povinné osoby podle § 3 ZKB, ale pro všechny správce a provozovatele všech informačních systémů, které mají větší než zcela okrajový význam. To samozřejmě neznamená, že tito ostatní správci a provozovatelé musejí splnit všechny povinnosti vyplývající ze zákona a vyhlášky o kybernetické bezpečnosti a aplikovat všechna doporučení obsažená v knize, nicméně jako zdroj inspirace lze i jim knihu výše uvedené trojice autorů plně doporučit. Varovné příklady z nemocnic a jiných, doposud z tohoto hlediska spíše přehlížených organizací, budiž motivací více než vysokou.

Miroslav Uřičař
miroslav.uricar@legalite.cz

Titul:	Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti
Autor:	SMEJKAL Vladimír, SOKOL Tomáš, KODL Jindřich
Vydal:	Nakladatelství Aleš Čeněk, Plzeň, 2019
Počet stran:	378 stran
ISBN:	978-80-7380-765-8
Cena:	490 Kč

Malvertising: Nenápadná hrozba na vzestupu

Internet je doslova zahlcený reklamními inzeráty. Uživatelé je už skoro nevnímají. Této nepozornosti stále častěji využívají útočníci k získání citlivých dat nebo k infikování uživatelského zařízení.

Lákavé reklamní nabídky mezi sebou uživatelé často sdílí i na sociálních sítích. Často propagují výraznou slevu. V záplavě podobných zpráv je pro útočníky poměrně snadné skrýt skutečné úmysly. Tedy šíření malwaru. Odborníci označují tento typ útoku jako malvertising. Termín spojuje výrazy malware (škodlivý kód) a advertising (reklama).

Brazilský malvertising obsahoval bankovní trojan

Velmi důmyslnou malvertisingovou kampaň analyzoval nedávno český tým reverzních inženýrů ze společnosti ESET. Podvodné reklamy na sociálních sítích v Latinské Americe (především v Brazílii a Mexiku) šířily bankovního trojského koně, kterého analytici pojmenovali Mispadu. Šířil se právě podvodnými reklamami na sociálních sítích a spamem, který je v posledních letech ve světě nejčastějším způsobem šíření malwaru vůbec.

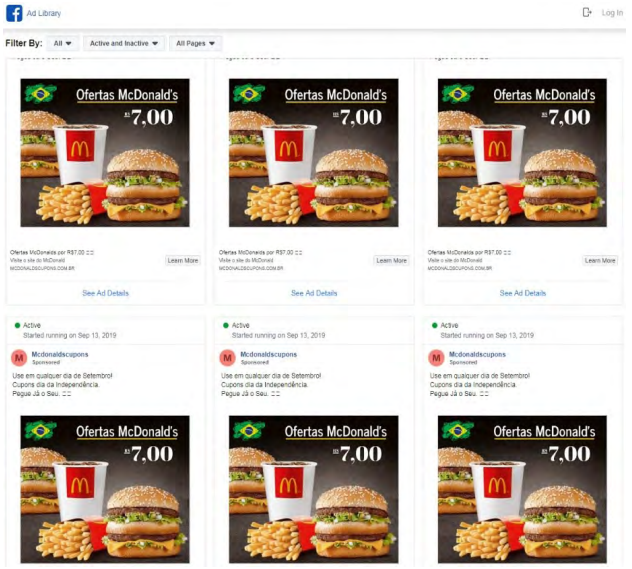
V případě Mispadu byly podvodné reklamy umístěny na Facebooku. Útočníci svým obětem slibovali falešné slevové kupony do fastfoodového řetězce McDonalds. V popisu pak apelovali na časový limit – fiktivní kupony byly vydány k brazilskému dni nezávislosti.

Z inzerátu se uživatel prolinkem dostal na podvodné webové stránky, které byly velice dobře zpracované a na rozdíl od některých jiných falzifikátů byly správně gramaticky včetně grafiky zneužitého fastfoodu. Jakmile uživatel kliknul na tlačítko „Vygenerovat kupón“, stáhl si do počítače malware ve formě instalačního MSI balíčku zabaleného do ZIP archivu. K infikaci zařízení došlo po spuštění zmíněného MSI souboru. Na jedné z podvodných stránek jsme zaznamenali téměř 100 000 otevření a to jen v Brazílii.

Konkrétní verze trojského koně a jeho instalátoru se lišila podle země, kde zrovna probíhal útok.

Na některých infikovaných zařízeních trojský kůň instalovat doplněk pro prohlížeč Google Chrome s názvem Security System 1.0. Doplněk měl nicméně jiný účel: sledoval vybraná klíčová slova ve formulářích na internetu jako text, e-mail, heslo či bezpečnostní kód z platební karty, tzv. CVV. Obsah těchto polí sbíral a odesílal útočníkům na kontrolní server. Zjevným cílem této komponenty malwaru tedy bylo odcizení informací o platebních kartách obětí.

Podobným způsobem se doplněk pokoušel kompromitovat platební platformu Boleto, která je v Brazílii velmi populární. Tato platforma využívá mechanizmus podobný našim složenkám, kdy každá z nich obsahuje unikátní identifikátor a čárový kód. Malware nahrazoval tyto údaje tak, aby platba přišla na účet útočníka.



Malvertising v České republice

Útoky prostřednictvím inzerátů se objevují v pravidelných vlnách i v českém prostředí. Nicméně prozatím analytici takto důmyslnou kampaň nezaznamenali. V našem prostředí se setkáváme především s phishingem, který zneužívá metody sociálního inženýrství, aby od uživatelů získal citlivá data, případně je zmanipuloval k odběru placených komunikačních služeb.

Stejně jako v případě Mispadu i v České republice útočníci zneužívají známé a důvěryhodné značky, často jsou to supermarkety, například Penny, Lidl, Kaufland a další. Nejčastěji se jedná o nabídku na slevové kupony v řádech tisíci korun, které může „omezený“ počet uživatelů získat zdarma.

V jedné české kampani, kterou analytici zachytili v srpnu, se uživatel prokliknul z reklamního inzerátu na podvodnou stránku, která zneužívala vizuální identitu značky Penny a byla napsána velmi dobrou češtinou. Po uživateli vyžadovala vyplnění krátkého dotazníku a telefonního čísla. Následně stránka požadovala sdílení na Facebooku a odeslání SMS ve znění ANO. Takto se uživatel přihlásil k odběru placeného obsahu v hodnotě 90 Kč měsíčně od nizozemské společnosti. Jediné podezření mohly vyvolat podmínky akce napsané drobným písmem. Ty ale uživatel mohl snadno přehlédnout.

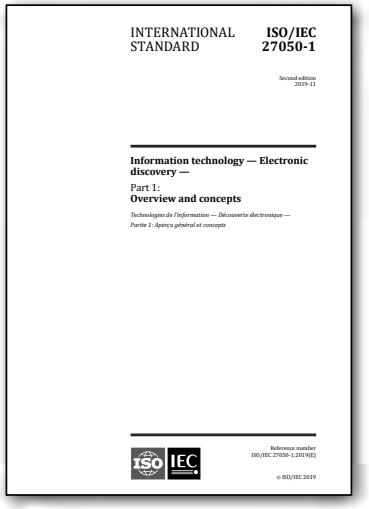
Chránit uživatele dokáže nejen vlastní pozornost

Podobné reklamy vypadají na první pohled přesvědčivě. Útočníci v rámci malvertisingu používají pokročilé manipulativní techniky. Například apelují na to, aby uživatel reagoval rychle, protože kuponů je omezené množství nebo jsou časově omezené. Prakticky vždy zneužívají renomé známých značek či produktů. Inzeráty samotné bývají dobře přeložené do mateřštiny potenciálních obětí. Propracované kampaně útočníkům vynášejí, což dokládá i fakt, že jsou ochotni inzeráty předem sponzorovat.

Pokud samotná podvodná stránka neobsahuje malware, je první úrovní obrany pozornost uživatele. Tou další je pak bezpochyby kvalitní bezpečnostní software, který je schopen podobné podvody zablokovat. Experti přesto apelují na uživatele, aby si lákavé akce raději prověřili, případně si vždy přečetli podmínky, které podle zákona firma musí uvádět.

Ondřej Šafář
ondrej.safar@eset.cz

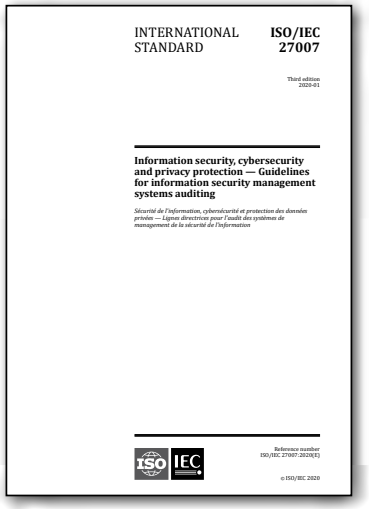
Aktuální normy a publikace o bezpečnosti



Zajišťování elektronických stop

Druhé revidované vydání *ISO/IEC 27050-1:2019 – Information technology – Electronic discovery – Part 1: Overview and concepts* bylo zveřejněno v listopadu 2019. Hlavní změny spočívají v aktualizaci odkazů na normy této řady a sladění terminologie. Normy jsou zaměřeny na postupy zajišťování a zkoumání elektronicky uložených informací, přičemž první část definuje pojmy spojené s identifikací, shromažďováním, zpracováním a analýzou elektronicky uložených informací. Sérii tvoří celkem čtyři normy, kde kromě první části byly publikovány *ISO/IEC 27050-2:2018 Guidance for governance and management of electronic discovery* a *ISO/IEC 27050-3 Code of practice for electronic discovery. ISO/IEC 27050-4 ICT readiness for electronic discovery* je stále ve verzi draft s předpokládaným termínem publikace v roce 2021.

https://www.iso.org/



Doporučení k auditu ISMS

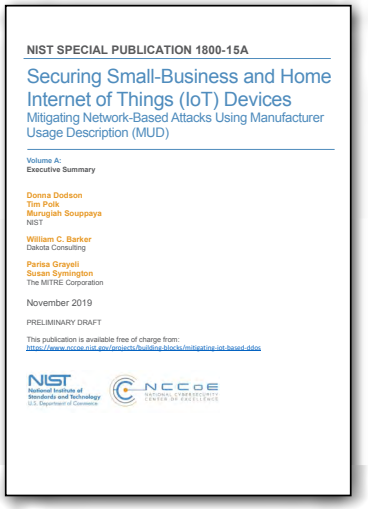
V lednu 2020 bylo publikováno třetí revidované vydání *ISO/IEC 27007:2020 – Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing*, v němž byla tato norma uvedena do souladu s nejnovější verzí ISO 19011: 2018 – *Guidelines for auditing management systems*. Norma obsahuje doporučení pro přípravu programu auditu systému řízení bezpečnosti informací (ISMS) a kontrolu shody s požadavky ISO/IEC 27001:2013. Obsahuje také doporučení a požadavky na kompetence auditorů ISMS, jakož i kritéria pro jejich hodnocení. Obsahově norma čerpá zejména z ISO 19011:2018. V rámci výčtu jednotlivých požadavků se buďto přímo odkazuje na ISO 19011 nebo uvádí požadavky specifické pro auditování ISMS.

https://www.iso.org/

Rámec pro sdílení informací

Letošní novinkou v řadě norem připravovaných technickou komisí ISO/TC 292 Security and resilience je standard *ISO 22396:2020 – Security and resilience – Community resilience – Guidelines for information exchange between organizations*. Činnost ISO/TC 292 je zaměřena na přípravu norem a doporučení pro zvýšení bezpečnosti a odolnosti společnosti. ISO 22396 poskytuje doporučení pro sdílení informací mezi organizacemi. Cílem spolupráce je identifikovat a iniciovat kroky ke zvýšení bezpečnosti a snížení potenciálních zranitelností. Výměna informací o možných rizicích a zranitelnostech pomáhá zvýšit účinnost a efektivitu organizací při řešení obdobných incidentů a mimořádných událostí. Norma zahrnuje zásady, rámec a proces výměny informací. Pro označování a sdílení informací s třetími stranami využívá klasifikaci podle TLP (Traffic Light Protocol).

https://www.iso.org/



Bezpečný provoz IoT zařízení

S tím, jak roste popularita zařízení internetu věcí (IoT), rostou také obavy o jejich bezpečnost. Jedním z nových standardů, které se věnují rizikům spojeným s provozem IoT, je také *SP 1800-15 Securing Small Business and Home Internet of Things (IoT) Devices*. Popisuje pro vývojáře a implementátory IoT přístup založený na standardu MUD (Manufacturer Usage Descriptions), založený na automatickém omezení síťové komunikace výhradně na provoz, který IoT zařízení vyžadují k plnění svých zamýšlených funkcí. Cílem MUD je, aby se IoT zařízení chovala pouze tak, jak bylo zamýšleno jejich výrobcem. Standard připravilo americké národní centrum pro kybernetickou bezpečnost NCCoE ve spolupráci s NIST.

https://csrc.nist.gov/publications/

Ing. Libor Široký, CISM, CRISC, AMBCI, *siroky@rac.cz*

Ohlédnutí za Svatomartinskou husou

Metamorfosa

Bankovní identita schválena. Ano, přesně tři měsíce poté, co na téma bankovní identity „Zákon o právu na digitální služby“ diskutovali Jan Blažek (ČSOB) a Vladimír Dzurilla (vládní zmocněnec pro IT a digitalizaci) na tradičním diskusně-společenském setkání Metamorfosa. Ve svém příspěvku představili legislativní novinku, kterou vzácně podpořili poslanci všech sněmovních klubů a která je po dlouhé době významným krokem k digitalizaci státní správy. Bankovní identita usnadní život až 5 milionům občanů, klientům českých bank, kteří získají snadný přístup k on-line službám soukromého sektoru i e-Governmentu, konkrétně Portálu občana.

Setkání u příležitosti oslavy svátku sv. Martina se uskutečnilo 12. listopadu 2019 v prostorách Klášterního pivovaru Strahov. Důstojné prostředí historického pivovaru, jehož počátky sahají až do 13. století, umožnilo vychutnat si výborně připravená husí stehna nejen se svatomartinskými víny, jak velí tradice, ale i s místními pivy Sv. Norbert. Ti, kteří upřednostňují k chutnému jídlu i posezení zlatavý mok, si jistě nenechali ujít prohlídku minipivovaru s odborným výkladem v rámci doprovodného programu.

Dalším z odborných témat večera byly výsledky průzkumu veřejného mínění na téma „Digitalizace, bezpečnost a etika“, se kterými hosty seznámil Pavel Východský (ČSOB Pojišťovna). Výsledky jenom potvrzují aktuálnost digitalizace a potřebu zodpovědného přístupu k tomuto tématu. Více informací v článku Průzkum stavu digitalizace, který naleznete v tomto čísle.

Na diskusní část večera volně navázala část společenská, která umožnila v příjemném prostředí pokračovat jak v odborných diskusích, tak přejít k neformálním tématům s kolegy. Živě diskutující skupinky zúčastněných, které nezmohla ani vydatná večeře a degustace Sv. Norberta, příjemná atmosféra a zajímavá témata jsou motivací pro další setkání. Za organizaci patří díky průvodci večerem Lukáši Klášterskému (Group CTO Governance, Erste Group a předseda PV IS2 2020), partnerům akce ICZ, Cisco, insighti, PwC, T-Mobile i celému organizačnímu týmu.

Radek Komanický

AFCEA ■ ARMED FORCES COMMUNICATIONS & ELECTRONICS ASSOCIATION

- Dne 23. dubna 2020 se uskuteční v Mladé Boleslavi třetí „FINÁLOVÉ“ kolo čtvrtého ročníku Středoškolské soutěže v kybernetické bezpečnosti. Sledujte *www.kybersoutez.cz*.
- V květnu 2020 bude pracovní skupina Inteligence pořádat v pořadí již třetí seminář na téma „Od dat ke znalostem“.
- Sekce komunikačních a informačních systémů Ministerstva obrany České republiky ve spolupráci s Českou pobočkou AFCEA za odborné podpory Vojenského technického ústavu, s.p., který je zároveň generálním partnerem celé akce, pořádá ve dnech **28.–29. 5. 2020** v pořadí již IV. konferenci Spojovacího vojska Armády České republiky. Konference s podtitulem „Cesta k federalizaci systému C2 AČR – i nové technologie – nadhledy a rozhledy“ proběhne v areálu Lipníku nad Bečvou a přilehlých lokalitách.
- V září 2020 se uskuteční již 8. ročník semináře „Kybernetická bezpečnost“, který tradičně Česká pobočka AFCEA, její pracovní skupina Kybernetická bezpečnost pořádá ve spolupráci s Národním úřadem kybernetické a informační bezpečnosti ČR.
- Na září 2020 plánuje AFCEA pracovní skupina Ochrana obyvatelstva ve spolupráci s Policejní akademií ČR v Praze a Komorou podniků komerční bezpečnosti ČR konferenci na téma „Ochrana měkkých cílů“.
- Ve dnech **3.–7. 11. 2020** se ve Vídni v Rakousku uskuteční evropské finále středoškolské soutěže v kybernetické bezpečnosti „ECSC 2020“. Národní tým České republiky bude nominován na základě výsledků finále Středoškolské soutěže v kybernetické bezpečnosti a letních soustředění, které pořádá Česká pobočka AFCEA.

www.afcea.cz

ČABM ■ ČESKÁ ASOCIACE BEZPEČNOSTNÍCH MANAŽERŮ

Problematika zadávání veřejných zakázek v oblasti ochrany majetku, osob a informací s důrazem na kvalitu poskytování služeb, byla hlavním tématem odborné konference pořádané koncem února v prostorách poslanecké sněmovny Parlamentu ČR. Tato akce byla pořádána ČESKOU ASOCIACÍ BEZPEČNOSTNÍCH MANAŽERŮ a pod záštitou poslance Poslanecké sněmovny ČR pana Roberta Králíčka. Co je důležitější – kvalita anebo cena? Jaká je optimální hranice? Jaká je zákonem stanovená minimální cena poskytované služby? Co dělat, když neúspěšní účastníci napadají výběrová řízení? Jaký je pohled dodavatelů? Jak připravit výběrové řízení, kde hlavním kritériem je kvalita a ne cena? Tyto a jiné otázky byly ve vztahu k hlavnímu tématu diskutovány účastníky po celou dobu konference. Jednotliví přednášející postupně otevírali témata, která pokrývala klíčové oblasti bezpečnosti – IT, fyzická ostraha, bezpečnostní technologie, informační bezpečnost apod.

www.cabm.cz

EAS ■ EUROPEAN ASSOCIATION FOR SECURITY

Dne 26. 3. 2020 bylo slavnostně otevřeno Junior centrum excellence pro kybernetickou bezpečnost a ICT při Střední škole informatiky, poštovnictví a finančnictví Brno - Čichnova Brno. Hlavním cílem projektu bylo vybudování moderního technologického centra v rámci České republiky, které bude zajišťovat výuku kybernetické bezpečnosti a absorbovat nové technologické trendy v této oblasti. Toto centrum bude schopno produkovat absolventy oboru kybernetické bezpečnosti a dalších ICT oborů, které základní principy kybernetické bezpečnosti rovněž potřebují ke správnému výkonu profese. Absolventi tohoto centra budou využitelní jak pro potřeby veřejnoprávních zaměstnavatelů, tak i pro soukromou podnikatelskou sféru *(https://www.cichnovabrno.cz/o-skole/projekty/aktualni-projekty/irop)*. Za podporou projektu stáli vedle členů platformy KYBEZ také organizace spojené s aktivitami EAS v České republice.

http://e-konference.utb.cz

ISACA Czech Republic Chapter ■ INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION

Konference IT Governance 2020 se bude konat ve dnech **20.–22. 10. 2020**. Rezervujte si prosím termín. Témata budeme postupně zveřejňovat na našem webu *www.isaca.cz*.

Konference mezinárodní ISACA **EuroCACS/CSX** se koná ve dnech **28.–30. 10. 2020** v Helsinkách ve Finsku. Více informací o konferenci, program a registraci naleznete zde *https://www.isaca.org/conferences/euro-cacs-csx-2020*.

Je možné se v průběhu celého roku registrovat na zkoušky k certifikacím **CISA** (Certified Information Systems Auditor), **CISM** (Certified Information Security Manager), **CGEIT** (Certified in the Governance of Enterprise IT), **CRISC** (Certified in Risk and Information Risk and Systems Control) nebo **CSX-P** (Cybersecurity Practicioner). Více informací o jednotlivých certifikacích naleznete na adrese *https://www.isaca.org/credentialing/certifications*.

ISACA Czech Republic Chapter připravuje na letošní rok několik přípravných kurzů na tyto certifikace. Termíny a podmínky si vyžádejte na adrese *certifikace@isaca.cz*.

www.isaca.cz

Zabijačka anebo workshop

Metamorfosa

Ani osvětlený Týnský chrám a dominanta Pražského hradu v pozadí nepřebila dojem z visícího prasete a řezníka obratně porcujícího maso na dřevěném pultu. Střecha obchodního domu Kotva s restaurací Sluneční terasa T-Anker by asi jen málokomu přišla na mysl jako prostor pro zabijačku. A přece, kolem páté hodiny se tu ve čtvrtek 28. listopadu 2019 scházely desítky předních českých manažerů a odborníků na kyberbezpečnost.

Mezi všudypřítomnými košilemi se vyjímají zelené zástěry, které hosté dostali u vstupu. Někteří je již stačili potřísnit krví, naštěstí ne svou, když si zkusili sami porcovat prase. Mnoho zúčastněných si vyzkoušelo s masem pracovat vlastníma rukama poprvé.

Hlavní část programu se však teprve chystá. Dnešním řečníkem v cyklu Metamorfosa není odborník na informační systémy ani kyberbezpečnost, ačkoliv má za sebou i technické vzdělání a již dříve se zúčastnil konference IS2. Vojtěch Eliáš, katolický kněz, kanovník Metropolitní kapituly u sv. Víta v Praze. Studoval v Římě na Papežské salesiánské univerzitě UPS. Působil mimo jiné na farnostech v Příbrami, na pražských Vinohradech a také jako proděkan a pedagog na katolické teologické fakultě Univerzity Karlovy. V roce 2015 odjel do Velké Británie, kde tři roky působil na největší katolické farnosti ve Wimbledonu. V roce 2018 se vrátil do České republiky a nyní působí mj. na farnosti u sv. Ludmily v Praze-Chvalech a farnosti v Praze–Jirny.

Všichni napjatě čekají, protože otec Eliáš se již zúčastnil panelové diskuze na konferenci Information Security Summit, která měla skvělý ohlas. Dnes by na talíři měla být kromě informační bezpečnosti a digitalizace především etika, která je záležitostí napříč obory, IT a církev nevyjímaje.

Po úvodu a představení otevíráme rozhovor otázkou, jak se dostal ke kněžské profesi. Eliáš vysvětlil, že šlo o silný rodinný vliv. Jeho dědeček, profesor Jiří Malášek, někdejší rada ministerstva školství, byl za svůj prokatolický postoj nejprve odsouzen k trestu smrti, poté na doživotí, a po 16 letech byl propuštěn a emigroval do Západního Německa. Jeho otec MUDr. Jaroslav Eliáš se výrazně zasloužil o rozvoj české duchovní hudby a strýc Petr Eliáš měl velký vliv na založení plzeňské diecéze.

Poté se rozhovor stáčí k praxi v Anglii: „Vy jste strávil 3 roky ve Wimbledonu, v největší katolické farnosti v Anglii. Co je možné říci o postavení duchovních v obou zemích v rámci pomyslného společenského žebříčku? Je vnímán kněz v Anglii odlišně od Česka?“ *„Přišel jsem tam jako hotový kněz, nebylo tedy třeba stoupat žádným společenským žebříčkem, měl jsem tam již místo jasně dané. Setkával jsem se ale hned od začátku se hříchy, které my tady v Česku tolik neřešíme, jako třeba doopravdy prožívaný rasismus. Jedna babička mě říkala: »Já jsem ráda že jste tady, a že jste přece jenom běloch!« Tak jsem se trochu zalekl. Ona pak pokračovala »Já vím že je to hřích, ale já jsem vám to stejně chtěla říct.«“* V místnosti zní smích, protože knězovo vyprávění je zajímavé a jeho řečnické schopnosti dodávají dynamiku celému večeru.

Pokračuje se na téma Afriky a misií, protože Eliáš sám působil jako prezident Likvidace lepry a celkem strávil na misii přes deset let. Na začátku vysvětluje, že je důležité chápat, že církev není organizací, která dělá humanitární pomoc těsně po přírodní katastrofě nebo konfliktu. Církve typicky dělají rozvojovou pomoc, tedy nastoupí, když opadne první krize, aby pomohly stabilizovat nebo znovu vybudovat společnost.

Zmiňuje se také problém korupce, se kterou se ale ve většině případů nic nedělá. O něco později na odlehčení tématu humorně poznamenává: *„V Bruselu bylo setkání představitelů pomocných organizací. Pamatuji se, že vystoupila jedna bruselská úřednice a oznámila, že musí s politováním, říct, že má ověřené informace, že dvě až tři procenta všech projektových peněz, které se posílají na rozvojovou pomoc do Afriky, skončí na úplatcích. My všichni, co jsme tam byli, jsme tak jako pokyvovali hlavou a smáli se. Já jsem to pak už ale nevydržel a přihlásil jsem se, že bych k tomu chtěl říct, že nemohu potvrdit, jestli jsou to dvě až tři procenta, nebo jenom jeden a půl až dvě procenta, ale že bezpečně můžu říct, že polovina peněz se rozkrade.“*

Po tématu misií se přesouváme k válkám, tentokrát přichází na řadu i zmiňované IT a řeší se i války v kyberprostoru. Eliáš poukazuje na jejich plíživost a zrádnost, že to, že jsou méně vidět, nijak nezlehčuje jejich dopad na společnost.

Rozhovor plyne přes otázku digitalizace a její vliv, například souvislost otevřených zdrojů, sociálních sítí a celkové dostupnosti kyberprostoru se změnou počtu věřících a s přijetím chování menšin do normálu.

„Jsou věci, které se dějí, co se dříve dít nemohly. Je předmětem mnoha studií, například i z amerického předvolebního období, jak může menšina působit na většinu. Jedním z kritérií pro to, aby se to mohlo dít, je, že menšina musí být ve svém požadavku konzistentní. To platí i v kyberboji – stačí, abych menšinu, která mě ohrožuje, rozdělil tak, aby nebyla jednotná ve svých požadavcích, a přestává mít svou průbojnost. Musím ale říci, že je pravda, že církev je teprve na začátku cesty k tomu, aby svou úlohu v kyberbojích plnila důsledně.“

Děkujeme panu Eliášovi za účast a obohacení večera svými myšlenkami a zážitky! Dále také naše poděkování patří partnerům akce, kterými byli ICZ, Cisco, insighti, PwC, díky kterým se skvělý večer mohl uskutečnit.

Daniela Seigová

Ptáme se právníka

JUDr. Martin Maisner, PhD., MCIArb.

Samostatný advokát a nezávislý rozhodce
Rybná 14
110 00 Praha 1
Tel.: 222 191 386
maisner@martin-maisner.com

Během volební kampaně jedna nejmenovaná strana použila klip jisté nadace, která pomáhá dětem s různými neurovývojovými poruchami. Klip byl zásadně změněn, názory tram (plným jménem) uvedených psychiatrů byly sestříhány tak, aby celý klip nepopisoval neurovývojové poruch u dětí (zde ADHD), ale hovořil o tom, že všichni mladí lidé protestující veřejně proti oné nejmenované straně jsou vlastně duševně nemocní. Celý klip byl prezentován i s logem oné dobročinný nadace na internetu. Je to v pořádku? Mohou se zneužité subjekty nějak bránit?

Uvedený případ jasně ukazuje, že data musí být chráněna před jakýmkoli zneužitím, tedy nejen před tím, aby bylo znemožněno jejich využití oprávněnými osobami, ale i před tím, aby byla jinak veřejně dostupná data zneužita v rozporu s vůlí osob, které s daty oprávněně disponují, a to k jinému účelu, než bylo subjekty údajů či jinak oprávněnými osobami zamýšleno.

V popisovaném případě je zřejmé, že se jedná o jednání nejen neetické, ale vysloveně protiprávní. V daném případě byla porušena celá řada právních předpisů, přičemž vůči každému z těchto porušení je možné využít trochu jiné zákonné prostředky. K jednotlivým porušením:

1. V první řadě je zcela nepochybně porušeno právo autorské. Autorem u realizovaného filmového díla (kterým uvedená reportáž či klip nepochybně je) je především režisér, který rozhoduje o jeho zveřejnění (včetně toho, k jakému účelu a jakým způsobem bude dílo zveřejněno). V daném případě bylo však především porušeno právo autora na jeho nedotknutelnost tím, že došlo k jeho změně a zásahu do něj bez souhlasu autora. Právo na nedotknutelnost díla je právo osobnostní, kterého se ani sám autor nemůže vzdát, a je nepřevoditelné. Dalším autorským právem, které bylo porušeno, je právo dílo užít, konkrétně právo na sdělování díla veřejnosti, které bylo porušeno tím, že bylo – byť částečně a v pozměněném stavu – použito v přestříhané a pozměněné formě. Nejedná se o tzv. bezplatnou zákonnou licenci, protože se nejednalo o řádnou citaci, tedy o zveřejnění výňatků v odůvodněné míře, kde by bylo uvedeno jméno autora, název díla a pramen. Vzhledem k tomu, že se jedná o jasné porušení autorského práva, může se poškozený autor domáhat u příslušného soudu návrhem, aby soud rozhodl o:

   a. stažení neoprávněně zhotoveného materiálu, který obsahuje části autorského díla,
   b. zničení takového díla obsahujícího neoprávněně užité části autorského díla,
   c. poskytnutí přiměřeného zadostiučinění, a to buď ve formě omluvy, nebo zároveň zadostiučiněním v penězích.

   K uvedeným krokům bude samozřejmě vědět, kdo se porušení autorského práva dopustil, protože návrh k soudu nelze podat vůči neznámému pachateli. Při zveřejnění na internetu je právě tato skutečnost často limitující, nehledě na to, že rychlost rozhodování soudu a rychlost šíření čehokoli na internetu jsou samozřejmě nesrovnatelné v čase. Spravedlnost zde bezpráví dohání se zpožděním několika let, pokud vůbec.

2. Druhým faktorem v daném případě je ochrana osobnosti konkrétních osob, jejichž projevy osobní povahy (v tomto případě obrazový a zvukový záznam jejich odborného vyjádření) byly nejen uveřejněny bez jejich svolení, ale navíc zásadně pozměněny a uveřejněny v souvislostech, které je jak osobně, tak profesně velmi poškozují.

   Obecně platí, že není možné zasáhnout do soukromí člověka, pokud s tím on sám předem nesouhlasí. Z tohoto pravidla existují výjimky, např. možnost užít bez souhlasu podobiznu, zvukový nebo obrazový záznam

pro tiskové, rozhlasové, televizní či obdobné zpravodajství nebo pro vědecký či umělecký účel.

Kromě soukromí člověka jsou chráněny i další stránky osobnosti, jako je důstojnost člověka, jeho vážnost, čest a projevy osobní povahy (např. jeho vyjádření zachycené zvukem i obrazem). Podle obecně akceptovaného výkladu zásahem do soukromí může být i taková situace, kdy je zveřejněn autentický text, který však – díky vytržení ze souvislostí – poškozuje pověst nebo dobré jméno osoby. Takové poškození je závažnější než právo veřejnosti mít přístup k takové informaci. Posuzování, zda došlo k porušení práva na soukromí, tak může být poměrně obtížné a závislé na konkrétních případech. Kdo se cítí dotčen na svých právech, může se obrátit buď přímo na poskytovatele internetové služby (provozovatele) a požadovat odstranění škodlivého obsahu, nebo na soud, po kterém může kromě odstranění škodlivých informací žádat i náhradu škody a nemajetkové újmy.

3. Další rovinou ochrany je rovina trestněprávní. Jediná ryze autorskoprávní skutková podstata trestného činu je obsažena v ustanovení § 152 trestního zákona. Pro spáchání trestného činu porušování autorského práva, práv souvisejících s právem autorským a práv k databázi je však nutný úmysl. Může však jít o tzv. nepřímý úmysl, kdy pachatel věděl, že může svým jednáním spáchat skutek obsažený ve skutkové podstatě trestného činu, a byl s tím srozuměn. Za tento trestný čin lze uložit trest odnětí svobody na dobu maximálně pěti let nebo peněžitý trest do 5 000 000 Kč. Významná je i možnost uložení trestu propadnutí věci, která sloužila ke spáchání trestného činu nebo která k tomu byla určena. To se týká např. počítačového vybavení či snímacího zařízení, kterým byl klip vytvořen a sestříhán. Za tento trestný čin je možné uložit také trest zákazu činnosti.

Limitujícím faktorem trestněprávního postihu je v tomto případě míra ochoty orgánů činných v trestním řízení se v dané věci angažovat, přesněji řečeno přisoudit uvedenému jednání takovou právní kvalifikaci, aby jej považovali za trestný čin. Na druhé straně je třeba zdůraznit, že v minulosti byla podobná jednání (samozřejmě v trochu jiných souvislostech) posuzována i jako šíření poplašné zprávy (§ 357), pomluva (§ 184) nebo křivé obvinění (§ 354).

4. Čtvrtým aspektem celé věci může být porušení právních předpisů, které se týkají etických aspektů veřejných projevů během volební kampaně. V tomto směru je právní úprava velmi kusá a žádné účinné speciální nástroje či sankce neexistují. Představa, že strana či kandidát, kteří se během volební kampaně chovali nepřijatelně a neeticky, budou z voleb vyloučeni nebo jejich dosažené výsledky anulovány, je samozřejmě naivní. Zákon sice zná trestný čin maření přípravy a průběhu voleb či referenda (§ 351), ale tím se rozumí jednání „...kdy pachatel jinému násilím nebo pohrůžkou násilí nebo lstí brání ve výkonu volebního nebo hlasovacího práva v referendu anebo jiného takovým způsobem k výkonu volebního nebo hlasovacího práva v referendu nutí, kdo jinému nebo pro jiného v souvislosti s výkonem volebního nebo hlasovacího práva v referendu poskytne, nabídne nebo slíbí finanční, majetkový nebo jiný obdobný prospěch, aby volil nebo hlasoval v rozporu s nezávislým vyjádřením své vůle, kdo padělá údaje v dokladu o počtu členů politické strany nebo na petici pro volební účely nebo v jiném dokumentu souvisejícím s volbami nebo referendem anebo vědomě použije takového dokumentu jako pravého, kdo vědomě nesprávně sečte hlasy či poruší tajnost hlasování nebo kdo jinak hrubým způsobem maří přípravy nebo průběh voleb do zákonodárného sboru nebo zastupitelstva územního samosprávného celku anebo přípravy nebo průběh referenda, až do vyhlášení jejich výsledků...“, což se dá na popsaný případ aplikovat jen s velkou představivostí.

Závěrem je třeba konstatovat, že ačkoli se jedná o jednání nečestné a lidsky hnusné, obrana proti němu nemusí být jednoduchá. Jsem přesvědčen, že pokud se kdokoli obrátí na ISP (poskytovatele internetových služeb), celkem určitě dosáhne zablokování (znepřístupnění) závadného příspěvku. Nicméně rozesílání závadného souboru z neutrálních adres (např. veřejné knihovny nebo internetové kavárny) na adresy zájmových osob nebo plošně tak jednoduše zabránit nejde. Rozhodnutí soudu, které zakáže materiál dále rozesílat, bude vždy směřovat vůči konkrétním osobám a na ostatní subjekty se nebude vztahovat – navíc než bude dosaženo pravomocného rozhodnutí, uplyne jistě několik měsíců, možná let – tedy dávno po tom, co již volební kampaň i volby proběhnou. Pokud se týče trestního postihu, je téměř určitě odsouzen k nezdaru, protože i kdyby se podařilo objevit šiřitele, bude mu obtížné prokázat, že věděl, že je materiál manipulovaný. A objevit toho, kdo sekvence sestříhal, aby měly jiný smysl, je téměř nemožné.

MANAGEMENT SUMMARY

These articles were subject to peer-to-peer review.
Articles marked with a company logo represent commercial presentations.

Interview with Jeffrey Bardin

page 7

Adam Lamser

Jeffrey Bardin is the executive director and chief intelligence officer at Treadstone 71. As a leading expert in both intelligence and cybersecurity, we asked him about cyber threat intelligence, what it means to be an intelligence officer in the private sector and captured his view of the progress cyber security made since its beginning.

Data Retention obligation in case law of the Court of Justice of the European Union and Constitutional Court of the Czech Republic

page 17

Miroslav Uříčař

The obligation to retain traffic and location data (Data Retention) has been criticized due to its interference with the right to privacy since its adoption. The Data Retention obligation has already been subject to three decisions of the Court of Justice of the EU and three decisions of the Constitutional Court of the CR, the most important from them being the judgment of the Court of Justice declaring the Data Retention Directive invalid. In the pending case the Court of Justice has been requested by the French, Belgian and UK courts to assess whether their national Data Retention obligations are compliant with the EU law. Advocate General of the Court of Justice has presented his Opinion in these cases on 15 January 2020. In his opinion the means and methods of combating terrorism must be compatible with the requirements of the rule of law. Therefore, he states that the ePrivacy Directive precludes such legislation which imposes the obligation to retain, in a general and indiscriminate fashion, the traffic and location data of all subscribers, as is the case of the French, Belgian and UK legislation. The ruling of the Court of Justice could be expected in the coming months.

DevOps – part VII.

page 30

Vladimír Kufner

This, last but one article of the whole series about DevOps summarizes achieved outcomes of transformation to DevOps and reflects future possible trends in DevOps. It discusses most often myths ad typical problems when transforming to DevOps.

Customers' privacy in the environment of online advertisement on Czech web

page 11

Libor Polčák

Bid requests in Internet auctions for advertisement impressions propagate details about users, their attributes, browsers, location etc. Recently, several complaints have been lodged with several supervisory data protection authorities. This paper shows that special categories of personal data are processed in RTB initiated by Czech websites without seeking consent.

Analysis of the situation of digitalization

page 23

Peter Chrenko

Nowadays, the terms „digitalization" and „digital transformation" are either becoming a cliché or their interpretation differs from one person to another. It seems that the most common idea of what they mean is associated with implementing new technologies and applications in companies to make our and clients' life easier. The more money the company invests in them, the more „digital" it is considered. The reality is, however, that these investments do not bring the desired effect, as we tend to get too caught up in this effort and forget about the most relevant – the client. The aim of this article is, using results of recent minisurveys, show what is the „digital reality" in big companies. Secondly, it aims to suggest how to approach this issue with all its complexity and spread awareness within the public sphere, because it impacts not only the companies themselves but their clients and consequently the society as well.

Two decades of United Nations' attempts for the cyberspace stabilization

page 36

Richard Kadlčák

This article provides a historical overview of UN efforts to stabilize cyberspace dating back to the 1990s. The article also covers the current round of UN cyber-negotiations and identifies the main cleavages between states calling for the preservation of free, open, and secure cyberspace and those trying to restrict freedom online under the pretext of strengthening cybersecurity. In its concluding section, the article positions the Czech Republic in the context of UN cyber-negotiations and offers practical suggestions for a way forward with a view of stabilizing cyberspace at the global level.

MANAGEMENT SUMMARY

Malware Emotet – Trickbot – Ryuk in the Benešov hospital

page 39

Adam Kučínský, Vojtěch Sikora

The article deals with the cyber attack on the hospital in Benešov, which took place in December 2019. The article describes the attack, the malware used in this case, the procedure after the detection of the attack and the measures to be applied to prevent and respond to these types of attacks.

Book review

page 50

Miroslav Uřičař

A review of the book Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti (authors: Smejkal Vladimír, Sokol Tomáš, Kodl Jindřich).

Reality can be worse than the expectation

page 44

Martin Hlaváč

At the end of the year 2019, IT administrators of major financial institutions in the Czech Republic encountered unusual activities in the IT infrastructure of the company. During the verification process they concluded that the company had been hacked, and they tried to solve the problem on their own. But after several weeks of unsuccessful efforts, the AEC team was asked for help. Cyber security experts soon managed to uncover the unprecedented scale of the incident. They also detected the input vector into the system and then stopped the attack with precisely coordinated action. The final elimination of the attackers in the infrastructure of the institution was made possible by the deployment of the EPP/EDR solution and by subsequent manual termination of remaining hacker activities. During the investigation of the incident, the hackers were identified as members of the globally active group called Cobalt Group, which specializes in the illicit transfer of funds from companies and institutions.

SECTIONS

Virus section	52
Standards and publications	54
Metamorfosa: Throwback to St. Martin's goose celebration	55
News from partner companies	56
Metamorfosa: Traditional pig-slaughter or a workshop	57
Legal advice	58
Management summary	60
Colophon	62

Vydává TATE International, s.r.o.

Adresa redakce
DSM – data security management
TATE International, s.r.o.
Hořejší nábřeží 21, 150 00 Praha 5
mobil: +420 737 215 220
e-mail: dsm@tate.cz, **web: www.tate.cz**

Sazba a grafika
Miroslav Kymla

Tisk
Princo International, spol. s r.o.

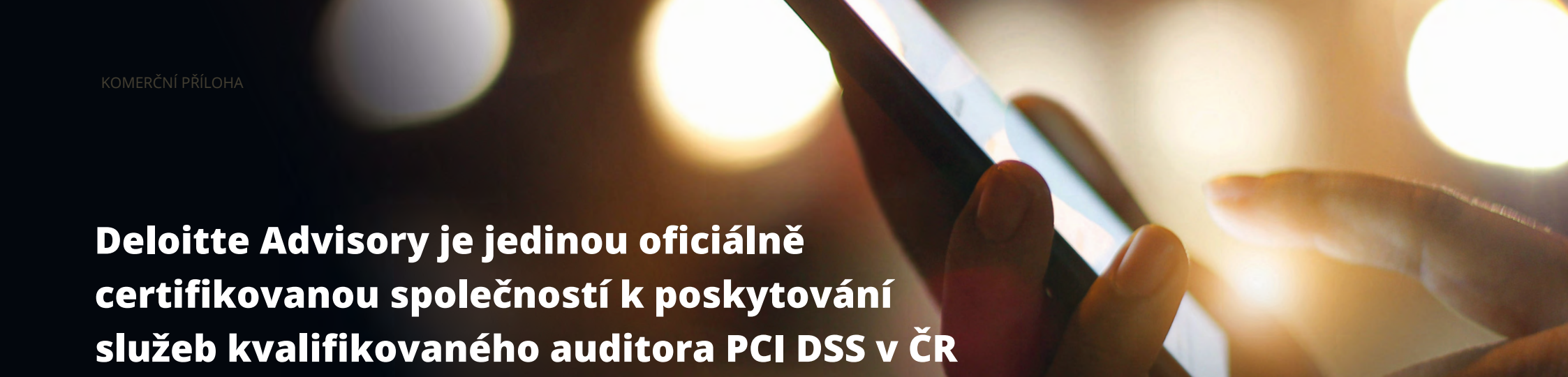
Inzerci a předplatné přijímá redakce

Registrováno MK ČR E 7803, ISSN 1211-8737.
ISSN 2336-6745 (elektronická verze)

Toto číslo vyšlo 26. března 2020.

Téma příštího čísla:

Rozhovor s osobností z konference IS2, Zákon o právu na digitální služby, ePrivacy...



Deloitte Advisory je jedinou oficiálně certifikovanou společností k poskytování služeb kvalifikovaného auditora PCI DSS v ČR

Prostřednictvím svých certifikovaných QSA pracovníků poskytujeme zákazníkům certifikační audit PCI DSS.

1. PŘÍPRAVA NA IMPLEMENTACI A AUDIT
2. ROZDÍLOVÁ ANALÝZA
3. DEFINICE AKČNÍCH PLÁNŮ
4. FORMÁLNÍ AUDIT
5. ŠKOLENÍ
6. PENETRAČNÍ A ASV TESTOVÁNÍ
7. VYPLNĚNÍ SAQ
8. PCI PROGRAM

1,8 miliard €

je suma z podvodných transakcí u platebních karet vydaných v regionu SEPA v roce 2016

22,8 milard $

je odhadovaná suma škod z podvodů u platebních karet zneužitých v roce 2016

Deloitte.

Jan Seidl
RISK ADVISORY LEAD
jaseidl@deloittece.com
+ 420 739 647 334

Deloitte je partnerem tištěné verze

Deloitte.

www.deloitte.cz **ncernomorsky@deloitteCE.com**