LUPA 3.0

SPECIÁL WEBU LUPA.CZ
LISTOPAD 2023
NEPRODEJNÝ VÝTISK

INTERNET | TECHNOLOGIE | ECOMMERCE | TELEKOMUNIKACE

ČESKÉ AI START-UPY
KTERÉ STOJÍ ZA TO SLEDOVAT

PROLOMENÍ SOUKROMÍ
JSME VŠICHNI PODEZŘELÍ ZE ZNEUŽÍVÁNÍ DĚTÍ?

DOKLADY V MOBILU
JAK BUDE FUNGOVAT ČESKÁ DIGITÁLNÍ OBČANKA?

ŽENY V IT
GENERATIVNÍ AI JE PŘÍLEŽITOST PRO ŽENY

JSME SVĚDKY NEBÝVALÉHO NÁRŮSTU HACKTIVISMU. DO VÁLKY SE NYNÍ MŮŽE V KYBERPROSTORU ZAPOJIT PRAKTICKY KDOKOLI. ČESKÁ REPUBLIKA ZAŽILA NAPŘÍKLAD HACKTIVISTICKÉ ÚTOKY BĚHEM PREZIDENTSKÝCH VOLEB.

LOVEC KYBERZLOČINCŮ

barion

Naskenujte qr kód

Základ pro online platby

Nechte růst svoje podnikání s využitím dat o chování nakupujících a poplatkem 0,99 % resp. nižším.

V technologiích běží čas neuvěřitelně rychle. V loňském vydání Lupy 3.0 spoluzakladatel Applu Steve Wozniak mluvil o své skepsi k umělé inteligenci. „Současná AI nepřemýšlí sama za sebe," říkal s tím, že si nedokáže poradit s problémy, na které není přímo naprogramována. Jen o pár týdnů později, 30. listopadu 2022, organizace OpenAI vypustila na veřejnost svého AI chatbota nazvaného Chat Generative Pre-trained Transformer, a zkratku ChatGPT brzy znaly a používaly stovky milionů lidí na celém světě. Reagovaly i další firmy (Google se svým Bardem, Anthropic s Claudem, Meta s modelem LLama…). Propuklo bezuzdné nadšení z umělé inteligence. Jak už to bývá, v průběhu roku jsme se propracovali od chytlavých, leč nerealistických prohlášení o tom, kolik lidí AI v jakých profesích už brzy nahradí, ke střízlivějšímu hodnocení přínosů a negativ umělé inteligence. Jde ale po dlouhé době o fenomén, který má skutečně potenciál výrazně proměnit naše životy. Doufejme, že hlavně k lepšímu. Téma AI se proto prolíná celým aktuálním vydáním našeho časopisu. Zakladatel bezpečnostní firmy Check Point Gil Shwed popisuje, jak se AI používá při vytváření kyberbezpečnostních hrozeb, ale i při prevenci a ochraně. Výkonná ředitelka vzdělávací organizace Czechitas Senta Čermáková zase mluví o tom, jak generativní umělá inteligence může proměnit trh práce a pomoci ženám se na něm uplatnit. A přinášíme také inspirativní výběr nejzajímavějších českých AI start-upů.

Příjemné čtení vám přeje

DAVID SLÍŽEK

šéfredaktor serveru Lupa.cz

LUPA 3.0
SPECIÁLNÍ MAGAZÍN WEBU LUPA.CZ
LUPA.CZ internet info

ŠÉFREDAKTOR: DAVID SLÍŽEK | **EDITOR SPECIÁLU:** JAN VACA | **VEDOUCÍ OBCHODNÍHO ODDĚLENÍ:** MONIKA STEJSKALOVÁ, MONIKA.STEJSKALOVA@IINFO.CZ | **GRAFICKÁ ÚPRAVA:** PETR KUBÁT **KOREKTORKA:** DANA ŠTROPOVÁ | **TISK:** TRIANGL | **ADRESA VYDAVATELSTVÍ:** INTERNET INFO, s.r.o., MILADY HORÁKOVÉ 116/109, 160 00 PRAHA 6 | **VÝKONNÝ ŘEDITEL:** MAREK ANTOŠ **INTERNET:** WWW.LUPA.CZ, WWW.IINFO.CZ, | **E-MAIL:** JMENO.PRIJMENI@IINFO.CZ | | **SNÍMEK NA TITULNÍ STRANĚ:** CHECK POINT

Obsah

6 GIL SHWED: KYBERZLOČINCEM SE I DÍKY AI MŮŽE STÁT PRAKTICKY KDOKOLI

Hacktivismus nebývale roste, ale vlády proti němu nemají účinné zbraně, říká zakladatel společnosti Check Point.

FOTO: CZECH POINT

20 JSME VŠICHNI PODEZŘELÍ ZE ZNEUŽÍVÁNÍ DĚTÍ?

V Evropě se schyluje k bezprecedentnímu narušení práva na soukromou komunikaci.

FOTO: JAN VACA

54

JOSEF PRŮŠA: TISKÁRNY OD NÁS ODEBÍRÁ NASA I SPACEX

Každý měsíc odchází z pražských Holešovic do 160 zemí z celého světa deset tisíc výrobků značky Original Prusa.

46

SENTA ČERMÁKOVÁ: NESLIBUJI, ŽE JSOU DIGITÁLNÍ DOVEDNOSTI NĚCO JEDNODUCHÉHO

Nová výkonná ředitelka organizace Czechitas mluví o svých plánech. „Generativní AI je pro ženy příležitost," říká.

FOTO: JAN VACA

FOTO: KAREL CHOC

82

MARTIN JEŘÁBEK: DÁVNO UŽ NEJSME JEN APLIKACÍ PRO TURISTY

Jak z mapového portálu spadajícího pod Seznam vyrostla služba, po které čím dál víc sahají i zahraniční uživatelé.

KYBER ZLOČINCEM SE DNES I DÍKY AI MŮŽE STÁT PRAKTICKY KDOKOLI

HACKTIVISMUS NEBÝVALE ROSTE, ALE VLÁDY ZATÍM NEMAJÍ ÚČINNÉ ZBRANĚ, KTERÝMI BY ODRAZILY KAŽDÝ KYBERÚTOK, ŘÍKÁ ZAKLADATEL A CEO MEZINÁRODNÍ KYBERBEZPEČNOSTNÍ SPOLEČNOSTI CHECK POINT GIL SHWED.

FOTO: CHECK POINT

Jak dnes vypadá prostředí kyberbezpečnostních hrozeb, jak se vyvíjí a které hrozby jsou podle vás největší?
Jsme svědky stále sofistikovanějších útoků ransomwaru. Kromě šifrování dat útočníci vyhrožují i zveřejněním ukradených citlivých informací. A výkupné se pak může pohybovat až v desítkách milionů dolarů. Mnoho hackerských skupin navíc spolupracuje, přičemž v každé fázi se používá jiný škodlivý kód a ransomware je až na konci infekčního řetězce. Například nemocnice jsou v poslední době velmi častým cílem. Zajímavé ale je, že dlouhodobě největšímu počtu kybernetických útoků čelí sektor vzdělávání a výzkumu. Množství citlivých dat a relativně slabé zabezpečení jsou pro kyberzločince velkým lákadlem.

Hackeři také využívají každou příležitost od velkých událostí, jako jsou olympijské hry, až po nejrůznější speciální dny, jako je například Valentýn. A někdy je snadné těmto trikům podlehnout, navíc počet lidí, kteří se k podobným událostem vážou, vždy přinese nějaké množství obětí. Ohrožena jsou ale i zařízení, jež jsme si dříve jako cíl útoků nedokázali představit a která mohou být hacknuta a využita k prolomení do podnikové sítě, jako jsou žárovky, lékařské přístroje, kamery a další zařízení internetu věcí. Proto klademe velký důraz na zabezpečení IoT.

Navíc, zejména v souvislosti s válkou, jako je ta, která je teď na Ukrajině, a náboženskými konflikty, jsme svědky nebývalého nárůstu hacktivismu. Do války se nyní může v kyberprostoru zapojit prakticky kdokoli. Česká republika zažila například hacktivistické útoky během prezidentských voleb nebo pokusy o zahlcení webových stránek a služeb českých bank a dalších organizací, novou masivní vlnu útoků na převážně vládní organizace v Česku registrujeme i v těchto dnech.

A mezi významná rizika a výzvy je potřeba počítat i nedostatek odborníků na kybernetickou bezpečnost. Počet kybernetických útoků roste, ale celosvětově je obrovský nedostatek bezpečnostních expertů. V Check Pointu klademe důraz na vzdělávání a nabízíme různé kurzy a školení. Spolupracujeme také se školami, v České republice například s Mendelovou univerzitou v Brně, abychom studenty vyškolili v oblasti kybernetické bezpečnosti. Nabízíme mnoho vzdělávacích programů a využíváme

i interaktivní herní prvky, abychom informační bezpečnost vyučovali zábavnou formou.

Jak kyberbezpečnost ovlivnilo masové rozšíření velkých jazykových modelů a generativní AI?
AI technologie se neustále vyvíjejí a postupně mění náš každodenní život. Oblast kybernetické bezpečnosti není výjimkou, a to jak v dobrém, tak i ve zlém. Kyberzločincem se dnes může stát prakticky kdokoli. Může za to nárůst kyberzločinu jako služby, takže si kdokoli může za pár dolarů koupit malware, pronajmout botnet nebo koupit cílené útoky včetně zákaznické podpory. Situaci ale zhoršuje právě i vzestup různých AI technologií. Ačkoli se tvůrci těchto služeb snaží rychle reagovat a zlepšovat bezpečnostní mechanismy, opakovaně jsme ukázali, že ChatGPT a Google Bard lze zneužít k vytváření kybernetických hrozeb. I amatéři bez technických znalostí mohou vytvořit malware, phishing, nebo dokonce základní ransomwarový kód.

> **AI technologie významně pomáhají zlepšit automatickou prevenci hrozeb, identifikovat podezřelé chování apod.**

Moderní technologie také usnadňují rychlé vytváření jazykových mutací, lokálních podvodů a cíleného škodlivého obsahu. Dříve byly gramatické chyby nebo nelokalizovaný obsah varovným znamením, dnes zabere vytvoření verze úspěšného a důvěryhodného podvodu v lokálním jazyce bez chyb jen chvilku.

S rozvojem AI služeb jsme také svědky prudkého nárůstu deepfake podvodů, hlasového phishingu a fake news. Hodně se mluví například o útocích na volební systémy, ale to je spíše mýtus; mnohem větším problémem pro demokracii jsou pokusy ovlivnit volby a veřejné mínění manipulací s lidmi pomocí obrovského množství manipulativního obsahu a fake news vytvořených s pomocí AI.

Využití umělé inteligence hackery a kyberzločinem zatím naštěstí není tak rozšířené jako využití AI k ochraně a vylepšení bezpečnostních řešení. AI technologie významně pomáhají zlepšit automatickou prevenci hrozeb, identifikovat podezřelé chování apod. Například náš ThreatCloud AI denně prověří tři miliardy webových stránek a souborů a k identifikaci a blokování i dosud neznámých hrozeb používáme více než 40 AI a machine learning technologií, což je více než 50 % všech našich enginů.

Co si myslíte, že bude dalším „velkým trendem“ v oblasti kybernetické bezpečnosti? Bude souviset s umělou inteligencí?
V současné době čelíme páté generaci kybernetických hrozeb, které jsou globální, kombinují různé metody a útočí v celosvětovém měřítku. Navíc jde o polymorfní hrozby, které mohou měnit svou strukturu, a maskovat se tak před běžnými bezpečnostními produkty.

Děsivé jsou zejména megaútoky ransomwaru, jako byly WannaCry a NotPetya. Také v důsledku různých úniků a krádeží dat se velmi výkonné hackerské nástroje vyvinuté vládními agenturami dostávají do rukou i menších skupin a jednotlivců. Takové útoky pak mohou mít pro mnoho organizací nedozírné následky. Kybernetickou bezpečnost si proto

dnes bez umělé inteligence prakticky nelze představit.

Dalším klíčovým problémem je konsolidace, protože existuje mnoho produktů, které se zabývají pouze jedním aspektem bezpečnosti, ale nespolupracují spolu. To je obrovská chyba. Mnoho produktů se může vzájemně duplikovat, způsobovat zbytečný zmatek v komunikaci a vytvářet falešná upozornění. Studie, kterou jsme uskutečnili s týmem Dimensional Research, ukázala, že téměř polovina všech organizací používá od šesti po čtyřicet bezpečnostních produktů, a prakticky všechny, bylo jich 98 %, spravují své bezpečnostní produkty pomocí několika konzolí. To vytváří řadu slepých a potenciálně zneužitelných míst. Konsolidovaná architektura zvyšuje zabezpečení a šetří rozpočty.

Zároveň je třeba klást důraz na prevenci. Mnoho bezpečnostních řešení se zaměřuje na detekci útoků a hrozeb a jejich následné zneškodnění. S tímto přístupem však budou útočníci vždy o krok napřed. Zastavení probíhajícího útoku pouze uhasí požár, který již dávno působí obrovské škody, a odstranění následků bude velmi nákladné. Jakmile dojde k úniku dat, už to nelze vrátit zpět, reputace je poškozena a sebelepší pojištění to nespraví.

Dalším z velkých témat bude zabezpečení cloudu. To je nyní na prudkém vzestupu a stává se klíčovým tématem mnoha nových projektů, přičemž jeho význam nadále poroste. Z našich údajů totiž vyplývá, že 35 % organizací má více než 50 % svých pracovních dat v cloudu. Stručně řečeno, vše musí být zabezpečeno.

Zmínil jste válku na Ukrajině, která se samozřejmě vede také v kyberprostoru. Jsou podle vás vlády na kybernetické války připravené?

GIL SHWED

Izraelský programátor, podnikatel a nadšenec do nových technologií. V roce 1993 založil spolu s kolegy společnost Check Point Software Technologies, která dnes patří k uznávaným bezpečnostním firmám po celém světě. Je autorem tzv. stavového firewallu. Podle časopisu Forbes byl v roce 2023 na 878. místě celosvětového žebříčku miliardářů. V roce 2005 byl v internetovém hlasování zvolen 69. největším Izraelcem všech dob. Před pěti roky byl izraelskou vládou jako první oceněn za přínos ke kybernetické bezpečnosti a ekonomice země.

A jsou některé země připravené lépe a některé hůře?
Kybernetické války neznají hranic. Na vládní úrovni zatím neexistují účinné mechanismy, jak úspěšně odrazit každý kybernetický útok. Také je potřeba říct, že pouhé zastavení probíhajícího útoku jako dostatečná ochrana nestačí. Vládám se daří úspěšně budovat především informační síť. Co zatím kriticky chybí, je aktivní část obrany. Když máte tradiční armádu, máte k dispozici řadu nástrojů, jak odrazit probíhající útok a rozprášit útočnou jednotku nepřítele. V kybernetické válce jsou ale v tomto ohledu vlády často bezzubé a nemají žádné kybernetické letectvo, dělostřelectvo nebo jinou aktivní jednotku, kterou by mohly proti nepříteli vyslat. Při kybernetickém útoku musíte být v ideálním případě schopní reagovat během několika sekund, ale realita je taková, že některé reakce jsou v řádu hodin, někdy i dnů. Pak se jen snažíte minimalizovat škody. Detekce nestačí, detekční strategie je mrtvá. Existuje jen jeden správný přístup, a tím je prevence s nejlepšími dostupnými nástroji.

Oproti tomu vidíme aktivity národních nebo státem sponzorovaných hackerských skupin. Odhalili jsme několik závažných špionážních kampaní. Například asijská hackerská skupina se zaměřila na evropská ministerstva zahraničí, velvyslanectví a vládní subjekty spojené se zahraniční a domácí politikou. Cílem kampaně SmugX bylo získat citlivé zahraničněpolitické informace, přičemž mezi oběťmi byly i Česká republika a Slovensko. Mezi tři nejčastěji napadaná odvětví navíc patří vládní a vojenské společnosti. Opatření, zákony a předpisy v oblasti kybernetické bezpečnosti se zlepšují, ale je to nikdy nekončící práce. Není snadné říct, kdo je lépe a kdo hůře připraven, ale usilovně pracujeme na tom, abychom pomohli vládám po celém světě být připraveni nejnovější kybernetická rizika úspěšně eliminovat.

Co musejí organizace a uživatelé udělat pro ochranu před kybernetickými hrozbami v době války? Je potřeba odlišný přístup, nebo v oblasti kybernetické bezpečnosti není velký rozdíl?
Spousta hrozeb se používá plošně, takže nezáleží na tom, jestli jste ve válečné zóně, nebo ne. Stále budete čelit v drtivé většině podobným hrozbám. Témata se však mohou lišit.

My věříme v prevenci, která je postavena na třech principech: komplexnost, konsolidace a spolupráce. Každý si zaslouží to nejlepší zabezpečení.

Například díky AI technologiím je snadné vytvořit různé mutace, které zohledňují válečnou tematiku a lákají na informace o konfliktu.

Jiné je to samozřejmě v případě kritické infrastruktury, jako jsou elektrárny, nemocnice, plynovody, úpravny vody, distributoři ropy a plynu a podniky důležité pro chod společnosti. Ty mohou čelit mnohem sofistikovanějším cíleným útokům. Ale i v době míru čelí tyto organizace například pokročilým ransomwarovým útokům, takže zabezpečení by mělo být prioritou bez ohledu na okolnosti. Přesto jsme svědky toho, že kyberzločinci pečlivě zvažují, kdy a jak zaútočí, aby maximalizovali úspěšnost. Například zimní období, svátky, nebo dokonce víkendy zvyšují riziko kybernetických útoků na energetické společnosti nebo kritickou infrastrukturu.

Někteří kyberbezpečnostní dodavatelé tvrdí, že ke kybernetickým útokům dojde bez ohledu na to, jak robustní je vaše zabezpečení. My však věříme v prevenci, která je postavena na třech principech: komplexnost, konsolidace a spolupráce. Každý si zaslouží to nejlepší zabezpečení.

Check Point letos slaví třicet let od svého založení. Můžete z vašeho pohledu stručně shrnout, jak se změnil trh kybernetické bezpečnosti od roku 1993 do současnosti? Od Firewallu-1 k nejnovějším komplexním bezpečnostním technologiím?

Pěkná, ale velmi složitá otázka, o které bychom mohli mluvit hodiny. Lidé si musejí uvědomit, že pojem hacker se

v průběhu času změnil. Na počátku internetu existovala jakási romantická představa hackera, který porušuje pravidla, posouvá hranice, testuje limity, objevuje nové věci a často jen dokazuje, co je technicky možné, aniž k tomu má nějaké negativní motivy. Nyní je lepším pojmem než hacker kyberzločinec. Vidíme organizované skupiny s velmi vysokými rozpočty, vidíme politicky motivované útoky a téměř za vším stojí peníze.

Před třiceti lety byl web ještě v plenkách, první prohlížeč byl představen v roce 1993 a jen malé procento organizací mělo o existenci internetu, natož o potenciálních bezpečnostních rizicích, vůbec tušení.

Check Point vznikl před třiceti lety a v roce 1994 jsme představili první komerční firewall na světě, který umožnil organizacím oddělit sítě a datovou komunikaci od internetu a chránit se před nejrůznějšími on-line riziky. Byla to vzrušující doba, která vedla ke zrodu kybernetické bezpečnosti jako odvětví. Od roku 2018 jsme na cestě transformace ze společnosti vyrábějící firewally na firmu, která poskytuje komplexní zabezpečení – od koncových zařízení přes sítě až po cloud. Naše transformace na platformovou společnost začala akvizicí Dome9 a uvedením produktové řady CloudGuard, která poskytuje cloudové zabezpečení. Díky dalším akvizicím a vlastním inovacím jsme mohli vytvořit komplexní portfolio bezpečnostních produktů. Transformace Check Pointu ovšem není zaměřena jen na produkty. Před několika lety bylo vedení společnosti jasné, že musí také transformovat systém uvádění produktů na trh.

Dostali jsme se z doby jednoduchých virů zaměřených na jeden počítač ke složitým a obtížně identifikovatelným vícevrstvým hrozbám, které útočí na různé cíle současně, aby způsobily co největší škody. Organizace po celém světě čelí kybernetickým hrozbám páté generace (masové multivektorové hrozby). Ničivými příklady jsou megaútoky ransomwaru WannaCry, který zasáhl 300 000 počítačů ve 150 zemích, nebo NotPetya, jenž způsobil škodu přesahující 300 milionů dolarů. Ale i přes obrovský nárůst hrozeb se většina firem stále chrání pouze proti hrozbám třetí generace. Klíčové je změnit strategii a zaměřit se na prevenci, nejen na detekci. A vše je nutné zabezpečit tou nejlepší ochranou. Proto je nám ctí, že Check Point získal v testech Miercom Firewall Benchmark první místo s 99,7% mírou blokování malwaru, nejbližší konkurent měl úspěšnost pouze 72,7 %. Já tvrdím, že být druhý nejlepší není dost dobré. Pokud nechcete

být obětí kyberzločinu, musíte používat to nejlepší zabezpečení.

Kyberzločinci plošně skenují sítě, aby našli slabá místa, a současný neustále se měnící malware může proniknout a šířit se prakticky v jakékoli části IT infrastruktury včetně lokálních sítí, cloudových prostředí, vzdálených kanceláří, mobilních zařízení či libovolných jiných vstupních bodů.

Další významnou změnou je přeměna samotného prostředí. Před třiceti lety nebylo tolik cílů. Dnes žijeme ve společnosti, kde je vše připojeno k internetu, kde jsou uloženy nejrůznější kritické údaje, jako jsou naše osobní, finanční nebo zdravotní informace. To vytvořilo dokonalou bouři: stále sofistikovanější útoky s exponenciálním nárůstem potenciálních cílů.

Organizace musejí přejít od jednotlivých vzájemně nepropojených řešení ke konsolidované infrastruktuře, která poskytuje prevenci hrozeb v reálném čase napříč celou IT infrastrukturou a disponuje centralizovanou správou.

Vše začalo před třiceti lety a jsme hrdí, že stále poskytujeme nejlepší kybernetickou bezpečnost na Zemi a nyní i ve vesmíru, kde jsme zabezpečili vesmírnou misi Rakia a vytvořili pro ni speciální řídicí místnost.

Podívali jsme se třicet let zpět, jak podle vás bude vypadat bezpečnostní prostředí za třicet let?

Bylo by hezké vidět tak daleko, ale předchozí vývoj ukázal, že oblast technologií se mění tak závratným tempem, že je těžké předvídat na několik let dopředu, natož na třicet let. Navíc bezpečnost jde ruku v ruce s technologiemi, a bude tedy záviset na vývoji služeb, hardwaru, softwaru a celkového přístupu do digitálního světa. Vezměme si příklad metaverzum, které slibovalo okamžitou revoluci, ale nakonec se nestalo tak žhavým trendem, jak se očekávalo. Místo toho se obrovským tempem rozvíjí umělá inteligence.

Jaká je tedy vize pro příštích třicet let? Budeme chránit celé organizace a jejich aktiva, od mobilních telefonů přes koncové body, cloud, sítě až po prakticky libovolný ekosystém. Zaměřujeme se na budování systémů pro spolupráci. Pokud někde zabráníme útoku, dokážeme ho okamžitě zastavit všude po celém světě. Díky ThreatCloudu máme jedinečnou schopnost najít infikovaný soubor a okamžitě upozornit všechny ostatní systémy, aby zabránily jeho šíření, ať už jde o jednu pobočku nebo nadnárodní společnost. Zásadním tématem bude spolupráce.

Budeme chránit celé organizace a jejich aktiva od mobilních telefonů přes koncové body, cloud, sítě až po prakticky libovolný ekosystém.

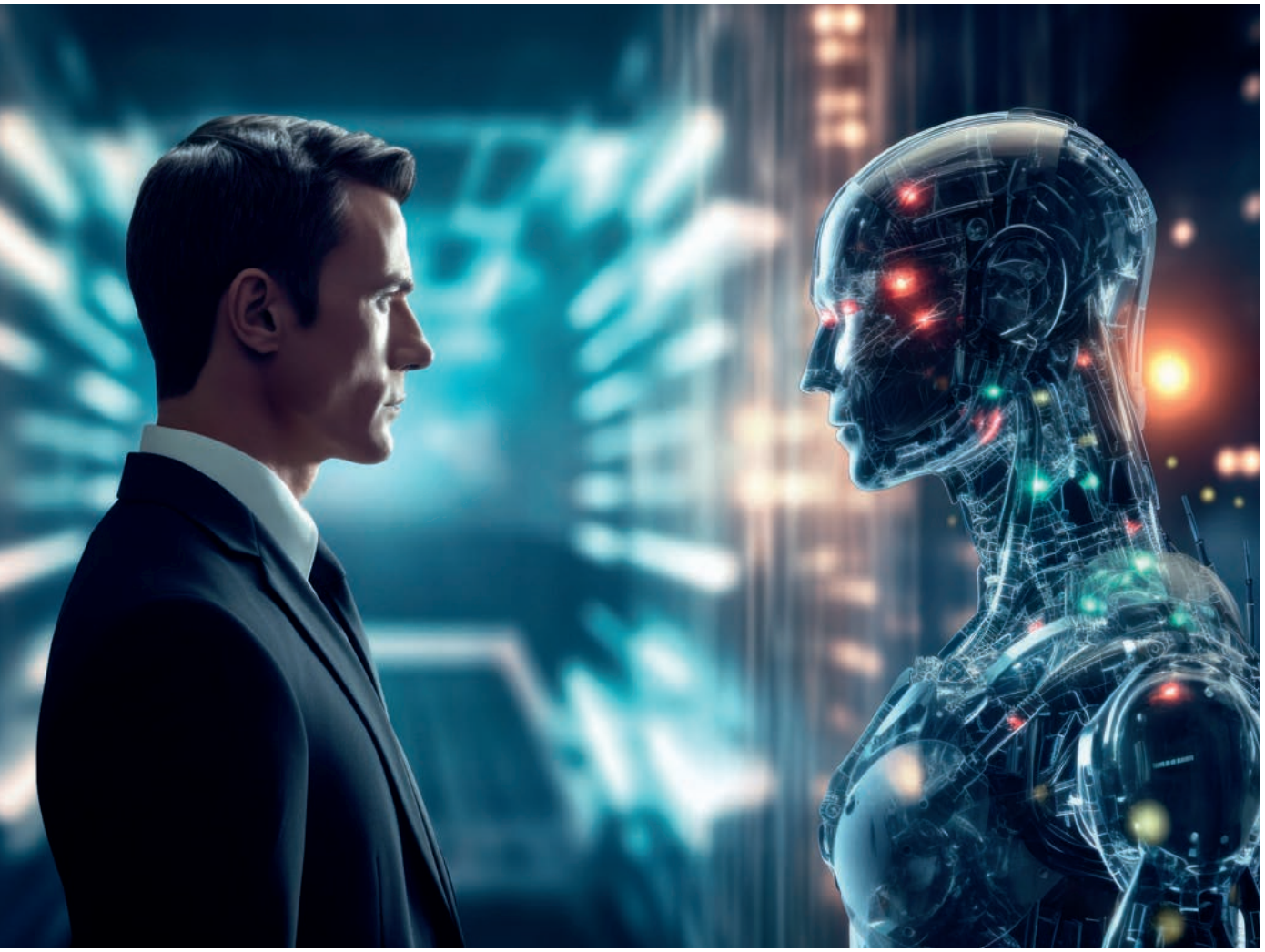
Je důležité si uvědomit, že všechny typy kybernetických útoků jsou nebezpečné bez ohledu na jejich povahu. V současné době se setkáváme s novými prvky, jako je umělá inteligence, které mají zásadní dopad na všechna odvětví včetně kybernetické bezpečnosti. Nelze však říci, že hrozby, které existují již několik let, nejsou nebezpečné – někdy je opak pravdou. Jsme svědky toho, že se do kritických infrastruktur, které v mnoha případech stále využívají starší zařízení, vracejí útoky staré mnoho let. Proto je nutné dívat se nejen na nejnovější technologie a postupy, ale nezapomínat ani na starší hrozby.

Rozhovor s Gilem Shwedem měl původně proběhnout on-line, kvůli aktuální situaci v Izraeli ale odpověděl na otázky e-mailem.

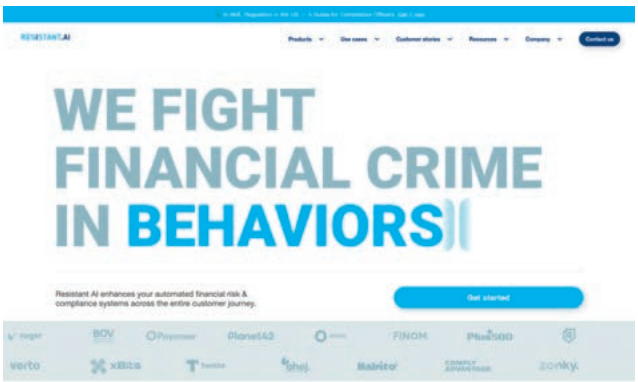
REDAKCE LUPA.CZ ■

ČESKÉ AI START-UPY, KTERÉ STOJÍ ZA TO SLEDOVAT

KONTROLA PROCESŮ V ENERGETICE, ANALÝZA FIREMNÍCH PROBLÉMŮ NEBO HLASOVÁ UMĚLÁ INTELIGENCE. NA ČEM PRACUJÍ TUZEMSKÉ AI START-UPY?



V médiích občas probleskne zpráva, že Česká republika zaostává ve využívání umělé inteligence. Není to až tak pravda. V Česku působí řada start-upů, které na umělé inteligenci založily svoje fungování. Vybrali jsme z nich osm, jež stojí za to sledovat.



https://resistant.ai

Resistant AI

Martin Rehák se s Michalem Pěchoučkem v minulosti podílel na jednom z prvních českých startupových exitů, který byl navíc postavený na spin-offu z univerzitního prostředí. Jejich firmu Cognitive Security koupil americký síťařský obr Cisco, jenž z českého softwaru udělal součást své nabídky pro využití AI v kybernetické bezpečnosti na síťové úrovni. Rehák s Pěchoučkem byli napřed, když viděli, že detekce anomálií skrze AI bude v tomto oboru důležitá.

Zatímco Pěchouček se stal technickým ředitelem kybernetické bezpečnostní firmy Gen (Avast), Rehák se společně s několika dalšími kolegy vrhl do dalšího start-upu. Když to hodně zjednodušíme, Resistant AI vytváří hodnou umělou inteligenci bojující proti útočícím umělým inteligencím. Software se zaměřuje zejména na finanční sektor, kde se podvody za využití AI stále více rozšiřují.

„Velká část rozhodnutí umělé inteligence, ačkoliv je bezpečná v průměrném případě, se neumí účinně bránit cílené manipulaci. To je přesně ten problém, který řešíme. Věnujeme se ochraně algoritmů před někým, kdo se je snaží zmanipulovat, aby nějak zvrátil jejich rozhodnutí," nastínil Rehák.

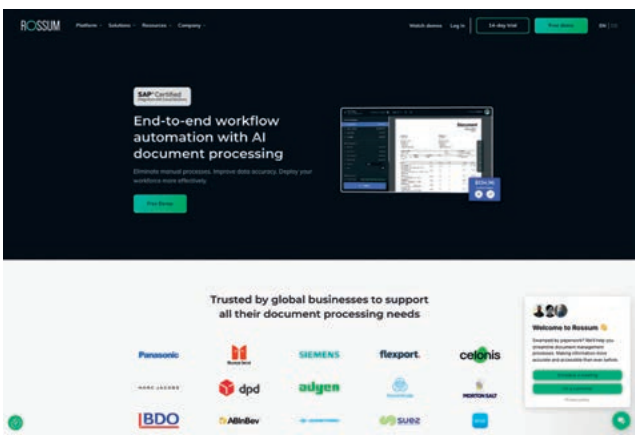
Start-up patří mezi ty nejlépe zainvestované v Česku a od roku 2019 posbíral zhruba 600 milionů korun. Mezi investory jsou i Index Ventures nebo Google.

Rossum

Technologie Rossum je další spin-off z tuzemského univerzitního prostředí, konkrétně z ČVUT. Petr Baudiš, Tomáš Tunys a Tomáš Gogár vytvořili umělou inteligenci schopnou na základě neuronových sítí číst data z faktur a dalších dokumentů a pak je digitalizovat. Je to řešení konkrétního otravného problému, který se ve firmách a organizacích často vyskytuje.

České trio na rozvoj této myšlenky vybralo 109 milionů dolarů, asi 2,5 miliardy korun. Peníze poslaly fondy Miton, LocalGlobe nebo General Catalyst. Potenciál této technologie je značný, mimo jiné totiž míří do bohatého enterprise prostředí.

Rossum nedávno získal statut certifikovaného partnera společnosti SAP. Český software je tak přímo integrován do všudypřítomného SAP, což mu zřejmě výrazně pomůže v prodejích. Ze svého oboru jde o prvního takto certifikovaného hráče. „Obrovská část naší cílové skupiny používá SAP, takže je to pro nás zásadní. I doteď spousta našich zákazníků používala Rossum se SAP. Současné propojení staví na všech zkušenostech, které jsme už nabrali. Kromě toho, že jde o lepší technické řešení, určitě oficiální certifikace usnadní Rossumu cestu skrze IT oddělení mnoha budoucích zákazníků," popsal Baudiš s tím, že podobné integrace chce Rossum udělat i s dalšími hráči v enterprise IT.



https://www.rossum.ai

Filuta AI

Filuta asi půl roku po založení získal největší pre-seed investici v historii českých start-upů. N1, Czech Founders, Microsoft, Horizon Europe a SPM Invest Marka Španěla a Slavomíra Pavlíčka z Bohemia Interactive do něj poslaly

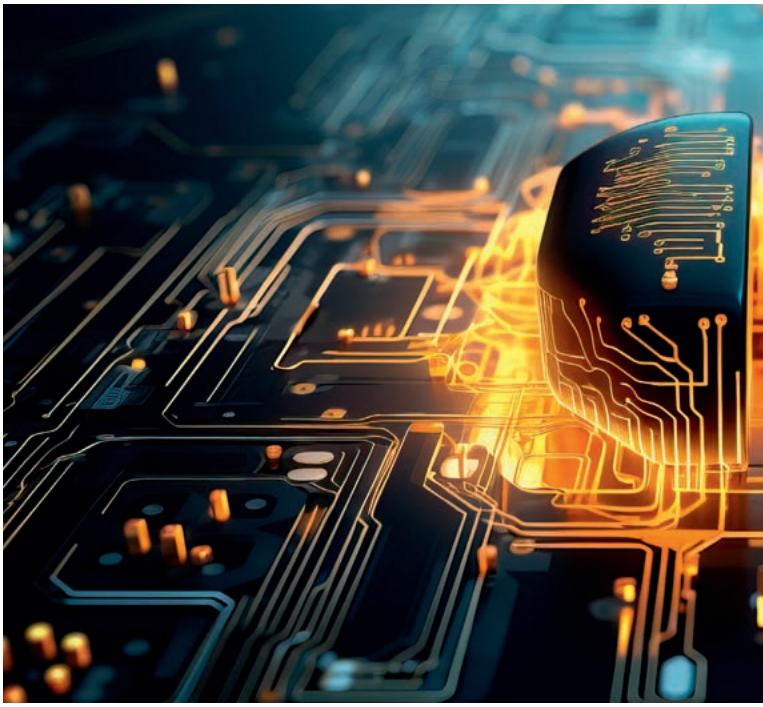
56 milionů korun. Po pár měsících je dorovnal další český start-up, E2B.

Investory mimo jiné zaujala historie dvou zakladatelů. Filip Dvořák získal dva doktoráty na matfyzu, zkoumal a vyučoval na univerzitě v Torontu a následně jako první Čech nastoupil jako hlavní vědecký pracovník do Palo Alto Research Center (PARC) v Kalifornii. Věnoval se tam výzkumu optimalizace dopravní infrastruktury v Los Angeles nebo výzkumným projektům pod vládní agenturou DARPA. Dvořák také pracoval pro Microsoft a Google. Jeho kolega Martin Doušek se v Microsoftu podílel na vývoji back-endu pro Teams a Dynamics 365.

Filutu je možné „nakrmit“ firemními daty, na základě čehož se uskuteční analýza a vznikne služba, která má dlouhodobě a autonomně navrhovat řešení libovolných firemních problémů.

„Naše technologie dramaticky zrychluje návrh řešení inteligentní automatizace, tedy kombinace z průmyslu známé automatizace a umělé inteligence. Navíc je široce aplikovatelná na celou řadu odvětví a v podstatě dokáže vyřešit jakýkoliv problém, pro který existují data,“ nastínil Dvořák.

Podle jeho slov je Filuta nová generace Composite AI, pomocí níž je možné „dosáhnout až desetkrát nižších nákladů a desetkrát vyšší rychlosti než v případě ručního vývoje řešení na míru“. Composite AI zjednodušeně znamená kombinaci několika odlišných technik v AI, jako jsou NLP, machine learning, deep learning, computer vision a další.



The MAMA AI

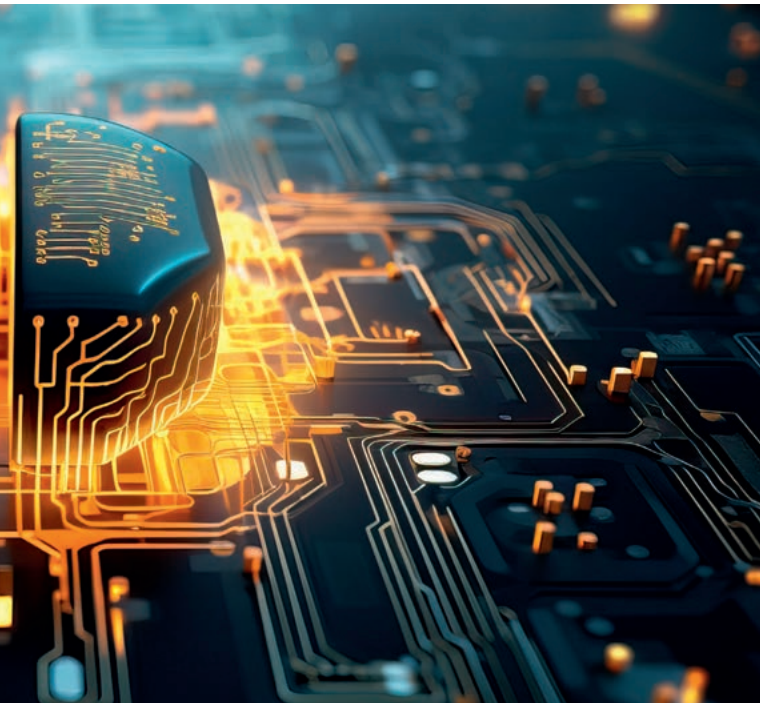
V kancelářích středoevropské centrály americké společnosti IBM v Praze na Chodově dlouhá léta probíhala část vývoje umělé inteligence Watson. IBM s ní měla velké plány, její projekt Watson v některých ohledech předběhl dobu, do toho ale přišly generativní modely typu ChatGPT a IBM část svých činností převedla na nově vzniklou firmu Kyndryl. Byť se Watson nadále rozvíjí, některé aktivity byly utlumeny.

Změna strategie dopadla i na český tým, který Watsona učil pracovat s jazykem. Pražský vývoj byl zrušen a IBM tyto aktivity začala centralizovat v USA. Část zdejšího týmu se osamostatnila a založila start-up The MAMA AI, který vyvíjí hlasovou umělou inteligenci pracující se syntézou a podobně. Ultimátním cílem může být třeba to, že si člověk bude moci přirozeně povídat se stroji pomocí hlasu.

Ukázkou je projekt The MAMA AI ze společnosti Seznam.cz. Rozhlasová stanice Expres FM, kterou Seznam provo-

https://filuta.ai

https://themama.ai

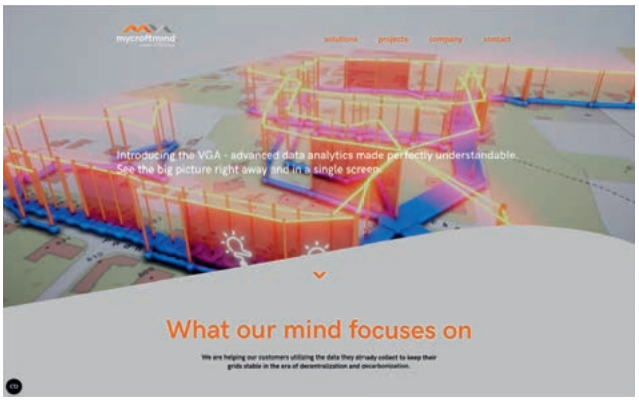


zuje, do svého živého vysílání začlenila umělou inteligencí vytvořený hlas moderátorky pojmenované Hacsiko. Slyšet ho lze během nočního vysílání. Umělá inteligence imituje hlas skutečné moderátorky Báry Hacsi. Botovi stačí pouze připravit texty, které má odříkat.

Mycroft Mind

Mycroft Mind je mladá firma, která se nedávno stala součástí české technologické skupiny TTC. Start-up z Brna se zabývá využitím umělé inteligence v energetice. Umožňuje například vizualizaci přenosových souprav včetně vysvětlení toho, co se v takových sítích děje. Dokáže monitorovat a vyhodnocovat data a hodí se pro nasazení v rámci internetu věcí, který je v energetice čím dál běžnější.

Brněnský univerzitní spin-off pracuje i na modelech umělé inteligence, jež mají být integrovány do čipů či dalšího hardwaru. Díky tomu bude možné například v měřácích elektřiny predikovat spotřebu a cenu. Evropská komise tento projekt vybrala mezi nejlepší na kontinentu, které je možné podpořit financováním v rámci projektu IPCEI Microelectronics. Stát si na tyto projekty takzvaného společného evropského zájmu chce půjčit 1,1 miliardy z Bruselu.



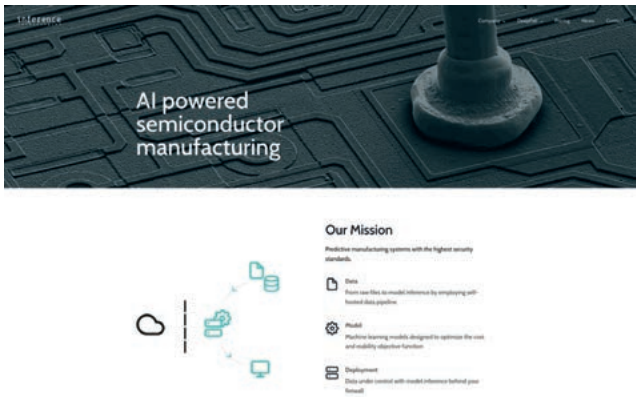
https://www.mycroftmind.com

Inference Technologies

Když před pár měsíci vyrazila na Tchaj-wan česká delegace zástupců státu, univerzit a polovodičových firem, byl mezi nimi i český start-up Inference Technologies. Ten byl mohl být jedním z těch, který zaujme náročné tchajwanské partnery z oblasti čipů. Ostrovní země vládne trhu se zakázkovou výrobou pokročilých čipů, zejména díky společnosti TSMC. Na to je napojený obrovský ekosystém dodavatelů a partnerů – od služeb designu přes dodavatele výrobních strojů až po producenty chemikálií.

České firmy Thermo Fisher Scientific a Tescan takto například dodávají elektronové mikroskopy používané pro vývoj čipů a následnou kontrolu kvality ve výrobě. Přerovská Meopta zase dodává optiku firmám ASML či Applied Materials produkujícím vysoce sofistikované stroje na výrobu čipů. Polovodičové továrny na Tchaj-wanu jsou jich plné.

Inference Technologies tvoří další část výroby. Firma vyvíjí software postavený na umělé inteligenci, schopný zajišťovat takzvanou prediktivní výrobu. Dokáže tak zlepšo-



https://www.inferencetech.com

vat kvalitu produkce, snižovat její cenu a zdokonalovat využití waferů, tedy křemíkových desek, na které se „vypalují“ samotné obvody.

Superface

Start-up Superface má ambiciózní misi, na kterou zatím od investorů posbíral asi sto milionů korun. Firma chce automatizovat to, jak si mezi sebou „povídají“ počítačové programy a systémy, hodlá tedy automatizovat komunikaci mezi aplikačními rozhraními (API).

API rozhraní je velmi mnoho a pro firmy je finančně i časově náročné udržovat napojení jejich aplikací na řadu externích služeb. Superface chce tuto komunikaci udělat bez toho, aniž se budou muset řešit nové verze, změny ve fungování API a tak dále.

„V Superface chceme změnit způsob, jakým se pomocí API propojuje byznys v digitálním světě. Tvoříme vrstvu nad API, pomocí které vše automatizujeme – API se tak stane minulostí. Naší vizí je vytvořit digitální tržiště pro AI, jež podle stanovených parametrů konkrétní službu vybere, propojí a v případě výpadku automaticky vymění za jiného vhodného poskytovatele,“ vysvětlil spoluzakladatel a technický šéf projektu Zdeněk Němec. Ten má s API značné zkušenosti, působil v českém start-upu Apiary, který koupil Oracle.

Superface také hodlá vytvořit největší katalog veřejných API, mluví o pojmu „Google od APIs“. Celé to určitě je téma. Největší cloud světa Amazon Web Services například spustil službu AWS Data Exchange for APIs, která dělá něco podobného jako Češi, ale zatím čistě v rámci AWS.

A co to má společného s AI? Superface používá prvky umělé inteligence. Ale hlavně dnešní svět je postavený na API a také systémy umělé inteligence pro své fungování tato propojení požadují. Superface se tak může stát takovým systémem pro propojování synapsí.

E2B

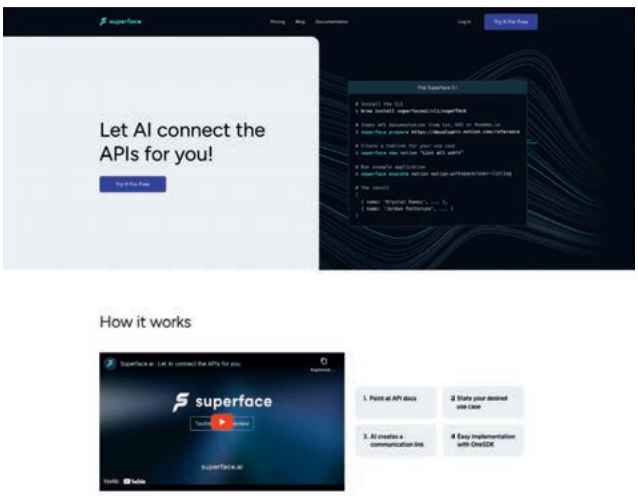
Mladý start-up E2B nedávno dorovnal český rekord ve výši investice ve fázi pre-seed, když podobně jako Filuta AI obdržel 2,5 milionu dolarů. E2B vychází z možností, které nabízejí nové LLM modely typu ChatGPT. Na nich si vývojáři stavějí takzvané AI agenty, které pomáhají s kdečím. Mohou tvořit softwarový kód, pomáhat s hledáním informací, navrhovat design a tak dále. Je to takový nový typ aplikací.

E2B pro tyto AI agenty vytváří cloudovou platformu, kde je možné je nechat běžet. Není tak nutné se starat o infrastrukturu a do své aplikace stačí vložit krátký kód.

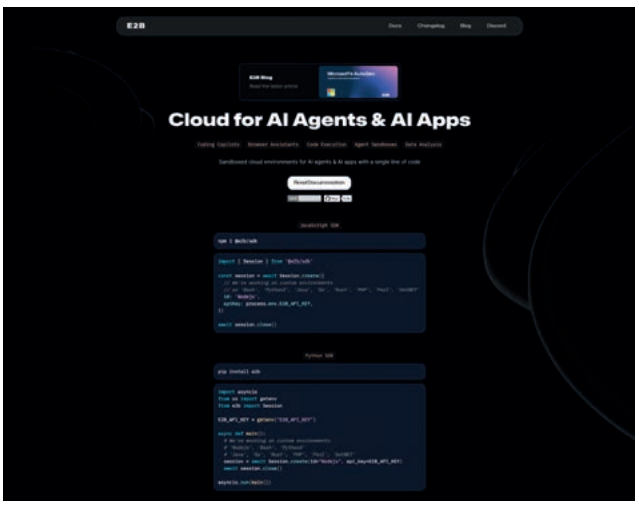
Dnes jsou AI agenty často označovány za budoucnost v rámci softwarového vývoje. Mluví se o nich jako o nových členech týmu nebo pevné součásti celého technologického stacku. Jako vždy, když se objeví nová zlatá horečka, vzniká řada firem, která chce všem těžařům poskytnout krumpáče a lopaty. Právě sem E2B míří. To, jak velké to skutečně může být, uvidíme po opadnutí hype a reálném začlenění do byznysu.

JAN SEDLÁK

Autor je kmenovým reportérem serveru Lupa.cz. O technologiích píše také do zahraničních médií. ■



https://superface.ai



https://e2b.dev

Elektronické podepisování pomůže českému pracovnímu trhu

COVIDOVÁ PANDEMIE ZNAČNĚ URYCHLILA DIGITALIZACI NA PRACOVIŠTÍCH. PRÁVNÍ NORMY V ČESKÉ REPUBLICE PŘESTO UPŘEDNOSTŇOVALY PAPÍROVOU FORMU TŘEBA I PRO SJEDNÁVÁNÍ BĚŽNÝCH PRACOVNÍCH SMLUV. AKTUÁLNÍ NOVELA ZÁKONÍKU PRÁCE, KTERÁ ZJEDNODUŠUJE ELEKTRONICKÉ PODEPISOVÁNÍ ŘADY PRACOVNĚPRÁVNÍCH DOKUMENTŮ, ZNAMENÁ ZÁSADNÍ POSUN VPŘED.

Nová právní úprava otevírá velkou příležitost většinu pracovněprávních dokumentů podepisovat elektronicky. Zároveň zužuje okruh písemností, které je i nadále nutné doručovat v režimu zákoníku práce. Sem spadají jednostranná právní jednání směřující k ukončení pracovního poměru či mzdové a platové výměry, a to především z důvodu ochrany zaměstnance.

Konec papírování

Díky této novele se digitalizace začne rychle prosazovat i v oblasti pracovněprávních vztahů. Významně se totiž rozšiřuje okruh dokumentů, pro něž stačí prostý elektronický podpis jak na straně zaměstnavatele, tak na straně zaměstnance. Jde o dokumenty zachycující dvoustranné právní jednání, jakými jsou např. pracovní smlouvy nebo dohody (DPP, DPČ) včetně veškerých dodatků a změn, dohody o výši mzdy, dohody o ukončení pracovního poměru, o práci na dálku, o srážkách ze mzdy a podobně.

„Z hlediska dostatečné průkaznosti při případném soudním sporu doporučujeme vyšší formu elektronického podpisu, například zaručený elektronický podpis vytvořený pomocí služby Bank iD SIGN," říká Jan Tomíšek z advokátní kanceláře Rowan Legal.

Zaručený elektronický podpis Bank iD SIGN je jednoznačně spojen s podepisující osobou a poskytuje vysokou míru právní jistoty, že dokument nebyl po podepsání změněn. Marek Růžička, výkonný ředitel společnosti Bankovní identita, dodává: „Nastal čas učinit elektronický podpis novou normou v HR dokumentaci. Bankovní identita zpřístupňuje elektronický podpis s právní jistotou doslova každému." ■

BANK iD SIGN

Zaručený elektronický podpis Bank iD SIGN umožňuje platně podepisovat všechny soukromoprávní dokumenty, pro které zákon nevyžaduje použití kvalifikovaného nebo uznávaného elektronického podpisu. Na rozdíl od prostého podpisu výrazně zvyšuje právní jistotu podepisujících.

- Jednoznačně identifikuje podepisující osobu
- Data potřebná k podpisu má podepisující osoba pod svou výhradní kontrolou
- Umožňuje zjistit jakoukoli změnu dokumentu po jeho podpisu
- Zajišťuje dostatečnou průkaznost při případném sporu

JSME VŠICHNI PODEZŘELÍ ZE ZNEUŽÍVÁNÍ DĚTÍ?

V EVROPĚ SE SCHYLUJE K BEZPRECEDENTNÍMU NARUŠENÍ PRÁVA NA SOUKROMOU KOMUNIKACI. VE JMÉNU OCHRANY DĚTÍ NA INTERNETU USILUJE EVROPSKÁ KOMISE O PRAVOMOC HLEDAT DĚTSKOU PORNOGRAFII I V ŠIFROVANÝCH ZPRÁVÁCH.

Terorismus a zneužívání dětí jsou snad odjakživa dvě témata, která otevírají legislativní dveře k ledasčemu. I jinak racionální lidé nad obrázky teroristických útoků nebo zneužívaných dětí ztrácejí rozvahu a jsou otevření nápadům, které nejen že problém neřeší, ale často vůbec nereflektují realitu našeho světa a jsou spíše proklamací politiků, kteří se pod ně podepíší. Bohužel proklamací, která v podobě platné legislativy může mít nepěkný dopad na práva a svobody nás všech včetně dětí, k jejichž ochraně má podle autorů sloužit.

Dalším z řady takových legislativních nápadů, tentokrát z dílny Evropské komise, je návrh nařízení, kterým se stanoví pravidla pro předcházení pohlavnímu zneužívání dětí a boj proti němu (dále jen CSAR). CSAR neboli Child Sexual Abuse Regulation má poskytovatelům internetových služeb uložit celou řadu povinností, jejichž cílem má být snížení zneužívání dětí v on-line prostoru a boj proti šíření dětské pornografie.

Evropské komisi na schválení nařízení zjevně velice záleží, a to dokonce tak, že se uchyluje k placené manipulaci prostřednictvím mikrocílení emotivních sdělení ve stylu „kdo s námi nesouhlasí – nechce ochránit děti“ na konkrétní skupiny prostřednictvím sociálních sítí. Pozadí manipulativní snahy ohýbat veřejné mínění, který si platila Evropská komise ve vybraných státech včetně České republiky a dává tím vzpomenout na dezinformační kampaně během amerických voleb nebo brexitu, popsal nizozemský deník De Volkskrantdne.

Evropská legislativa proti sexuálnímu zneužívání dětí on-line

Pro pochopení toho, co má vlastně nařízení řešit a proč je na jeho schválení činěn ze strany Komise tlak, aby se schválilo ještě před evropskými volbami v roce 2024, je potřeba ho zasadit do kontextu současné právní úpravy.

Návrh navazuje na dosavadní právní úpravu v směrnici 2011/93/EU, o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, a prozatímní nařízení 2021/1232, o boji proti pohlavnímu zneužívání (dále jen „prozatímní nařízení“).

Právě toto prozatímní nařízení, které platí od srpna 2021, v současné době upravuje možnost digitálních platforem dobrovolně vyhledávat v uživatelské komunikaci či obsahu dětskou pornografii. Obsahuje totiž výjimku z ochrany důvěrnosti komunikace zakotvené ve směrnici 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (ePrivacy směrnice). Eprivacy směrnice přitom jinak podobné zásahy do důvěrnosti komunikace jednoznačně zakazuje. Prozatímní nařízení ovšem platí pouze do 3. 8. 2024. Pokud by nedošlo k přijetí nařízení nového, mělo by i dobrovolné prohledávání uživatelského obsahu skončit.

Návrh nového nařízení ukládá povinnosti zejména provozovatelům hostingových služeb a dále interpersonálních komunikačních služeb, které veřejně nabízejí nástroje pro komunikaci mezi uživateli, a to třeba

Cílem CSAR neboli Child Sexual Abuse Regulation má být snížení zneužívání dětí v on-line prostoru a boj proti šíření dětské pornografie.

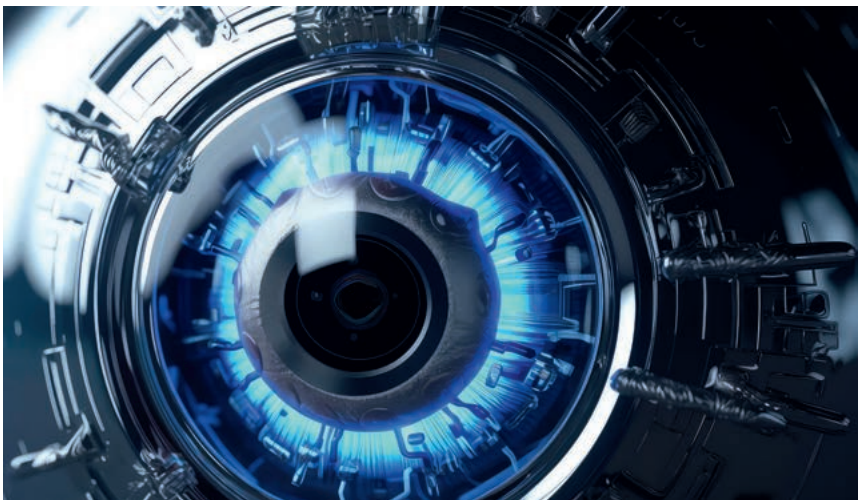
i jen jako doplněk nějaké jiné služby. Jde o širokou paletu povinností od prevence a zmírňování rizik zneužití služby k šíření dětské pornografie nebo navazování kontaktů s dětmi za sexuálním účelem až po povinnosti vyhledávat, oznamovat nebo odstraňovat závadný obsah.

Detekční příkazy k plošnému zásahu do soukromí

Velmi kontroverzní je zejména návrh na zavedení tzv. detekčních příkazů. To, co bylo dosud pro poskytovatele služeb dobrovolné, má být nově povinné. To je základní idea detekčního příkazu. Nově zřízený koordinační orgán členského státu má mít možnost zažádat soud nebo v daném státě k tomu určený správní úřad, aby nařídil až na dobu dvou let konkrétnímu poskytovateli hostingových nebo interpersonálních komunikačních služeb, aby začal v konkrétní službě v uživatelském obsahu odhalovat případy pohlavního zneužívání dětí.

Prohledávání uživatelského obsahu se nemá vázat na konkrétní osoby či případy, jako je tomu třeba u odposlechů, ale má dopadat plošně na všechny uživatele dané služby. Právní úprava sice umožňuje vydávat detekční příkazy, pouze pokud to bude přiměřené s ohledem na práva uživatelů. Bude to ale dostatečná ochrana před nadužíváním těchto příkazů? Příkladem nám může být třeba česká praxe vyžadování výpisů provozních a lokalizačních údajů ze strany policie. I zde je třeba povolení soudu a poskytnutí výpisu od operátorů lze použít pouze v případě, kdy není možné cíle dosáhnout jinak. Přesto si policie s povolením soudu vyžádá každoročně podle policejních statistik vyšší desítky tisíc těchto výpisů.

To, že zavedení detekčních příkazů bude velkým zásahem do soukromí občanů, kritizovali mnozí počínaje nevládními organizacemi přes vědecké kapacity až po Evropský sbor pro ochranu osobních údajů. Argumentace zásahem do soukromí je ale do značné míry otázkou hodnotovou, byť i zde máme nějaká vodítka k tomu, jaký pohled upřednostnit, třeba v judikatuře Soudního dvora EU k problematice plošného sledování elektronické komunikace (tzv. data retention), které tento soud dlouhodobě odmítá, a lze předvídat, že obdobný problém by měl i s tímto návrhem. Existuje ale i celá řada dalších argumentů více praktického a méně hodnotového rázu, které odkazují možnost skutečně efektivní realizace takového sledování do oblasti utopie.



Velmi kontroverzní je zejména návrh na zavedení tzv. detekčních příkazů. To, co bylo dosud pro poskytovatele služeb dobrovolné, má být nově povinné.

Jak by to vlastně bylo možné dělat?

Prohledávání obsahu, které požaduje Komise, lze dělat pouze strojově. Narážíme zde ale na limity technologií. Jako dětská pornografie mohou být hlášeny jak fotografie dětí z dovolených sdílené mezi rodinnými příslušníky nebo na různých serverech, ale i tzv. self-generated content, tedy explicitní obsah produkovaný samotnými dětmi. Jak vyplývá z výroční zprávy Internet Web Foundation z roku 2020, oproti kontaktní dětské pornografii představoval takový obsah u věkové skupiny 11–13 let 57 % celkového explicitně sexuálního obsahu. Ačkoli sdílení takových fotografií nebo videí je jistě něčím, co by děti raději dělat neměly, je otázka, jestli může být přínosné, pokud by takové intimní fotografie procházely rukama policistů a děti by čelily následnému vyšetřování. Na riziko dopadu nové regulace na samotné děti ostatně upozorňují i odborníci či nevládní organizace, které se zaměřují právě na zneužívání dětí, jakož i samotné oběti zneužívání.

Překážkou pro přesnější fungování technologií jsou přitom i právní limity. Jak upozornil např. Martin Kožíšek z CZ.NIC na semináři k této problematice, který se konal v květnu 2023 v Poslanecké sněmovně, rozvoji technologií, které budou založeny na strojovém učení, brání to, že za tímto účelem nelze přechovávat dětskou pornografii, na níž by se technologie učila.

V neposlední řadě je třeba zmínit i to, že některé služby fungují decentralizovaně, a bude tedy vůbec obtížné najít někoho, kdo by měl takový detekční příkaz realizovat.

Šifrovaná komunikace

Velká otázka se pak vznáší kolem toho, jestli je žádoucí, ale i technicky možné uplatňovat detekční příkazy na šifrovanou komunikaci. Fakticky by tak muselo dojít k jejímu rozšifrování, aby v ní bylo možné dětskou pornografii vyhledávat. I některé členské státy včetně České republiky upozornily na to, že šifrování je přitom zcela zásadní nástroj ochrany dat. Jakékoli otevírání zadních vrátek i pro samotné poskytovatele služeb by představovalo ohrožení bezpečnosti šifrování i dat samotných.

> **Velká otázka se pak vznáší kolem toho, jestli je žádoucí, ale i technicky možné uplatňovat detekční příkazy na šifrovanou komunikaci.**

Na stole se tak objevila varianta, podle níž by se detekční příkazy neměly vztahovat na obsah, který je opatřen koncovým šifrováním. Takové šifrování používají i zcela běžné komunikační platformy, jako jsou WhatsApp nebo Signal. Nejde tedy o žádný vynález pro nerdy. Je jen obtížně představitelné, že by pachatelé trestné činnosti nepoužívali takové šifrované komunikační nástroje nebo úložiště, kde nehrozí riziko detekce. V síti strážců zákona by tak pravděpodobně uvízli jen ti, kteří si neuvědomují, že dělají něco špatného, případně ti, kteří sku-

Prosazení možnosti povinné detekce dětské pornografie by bylo bezprecedentním prolomením soukromé komunikace, které může představovat důležitý precedent.

tečně nic nezákonného nedělají a pouze se dostali do hledáčku kvůli nedokonalosti použité technologie.

Ostatně zřejmě tak to do jisté míry funguje už dnes. Pokud se podíváme na čísla o kriminalitě, za rok 2022 česká policie eviduje 780 trestných činů spojených s vytvářením, šířením či držením dětské pornografie. Objasněnost byla 57,4 %. Jde o čísla srovnatelná s předchozími lety. Přitom jen v roce 2022 přišlo podle informací policie na výše zmíněném semináři od Interpolu celkem 21 605 reportů o záchytech sexuálně explicitního obsahu. Zjevně tedy drtivá většina takového obsahu není policií dále řešena.

Je to jen začátek?

Prosazení možnosti povinné detekce dětské pornografie by bylo bezprecedentním prolomením soukromé komunikace, které může představovat důležitý precedent. V minulosti obvykle v podobných případech následovalo klasické „vaření žáby“. Jak upozornila skupina novinářů v investigativním článku „‘Who Benefits?’ Inside the EU’s Fight over Scanning for Child Sex Content“, který byl publikován v několika evropských denících v září 2023, například Europol by podle zápisů z organizačních schůzek se zástupci Komise ohledně chystané regulace uvítal možnost detekci využívat i u dalších trestných činů. Komise vyjádřila pochopení, ale vzhledem k citlivosti tématu je prý třeba být realistický. Je tak zřejmé, že pokud navrhovaný návrh projde, hned po evropských volbách zde budeme mít další skvělé nápady, kam bychom se mohli ve skenování komunikace a uživatelského obsahu dále posunout.

JAN VOBOŘIL

Advokát, výkonný ředitel nevládní neziskové organizace Iuridicum Remedium. Specializuje se na vztah lidských práv a nových technologií, zejména pak na problematiku ochrany soukromí.

Luděk Ohnoutek
Vedoucí firemních procesů
KOMA MODULAR s.r.o.

Informace jsou drahé,
inteligentní informace jsou k nezaplacení.

Informační systémy pro řízení firmy

helios.eu

HELIOS
Rozšiřte své možnosti

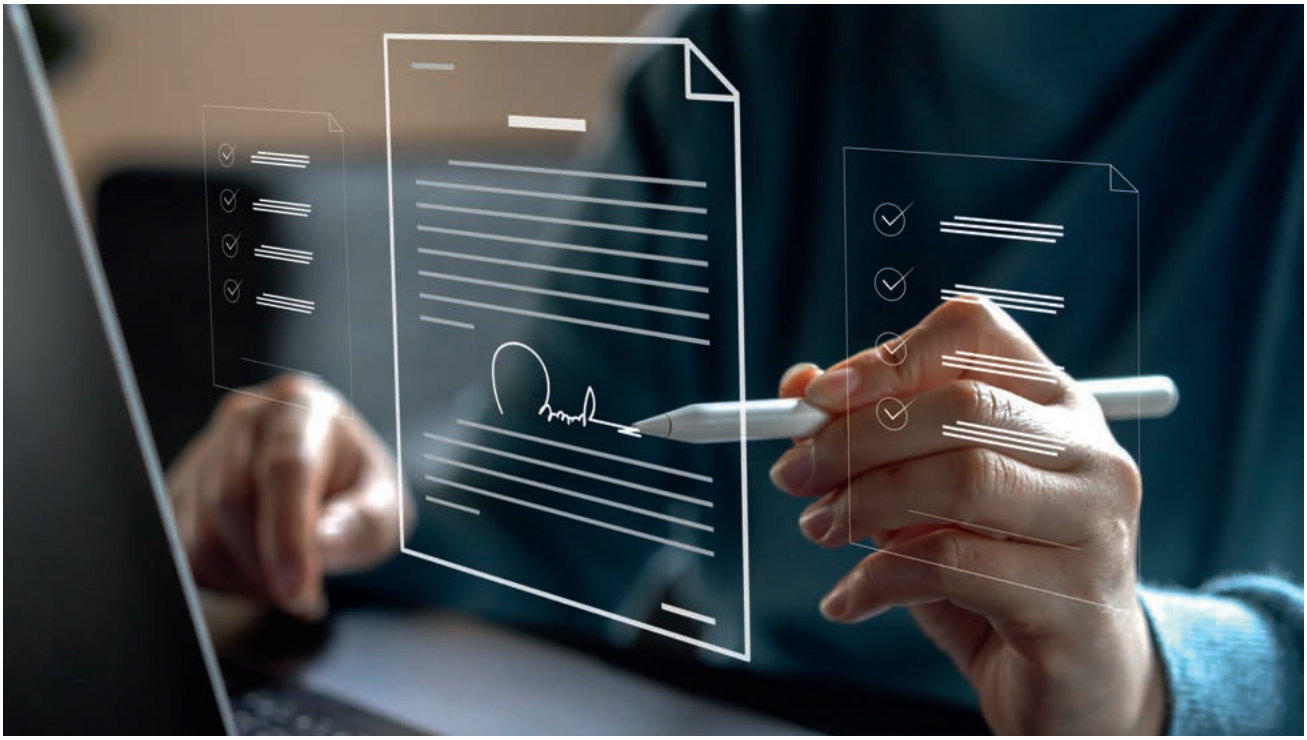
EGOVERNMENT V ROCE 2024:

ZÁVĚREČNÝ FINIŠ, NEBO DOCHÁZÍ DECH?

AMBICE V OBLASTI EGOVERNMENTU, NASTOLENÉ (NEJEN) DIGITÁLNÍ ÚSTAVOU, JSOU VELIKÉ A JEJICH VRCHOL BY MĚL PŘIJÍT NEJPOZDĚJI K 1. ÚNORU 2025. NEJDE O NIC MENŠÍHO NEŽ O PLNOU DIGITALIZACI VŠECH AGEND A ÚKONŮ VEŘEJNÉ SPRÁVY. TO VŠE V SITUACI, KDY SE NEDOSTÁVÁ ODBORNÝCH KAPACIT ANI FINANČNÍCH ZDROJŮ NA JEJICH ZAPLACENÍ.

Dění v oblasti eGovernmentu začíná v poslední době připomínat houpačku: nejprve jsou nastoleny velké a ambiciózní cíle, aby se záhy narazilo na realitu a na poslední chvíli se z nich zase notně slevilo.

Před rokem, v závěru roku 2022, šlo o zřizování datových schránek všem fyzickým osobám, které na sebe prozradí, že jsou informačně gramotné. Konkrétně tak, že se dokážou někam přihlásit pomocí své identity občana. Dnes již víme, jak to dopadlo: s velkým vypětím a doslova na poslední chvíli se podařilo od tohoto záměru ustoupit. A ještě se to svým způsobem oslavovalo jako úspěch: že se podařilo zabránit nejhoršímu. Byť jen u nepodnikajících fyzických osob.



S příchodem letošního roku vznikla nová Digitální a internetová agentura a po třech měsících převzala eGovernment do své gesce.

Z čeho se nakonec ani na poslední chvíli neslevilo, bylo kompletní „přepřáhnutí“ českého eGovernmentu. To když s příchodem letošního roku (2023) vznikla nová Digitální a internetová agentura (DIA) a po třech měsících převzala eGovernment do své gesce. Byl to luxus, jehož pouhá implementace (vybudování a rozjezd agentury) si vyžádala nemalé lidské a finanční zdroje, které se musely někde vzít (a jinde nutně budou chybět). Nehledě na důsledky v podobě odkladu jiných věcí, které musely počkat na zřízení a „záběh“ nové agentury.

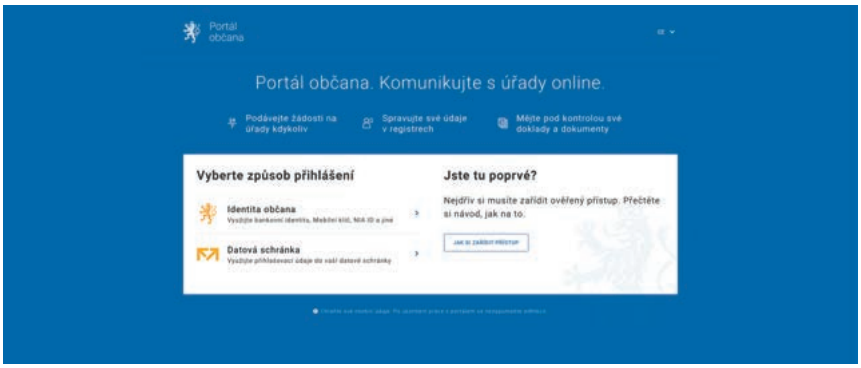
Co se bude řešit na poslední chvíli letos?

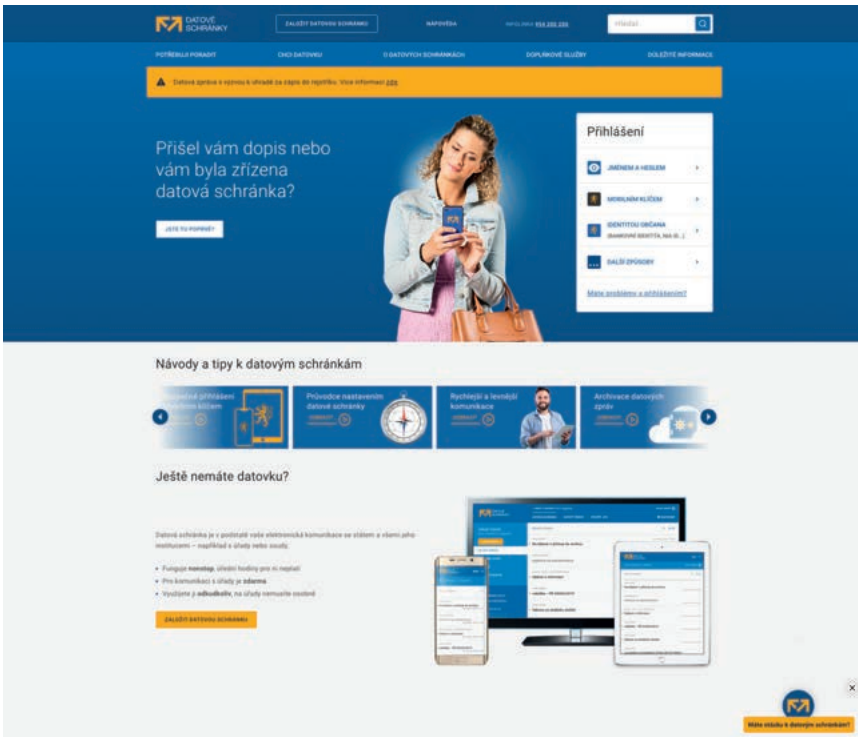
V závěru letošního roku by se dramatický „vývoj na poslední chvíli“ mohl opakovat. Tentokrát kolem našeho národního projektu digitalizace osobních dokladů, známého jako eDoklad (dříve též eDokladovka), a spočívajícího v zavedení tzv. digitálních stejnopisů průkazů. Zpočátku hlavně občanského průkazu, ale potenciálně i dalších průkazů a osvědčení (obecně: dokladů). Celý projekt eDoklad je „rozfázován“ do tří etap:

- od 1. 1. 2024 mají mít povinnost přijímat digitální stejnopisy průkazů (pro potřeby ověřování totožnosti) ústřední správní orgány.
- od poloviny roku 2024 pak mají mít stejnou povinnost i ostatní státní orgány, kraje a obce s rozšířenou působností.
- od počátku roku 2025 pak budou mít tuto povinnost ostatní orgány veřejné moci a také soukromoprávní osoby (pokud jim zákon uloží povinnost ověřovat totožnost).

Dobré je ale vědět, že tímto projektem se pouštíme do vlastního řešení něčeho, o čem dobře víme, že záhy přijde jako jednotné celounijní řešení, s větším repertoárem funkcí a širšími možnostmi využití, v podobě tzv. evropské peněženky digitální identity (EUDIW, EU Digital Identity Wallet). Práce na implementaci již probíhají a s plnou dostupností se počítá pro rok 2026.

A i když něco z našeho vlastního řešení snad bude možné využít i v rámci celounijního řešení, přece jen je otázka, zda je rozumné a efektivní pouštět se na přechodnou dobu do vlastního řešení využitelného jen





Projektem eDoklad se pouštíme do vlastního řešení něčeho, o čem víme, že záhy přijde jako jednotné celounijní řešení.

v tuzemsku – když poměrně brzy (cca v roce 2026) budeme muset nasadit a podporovat i řešení s evropskou peněženkou, fungující v celé EU. Jako bychom snad měli přebytek odborných kapacit a finančních zdrojů a hledali pro ně nějaké uplatnění.

Pokud jde o očekávané náklady na naše vlastní eDoklady, ty opravdu nebudou malé. Centrální vývoj celého řešení podle odhadů přijde jednorázově na cca 50 milionů korun. Mnohem větší (desetinásobné, cca půl miliardy) pak mají být jednorázové náklady napříč veřejnou správou.

Nad vším se ale ještě vznáší důležitý otazník: aby mohl být celý náš národní projekt eDoklad uveden v život, musí pochopitelně být nejprve ukotven v právní úpravě. Konkrétně do zákona č. 12/2020 Sb., o právu na digitální služby, musí být vloženo nové právo: na využití digitálního stejnopisu průkazu.

Příslušný legislativní návrh již je v Poslanecké sněmovně (jako sněmovní tisk č. 548), kam se dostal na konci září. Šance na jeho řádné přijetí ještě v letošním roce a nabytí účinnosti k 1. 1. 2024 tak stále je. Ale také se to nemusí stihnout.

Jak se z 1 GB stane 100 MB?

Jiným příkladem rozporu mezi ambicemi a realitou, který vedl k odkladu a redukci původních záměrů, je snaha

o zvětšení maximální velikosti datových zpráv v datových schránkách. Dnes je maximem 20 MB a u privilegovaných datových schránek (typu OVM, zřizovaných na žádost) 50 MB. Což ale mnohdy nemusí stačit.

Proto je již nějakou dobu „v plánu“ významné zvětšení velikosti datových zpráv, až na 1 GB, v podobě tzv. velkoobjemových datových zpráv (VoDZ). Původně k tomu mělo dojít již k počátku roku 2023. Pak to bylo posunuto na polovinu roku 2023. Letos to bylo opět odloženo, na počátek roku 2024 – navíc s tím, že místo 1 GB bude maximální velikost jen desetinová, tedy pouze 100 MB. Vyhovělo se tím připomínkám z mezirezortního připomínkového řízení, které poukazovaly na nepřipravenost spisových služeb na tak velké datové zprávy.

Aby to ale vůbec bylo alespoň oněch 100 MB místo původně zamýšleného 1 GB a současných 20 (či 50) MB, musí být ještě včas schválena novela prováděcí vyhlášky č. 194/2009 Sb. K původní verzi návrhu novely, která počítala s 1 GB a je v eKlepu od února, se teprve 20. září přidala novější verze, která počítá již jen s oněmi 100 MB.

Kdy bude eSbírka a eLegislativa? Kdy digitální stavební řízení?

Skutečným rekordmanem v odkládání je záměr digitalizace (původně ještě: elektronizace) celého legislativního procesu a Sbírky zákonů. První zmínky o projektech eLegislativa a eSbírka pocházejí ještě z let 2006 až 2007, z éry ministra vnitra Ivana Langera a jeho náměstka Zdeňka Zajíčka, a vznikly jako součást projektu eGon. Tedy souběžně s projekty datových schránek či základních registrů. Na rozdíl od nich ale eSbírku ani eLegislativu dosud nemáme.

> **Skutečným rekordmanem v odkládání je záměr digitalizace celého legislativního procesu a Sbírky zákonů.**

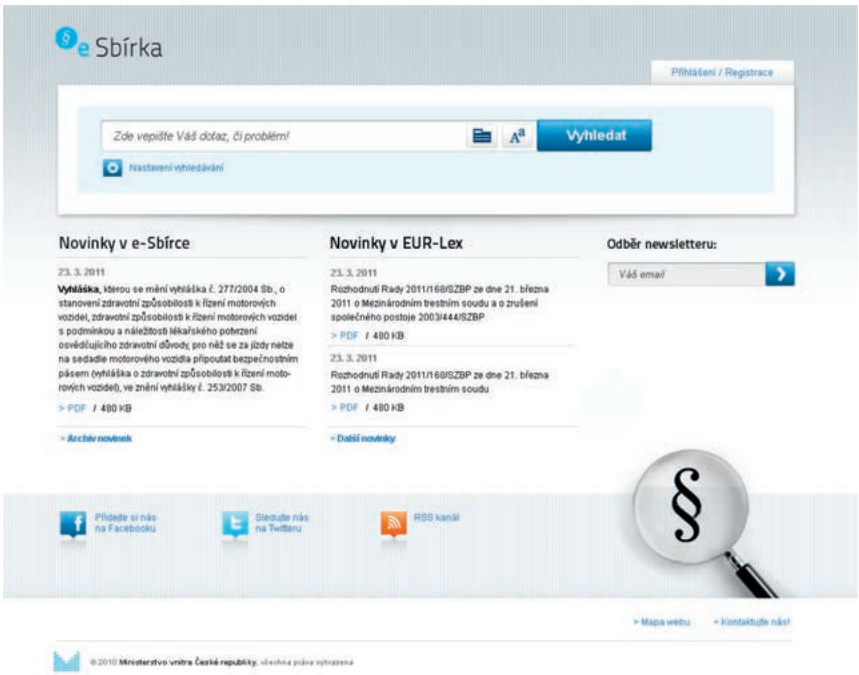
Po všech možných odkladech by nejnovějším termínem ostrého startu eSbírky a eLegislativy měl být 1. leden 2024. Opět ale má být na poslední chvíli fakticky odložen. Formálně: nahrazen postupným náběhem, rozfázovaným do několika etap. Takže třeba zákony mají být v eSbírce dostupné až od roku 2025.

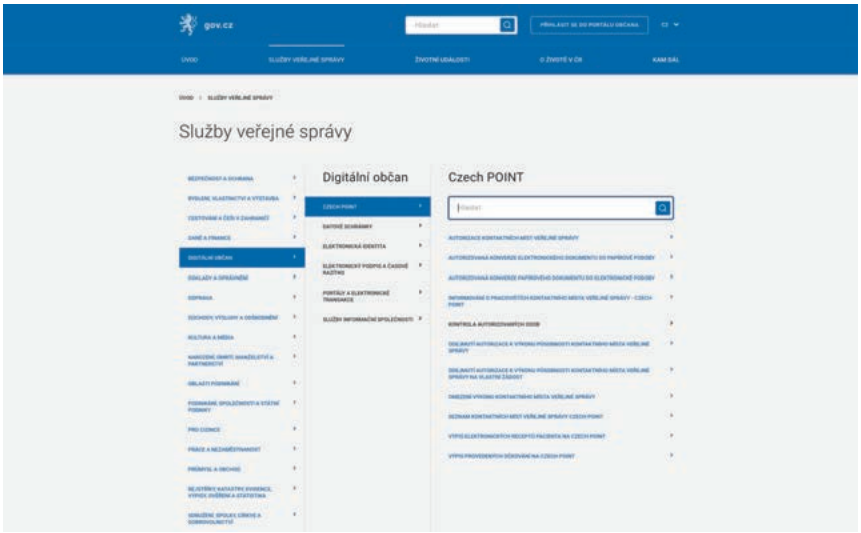
Jinou ukázkou „nárazu na realitu“ může být i osud digitalizace stavebního řízení. Ta má být spuštěna k 1. 1. 2024 (u vyhrazených staveb), resp. k 1. červenci 2024 u ostatních staveb. Ovšem poté, co ÚOHS nedávno zastavil zakázku na realizaci nezbytného informačního systému pro digitalizaci stavebního řízení, se řeší, „jak dál“. Jednou z navrhovaných možností je i další odklad celé digitalizace.

Osvědčení o digitálním úkonu: Co to vlastně má být?

Rozpor mezi ambicemi a realitou je dobře vidět i na praktickém naplňování „vlajkové lodi“ naší digitalizace, a to zákona č. 12/2020 Sb., o právu na digitální služby. Byl přijat s velkou slávou, stal se zákonem roku 2019 a dodnes je přirovnáván k digitální ústavě. Jeho ustanovení nabývají účinnosti postupně, ale s jejich praktickým naplněním to už taková sláva není.

Například již od února 2022 mají uživatelé služeb eGovernmentu právo získat osvědčení o digitálním úkonu. Reálně jej skutečně mohou získat, ale jen pro několik málo konkrétních úkonů v rámci několika specifických služeb. Protože ty ostatní dodnes řeší, jak rozumět tomu, co si zákon navy-





myšlel, a jak (a zda vůbec) se tomu dá dostát. Problém je mj. v tom, že zákon si přeje, aby osvědčení obsahovalo identifikaci digitálního úkonu v rámci určité služby a také určení toho, kdo úkon činí. Jenže dokud bude existovat možnost nestrukturovaného podání neboli možnost napsat volným textem, co a kým je požadováno, a možnost odeslat to různými způsoby (třeba z cizí datové schránky či z anonymního e-mailu), musí někdo přečíst obsah, pokusit se mu porozumět a určit, o jaký konkrétní úkon jde a kdo jej činí. Dokud to nenaučíme umělou inteligenci, musejí to dělat lidé a nelze to zautomatizovat.

Ale jelikož by to „dalo moc práce“, objevují se snahy zredukovat osvědčení o digitálním úkonu na prosté potvrzení o dodání nějaké zásilky. Takové, jaké již dnes automaticky generují elektronické podatelny, když jim přijde nějaký e-mail, aniž ještě zkoumají jeho obsah.

Kompletní digitalizace: Do února 2025 má být hotovo

Digitální ústava neboli zákon č. 12/2020 Sb., o právu na digitální služby, má ještě řadu dalších cílů.

Ambiciózním cílem zákona č. 12/2020 Sb., o právu na digitální služby, je záměr zdigitalizovat všechny služby uvedené v Katalogu služeb.

A jeden, který je určitě nejambicióznější. Není to nic menšího než záměr zdigitalizovat všechny služby uvedené v Katalogu služeb. Zjednodušeně všechny služby eGovernmentu, u kterých je to principiálně možné a u nichž právní úprava nepředepisuje něco jiného. A to do 1. února 2025 a v tom smyslu, aby pro všechny úkony v rámci těchto služeb existoval inteligentní formulář umožňující přihlášení uživatele a předvyplnění všech již známých údajů.

Takových služeb je opravdu hodně (přes 7 000) a jednotlivých úkonů v rámci těchto služeb ještě více (přes 32 000). Všechny tyto úkony mělo být možné činit jak skrze (samoobslužný) portál, tak i datovou schránkou nebo e-mailem (s alespoň uznávaným elektronickým podpisem).

Asi není nutné zdůrazňovat, jak mamutí úkol to je, kolik práce to obnáší i jak velké náklady si to vyžádá.

Dlouholetý prezident ICT Unie a nyní i prezident Hospodářské komory Zdeněk Zajíček coby jeden z duchovních otců nynější digitální ústavy opakovaně burcuje celou veřejnou správu před blížícím se termínem 1. února 2025, do kdy má „být hotovo“. A apeluje i na včasné rozpočtování zdrojů pro rok 2024, potřebných pro dosažení tohoto cíle.

Ano, bez toho to nepůjde. Ani bez lidí s potřebnou kvalifikací, schopnostmi a ochotou pracovat. Zatím jsme ale až tak moc nepokročili. Navíc se nacházíme v době, kdy celá společnost musí šetřit, a většina orgánů veřejné moci musí řešit mnohem přízemnější věci: jak i přes nejrůznější škrty a redukce finančních prostředků i tabulkových míst „zůstat naživu“ a fungovat alespoň tak jako doposud.

Takže: bude po letech bez výraznějšího spěchu rok 2024 rokem velkého vzepětí a závěrečného finiše před cílovou metou digitální ústavy? Podaří se zmobilizovat dostatek kapacit i zdrojů a dohnat to, co se dosud až tak moc nedařilo? Nastane konečně onen slibovaný digitální ráj na zemi, kdy mezi úřady a jejich plně digitalizovanými agendami konečně nebudou obíhat lidé, ale jen data?
Nebo přijde na poslední chvíli další odklad či jen nějaké snížení opravdu hodně vysoko nastavené laťky?

JIŘÍ PETERKA

Člen rady Českého telekomunikačního úřadu. Pedagog a publicista, který se specializuje na oblast eGovernmentu. ■

Nechte vaše data pracovat.

Chytře a pro vás.

IBM Platinum Partner

datera.cz


eDoklady
Nová éra prokazování totožnosti? Už brzy.
Co očekávat na začátku?

DIGITÁLNÍ OBČANSKÝ PRŮKAZ V MOBILU SE BLÍŽÍ

JAK BUDE FUNGOVAT ČESKÁ DIGITÁLNÍ OBČANKA A JAK SE TO S NÍ MÁ VZHLEDEM K CHYSTANÉ EVROPSKÉ DIGITÁLNÍ PENĚŽENCE?

Vláda v polovině září schválila novelu zákona o právu na digitální služby, která zavádí eDoklad – tedy možnost uložit občanku a další průkazy do mobilu. Návrh novely je k dispozici na portálu VeKLEP a čeká jej ještě schválení Parlamentem (do uzávěrky vydání se hlasování ještě neuskutečnilo, pozn. red.). Na základě jeho znění a obsahu důvodových zpráv se podíváme na to, jak by měl eDoklad fungovat a jak je to s ním vzhledem k chystané Evropské peněžence digitální identity.

Novela zavádí pojem „digitální stejnopis průkazu“ a definuje potřebnou infrastrukturu a procesy pro poskytování, používání a ověřování digitálních stejnopisů průkazů. Průkazem je možné prokazovat totožnost a případně jiné skutečnosti (libovolný průkaz, který má obraz v některém z agendových systémů).

EDoklad funguje následovně: úřad odpovědný za vydávání fyzického průkazu rozhodne o vydávání jeho digitálního stejnopisu. Zaregistruje průkaz do seznamu vedeného DIA a připraví technickou integraci s Portálem občana. Důležité je, že pro zavedení nových typů průkazů není potřeba změna zákona, jde o operativní akci, kterou legislativně plně pokrývá navrhovaná novela.

Pokud se držitel průkazu rozhodne, že chce využívat jeho digitální stejnopis, přihlásí se na Portál občana svou elektronickou identitou a vyžádá si vydání digitálního stejnopisu. Vydavatel průkazu údaje, které je možné z fyzického průkazu přečíst při jeho předložení, převede do elektronické formy.

Pokud je údajů větší množství, může vydavatel průkazu vytvořit několik „balíčků“, aby bylo možné předkládat jen část údajů z průkazu. Takto vytvořené balíčky informací zapečetí zaručenou elektronickou pečetí založenou na kvalifikovaném certifikátu a skrze Portál občana umožní jejich uložení do mobilní aplikace eDoklad držitele průkazu. Takto vydané digitální stejnopisy mají platnost 48 hodin a vydavatel průkazu je musí každých 24 hodin obnovovat a aplikace eDoklad je zřejmě bude automaticky pravidelně stahovat.

Držitel průkazu má vydané digitální stejnopisy uložené v mobilní aplikaci eDoklad a může je používat místo fyzické verze průkazu. Držitelem digitálního stejnopisu mohou být i nezletilí, pokud mají elektronickou identitu. Digitální stejnopis lze vydat pouze k průkazu, který existuje ve fyzické podobě. Digitální stejnopis je určen k použití výhradně za osobní přítomnosti jak držitele, tak zástupce ověřovatele.

Digitální stejnopisy průkazu může ověřovat jak veřejnoprávní, tak soukromoprávní subjekt, tzv. ověřující. Ověřující se nejprve musí zapsat do neveřejného seznamu ověřujících, který vede DIA a do něhož je možné se zapsat pomocí aplikace pro správu ověřujících s využitím elektronické identifikace. Jakmile je ověřující zapsán v seznamu, může umožnit držitelům digitálního stejnopisu průkazu jeho použití.

Pro ověření průkazu je možné využít buď mobilní aplikaci eDoklad Ověření (název zavedený autorem článku), která funguje i bez připojení k internetu, nebo webovou aplikaci, pro jejíž použití musejí být obě strany „on-line“ a komunikace probíhá přes centrální server.

Kdo musí eDoklad akceptovat

Návrh zákona předepisuje povinnost akceptovat průkazy z aplikace eDoklad všem subjektům, kterým zákon ukládá

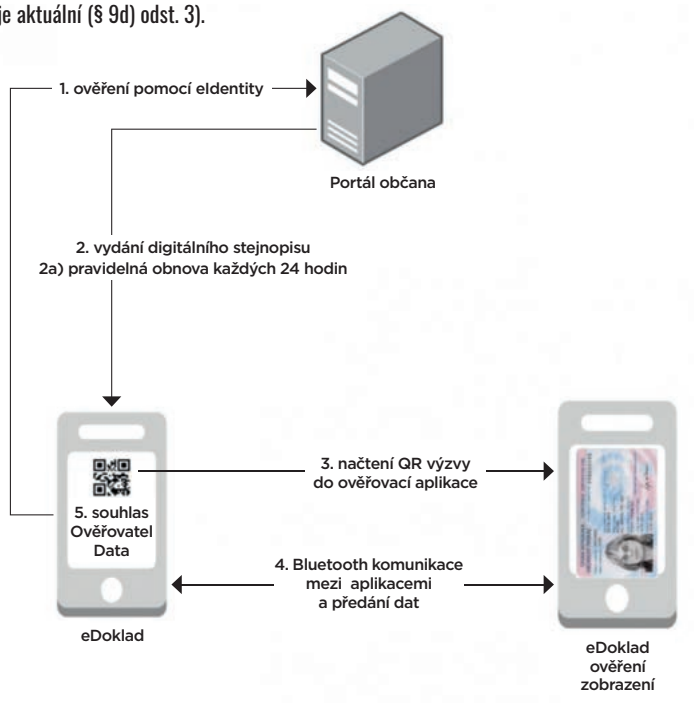
OVĚŘENÍ POMOCÍ MOBILNÍ APLIKACE

Ověření pomocí mobilní aplikace v off-line režimu je zachyceno na následujícím schématu a proces ověření je popsán pod obrázkem:

Držitel digitálního stejnopisu průkazu si zajistí jeho vydání na Portálu občana (1, 2). Při předkládání digitálního stejnopisu vyzve ověřovatel držitele. Držitel spustí mobilní aplikaci eDoklad a zobrazí QR kód. Ověřovatel spustí ověřovací mobilní aplikaci a načte QR kód z aplikace držitele (3). Na základě údajů z QR kódu navážou aplikace komunikaci pomocí Bluetooth a dojde k výměně dat (4). Před odesláním údajů z průkazu je držiteli zobrazena informace o identitě ověřovatele a požadované sadě dat. Držitel schválí (nebo odmítne) poskytnutí údajů (5). Údaje jsou poté přeneseny přes Bluetooth spojení (4) a ověřovací aplikace údaje (pečeť) ověří a zobrazí.

Celá komunikace může probíhat bez připojení k internetu. Při off-line režimu použití musí mít držitel v aplikaci dostatečně „čerstvou“ verzi digitálního stejnopisu. Nesmí být starší 48 hodin. Tzn. aplikace eDoklad musela být připojena k internetu v uplynulých 48 hodinách před ověřováním, jinak jsou digitální stejnopisy neplatné.

Pokud aplikace eDoklad má k dispozici připojení, musí ověřit, zda předkládaný digitální stejnopis je aktuální (§ 9d) odst. 3).



Návrh zákona předepisuje povinnost akceptovat průkazy z aplikace eDoklad všem subjektům, kterým zákon ukládá povinnost ověřovat totožnost. Nedopadá tak jen na veřejnoprávní subjekty, ale také na subjekty soukromoprávní.

povinnost ověřovat totožnost. Nedopadá tak jen na veřejnoprávní subjekty, ale také na subjekty soukromoprávní. Protože časový plán vydání zákona je ambiciózní, je povinnost akceptovat eDoklady rozvolněna v čase. EDoklad budou muset akceptovat:

- Od vyhlášení zákona ústřední správní orgány
- Od 1. 7. 2024 ostatní orgány veřejné správy včetně krajů a obcí (dobrovolně mohou kdykoli od vyhlášení zákona)
- Od 1. 1. 2025 soukromoprávní subjekty povinné ověřovat totožnost (finanční instituce v rámci AML, školy, zdravotnická zařízení apod. – dobrovolně mohou kdykoli od vyhlášení zákona)

Kromě subjektů, pro které je akceptace eDokladu dříve či později povinná, návrh zákona umožňuje využít eDoklad prakticky komukoli v rámci soukromoprávního jednání. Alespoň prozatím se nezdá, že by zápisu na seznam ověřovatelů byly kladeny nějaké překážky. Kdokoli má zaručenou identitu, může se na seznam zapsat. Doufejme, že toto paradigma bude přejato také pro budoucí implementaci ekosystému Evropské peněženky digitální identity a systém státem garantované identity se zcela otevře.

Uvidíme, jestli již od vyhlášení zákona bude kromě povinnosti eDoklad akceptovat také možné eDoklad získat.

Údaje získané při ověřování z digitálních stejnopisů průkazů bude možné přímo ukládat do informačních systémů. Pro přímé uložení elektronické verze je jako součást novely upravena textace AML zákona, který ukládá finančním institucím pořizovat kopie dokladů.

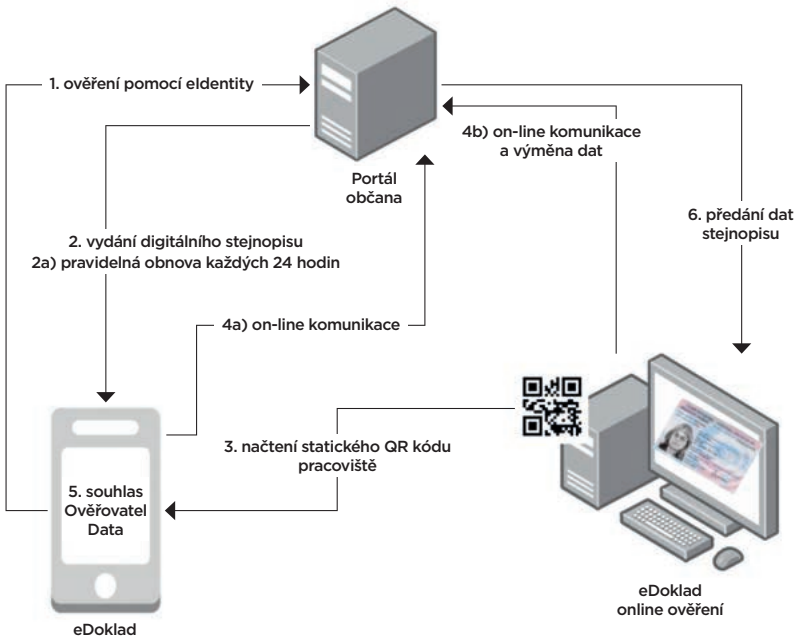
Náklady na akceptaci

Důvodová zpráva uvádí, že státní správa na zavedení a akceptaci dokla-

OVĚŘOVÁNÍ U WEBOVÉ APLIKACE

Při použití webové aplikace je postup ověřování následující:

Držitel digitálního stejnopisu průkazu si zajistí jeho vydání na Portálu občana (1, 2). Na ověřovacím pracovišti je umístěn statický QR kód. Ověřovatel vyzve držitele k naskenování QR kódu pracoviště. Držitel spustí mobilní aplikaci eDoklad, naskenuje QR kód (3). Aplikace eDoklad naváže na základě QR kódu spojení se serverem (4a). Prostřednictvím serveru se propojí webová aplikace s mobilní aplikací. Držiteli je v aplikaci eDoklad zobrazena informace o identitě ověřujícího a výčet požadovaných údajů. Držitel průkazu odsouhlasí (nebo odmítne) předání údajů. Webová aplikace pak ověří údaje (pečeť) a zobrazí získané údaje.



EDoklady jsou českým předvojem připravované Evropské peněženky digitální identity (EDIW). EDoklady mají jisté rysy shodné se zamýšlenými funkcemi EDIW a lze předpokládat, že jednoho dne se možná aplikace eDoklady změní na implementaci právě jednotné evropské peněženky.

dů vynaloží padesát milionů korun na centrální části řešení a aplikace v průběhu let 2023 až 2026. Celkové náklady napříč státní správou na akceptaci eDokladu jsou odhadovány na cca půl miliardy korun jednorázově a následně cca šedesát milionů korun ročně provozních nákladů.

Převážná část nákladů je vyvolána nákupem mobilních zařízení pro ověřování, kde se předpokládá cena přibližně tři tisíce korun na jedno zařízení. Náklady, které se zavedením eDokladu budou mít samosprávy, jsou odhadovány asi na 135 milionů korun jednorázových nákladů.

Evropská peněženka digitální identity

EDoklady jsou českým předvojem připravované Evropské peněženky digitální identity (EDIW). EDoklady mají jisté rysy shodné se zamýšlenými funkcemi EDIW a lze předpokládat, že jednoho dne se možná aplikace eDoklady změní na implementaci právě jednotné evropské peněženky. Pro EDIW existuje již druhá verze (1.1.0) referenční architektury Evropské peněženky digitální identity, a můžeme tedy srovnávat.

Digitální stejnopis průkazu je obdobou elektronické atestace atributů, jak je zavádí EDIW.

Vytváření balíčků nesoucích jen podmnožinu údajů průkazu odpovídá funkci tzv. selective disclosure, která je také součástí ARF.

EDIW má také on-line a off-line scénáře. V případě EDIW je vidět silnější důraz na ochranu soukromí, kde při ověřovacích procesech je zakázáno, aby se o použití peněženky dozvěděl vydavatel průkazu (atributů), a to i při on-line scénáři, kdy ověřování probíhá přímo mezi dvěma zúčastněnými subjekty, a ne přes třetí server.

EDIW zavádí rejstříky vydavatelů atributů a rejstřík spoléhajících stran. EDoklad analogicky pracuje se seznamem ověřovatelů a také se seznamem průkazů, k nimž lze získat digitální stejnopis. EDIW je v tomto bodě výrazně otevřenější, zavádí dvě úrovně atributů (kvalifikované a ostatní) a otevírá celý ekosystém jak veřejnoprávním, tak soukromoprávním vydavatelům atributů. Součástí ARF je navíc rejstřík schémat atributů.

Platnost atributů

Problematiku odvolávání platnosti průkazu/atributů řeší eDoklady striktním nastavením délky platnosti na 48 hodin. Jde o kompromis mezi spoléháním se na platnost údajů a nutností obnovovat neustále doklad uložený v telefonu. Celá odpovědnost zajištění platného stejnopisu je na jeho držiteli a neexistuje svoboda volby, kdy by si ověřovatel mohl rozhodnout,

nakolik bude důvěřovat údajům v digitálním stejnopisu v off-line scénářích a sám si řídit riziko.

DIA si na sebe šije bič neustále vytěžovaného datacentra. Každý stejnopis musí být nejméně jednou za den podepsán a nová verze podepsaného balíku stažena do telefonu držitele. Dovedu si představit, že správci infrastruktury se modlí, aby eDoklady nebyly přespříliš úspěšné. Pokud by eDoklady používaly miliony lidí a měly vydané desítky průkazů, mají centrální servery zaděláno na neustálou zátěž spojenou s nekončícím přepočítáváním podpisů.

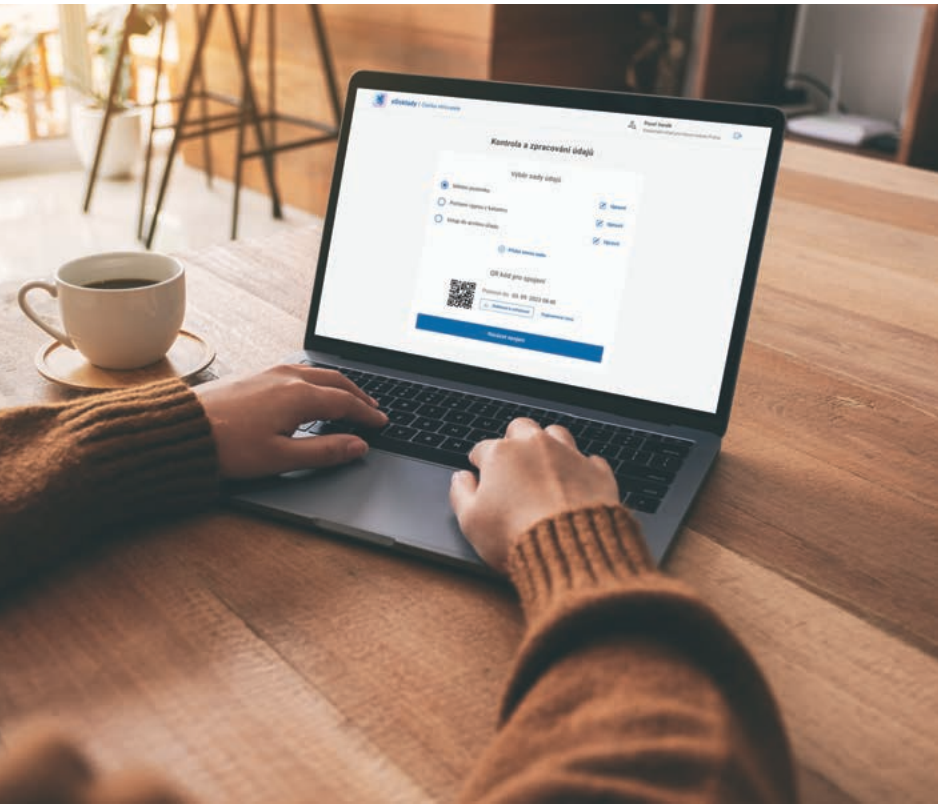
Odvolávání platnosti atributů je jednou z nejtěžších úloh i pro EDIW založenou na Self Sovereign Identity. Při kontrole platnosti atributu je třeba zachovat soukromí uživatele. Není tedy možné se doptávat na atributy konkrétního držitele u vydavatele atributu, ale je potřeba definovat protokol poskytující alespoň částečné soukromí na bázi seskupování stavů platnosti pro dostatečně velkou skupinu držitelů.

Ochrana osobních údajů

Součástí návrhu zákona ani v souvisejících dokumentech není nijak hodnocen dopad používání eDokladu na soukromí při použití eDokladu. Důvodová zpráva se zabývá ochranou osobních údajů, ale už ne soukromím při použití. Není se však čemu divit. Soukromí v dnešním centralizovaném nastavení systému elektronické identity je nulové a zjevně není něčím, s čím by si státní úředníci lámali hlavu. Jenže eDoklad mění paradigma. Elektronickou identitu je dnes v ČR možné použít pouze vůči orgánům veřejné správy a výjimečně vůči soukromoprávním subjektům.

Nyní se nově otevírá možnost použít eDoklad i v soukromoprávním jednání. Pro tuto novou situaci je ignorace požadavků na soukromí při použití problematická. Pokud se já jako soukromá osoba rozhodnu použít eDoklad a předložím ho jinému soukromému subjektu, nemusí mi být milé, že by se o této interakci dozvěděl vydavatel dokladu.

Když tuto transakci uskutečním plastovou občankou, informace nikam neunikají. Pokud zvolím eDoklad, i v případě mobil-mobil interakce zákon ukládá ověřit platnost stejnopisu, a dojde tedy k záznamu o jeho použití. Při mobil-desktop variantě je



> **V průběhu připomínkování byla ze zákona vyjmuta možnost získat digitální stejnopis průkazu také přímo na Portálu občana.**

dokonce zaznamenána identita ověřujícího na centrálním serveru. Tenhle aspekt by bylo vhodné doladit.

V důvodové zprávě se připouští, že ověřovací aplikace v budoucnu bude moci být nejen ta státem poskytnutá, bude definován proces akreditace jiných implementací.

Digitální stejnopis na Portálu občana

V průběhu připomínkování byla ze zákona vyjmuta možnost získat digitální stejnopis průkazu také přímo na Portálu občana. Panovala obava, že kdyby bylo možné získat přímo použitelný digitální stejnopis, mohly by přijít pokusy o použití na dálku.

Nejsem si jist, zda se podařilo toto riziko eliminovat. Při použití modelu desktop-mobil, kdy je na desktopu používána webová ověřovací aplikace a na straně držitele mobil, nic nebrání tento scénář uskutečnit na dálku. Stačí přenést statický QR kód do aplikace eDoklad. Při komunikaci přes server nemusejí být účastníci transakce na stejném místě. Bude to v rozporu se zákonem a nebudou existovat žádné garance vyplývající z legislativy, ale zřejmě to bude možné.

Něco na závěr

A na závěr jedna perlička z připomínek. Ministerstvo dopravy vyjádřilo názor, že některé průkazy jsou podle jeho názoru nedigitalizovatelné. Silně to připomíná reakce úřadů při tvorbě katalogu služeb a hodnocení možnosti jejich digitalizace, kdy se hledaly důvody, proč něco nejde digitalizovat, ale ve skutečnosti šlo pouze o zkostnatělost. Ministerstvo dopravy v roce 2023 prohlašuje, že například průkaz řidiče taxislužby je nedigitalizovatelný, protože:

„Průkaz řidiče taxislužby prokazuje, že jeho držitel je oprávněn vykonávat práci řidiče taxislužby, přičemž dle ustanovení § 21d odst. 3 zákona o silniční dopravě má být ve vozidle vystaven tak, aby se cestující mohl seznámit s údaji na něm uvedenými. Nadto zákon o silniční dopravě zná institut zadržení průkazu řidiče taxislužby v případě podezření ze spáchání závažného přestupku způsobujícího nespolehlivost. Pokud by tento průkaz mohl být v digitální podobě, nebylo by možné průkaz zadržet.“

Žádný z argumentů zde uvedených není relevantní. Vystavit informace o identitě řidiče taxíku lze na libovolném kusu papíru třeba v předepsaném formátu a klidně vybaveném QR kódem pro digitální ověření. U řidičského průkazu také existuje možnost odebrání, a přesto nebude od příštího roku povinnost ho nosit. Tuhle posedlost laminovanými papírky je potřeba vymýtit. Ve skutečnosti je jen velmi málo dokladů, které nelze digitalizovat. Ostatně jsou to vždycky pouze nosiče informace.

LUDĚK RAŠEK

Autor je open [mind|source|data] positive IT architekt idealista snažící se přežít v korporaci s touhou i po dvaceti letech v oboru tvořit systémy, které pomáhají nebo aspoň neprudí. ■

Pro bezpečí i pohodlí

K OBLASTEM S NEJRYCHLEJŠÍM RŮSTEM A NEJVĚTŠÍM TEMPEM ZMĚN DNES PATŘÍ INFORMAČNÍ TECHNOLOGIE. JEDEN SEGMENT ROSTE V RÁMCI CELÉHO IT JEŠTĚ VÝRAZNĚJI. JE TO CLOUD.

V cloudu lze provozovat nejrůznější produkty, tedy i ERP systémy. Proto i lídr na trhu podnikových informačních systémů Asseco Solutions poskytuje již řadu let svým klientům možnost provozovat své ERP systémy Helios v cloudu. Posledních osm let se tak děje ve spolupráci s expertem na multicloudová řešení, společností Geetoo Technology, díky níž vzniklo cloudové řešení ERPORT.

„Pokud používáte Helios, měli byste používat ERPORT. Kvůli bezpečí a jistotě, ale také z pohledu nákladů. ERPORT totiž mění nastavení podle vašich potřeb, takže minimalizuje zbytečné náklady, nebo naopak umožní rychle růst a absolutně neřešit infrastrukturu," říká Jakub Herink, obchodní ředitel Geetoo Technology.

Eliminovat riziko kyberútoků

Ochrana dat je totiž čím dál aktuálnější a týká se všech firem. Souvisí s postupující digitalizací pracovního prostředí, která přináší nejen řadu výhod, ale též mnohá rizika. Největší z nich představují kybernetické útoky. Jedním ze způsobů, jak jejich riziko snížit, je využívání cloudu.

„Doby, kdy si firmy nedovedly představit, že by své systémy a svá data měly ‚někde v cloudu', už je minulostí," říká Michal Andraško, obchodní ředitel Asseco Solutions. „Dnes je již všeobecně známo, že data uložená v cloudu jsou ve větším bezpečí než na vlastním serveru. Přičemž právě díky sofistikované cloudové infrastruktuře od Geetoo a službě ERPORT od Asseco Solutions mohou mít firmy opravdový pocit jistoty," dodává.

Věnovat se naplno vlastnímu byznysu

Během let, kdy Asseco Solutions nabízí cloudovou infrastrukturu ERPORT, se počet jejích zákazníků více než ztrojnásobil. Jednou z firem, které možnosti ERPORT vyzkoušely, je i logistická společnost Rohlig SUUS Logistics. Ta již od vstupu na český a slovenský trh systém využívá Helios. Firma však nechtěla systém provozovat sama, protože nemá potřebné IT pracovníky, a tak ho od počátku využívala v cloudu. Po nepříznivé zkušenosti s jiným poskytovatelem přešla na službu ERPORT od Asseco Solutions.

„Přínosy pro firmu vnímám zejména v dostupnosti našeho provozního systému odkudkoliv, v zabezpečení dat, v možnosti navýšit kapacitu i objem uložených dat téměř okamžitě a ve vlastní podpoře ze strany dodavatele," říká Jiří Chládek, výkonný ředitel Rohlig SUUS Logistics pro Česko a Slovensko, a dodává: „O technické řešení se starají odborníci, my máme možnost se věnovat naplno oboru naší činnosti, kterému rozumíme, a tím je doprava a logistika. Standardní součástí služby ERPORT je navíc zabezpečení našich dat i celého systému na korporátní úrovni, a to je výhoda, kterou si nemůže dovolit každá firma."

REA KŘÍŽOVÁ
Brand manager ve společnosti Asseco Solutions ■

Michal Andraško, obchodní ředitel Asseco Solutions, a Jakub Herink, obchodní ředitel Geetoo Technology, při předávání ocenění Partner roku.

PROPUSTILI JSME PĚTINU FIRMY, ALE BYLO TO SPRÁVNÉ ROZHODNUTÍ

LIDÉ UŽ SE NAUČILI NAKUPOVAT NÁBYTEK A BYTOVÉ DOPLŇKY ON-LINE, ŘÍKÁ PAVEL VOPAŘIL, VÝKONNÝ ŘEDITEL E-SHOPU BONAMI. OBCHOD S TÉMĚŘ DESETILETOU HISTORIÍ SE MUSEL VYPOŘÁDAT S ROSTOUCÍ KONKURENCÍ, TLAKEM NA CENY I POSTCOVIDOVÝM PROPADEM TRHU. TEĎ SE CHYSTÁ NA EXPANZI.

Když jste v roce 2019 nastupoval na pozici ředitele Bonami, mělo tržby někde kolem půl miliardy korun a tehdy jste v rozhovoru na Lupě říkal, že do tří let z něj bude třímiliardová firma. Povedlo se? A jak vlastně na tom Bonami dnes je?
Nepovedlo se to. Ta čísla, která vidíte v obchodním rejstříku, jsou čisté tržby neboli to, co se vyveze ze skladu. Když vezmu hodnotu objednávek, pak v roce 2018 to bylo někde kolem 800 milionů. V roce 2019 jsme poprvé překonali miliardu, a proto jsem doufal a věřil, že růst akceleruje. Nakonec zrychlil podstatně rychleji v době covidu, kdy jsme se přiblížili dvěma miliardám. Takže jsme měli velmi záhy nakročeno k té třímiliardové firmě, ale pak se začalo dít to, co se začalo dít, a v loňském roce jsme oproti roku 2021 poklesli. Teď si vlastně potřebuji dát nový cíl a nové číslo, ke kterému chci směřovat.

Pořád můžete mířit ke třem miliardám a jen si prodloužit ten termín…
Spíš bych teď chtěl směřovat k deseti miliardám a ten termín prodloužit trošku víc, takže to je zhruba střednědobý cíl (smích).

Když Bonami startovalo, hodně se mluvilo o tom, jestli se lidé naučí nakupovat nábytek a bytové doplňky přes internet. Vypadá to jako specifická disciplína – když si chci koupit pohovku, chci si na ni nejdříve sednout, nestačí mi vidět jenom obrázky. Jak to vidíte z dnešního pohledu – naučili, nebo nenaučili?
Krátká odpověď zní, že naučili. Delší odpověď je, že Bonami prvních, řekněme, pět šest let své existence nebylo moc nábytkové. Vlastně skoro vůbec. Dokonce bych řekl, že Bonami prvních pět šest let nebylo ani e-commerce v tom pojetí, jak ten pojem asi všichni chápeme. E-commerce děláme tak tři čtyři roky. Do té doby bylo Bonami nákupním klubem, který fungoval na dost jiných principech a všechny dovednosti, které potřebuješ mít pro e-commerce, jsme se postupně museli učit. I dnes, po deseti letech

FOTO: DANIEL ČÁHA

na trhu, máme z nábytku zhruba 40 procent tržeb a 60 procent jsou stále bytové doplňky. K tomu, aby lidé začali nakupovat víc nábytek, nám pomohlo několik věcí. Výrazně jsme rozšířili nabídku. To znamená, že je pro zákazníka možnost volby v porovnání s kamennými obchody podstatně širší, ať už jde o cenové úrovně, styly nebo i barvy. A druhá věc je, že jsme po mém nástupu výrazně investovali do infrastruktury – od velikosti skladu a zásob až po logistické cesty. Důležité je nejenom zboží dostat ze skladu ven, ale hlavně je potom doručit zákazníkovi až do bytu.

Spustili jsme službu Bonami Kurýr, což je dvoučlenná posádka, která pohovku vynese do bytu, rozbalí, složí, odveze obaly a třeba odstěhuje i starou pohovku. Tato nadhodnota je pro některé zákazníky důležitější než možnost si na tu pohovku sednout. Kromě toho nabízíme 365 dní na vrácení zboží. Pokud by vám ta pohovka nevyhovovala, přijedeme si ji zdarma vyzvednout a zase ji odvezeme. A když mluvíme o pohovkách, spustili jsme nedávno službu, že si zákazník může ještě před nákupem objednat domů vzorek potahu. Snažíme se co nejvíc přiblížit zkušenost, kterou zákazník má, když jde do kamenného obchodu. Máme i projekty typu testování tvrdosti sedáku a tak dále.

Taky vám vyrostla konkurence. V Česku se říká, že většina lidí nakupuje nábytek v IKEA. A IKEA se taky vrhla do on-linu, byť z mé zkušenosti je zážitek z jejich e-shopu dost tragický a je vidět, že jej nemají jako hlavní způsob prodeje. Zaznamenali jste vstup IKEA do on-linu nějakým způsobem u svých zákazníků? Neučí IKEA lidi nakupovat on-line a nepo-

máhá to i vám? Nebo je to naopak konkurence, která vám ubírá?
Asi od obojího trochu, ale já to spíš vítám. Když hlavní tržní síla začne učit lidi kupovat on-line, trošku se nám vyrovnávají karty v ruce. Od začátku jsem věděl, že chci, aby náš byznys měl i nějakou kamennou nohu. Chci umožnit zákazníkům, pro které je on-line moc, aby si mohli jít zboží vyzkoušet nebo se poradit či si na ně sáhnout. A z druhé strany, pokud kamenní hráči budou dále učit celou populaci, že on-line je fajn, tak já to jenom vítám.

Bonami dnes působí v jedenácti zemích, to už je opravdu velké číslo. Jak na tom vlastně je obratově Česká republika ve srovnání s tím, co utržíte v zahraničí?
V Česku děláme lehce pod 40 procent celku, takže už jsme více mezinárodní než česká firma a roste to.

Polsko, Slovensko, Chorvatsko, Maďarsko, Litva, Lotyšsko, Slovensko, Bulharsko a teď nedávno Estonsko. To je velký rozstřel. Jak při té expanzi vlastně postupujete? Zakládáte v cizině vlastní týmy, vlastní pobočky, vlastní sklady, nebo všechno řídíte z Prahy?
Přístup Bonami k expanzi byl od začátku, řekněme, „light“ a používáme centrální model. Nemáme v zahraničí lokální týmy a všechno obsluhujeme z Prahy – jak z hlediska lidí, tak logisticky. Jediná změna, která nastala v době covidu, je, že nenajímáme lidi v Praze, ale v těch lokálních zemích, ale oni pracují z těchto zemí vzdáleně. Když dnes rozjíždíme expanzi, máme určitý „playbook“, který je vyladěný. Spustit novou zemi nám trvá dva tři měsíce. Nejvíce času zaberou překlady, protože je náš katalog poměrně obsáhlý.

Chci umožnit zákazníkům, pro které je on-line moc, aby si mohli jít zboží vyzkoušet nebo se poradit či si na ně sáhnout.

Který z těch deseti trhů mimo Českou republiku vám dnes nejlépe funguje? A které naopak překvapily tím, že jste tam vstoupili, čekali jste, že to bude dobré, a nakonec to tak dobré není?
To je hrozně těžké říct, protože z doby, kdy trh rostl lineárně a 20% růst byl standard a podle toho bylo možné posuzovat, jak trhy fungují, jsme dnes v situaci, kdy čísla skáčou nahoru dolů. Za covidu jsme měli 100% nárůsty a pak zase někde desítky procent pokles. Nicméně asi lze říct, že dnes celý jih, od Maďarska dolů, roste hrozně pěkně, posilujeme tam o 50 % ročně a jsem hrozně spokojený. Stejně dobře nám to paradoxně nejde na našich nejsilnějších a nejstarších trzích, to znamená v Česku, na Slovensku a v Maďarsku, kde je ekonomická situace objektivně problematická, panuje tam vysoká inflace a obchodní tržby jdou už mnoho měsíců dolů. Ale ten jih, třeba Chorvatsko, nám jede fakt velmi, velmi dobře.

Nedávno jste také začali nabízet jednu novinku, která byla dosud typická pro IKEA. Začali jste prodávat kuchyně, které si zákazník může nechat poskládat na míru. Co je to za expe-

riment, jak funguje a kolik kuchyní takhle prodáváte?
Kuchyně jsme měli v hlavě už mnoho let. Vlastně skoro od začátku, co jsem přišel. A ta myšlenka je velmi jednoduchá: pokud chceme aspirovat na to, že budeme nabízet vše, co se týká bydlení, kuchyně prostě musíme mít. Na druhou stranu je to úplně jiný typ byznysu, přecházíme do vztahu jeden k jednomu, kdy komunikuje designér s koncovým zákazníkem. Ale po složitém loňském roce jsme si řekli, že se fakt chceme naučit nové věci, a víme, že si to náš zákazník zaslouží. Z výzkumů jsme věděli, že to od nás očekávají, tak jsme se do toho pustili.

Tak jako vždycky chceme i teď na trhu trošku udělat vítr a kuchyně dělat jinak, co nejvíce digitálně, aby byly pro zákazníka co nejjednodušší. Službu jsme spustili v červnu. V létě jsme jeli v pilotním režimu, teď už fungujeme naplno. Je ještě brzo hodnotit, jak to jde, protože ten obchodní případ trvá typicky mnoho měsíců, takže nám teprve dobíhá první vlna zákazníků. Ale prodáváme, skládáme, montujeme, všechno probíhá dobře. Od klientů máme fantastickou zpětnou vazbu, kdy nám říkají, že to pro ně bylo výrazně snazší než běhat po kuchyňských studiích a ztrácet tím hodně času.

To zní jako docela zajímavý princip, který by se mohl přenést od kuchyní i na další interiérové návrhy.
Vidím, že v tomhle selhává náš marketing, protože tuhle službu už máme (smích). Jmenuje se „Bonami návrh interiéru“. Zákazníkovi umíme navrhnout celý byt a vybereme mu do něj produkty. Pokud v naší nabídce ten správný produkt není, koupíme ho od konkurence, všechno to klientovi dovezeme k němu domů a zajistíme instalaci nebo složení všech těch věcí.

Skoro to vypadá, že Bonami opravdu není e-shop, ale spíš interiérové studio, které mimochodem taky prodává nábytek a doplňky. Je to směr, kterým chcete jít? Nabízet primárně služby s tím, že do bytu ve výsledku dodáte i nábytek?
Pro určitou část zákazníků ano. Je to pro nás jednoznačně strategická pozice, kde se vidíme, protože je pro nás velice složité v této době bojovat jen cenou. Věříme, že je oblast služeb neobsazená, protože pro velké off-line hráče bude vždycky klíčové dostat lidi do obchodu a všechno ostatní je pro ně komplikace. Vidíme také obrovský nástup marketplaců, které bezpochyby umějí nabídnout velký výběr, na některých vybraných kategoriích dokážou poskytnout i lepší ceny, ale je velice nepravděpodobné, že by nabízely služby, které máme my. Dál budeme fungovat pro velkou většinu zákazníků jako e-shop, ale pro nároč-

Tím, jak pocházím z finanční školy, jsem spíš opatrný a snažím se vždycky vytvářet scénáře, co všechno se může stát.

nější zákazníky chceme být digitálním interiérovým designérem.

Současná ekonomická situace není úplně dobrá. Česká e-commerce v průměru neroste, inflace nebo válka na Ukrajině vedou k tomu, že lidé šetří a míň nakupují. I Bonami si v loňském roce prošlo složitějším obdobím. Jak to vypadalo a jak jste se z něj zvedli?

Po covidu, který znamenal enormní nápor, jsme někdy od druhé poloviny roku 2021 pozorovali ochlazování. Tím, jak pocházím z finanční školy, jsem spíš opatrný a snažím se vždycky vytvářet scénáře, co všechno se může stát. A některé předpovědi se mi nelíbily a byl jsem z nich nervózní. Některé scénáře totiž znamenaly, že bychom potřebovali hodně dodatečného kapitálu. Ty peníze mohly přijít buď zevnitř firmy, nebo od akcionáře, nebo od bank, které jsou ale velmi opatrné. Abychom v žádném případě neohrozili finanční stabilitu firmy, zastavili jsme nejdříve investice a přestali jsme vkládat peníze do infrastruktury. Potom jsme ještě v roce 2021 udělali druhé kolo, to byla revize nepersonálních nákladů.

Pak začala válka na Ukrajině, a výhled do budoucna nebyl moc pozitivní. Někdy v dubnu 2022 jsem se rozhodl, že se na náraz začneme připravovat velmi rychle, a začali jsme spořit hlavně na fixních nákladech. Bohužel se to dotklo dvou skupin, které mně nedělaly radost. První byli moji kolegové – odešlo skoro dvacet procent firmy. A pak se šetření dotklo zákazníků – na některých zahraničních trzích jsme prodloužili frekvenci dopravy, tudíž jsme dočasně zhoršili služby. Byla to složitá rozhodnutí, ale teď retrospektivně viděno byla správná, protože hráči, kteří podobná opatření v naší vertikále neudělali, už tady dnes nejsou. Jsem hrozně rád, že jsme škrty udělali najednou, nesalámovali jsme je ve smyslu, že bychom každý měsíc oznamovali, že odejde těchto pět lidí a pak další tři, ale udělali jsme velký řez. Nějak jsme se z toho oklepali, firmu jsme nastavili podstatně efektivněji, a to nám umožnilo před letošním rokem dělat projekty, jako byly kuchyně. Teď nám to dává náskok před konkurencí, protože už mentálně čekáme, až se trh zase odbrzdí a pojede nahoru.

Jak vypadá letošní rok? Je možné odhadovat výsledek Bonami?

V prvním čtvrtletí, které jsme srovnávali ještě s předválečnou základnou, jsme jako celek klesali, ale od dubna rosteme. Růst vidíme hodně na jihu a podstatně méně ve střední Evropě. Věřím, že za celý rok budeme v růstu, a každý měsíc jsem optimističtější než ten měsíc předtím. Kdybych porovnal svůj optimismus v roce 2019 a teď, pak jsem optimističtější než tehdy.

Už rozumím těm deseti miliardám. V poslední době jste nabírali nové lidi do vedení firmy. Zaznamenal jsem třeba jedno hodně zajímavé jméno: v Bonami teď nějakým způsobem funguje bývalá šéfka CZC.cz Jitka Dvořáková. Co u vás dělá a jak jste ji přemluvil?

S Jitkou jsem se poslední roky potkával pravidelně, debatovali jsme o různých tématech a pro mě to vždycky bylo nesmírně obohacující a inspirativní povídání. Když skončila v CZC.cz, řekl jsem jí, že bych potřeboval parťáka a pomocníka k uvažování o tom, jak

s Bonami dál. Ona má s touhle fází rozvoje firmy zkušenost – když přišla do CZC.cz, ten e-shop dělal miliardu, miliardu a půl a Jitka končila na šesti. Myslím, že ta zkušenost je obrovsky cenná a relevantní. Lidsky si sedíme, jí se líbí naše firma, má k ní blízko, tak jsme se velmi snadno domluvili.

A co tedy má na starosti?
Její pozici bych obecně nazval jako CEO advisor.

Těch nástupů bylo více a pořád hledáte další lidi. Nedávno jste vypisovali výběrové řízení na obchodního ředitele. Znamená to, že více lidí potřebujete na nějakou expanzi?
Souvisí to s mým optimismem a s chutí celkově jít na další trhy a neustále naši službu vylepšovat. K tomu potřebujeme hodně zkušených lidí. Máme jedenáct trhů, různé prodejní kanály – on-line, velmi úspěšně se rozvíjející B2B kanál, pak kuchyně a k tomu prodejny. Každý z nich funguje malinko jinak a potřebuje zkušeného člověka, který je umí posunout na další úroveň.

Bonami funguje skoro jedenáct let. Jak to vypadá s výhledem firmy do budoucna? Plánujete prodej, nebo je to pořád společnost, která by měla Mitonu zůstat a rozvíjet se v rámci skupiny?
Prodej teď neplánujeme, ale z principu fungování Mitonu k němu může dojít. Myslím, že teď na něj není správná doba ani tržní, ani z hlediska fáze vývoje naší firmy. Mě Bonami pořád hrozně baví a chci si naplnit ten svůj optimismus, takže bych řekl, že teď prodej není na pořadu dne.

DAVID SLÍŽEK

Šéfredaktor Lupa.cz, web vede od roku 2012. Věnuje se především telekomunikacím. Je autorem podcastu Příběhy z historie českého internetu. ■

NESLIBUJI, ŽE JSOU DIGITÁLNÍ DOVEDNOSTI NĚCO JEDNODUCHÉHO

CHCI ZACHYTÁVAT TECHNOLOGICKÉ TRENDY A RYCHLE V NICH VYCHOVÁVAT ŽENY. TY SE PAK STANOU SILOU, KTERÁ BUDE POHÁNĚT ČESKOU EKONOMIKU, ŘÍKÁ SENTA ČERMÁKOVÁ, NOVÁ VÝKONNÁ ŘEDITELKA NEZISKOVÉ ORGANIZACE CZECHITAS, KTERÁ SE ŽENÁM SNAŽÍ OTEVÍRAT SVĚT IT.

Máte za sebou 25letou kariéru ve velké korporaci Hewlett-Packard, posléze HP. Pak jste pracovala také v poradenské firmě Deloitte. Bylo pro vás v rámci vaší kariéry složité se jako žena v IT firmách prosadit a změnila se za ty roky nějakým způsobem role žen v IT?
Pro mě to obtížné nebylo a bylo to tím, že jsem hned zamlada šla studovat počítače, konkrétně kybernetiku, biokybernetiku a těch pět let života v mužském světě na univerzitě pro mě bylo dobrou průpravou. Studovalo tam tehdy málo žen, jestli si dobře pamatuji, v naší paralelce bylo dvě stě lidí a z toho jsme byly čtyři ženy. Naučila jsem se s tím žít. V současné době máme v České republice jenom v IT jen deset procent žen, kdežto třeba v Estonsku mají 44 procent, v Saúdské Arábii 37 procent, v americkém Silicon Valley 22 procent. Myslím, že žen v IT bychom potřebovali mnohem víc, ale nehrnou se sem, protože je to takové mystické odvětví, kde se ženy možná ani necítí vítány. Přitom je to blbost. Ženy do IT přinášejí fantastické schopnosti, jednou z nich je spolupráce, týmovost, ale taky cit pro detail, pro design, pro zákaznickou službu, pro to, jak programování souvisí s celkem. Máme fantastické datové analytičky i programátorky. V IT je spousta profesí, kde může chytrá a ambiciózní žena zazářit. Navíc je obklopená velmi chytrými lidmi, kteří se v IT pohybují. Jako mentorka často ženám a holkám vysvětluji, že jít do chytrého technologického světa je fantastická záležitost. Navíc nám práce v IT dává flexibilitu, je možné ji skloubit třeba s mateřskou dovolenou nebo s výchovou několika dětí a nadto jsou v tomto oboru dobré platy. Myslím, že to je jenom o nastavení mysli.

No a v čem je tedy jádro problému? Za chvilku se dostanu k číslům o tom, kolik žen a dívek v České republice studuje IT obory…
To jsou asi tristní čísla.

Ano, ale hlavně se v průběhu let moc nemění. Na IT oborech se zvyšuje podíl studentek, ale je to hlavně díky tomu, že stoupá počet zahraničních

FOTO: JAN VACA

studentek, zejména ze Slovenska. Proč se to podle vás nelepší?
Měla jsem spolu se svou sestrou štěstí, že jsme měly tatínka, který nás na technické obory hodně připravoval. Když jsme už jako mladé holky chtěly tatínkovi udělat radost, počítaly jsme matematickou olympiádu nebo jsme musely mít jedničku z matematiky. Také jsme šly na gymnázium, které bylo na matematiku speciálně zaměřené. Nebraly jsme to jako něco výjimečného. Problém podle mě je, že stereotypizujeme děti a chlapečky posíláme víc do technologií a ženy spíš do humanitních oborů. To je ale hloupost, jako společnost se tím obíráme o talentový potenciál žen. Myslím si, že se to sice mění, ale strašně pomalu.

Tady jsou slíbená čísla. Pocházejí z publikace Českého statistického úřadu Ženy, muži a digitalizace, podle které v roce 2022 studovalo IT obory na českých vysokých školách celkem 4 173 žen, což samo o sobě vypadá jako slušné číslo. Zároveň ale stejné obory studovalo 19 315 mužů. Nepoměr je opravdu velký. Oproti předchozím letům je to v absolutních číslech zvýšení, ale muži pořád výrazně převažují a ženy tvoří asi osmnáct procent ze studentů a studentek vysokých škol v IT oborech. Czechitas už fungují devět let a podle čísel by se dalo říct, že se vám ta osvěta zatím moc nevede.
To bych netvrdila. Myslím, že naše organizace má obrovské pozitivní výsledky a že ženy nejenom učíme digitálním dovednostem, ale dáváme jim sílu komunity. Když k nám přijdou, vlastně už neodejdou. Buď studují dál, nebo se stávají mentorkami, koučkami. Vlastně jsou pak součástí komunity, kterou samozřejmě netvoří jenom ženy, ale i velmi důležití jsou v roli mentorů a lektorů muži – a často to pro nás pracují úplně zadarmo. Ale samozřejmě potřebujeme ještě lepší výsledky, abychom zaplňovali propast mezi ženami a muži v IT nebo digitálních oborech. A myslím si, že budeme spokojení, až prostě ten poměr bude půl na půl.

Když jsem o číslech ČSU přemýšlel, napadlo mě ještě jedno možné vysvětlení. Nemůže to být tím, že se vzdělávání v IT přesouvá z vysokých škol někam jinam? Neklesá zájem o studium IT na vysokých školách, protože existuje možnost si to vzdělání doplnit mimo ně?
Myslím, že je důležité obojí. Záleží na tom, v jakém momentě se třeba v pubertě rozhodujete o svém budoucím povolání, v jakém momentě vám jako ženě, když se teď zaměříme na ně, dojde, že jste chytrá, strategická a analytická žena a že vás baví technologie. Pokud vám to dojde, většinou jdete na vysokou školu IT studovat a jste velmi úspěšná a aktivní. Ženy, které to napadne později, myslím, právě zachytáváme v Czechitas. Říkáme jim, on vám neujel vlak, pořád jste stejně chytré, i když se třeba vracíte po mateřské dovolené a myslíte, že

> **Myslím, že naše organizace má obrovské pozitivní výsledky a že ženy nejenom učíme digitálním dovednostem, ale že jim dáváme sílu komunity.**

jste všechno zapomněla, že na tu expertizu už nemáte. Základní chytrost ve vás zůstala a vlastně jste právě dodělala projekt svého života – stvořila a vyslala jste do světa nový život. To je opravdu obrovský, složitý projekt a spousta chytrých žen jej zvládne a pak jim klesne sebevědomí na bod nula, což je strašná škoda. Právě ženám na mateřské radíme, aby se zamyslely, jestli by jim digitální dovednosti nemohly umožnit plynulý návrat na trh práce. Rádi s těmito ženami pracujeme a motivujeme je, protože v nich je opravdu obrovský potenciál, síla a energie.

Technologie se hodně rychle vyvíjejí. Lze do IT opravdu takhle naskočit, třeba i když uchazečka má těch mateřských za sebou několik, takže z práce vypadla třeba na deset let?
Samozřejmě bych lhala, kdybych tvrdila, že v IT může pracovat každá žena. Může to udělat žena, která má inteligenční předpoklady, to znamená, že je analytická, bavila ji matematika, fyzika a podobné obory. Navíc to může udělat žena, jež má během studia postaráno o děti, protože bez toho to bude mít hodně těžké. Nikomu neslibuji, že digitální dovednosti jsou něco jednoduchého. Je tam velký práh bolesti, ale řekla bych, že žena, která je ambiciózní, inteligentní a má nějak postaráno o děti, aspoň třeba o víkendech nebo po večerech, může začít a oťukávat možnosti, jež v Czechitas nabízíme. V současné době máme jedenáct profesních cest, od testování až po kybernetickou bezpečnost. Jsou tam obory, které mají blízko k datové analytice nebo k navrhování takzvaných UX, to znamená uživatelských rozhraní, nebo nabízíme třeba webdesign. Na tyto IT obory jsou ženy opravdu přirozeně talentované a stačí studiu věnovat čas a opravdu si na trhu práce vytvoříte unikátní výhodu. Vidím také jeden

velký trend, který je možná jednou z velkých motivací, proč jsem Czechitas na roli CEO kývla. Trh digitálních dovedností se momentálně dramaticky mění. Způsobila to loni v listopadu společnost OpenAI, která spustila lavinu takzvané generativní umělé inteligence a velkých jazykových modelů. Všem holkám a ženám všech generací teď říkám, že generativní AI je pro ně příležitost, jak si s malým prahem bolesti zlepšit svou situaci na trhu práce, protože obor, který předtím vystudovaly, mohou tou umělou inteligencí akcelerovat. Týká se to samozřejmě obou pohlaví, ale u žen vidím velké talentové předpoklady, protože generativní umělá inteligence je hodně nepředvídatelná. A kdo umí lépe zacházet s nepředvídatelným světem než ženy, které pracují ve své profesi a do toho ještě vychovávají rodinu a starají se navíc třeba o své rodiče nebo prarodiče? Generativní AI jsme na trhu potřebovali, abychom do digitálního světa vtáhli více chytrých žen.

Některé předpovědi ale mluví spíš o tom, že generativní umělá inteligence řadu programátorů nahradí.

Samozřejmě, s tím souhlasím, ale ona nahradí jen standardní programátory. Nenahradí ty, již jsou kreativní a dovedou programování propojit s nějakou další profesí. Čím víc budete mezioborový, tím víc vás trh bude potřebovat. Souhlasím s tím, že generativní umělá inteligence spousty profesí zhruba do pěti až deseti let úplně vygumuje. Ale zároveň vzniknou profese, které budou úplně nové, o nichž dnes nemáme vůbec tušení. Správný přístup je mít unikátní dovednosti a s těmi pak být připraven na to, co trh práce sám udělá. A to my ještě moc nevíme.

Ale pokud se vrátíme ke generativní umělé inteligenci, tam jsou ty předpoklady v podstatě velmi malé, protože generativní AI začne různá odvětví našich lidských činností propojovat. Kdo se chce stát odborníkem na velmi dobré nasazení generativní umělé inteligence, vůbec nemusí být matematik. Může to spíš být člověk, kterého baví lidské bádání, něco se nového učit, něco nového objevovat, cestovat.

Je důležité uvědomit si, na co je člověk opravdu dobrý. U každého jde o něco jiného. Já jsem třeba dobrá na tvoření strategií. A zjistila jsem, že tvořit strategie s použitím generativní umělé inteligence mi zabere třeba o dvě třetiny méně času, než když to dělám sama. Samozřejmě musím vědět, co to ty strategie jsou, a musím vědět, jak se vytvářejí, ale AI mi dá křídla a odpich, abych je tvořila rychleji, lépe, kvalitněji, abych jich třeba nasadila víc a pak zjistila, který model nejlépe funguje. Je to taky fantastický nástroj pro rozhodování o čemkoliv – třeba o tom, kam chcete cestovat, kam chcete jít studovat, kde chcete bydlet. Nedívám se na AI jen jako na software, ale spíš jako na svého asistenta, možná i kouče. A stejně tak, jak funguje v mých strategiích, může fungovat ve všech lidských profesích. Stačí jen do toho trochu vniknout.

Souhlasím s tím, že generativní umělá inteligence spousty profesí zhruba do pěti až deseti let úplně vygumuje. Ale zároveň vzniknou profese, které budou úplně nové.

Říkala jste, že o kariéře v IT může uvažovat žena, která má analytické myšlení a podobné předpoklady. Jak se to pozná? Jak má poznat, že ty předpoklady pro informatické myšlení, jak se dnes říká, nebo analytickou práci má?

Jednoduše se to pozná tak, že ji baví čísla a že ji baví v číslech hledat jisté vzorce chování nebo podobnosti. To třeba byl můj případ. Strašně mě bavilo počítat slovní úlohy, příklady, přemýšlet, číst, analyzovat, logicky myslet. Pokud tohle v sobě, holky a ženy, cítíte, je to dobrý indikátor toho, že se budete hodit na techničtější obory. Dalším ukazatelem je, když třeba hrajete videohry, ale ne střílečky, spíš strategické hry. Když vás baví přemýšlet, co kde postavit, co kde vybudovat, to je, myslím, také velmi dobrý indikátor toho, že se budete do technologií hodit.

Nabídnu ještě dvě čísla ze statistik Českého statistického úřadu. Podle něj byla průměrná hrubá měsíční mzda ICT odborníků v roce 2022 v Česku 71 690 Kč u mužů, ale u žen jen 61 992 Kč. Osobně mě napadají dvě možná vysvětlení. Jedno je, že ženy v ICT oboru působí na nižších, juniornějších pozicích, tím pádem by ten průměr asi odpovídal. Nebo berou za stejnou práci méně peněz než muži. Jaké máte v tomto ohledu zkušenosti?

Myslím, že pravda bude v obou vysvětleních. Ženy v České republice jsou pořád méně finančně kompenzované než muži a myslím si, že to je dané historicky a také našimi stereotypy. Na digitálních technologických místech pořád raději vidíme muže, který tam vždycky byl, a ženy se tam teď postupně dostávají. Takže to je první věc, stereotyp. A druhá věc je, že ta juniorita může být dána ne tím, že ženy neměly na IT obory takové předpoklady, ale tím, že se tam dostávají později. A potom, když už v oboru pracují, je tam většina velmi spokojená a jde kariérou dál a dál, ale potom přicházejí profesní propady, když žena má děti. Muži ji pak v kariéře předběhnou. To se bude srovnávat ještě dlouhá léta, ale myslím si, že ještě předtím přijde nějaké vládní nařízení, aby se platy mužů a žen na stejných místech srovnaly, což je, myslím, velmi férový přístup.

Czechitas vznikla jako organizace na podporu vstupu žen do IT. Později ale svůj záběr rozšířila a pomáhala také třeba s rekvalifikacemi horníků z Ostravska a podobně. Jak je to dnes? Jsou ženy pořád vaším hlavním cílem?

Ano, rozšířili jsme se na různé další cílové skupiny, ale bylo to v souvislosti s granty, které jsme dostávali. Zůstáváme však primárně strategicky zaměření na ženy všech věkových skupin. Pokud však na kurzu nebo na digitální akademii zbývají nějaká místa, nabízíme je volně do společnosti.

Chtěla bych vidět armády spokojených žen, které s námi nejenom studují IT, ale pracují i jako naše mentorky a lektorky.

Vaše organizace je financována převážně z darů. Za rok 2022 Czechitas od dárců získala celkem 35 milionů korun a mezi největšími dárci jsou samozřejmě IT firmy, jako jsou Google, IBM, Microsoft, AT&T nebo SAP. Zaujalo mě ale, že nejštědřejším dárcem byla se skoro patnácti miliony korun nadace dánské firmy na výrobu oken Velux. Jak se okna rýmují s IT?

Selský rozum říká, že bychom měli mít nejvíc partnerů v IT firmách, ale zdaleka tomu tak není. Naši partneři se nyní rekrutují ze všech možných oblastí a odvětví a průmyslů. Jde o firmy, které jsou pokrokové a pokročilé z hlediska diverzity, inkluze a rovnoprávnosti. To je vlastně také případ Veluxu. Takové společnosti se na nás obracejí a žádají, abychom jim připravili třeba speciální programy pro nástup žen po mateřské. Jde o celospolečenský problém, protože v Česku jsou mateřské hodně dlouhé, a čím delší jsou, tím se maminkám obtížněji vrací na trh práce, zejména do kvalifikovaných míst. Zdaleka už nejde jen o IT profese. Obracejí se na nás firmy z finančního světa, z výrobního světa, z biotechnologií, všechny pokrokové firmy, které pochopily, že pokud diverzita nebude jejich strategií, bude odrazovat nejenom ženy, ale i muže. Navíc nemáme pouze partnery, máme i osobní dárce, kteří podporují myšlenku, že když svět bude spravedlivější a bude v něm více žen, rozjede se česká ekonomika a bude se nám dýchat lépe a radostněji. Loni jsme také založili nadaci Czechitas, ve které sbíráme peníze pro ženy a dívky, jež by si naše kurzy jinak nemohly dovolit. Nabízíme jim stoprocentní stipendia. Každopádně máme řadu fantastických partnerů a já jim moc děkuji.

To je nejspíš vaše hlavní role jako CEO, komunikovat s partnery a shánět nové firmy, které by vás podpořily.

Mám jako CEO hodně rolí. První je dát společnosti vizi do budoucna. Vidím ji v tom, že by Czechitas měla být organizací, která bude určovat trendy ve vzdělávání žen. Chci k nám přivést i nové ženy, jež jsou ambiciózní a chtějí být neustále relevantní pro trh práce, který se nám velmi rychle mění pod rukama. Moje hlavní mise pro Czechitas je být silnou CEO v oblasti strategie a vedení firmy správným směrem. Mou další rolí je samozřejmě přinést peníze, aby se tato strategie dala uskutečnit. A třetí důležitou rolí je vychovávat naše manažery a lídry, aby se stále zlepšovali a abychom zvládali stále větší úkoly.

Až se třeba za tři, za pět let ohlídnete za svým působením v Czechitas, co byste ráda viděla, abyste mohla říct, ano, uspěla jsem?

Chtěla bych vidět armády spokojených žen, které s námi nejenom studují IT, ale pracují i jako naše mentorky a lektorky. Chtěla bych, abychom učili také v angličtině, abychom naši misi rozšířili i tam, kde může být čeština bariérou, a chtěla bych, abychom zachycovali trendy, které budou na trh postupně přicházet. Od loňského roku je to generativní umělá inteligence, ale brzy přijdou také kvantové technologie a biotechnologie.Chtěla bych být vyhodnocená jako šéfka vzdělávací organizace, která věděla, jaké trendy přicházejí, a rychle v nich začala vychovávat ženy, jež pak budou pohánět českou ekonomiku na dlouhé roky dopředu. Neomezila bych to také jenom na tři až pět let, v Czechitas plánuji být dalších 25 let, jako jsem byla v Hewlett-Packard (smích).

DAVID SLÍŽEK ■

Dostanou se hackeři k vašim datům?

Odpověď dají nově i automatizované penetrační testy

KYBERNETICKÁ BEZPEČNOST JE DNES VELKÝM TÉMATEM, KTERÉMU SE VĚNUJÍ FIRMY NAPŘÍČ VŠEMI OBORY A VELIKOSTMI. SPOLEČNOSTI INVESTUJÍ MILIONOVÉ ČÁSTKY DO NÁSTROJŮ PROTI ÚTOKŮM HACKERŮ, ALE PŘITOM SI ČASTO POKLÁDAJÍ OTÁZKU, JAK ZJISTIT, ZDA TATO OPATŘENÍ FUNGUJÍ? ODPOVĚĎ MOHOU NOVĚ POSKYTNOUT I AUTOMATIZOVANÉ PENETRAČNÍ TESTY.

Penetrační testy byly ještě donedávna výhradní doménou etických hackerů. Jejich úkolem je napodobit kybernetický útok a pokusit se prolomit firemní ochranu. Výsledkem může být vyřazení firemní sítě z provozu, krádež dat, jejich zašifrování nebo jakákoli další činnost poškozující provoz společnosti. V dnešní době lze značnou část těchto testů automatizovat, a zpřístupnit je tak i menším firmám.

Automatizované penetrační testy, které nabízí například izraelská Pentera, využívají celou škálu technik, jež byly dosud vyhrazeny pouze lidem. Jakmile se nástroj dostane do sítě, dokáže se v ní sám nepozorovaně pohybovat a vyhledávat dostupné přístupové údaje, které zkusí použít pro to, aby se dostal i do dalších částí sítě nebo do jiných síťových prvků. Zároveň zkouší interní zabezpečení prolomit hrubou silou, automaticky navazuje spojení s dalšími počítači a prvky v síti a všude sbírá dostupná data. Díky tomu se také postupně dokáže šířit do dalších částí sítě. Důležitým faktorem je také schopnost nástroje zvyšovat v rámci infrastruktury svoje privilegia, což je obvykle klíčový prvek úspěšných hackerských útoků.

Poté, co test skončí, vytvoří podrobný popis toho, jak probíhal, co se v rámci něj podařilo a jak velké to je pro firmu riziko. Společnost se tak dozví, které chyby nebo jejich kombinace jsou opravdu nebezpečné, a zároveň obdrží doporučení, jak tyto díry v zabezpečení odstranit. To je přitom klíčový bod celého testu. Z našich zkušeností totiž řada firem, které během testování své odolnosti zjistí nějaký nedostatek, nakonec selhává právě v tom, jak ho napravit.

Kybernetická bezpečnost je neustále se měnící pole hry a to, co fungovalo včera, nemusí nutně fungovat zítra. Testovat je však nutné komplexně a důsledně, což je moment, kdy automat získává náskok nad manuální prací. Klíčem k validaci toho, zda je firemní obrana stále silná, může být právě automatizace penetračních testů. Ty lze spouštět v krátkých intervalech, díky čemuž dokážou poskytnout potřebnou jistotu, že firemní bezpečnostní opatření stále fungují.

PETR MOJŽÍŠ

Security architect ve společnosti ANECT ■

TISKÁRNY OD NÁS ODEBÍRÁ NASA I SPACEX

3D TISK SE ZA POSLEDNÍ DEKÁDU NEJEN V TUZEMSKU DOČKAL NEBÝVALÉHO ROZMACHU. ZÁSLUHU NA TOM MÁ JOSEF PRŮŠA, KTERÝ SVÉ JMÉNO SPOJIL SE ZNAČKOU 3D TISKÁREN. KAŽDÝ MĚSÍC ODCHÁZÍ Z PRAŽSKÝCH HOLEŠOVIC DO 160 ZEMÍ Z CELÉHO SVĚTA DESET TISÍC VÝROBKŮ ORIGINAL PRUSA.

FOTO: JAN VACA

Vaše tvář se objevuje jako jeden ze vzorových výtisků pro otestování správného nastavení tiskárny. Nevadí vám, že než se tiskárna odladí, bude vytisknutý zmetek mít vaši podobu?
Ve firmě máme spoustu vtipálků, kteří vědí, že mi nevadí si ze sebe trošku občas dělat srandu. Když zjistím, s jakým testovacím modelem přijdou nebo kam nainstalují moji figurku, musím se tomu smát. Ale nevadí mi to. Hlavně že je to dobrý model a uživatelé vyzkoušejí sestavení, že ta tiskárna funguje na sto procent.

Jak dlouho trvá takovou tiskárnu vyladit?
U stavebnic záleží na tom, jak dobře lidé sledují přiložený návod. Za dobu, co tiskárny takto nabízíme, jsme pokyny dostali do skoro perfektního stavu. Ale neprodáváme jen stavebnice.

A o co je větší zájem, o hotové výrobky, nebo o levnější možnost si tiskárnu sestavit svépomocí?
Během roku se to střídá. Třeba je to z 60 % stavebnice, ze 40 % už hotové sestavy, ale dost často se to mixuje. Sami jsme překvapeni, že třeba i firmy si kupují spíše stavebnice. Dává jim to možnost při stavbě si tu technologii osahat, nacítit a získat nástroj, který znají.

Postupují tito kutilové podle návodu, jak mají, nebo se vám vrací v reklamacích, že tiskárna netiskne správně?
Reklamovanost máme obecně extrémně nízkou. Na webu jsou on-line návody, ke kterým je možné přidávat komentáře. Občas se tam objeví perličky typu: tady jsem to chtěl předběhnout, a musel jsem se vrátit. Doporučuji všem, aby šli přesně krok za krokem podle návodu.

Jak vůbec je těžké ze stavebnice poskládat hotovou tiskárnu a mění se s verzemi zařízení doba nutná pro kompletaci?
S novou MK4 je stavba zase o velký kus příjemnější. Lidi, kteří rádi skládají LEGO, si s chutí složí i svou tiskárnu. Je to možná v lecčems snazší. A nenahraditelný je ten magický moment, kdy člověk tiskárnu zapne a ona funguje a dělá to, co má.

Čím snižujete prostor pro chyby, aby se špatný postup při stavbě nepodepsal na výsledku a uživatelský zážitek tím nebyl poznamenán?
Tiskárna buď tiskne, nebo netiskne. Už po prvotním zapnutí probíhá samodiagnostika. A pokud tam něco není úplně správně, jak by se to tiskárně líbilo, pak uživatele navede, co s tím má dělat. Na displeji se ukáže QR kód, který si uživatel načte telefonem a zjistí, o co jde a jak to může napravit.

Ještě přikládáte ke stavebnicím gumové medvídky na nervy?
Stále (smích). Doporučuji všem podívat se na naše on-line manuály. Je v nich dokonce i doporučené správné dávkování gumových medvídků (smích). Snažíme se nebrat se tak úplně vážně. Mimochodem, k minitiskárně dostanete malé balení, k MK4 standardní a k XL tiskárně to obrovské balení.

Pojďme se podívat na vaši společnost Průša Research. Začínali jste ne jako garážová firma, ale společnost, která má své začátky ve sklepě. Co bylo tím impulzem, proč se pustit do 3D tisku?

Úplně na začátku nebyla firma. 3D tiskárny byly tři roky před jejím založením mým koníčkem. A pak se mi z nějakých důvodů úplně nelíbilo na škole, kterou jsem studoval. Ve stejný den jsem ukončil studium na vysoké škole a založil firmu. Od začátku bylo jasné, že budu dělat 3D tiskárny. Už to nějakou dobu fungovalo jako open source projekt, lítal jsem po světě, dělal přednášky. Lidi pak na mě trochu tlačili, že přednášky fajn, ale já bych si tu tiskárnu od tebe chtěl koupit!

Zmiňujete, že všechny komponenty nebo díly k tiskárně jsou open source projekt. Nevadí vám, že tím usnadňujete vznik možných plagiátů vaší tiskárny?
Aktuálně děláme to, že některé části tiskárny zveřejňujeme jako open source opožděně. Abychom neměli kompletní klon jedna ku jedné v okamžiku, kdy novinku vydáme. To znamená, že vznikají plagiáty, ale nepřicházejí na trh současně s vydáním nového produktu, je tam zpoždění.

To vám nevadí?
To je v pohodě. Důvod, proč mám rád open source, je ten, že vývoj pak nedělá jeden člověk. Mohou do něj přispívat všichni najednou. Celý obor se posouvá rychleji. Hodně ale záleží na tom, aby ti ostatní skutečně přispívali, což je poslední dobou o něco horší.

Lze dnes 3D tisk ještě někam posouvat?
Už je v tak pokročilé fázi, že jednotlivec není schopný na tiskárně udělat markantní zlepšení. Je to spíš výzva pro specializované firmy. Poslední dobou se ale děje to, že hlavně čínští výrobci, kteří používají open source firmwary, je označují za vlastní. Ne konkrétně ty naše, ale open source. Oni vlastně na open source modelu parazitují, ale

A můžeme tedy srovnat tuto úspěšnost, jestli je třeba možné říct, jak si vede MK4 a jak si v tom srovnání počínají miniverze a XL varianty?
Mini a MK4 se nedá úplně moc srovnávat, protože to je přece jen trošku něco jiného. Mini už je s námi nějakou dobu, tam to srovnání máme jako u každého produktu. Po čase se ty prodeje stabilizují a najde se nějaké to ekvilibrium. U MK4 jsme měli úplně nejúspěšnější start a tam ještě pořád dodělváme objednávky z prvních týdnů. Aby to bylo možné srovnat s MK3, musíme se dostat do fáze stabilních prodejů, kde už ty předobjednávky budou vyřízené.

> **Ve stejný den jsem ukončil studium na vysoké škole a založil firmu. Od začátku bylo jasné, že budu dělat 3D tiskárny.**

přiznají se k tomu, až když je někdo odhalí. A pak se samozřejmě komunita dočká krásné omluvy od ChatGPT a vše je zase zalité sluncem.

Aktuálně vaše tiskárna nese označení MK4, už tady o ní byla řeč. Předtím to byla MK3. Co vlastně ta zkratka MK znamená?
Znamená Mark a je to prostě označení verze. MK1, MK2, MK3.

Teď tedy máte v nabídce tiskárnu MK4, pak také miniverzi a mluvil jste i o té XL variantě. Jak si ty produkty ve vzájemném srovnání vedou?
Přijde na to, jak to měříte. Konstantně máme skoro na všechny produkty čekací dobu. Přitom vyrábíme a škálujeme výrobu tak rychle, jak jen můžeme. To je asi dobré měřítko úspěšnosti těch produktů. Jedeme na plné obrátky, a ještě stále přibíráme nové kolegy.

Ke každé verzi přidělváte s odstupem času určitá vylepšení. Označujete to jako poloviční verzi. Je o to zájem, upgradovat si už zakoupenou tiskárnu a vylepšit ji na ten mezistupeň?
Úplný upgrade třeba z MK3 na MK4 není tak efektivní. Lidé sice chtějí mít plné upgrady, ale vymění se při tom ohromné množství součástek. Proto jsme se rozhodli nabízet meziverzi. Třeba MK 3.5 upgrade obnáší novou elektroniku, která umožňuje s grafickým displejem rychlejší tisk. Ale hardwarově ta tiskárna zůstane skoro stejná. Takový upgrade pak je řádově levnější než vyměnit kompletně celou tiskárnu. A vy získáte klidně dalších pět let bezproblémového užívání. V dnešní době tlaku na udržitelnost v tom vidím ohromný přínos.

Když bych před vás postavil výrobek vytištěný na 3D tiskárně té původní generace, MK3 a vedle toho stejný z tiskárny MK4, poznáte rozdíl?
Řekl bych, že ano. Ale dostávám se s kvalitou tisku do bodu, kde to bude těžko rozeznatelné. Každý malý přínos stojí násobně víc práce. Pro člověka, který nezná jemné nuance, budou díly vypadat identicky.

Relativně nedávno jste se pustili do nákladnějšího, ale na detaily zaměřeného SLA tisku. Výtisk se tu rodí zjednodušeně řečeno z vysrážené tekutiny. Našla si tato technologie zájemce?
Ano, ale jak správně říkáte, tato technologie se hodí na úplně jiné typy dílů. U SLA tiskáren se fotopolymer vytvrzuje světlem. Je možné přitom dosáhnout o mnoho větších detailů. Ale není to úplně technologie, kterou by chtěl mít každý člověk doma.

Pro koho se to tedy hodí? Pro šperkaře?
Typicky pro šperkaře nebo lidi, kteří vyrábějí figurky pro hru Dračí doupě. Nebo třeba cukráři si často vytisknou formu, respektive její základ. Z něj pak odlijí silikonovou formu a tu pak využijí pro finální výrobek z čokolády. A to je často u 3D tisku opomíjená věc, kterou si běžně člověk neuvědomuje.

Že tiskárna nemusí nutně produkovat finální produkt. Že vytiskne jenom tvar nebo třeba jen nástroj. Díly jsou často použitelné i na ražení do kůže nebo formování. Dokonce jsem viděl i vytištěnou předlohu kopyta na tvarování plechů.

Kam čekáte, že se bude 3D tisk ubírat dál?
U technologie FDM, kde se taví struna, nečekám, že za dva tři roky budou součástky vypadat úplně jinak. Že si člověk řekne „wow!“. Očekávám spíše postupnou evoluci než revoluci. Spousta prostoru ke zlepšování je ale v uživatelské přívětivosti. Musíme dostat technologii do takové fáze, aby

byli i netechnicky založení uživatelé schopni vytisknout, co potřebují.

Je to pořád ještě jen zábava pro nadšence, nebo už má 3D tisk masovější charakter?
Nikdy to nebyla jen zábava pro nadšence. Pohled na to, co lidé tisknou na našich tiskárnách, je hodně zkreslený tím, co se objevuje na internetu. Právě ti nadšenci posílají fotky modelů, které si tisknou pro sebe. Pak jsou tady firmy, jež 3D tisk používají opravdu hodně. Ale pro ně je to často něco, co chápou jako konkurenční výhodu, že mají zkušenost s touto technologií. A ne všichni chtějí sdílet své know-how, jak 3D tiskárny používají, protože pak by z toho mohla těžit jejich konkurence.

A vy víte, jak to používají? Jestli je to třeba jenom na prototypování, nebo na hotové funkční výrobky?
Je to mix všeho. Máme firmy, kde tisknou celý produkt. Často jde o malý trh, kde se nevyplatí použít klasické výrobní metody jako vstřikolis. Když vyrobíte pár desítek kusů měsíčně, ty náklady by se nikdy nevrátily. Nebo by ten produkt ani nedával smysl. Pak se dělají přípravky na výrobu, tisknou se třeba náhradní díly. Snažíme se některé zajímavější případy využití sdílet. Máme to u nás na blogu, říkáme tomu Průša Stories. Třeba firma Knorr Bremse, jež se stará o dánské železnice, tiskne náhradní díly pro starší vlaky, které už často nejsou dostupné, nebo ten náhradní díl stojí patnáct eur, zatímco oni jsou schopní ho vytisknout za dvě eura. Ve spolupráci s nimi se nám podařilo dotáhnout samozhášivý filament, který je pro takové použití nezbytný. Pokud dojde k zahoření takového materiálu, jsou tam parametry, že z toho nesmí nic odkapávat a do nějaké doby se musí sám uhasit.

Zmínili jsme, že 3D tisk používají firmy, co třeba ale věda nebo vývoj?
Tam o příkladech použití nevíme. Ani si nejsem jistý, jestli jsme schopní to zjistit. Na druhou stranu máme opravdu velké množství tiskáren dodaných do NASA nebo do SpaceX. Zmiňoval jsem ten samozhášivý filament, ale nedávno jsme vydali filament vhodný pro radiační stínění. Ten je plněný wolframem. Sami jsme byli překvapení, kolik se ho prodá – máme zákazníky, kteří tohoto materiálu objednávají stokilové várky. Předtím na trhu nic takového nebylo, a najednou je to velký trhák. Samotného by mě zajímalo si s každým z těch zákazníků sednout a popovídat si o tom, k čemu to vlastně používají.

Ideální by bylo najít materiál, ze kterého se snadno tiskne, je v podstatě nezničitelný a nepotřebuje vyhřívanou podložku ani komoru. A ještě bude kompostovatelný.

3D tisk je poměrně náročný na spotřebu energie. Jak do zájmu zákazníků promlouvá rostoucí cena elektřiny?
S tím bych si dovolil nesouhlasit. Spotřeba tiskárny je dost malá. Naše nejpopulárnější MK3 a MK4 si v průměru při tisku PLA berou pod 100 W.

A co na teplo náročnější materiály PETG, ABS a podobně?
Není to tak, že by to bylo násobně víc. Kdybychom vzali úplně ty extrémní případy s nejnáročnějšími materiály, bude ta spotřeba v průměru kolem 200 W. Za pět hodin tisku je to jedna kWh, takže při dnešních cenách kolem jedenácti korun. Nemyslím si, že elektrická energie je to, co lidi při 3D tisku na našich tiskárnách trápí.

Máte vždy k dispozici dostatek dílů pro sestavování tiskáren? Nebo vám třeba někdy nějaká komponenta vypadne, a tím pádem si zájemci musejí na tiskárnu počkat?
Teď už je to dobré. Problémy v dodavatelských řetězcích nám spíše pozdržely prvotní vydání tiskáren. Ale že bychom museli zastavit výrobu, to

se nám stalo snad jen dvakrát a třeba jen na jednu dvě směny. Nicméně určitě se stane, že se dostaneme do stavu, že máme něčeho na skladě nekomfortně malé množství. Pak člověk musí místo ekonomické dopravy ty součástky dovézt expresně. Před covidem jsme nakupovali na tři měsíce dopředu a nikdy jsme neměli problém. A teď najednou zjišťujete, že čipy, které používáme v nové tiskárně, mají dodací dobu 90 týdnů. Takže nejenže objednáváte dva roky dopředu, ale ještě na dva roky produkce.

Takže jste se také potýkali s nedostatkem čipů? Jak jste si poradili?

Nakupovat od překupníků je opravdový hazard. Existují podvrhy čipů, které jsou laserem přeznačené na jiný model. U nás na výrobě máme i rentgen, takže bychom byli schopní to odhalit. Díky tomu víme, že není úplně dobré si zahrávat a nakupovat od neznámých zdrojů.

Váš byznys kromě vlastních tiskáren je rozprostřen i do dalších podpůrných oborů. Věnujete se třeba i vývoji filamentů. Jak se rozšiřuje rozmanitost materiálů? Z čeho všeho lze dnes tisknout?

Běžný základ pro tiskaře je PLA, tedy kukuřičný škrob. Není nikterak náročný na přípravu, existuje z něj asi nejširší paleta všech barev. Pak je to PETG, trochu podobné PET lahvím, ale přece jen trochu jiný polymer, mechanicky o něco houževnatější. A pak ABS. Z toho se vyrábějí lego kostičky. Tedy hezký příklad toho, když se někdo zeptá, jak jsou takové součástky pevné, každý si asi někdy šlápl na kostičku lega. Nic příjemného (smích).

A co raritní materiály, kdy se do základních složek přidávají příměsi, které výrobku dodají určité vlastnosti?

Z těch specialitek máme třeba polykarbonát. Z něj se dělají neprůstřelná skla. Polykarbonová vlákna se přidávají jako určitý blend. Jak se říká, že americké firmy mají recept zavřený v sejfu a znají ho pouze dva lidé, něco podobného je s tímto blendem. Polykarbonát jako takový není úplně dobře tisknutelný na tiskárnách bez vyhřívané komory. Ale my ten materiál máme dotažený tak, aby s ním bylo možné tisknout i na tiskárnách s otevřenou konstrukcí. A pak mám ještě vyšší verzi, do které je přimíchané uhlíkové vlákno. To tomu dává zase jiné vlastnosti.

Kam se ten směr může ubírat dál? Z čeho všeho bude možné v budoucnu tisknout? Kam byste se rádi dostali?

Ideální by bylo najít materiál, ze kterého se snadno tiskne, je v podstatě nezničitelný a nepotřebuje vyhřívanou podložku ani komoru. A ještě bude kompostovatelný. To by byl takový svatý grál.

MARTIN DRTINA

Redaktor serveru Lupa.cz se zaměřením na telekomunikace, média, IT a právo. Dříve šéfredaktor Právního rádce a mluvčí Českého telekomunikačního úřadu.

DO VÁNOC POKRYJEME KOLEM OSMDESÁTI PROCENT ČESKA

ROZVÁŽET PO CELÉM ČESKU BYCHOM MOHLI V PODSTATĚ ZÍTRA, ALE UTRPĚLA BY TÍM KVALITA NAŠICH SLUŽEB, A TO NECHCEME, ŘÍKÁ MARTIN BEHÁŇ, KTERÝ OD LOŇSKÉHO PROSINCE VEDE TUZEMSKOU POBOČKU ON-LINE SUPERMARKETU ROHLÍK.CZ. PŘEDTÍM DLOUHÉ ROKY PŮSOBIL V TESCU A PAK KRÁTCE I V KAUFLANDU.

Výsledky fiskálního roku jste ještě nezveřejnili. Určitě ale už nyní víte, jak na tom Rohlík je.
Díky dlouhodobé práci a krokům, které podnikáme, rosteme. A to i přesto, že jsme se na začátku roku poměřovali s čísly z předchozího roku, kdy byl covid. I tak jsme byli schopní vyrůst. Ten trend je velmi konzistentní. Růst dosahuje double digit number.

Jak jste na tom s počtem zákazníků?
Ono se to vyvíjí. Byl tady covid, kdy s námi nakupovalo po dobu dvou let velké množství klientů, protože neměli jinou volbu. Covidové období je pryč a samozřejmě se stalo, že někteří zákazníci, kteří s námi během tohoto období nakupovali, odešli. Někteří s námi ale zůstali, protože jim vyhovovala naše služba a naše nabídka. A zároveň nám postupně přibývají i noví zákazníci. Na začátku tohoto roku jsme pokrývali už asi 45 procent území České republiky a tento rok jsme naše pokrytí docela zásadně zvýšili. A začínáme nabírat dost zákazníků právě z oblastí, kde jsme předtím nevozili.

To konkrétní číslo je tedy jaké?
Dohromady se bavíme o stovkách tisíc klientů, kteří s námi nakupují. Aktivně jich je každý měsíc tak dvě stě tisíc.

Určitě máte i přehled o počtu objednávek. Ty rostou, počítám, také, pokud vám přibývají zákazníci.
Tam je to přímá úměra. Tak, jak rosteme v zákaznících, stoupáme i v objednávkách. Blížíme se momentálně ke dvouciferným číslům.

A máte představu, jak často aktivní zákazníci nakupují, kolik udělají v průměru do měsíce objednávek?
V průměru jsou to přes tři objednávky měsíčně. Ale liší se to. Někteří hodně loajální zákazníci s námi nakupují desetkrát až dvacetkrát. A pak jsou ti, kteří nakupují jednou dvakrát do měsíce. Poměrově je to zhruba tak, že třetina nakupuje u nás tak jednou dvakrát do měsíce, zhruba třetina tak dvaapůlkrát do měsíce a zbytek je pak hodně nad.

Už jste naznačil, že hodně objednávek dělají především velká města jako Praha, Brno, Ostrava. Lze to vyjádřit poměrem?

FOTO: ROHLIK.CZ

Velká města samozřejmě dělají velkou část objednávek, ale neřekl bych, že jsou úplně dominantní. U nás se to těžko posuzuje, protože pro nás Praha není jenom Praha, ale je to Praha plus velké okolí, kdy jsme schopní naše služby poskytovat v té nejvyšší kvalitě. Tím myslím, že jsme tam schopní dovézt expres objednávku do šedesáti až devadesáti minut. Stejně to platí i pro Brno, tedy pro Brno a jeho okolí. A pak máme vzdálenější oblasti jako Plzeň nebo severní Čechy, Karlovy Vary a Ostrava. V každé této oblasti máme trošku jiný model. Někde to vozíme přímo z Prahy, někde to překládáme.

Lze říct, co si nejvíc lidé u vás objednávají? Jestli to je základní spektrum potravin, nebo nějaké speciality?
Největší zájem je o čerstvé potraviny a pak o trvanlivé potraviny. Tento sortiment s námi nakupuje skoro každý zákazník. Jiná situace je v nepotravinách u drogérie nebo kosmetiky. Tam máme penetraci u klientů výrazně nižší.

Čerstvé potraviny vedou, protože jimi jsme unikátní. Jsme je schopní nabídnout za ceny kamenných obchodů a naší konkurence. Jde o základní potraviny i o značky, které každý zná, jako je třeba Hollandia nebo Danone. Zároveň ale máme velké zastoupení sortimentu ve značkách, které standardně nekoupíte. Nebo by vás to stálo moc úsilí. Jako jediní třeba prodáváme vraňanské jahody, pro které byste jinak musel jet do Vraňan, abyste si je koupil. Nebo pokud byste chtěl borůvky od pana Karla Rodena, které my prodáváme, nikde jinde je nekoupíte.

Tím, že podporujeme malé farmáře, jsme schopní nabídnout lepší kvalitu a rychlejší servis. Třeba borůvky od pana Rodena jsme schopní mít u zákazníka zhruba za šest hodin od doby, kdy byly sklizené.

Jak si vedou vaše privátní značky?
Za poslední rok se ekonomická situace zcela zásadně změnila, máme tady obrovskou inflaci a zdražila se energie. My jsme to také vnímali a zákazníci byli daleko obezřetnější. A někteří se rozhodli, že zváží, kolik investují do jednotlivých nákupů.

Privátní značka se vyznačuje tím, že většinou jde o produkt v nižší cenové kategorii, ale my jsme i tak schopní nabídnout třeba plnotučné mléko, které má jako jediné, když nebereme selská mléka, obsah tuku 3,8 %, za cenu plnotučného mléka, které se nabízí v kamenném obchodě.

Privátní značky každopádně dál rozšiřujeme. Za poslední rok se nám jejich podíl zvedl z nějakých devíti na dvanáct procent. Pravidelně každý kvartál rozšiřujeme portfolio našich privátních značek o desítky produktů. Jako poslední to bylo třeba krmivo pro zvířata. Předtím jsme představili značku Kitchin, což jsou základní trvanlivé potraviny. Chtěli bychom mít postupně privátní značku ve všech kategoriích, kde to má význam, tedy kde je objem prodaného zboží dostatečný, aby to dávalo smysl pro nás i pro dodavatele.

A rozšíření dalšího sortimentu?
Těch možností je samozřejmě stále hodně. Na začátku roku jsme třeba významným způsobem rozšířili sortiment veganské stravy. Nabízíme také víc potravin bez lepku, zároveň jsme zastropovali u čtyřiceti produktů cenu, protože obecně je tohle zboží hodně drahé.

Náš fokus je samozřejmě na potraviny, ale rozšiřujeme sortiment dlouhodobě, a to i v dalších segmentech.

> **Největší zájem je o čerstvé potraviny a pak o trvanlivé potraviny. Tento sortiment s námi nakupuje skoro každý zákazník.**

FOTO: KAREL CHOC

Momentálně pracujeme na rozšíření sortimentu třeba u krmiva pro zvířata. V tom vidíme velkou příležitost.

V několika vašich skladech máte i vlastní pekárny. Jak jste s nimi spokojení?
Vidíme, že pekárny, které máme, nám ve skladech fungují. Nejste závislý na tom, že to někdo někde upeče, pak vám to musí dovézt, přijmete to a až pak to vezete zákazníkovi. Ten moment od pečení po expedici je proto nyní výrazně kratší. Jste schopní péct v průběhu celého dne, nevozíte pečivo jen v sedm ráno a pak ve dvanáct. Můžete prostě péct kontinuálně množství, které potřebujete. Navíc naše pečivo pečeme až tak třicet čtyřicet minut před odvozem objednávky. Zákazníci ho proto dostávají v maximální kvalitě.

Naši zákazníci proto nyní mnohem méně reklamují kvalitu pečiva, ale není to vlastně jen těmi vlastními pekárnami. Domluvili jsme se na určitých změnách s pekárnami, které k nám zavážejí svoje zboží, jako jsou Arctic Backery, Zrnozrnko nebo Eska. Jejich pečivo jsme totiž zákazníkům, kteří nejsou z Prahy nebo Brna, nemohli dovézt už na osmou hodinu ráno. Prostě to nešlo. Pekárna nám svoje výrobky dovezla ve chvíli, kdy už byla ta zakázka pro klienta na cestě. Už jsme to ale změnili a dnes i pečivo od těchto výrobců dovážíme všem zákazníkům už v prvním ranním slotu. Tedy s výjimkou těch, kteří objednávají do Rohlík Pointů. Tam to ještě neumíme.

Vaše centrum v Chrášťanech je plně automatizované. Co to znamená?
Je tam plně automatizovaný picking, česky vychystávání zboží. V podstatě je to o tom, že přijmete zboží, které vložíte do tzv. autostoru. A ten to následně automaticky chystá. Funguje to tak, že když si zákazník objedná, objednávka se takzvaně rozpadne a systém ví, ve které bedně je který produkt, a ty bedny posílá na místo, kde je člověk, jenž ten produkt vezme a vloží do tašky.

V manuálním skladu by to znamenalo, že všechno musejí odbavit zaměstnanci. Prostě to, co nyní zvládá automat, by museli řešit oni. Chodili by po skladě a vybírali jednotlivé objednané položky. V Chrášťanech stojí naši lidé na místě a autostore jim to doveze.

Jiné podobné centrum neplánujete?
Pracujeme na druhém automatizovaném centru. Je v Horních Počernicích. Otevřeli jsme ho před třemi roky, zatím je plně manuální. Chceme to ale změnit, protože vidíme, že nám automatizace výrazně pomáhá. Přestavba se nyní dokončuje, na podzim bychom ho měli mít už plně funkční.

U centra v Brně zatím o automatizaci neuvažujeme, protože spíš narážíme na jeho kapacitu. Zvažujeme pro-

FOTO: ROHLIK.CZ

Chceme dál doručovat zboží ve fantastické kvalitě a v co nejkratším možném termínu.

to varianty, co s tím centrem udělat, jestli ho bude možné zvětšit, nebo otevřít druhé. Automatizované nebude zatím ani nové centrum, které jsme nyní otevřeli v Ostravě.

Jak je na tom Rohlík s přechodem na elektroauta, o čemž opakovaně mluvili vaši předchůdci? Vlastně říkali, že v této době už budete využívat jen elektroauta.
My máme v současné době patnáct až dvacet procent aut, která jsou čistě na elektrický pohon. Jejich flotilu nadále rozšiřujeme, ale komplikací je dojezdová vzdálenost těchto aut. Takže je nyní využíváme hlavně v Praze a v Brně, kde to není k zákazníkům tak daleko. Za těmi vzdálenějšími pořád jezdí dodávky na CNG. Když to shrnu, je pořád naším cílem přejít plně na elektřinu a intenzivně na tom pracujeme. Jen nás limituje dojezdová vzdálenost aktuálně dostupná u těchto aut.

Už jste zmínil, kam všude dovážíte. Podle mapy pokrytí, kterou máte na webu, je ale stále řada bílých míst, třeba jižní Čechy nebo severovýchod země, kde nejste. Váš konkurent Košík se přitom chlubí, že dováží po celém území České republiky. Kolik je tedy vaše aktuální pokrytí?
Myslím, že dnes jsme někde kolem 65 procent. On by nebyl problém zavážet celou republiku, byli bychom to schopní udělat v podstatě zítra. Ale my si říkáme, že chceme naši službu nabídnout v maximální možné kvalitě. Nechceme limitovat sortiment a nechceme omezovat zákazníka tím, že mu nákup dovezeme až další den a v časovém oknu čtyř hodin. To je cesta, jakou bychom k tomu mohli dojít. Je to nejjednodušší.

Ale my jsme unikátní servisem, a když už něco otevřeme, chceme zaručit, že náš klient dostane službu ve stoprocentní kvalitě.

Proto jsme zatím na šedesáti pěti procentech. Ale brzy oznámíme něco většího a měli bychom se výrazně posunout. Určitě nějaká bílá místa zůstanou, hlavně to bude v jižních Čechách. Důvod je ten, že denzita obyvatelstva je tam taková, že jde o veliké území a máte víc bodů, kde nežije tolik lidí na jednom místě. A my bychom byli nuceni prodlužovat závozová okna, abychom to byli schopní efektivně rozvážet. V těch místech proto aspoň používáme formu Rohlík Pointů.

A pak je tam ještě malý kousek na severovýchodě Česka, který velice brzy pokryjeme. Počítáme s tím, že tyto Vánoce už bude mít osmdesát procent obyvatel možnost na Rohlíku nakoupit.

Současným trendem je budování marketplace – tržišť, kde jeden výrazný hráč spojuje v jednu platformu malé prodejce. Nechystá se něco podobného u Rohlíku?
Ne, v tuhle chvíli nic takového neplánujeme. Je to kvůli tomu, že chceme, aby naše služba zůstala unikátní. Chceme dál doručovat zboží ve fantastické kvalitě a v co nejkratším možném termínu. V momentě, kdy bychom šli do marketplace, museli bychom někde slevit, protože bychom nebyli schopní skladovat a rychle rozvážet třeba 150 tisíc produktů. Museli bychom celý koncept přebudovat, a to nechceme.

JAN VACA

Autor je od ledna 2018 ředitelem médií vydavatelství Internet Info. Předtím šest let vedl zpravodajskou sekci portálu iDNES.cz, ještě předtím byl několik let reportérem celostátní redakce MF DNES. ■

Kia Sportage.

Akční model EDICE 30.

Movement that inspires

Úrok již
3,99 % p. a.

Oslavte s námi 30 let Kia Sportage. Objevte nový akční model Kia Sportage EDICE 30 s atraktivním designem, bohatou výbavou a sadou pokročilých asistenčních systémů. K dispozici s benzinovými, mild-hybridními a hybridními motory a výhodným financováním.

Kombinovaná spotřeba a emise CO_2 (WLTP). Kia Sportage: 1,1–7,3 l/100 km, 25,5–166 g/km. Reprezentativní příklad financování Sportage EDICE 30 1,6 T-GDI 110 kW 4x2 s financováním Kia Select; pořizovací cena 784 980 Kč vč. DPH, výše úvěru 627 984 Kč, akontace 20 % (156 996 Kč); pevná výpůjční úroková sazba 3,99 % p. a., RPSN 9,50 % p. a.; měsíční (1.–47.) splátka úvěru 12 998 Kč, měsíční (48.) splátka úvěru 158 620 Kč, měsíční splátka pojištění HAV 1 289 Kč, POV 335 Kč; poplatek za poskytnutí úvěru 5 495 Kč; délka úvěru 48 měsíců. Celková částka k uhrazení (jistina, úrok, hav. pojištění, pov. ručení, poplatek): 769 526 Kč, pojištění sjednáno u pojišťovny UNIQA. Nabídka platí do 30. 11. 2023. Vyobrazení vozů je pouze ilustrativní a může obsahovat doplňkovou výbavu. Pro bližší informace navštivte www.kia.com.

FIASKO SUPERMINISTRA H.:

ZABETONOVANÝ MOBILNÍ TRH SE VĚTŠÍ KONKURENCE NEDOČKÁ

SLIBY NĚKDEJŠÍHO MINISTRA KARLA HAVLÍČKA O POSÍLENÍ KONKURENCE NA MOBILNÍM TRHU SKONČILY PŘEDPOVÍDANÝM KRACHEM, POTVRZUJE TO DALŠÍ PRODEJ VYDRAŽENÝCH KMITOČTŮ. ŠLO O NESCHOPNOST, NEBO O ÚMYSL?

S odstupem téměř tří let je jasná jedna věc: aukce 5G kmitočtů, která se konala v roce 2020, posílila pozici tří velkých operátorů a pomohla na dlouhá léta zabetonovat český mobilní trh. Tento výsledek si může připsat na účet někdejší superministr Karel Havlíček, který výsledný model dražby prosadil. Pomohl si přitom i brutálním zásahem do fungování Českého telekomunikačního úřadu (ČTÚ), který kvůli němu několik let ovládala jedna z nejhorších hlav v jeho historii.

Neslavný dopad aukce potvrdil červencový prodej kmitočtů v pásmu 3,5 GHz, vydražených v aukci skupinou Kaprain, T-Mobilu. Už dříve se svých frekvencí v pásmu 3,7 GHz zbavil také operátor PODA. Velká trojka tak nakonec získala všechny kmitočty, které stát v roce 2020 dražil, s výjimkou 20MHz bloku v pásmu 3,5 GHz, který stále drží Nordic Telecom.

Havlíčkovy někdejší sliby, jak 5G aukce přivede několik menších operátorů, kteří díky tzv. národnímu roamingu zvýší konkurenci na trhu a přispějí ke snížení cen, se prostě ukázaly být zcela mimo. Ne že bychom na Lupě tento výsledek nepředpokládali…

Pátek třináctého

Aukce 5G kmitočtů byla vypsaná pro jednu konkrétní firmu, zdůvodňoval v roce 2019 ministr průmyslu a obcho-

du Havlíček, proč se musejí chystané podmínky dražby výrazně změnit (z kontextu bylo jasné, že jde o Nordic Telecom). Máme od tajných služeb informace o nestandardním průběhu přípravy aukce, tvrdil také (kupodivu se nic takového nepotvrdilo). Z čela Rady Českého telekomunikačního úřadu (ČTÚ) pod touto záminkou vystrnadil respektovaného Jaromíra Nováka a na jeho místo protlačil svého koně – poslušnou Hanu Továrkovou. Pod jejím vedením se ale příprava důležité dražby změnila ve frašku.

Továrková během několika měsíců bez uzardění dokázala přejít od Havlíčkovy teze „nejsou žádní zájemci o celoplošné kmitočty v pásmu 700 MHz“ ke tvrzení, že „je významný počet subjektů, které o ně mohou mít zájem“, a podmínky předělala tak, že nakonec celoplošné frekvence nemohly být zajímavé pro nikoho jiného než velkou trojku síťových operátorů.

Přišel pátek třináctého českých telekomunikací. 13. listopadu 2020 ČTÚ oznámil výsledek aukce, a světe, div se: pásmo 700 MHz, které teoreticky mohlo posloužit k výstavbě čtvrté celoplošné sítě v Česku, si bez většího boje a za v podstatě vyvolávací ceny rozdělily T-Mobile, O2 a Vodafone.

V pásmu 3,5 GHz se k velké trojce přidaly společnosti Nordic Telecom a Kaprain (tehdy prostřednictvím operátora CentroNet). A na národní roaming v síti O_2 získal díky podmínkám aukce právo i třetí menší operátor, PODA.

Ručníky v ringu

Hned po aukci se ovšem Havlíček nechal za výsledek dražby veřejně vychválit svým náměstkem Petrem Očkem. Vzhledem k tomu, že média tehdy psala spíš o debaklu, muselo si ministerstvo pro tyto ódy objednat placený článek v ČTK. Přidala se i Továrková, která slibovala, že tarify budou do roka levnější minimálně o patnáct až dvacet procent.

Vyjednávání o národním roamingu se ale několik let bezvýsledně táhla a podezření, že nakonec žádný nový

celoplošný operátor nevznikne, posilovala i skutečnost, že se tři menší hráči zásadně odmítali o možném spuštění svých služeb bavit (s občasnou výjimkou).

Firma PODA i holding Kaprain nakonec hodily ručníky do ringu. Přinejmenším u firmy Karla Pražáka to vypadá, že frekvence koupila rovnou na spekulaci, podle dostupných informací totiž za více než dva roky s přípravou budoucí sítě ani nezačala. Nordic Telecom o svých plánech mlčí.

Jak se měnily ceny

A jak se zatím změnil trh? Připomeňme, že začátkem roku 2019 mohli zákazníci v Česku podle ceníkových nabídek velkých operátorů pořídit za pětistovku měsíčně (bez závazku) k neomezenému volání a SMS obvykle tak 500 MB dat.

Na podzim stejného roku došlo k velké změně: nejdřív T-Mobile a pak postupně i ostatní dva síťoví operátoři přišli s prvními tarify obsahujícími neomezená data. Pět set korun sice stále stačilo tak na 1,5 GB dat (plus neomezené volání a SMS), ale tisíc korun měsíčně už dokázalo zaplatit tarif s 16 GB dat. Kompletní neomezenou nabídku (hovory, SMS, data) bez rychlostních či jiných limitů bylo možné pořídit zhruba od 1 600 Kč měsíčně (a dráž).

Letos, o necelé čtyři roky později, můžete mít za částku kolem pěti set korun k neomezenému volání a SMS pořád pouze mezi 500 MB až 2 GB dat

To, že nakonec žádný nový celoplošný operátor nevznikne, posilovala i skutečnost, že se tři menší hráči zásadně odmítali o možném spuštění svých služeb bavit (s občasnou výjimkou).

(a za necelých 600 Kč se dostanete na 4 GB). Neomezená data se zpomalenou rychlostí začínají na cenách mezi 900 a 1 000 Kč a balíčky s nezpomalenými neomezenými daty startují kousek nad 1 300 Kč měsíčně.

Je vidět, že u levných tarifů se situace nemění, pětistovkové balíčky jsou reliktem minulosti a nové minimum síťoví operátoři posunuli k 600 Kč měsíčně. U dražších tarifů a balíčků s neomezenými daty můžeme sledovat přidávání GB či zvyšování rychlostí a víceméně stagnující ceny.

Prostě: žádný velký posun se od roku 2019 nekoná, nová konkurence díky zbabrané Havlíčkově (a Továrkové) aukci nepřijde a velká trojka má i nadále vše pevně v rukou.

DAVID SLÍŽEK

Šéfredaktor webu Lupa.cz. ■

PODVODNÝCH TELEFONÁTŮ PŘIBÝVÁ. FIRMY TO VĚTŠINOU NEŘEŠÍ

PŘI JAKÝCHKOLI POCHYBNOSTECH ZAVĚSTE A ZAVOLEJTE ZPÁTKY NA OFICIÁLNÍ ČÍSLO, RADÍ SPOLEČNOSTI. S IMPLEMENTACÍ POKROČILÝCH ŘEŠENÍ BOJE S PODVODNÝMI TELEFONÁTY ALE ČESKO PŘÍLIŠ DALEKO NENÍ.

- „DOBRÝ DEN, TADY MAREK Z O_2, ODDĚLENÍ PRO ZÁKAZNÍKY. RÁD BYCH S VÁMI PROŠEL VAŠE SLUŽBY."
- „JAK MÁM VĚDĚT, ŽE JSTE OPRAVDU Z O_2?"
- „JSEM MAREK Z O_2, ODDĚLENÍ PRO ZÁKAZNÍKY. MŮŽETE MI ŘÍCT CELÉ VAŠE JMÉNO?"
- „ALE JAK MÁM VĚDĚT, ŽE JSTE Z O_2?!"
- „JSEM MAREK..."

Znáte to: zazvoní telefon a hlas na druhé straně vás osloví s tím, že zastupuje banku, mobilního operátora nebo třeba energetickou společnost. Někdy z kontextu hovoru vyplyne, že jde o skutečného zástupce firmy, obzvláště pokud nejde o první kontakt, ale například o reakci na naše předchozí volání, e-mail nebo jiný podnět. Ale často tento kontext chybí, a začnete mít pochybnosti o tom, s kým to vlastně mluvíte.

Opatrnost je přitom namístě. Pokusy o vylákání osobních dat nebo přímé podvody prostřednictvím falešných telefonátů jsou dnes velmi reálnou hrozbou. Volající z call centra přitom obvykle nemá možnost, jak svou identitu potvrdit. A české firmy se tomuto problému – až na výjimky – nevěnují. Technické možnosti, jak tuto situaci řešit, přitom existují.

Útočníci mění postupy

„Dříve šlo jen o prosté e-mailové či SMS výzvy k přihlášení se do internetového bankovnictví, případně se útočníci po telefonu vydávali za zaměstnance technické podpory banky a tvrdili, že účet byl napaden a potřebují potvrdit vaše přihlašovací údaje nebo údaje k platební kartě. Dnes však útočníci vymýšlejí složitější scénáře," potvrzuje změnu postupů specialistka kybernetické bezpečnosti společnosti Eset Vladimíra Žáčková.

Jako příklad zmiňuje postup, kterým se útočníci snaží přesvědčit oběti k výběru peněz, nebo dokonce k podání žádosti o úvěr či vložení hotovosti do automatů na bitcoiny nebo na jiný účet. Důvodem k tomu má být údajně zcizená bankovní identita klienta banky a bezprostřední ohrožení jeho peněz na účtu.

„Dalším scénářem jsou útoky, kdy se podvodníci vydávají přímo za brokery a pod záminkou investiční příležitosti se snaží získat přístup přímo k ovládání počítače oběti. Útočník oběť kontaktuje telefonicky a přesvědčí ji k nainstalování programů pro vzdálený přístup jako AnyDesk nebo TeamViewer. Získá tím moc nad počítačem oběti a uloženými přihlašovacími údaji do internetového bankovnictví a dalších aplikací," vyjmenovává nejčastější motivaci k vishingu Žáčková.

Nemusí ale hned nutně jít o pokus vybílit bankovní účet nebo si na cizí úkor vzít úvěr. V ohrožení mohou být i „jen" osobní data. Například v případě, kdy volající pod záminkou dojednání lepšího pojištění vyzvídá rodné číslo.

VISHING

Vishing – tzv. hlasový phishing nebo voice phishing je typ phishingového útoku, který používá hlasový hovor a techniky sociálního inženýrství. Útočníci se prostřednictvím telefonního hovoru snaží z oběti vylákat osobní nebo platební údaje, nebo ji rovnou přimět k převodu peněz. Zjednodušeně řečeno jde o podvodné volání.

Při jakémkoli podezření zavěste

Jaké v tu chvíli máme možnosti ověřit si identitu volajícího? Jak můžeme zjistit, že osoba na druhé straně linky je skutečně zástupcem korporace, za kterou se vydává? A co dělat, když máme pochybnosti?

Firmy provozující call centra jsou si problému vědomy a většinou připouštějí, že k takovým případům může dojít. Některé společnosti už se s nimi dokonce setkaly. Účinnou obranu, resp. zavedenou možnost si okamžitě v průběhu hovoru ověřit, že věci jsou tak, jak vypadají, ale má zatím jen jediný subjekt a další na něm pracuje.

Tím, kdo zaslouží za boj s vishingem pochválit, je Česká spořitelna.

Jak můžeme zjistit, že osoba na druhé straně linky je skutečně zástupcem korporace, za kterou se vydává? A co dělat, když máme pochybnosti?

„Jako první banka od loňska umožňujeme okamžité zjištění identity volajícího bankéře. Vzdálené ověření v aplikaci George Klíč měsíčně využijí desítky tisíc klientů," říká mluvčí spořitelny Filip Hrubý. Banka umí v mobilní aplikaci uživateli potvrdit, že hovor skutečně iniciovala. Jde přitom o zabezpečený kanál využívaný i pro potvrzování prováděných transakcí. Útočník, který může snadno podvrhnout své číslo tak, že se zdá, že volá z oficiální linky firmy, už nedokáže zajistit, aby se podvodný hovor zobrazil i v aplikaci. Při troše obezřetnosti tak zákazník může mít do několika sekund jasno.

Stejnou službu zatím připravuje T-Mobile. „Na dvoufaktorové autorizaci prostřednictvím aplikace včetně autorizace hovoru aktuálně pracujeme," říká mluvčí operátora Patricie Šedivá. T-Mobile přitom potvrzuje, že se s případy, kdy se někdo vydává

V případě podezřelého nebo obtěžujícího volání doporučuji neváhat, ukončit hovor a nahlásit jej na Policii ČR.

za jeho zaměstnance, setkává. Denně detekuje a zablokuje přes čtyři tisíce podezřelých aktivit, které často cílí na citlivá a osobní data uživatelů. „Hovory velmi často pocházejí ze zahraničí, kde je zdrojové zařízení nedohledatelné a pro útočníka představuje pohodlnější způsob podvodu," dodává Šedivá.

Operátor aktuálně přišel také s bezpečnostním řešením Firewall 2.1, které nově ověřuje původ hovoru, tedy to, zda se telefonní číslo nachází v domácí síti, nebo v zahraničí. Podvržené hovory pak v případě, že je aktivní číslo přihlášené do domovské sítě firewall, blokuje. Funguje to ale jen v případech, kdy jde o zneužití čísel T-Mobilu při volání do sítě T-Mobilu.

Ve všech případech při jakýchkoliv pochybnostech operátor doporučuje hovor okamžitě ukončit a zavolat zpátky na call centrum. Tam jsou schopní potvrdit, jestli předchozí hovor skutečně pocházel od operátora, případně si potvrdit provedené objednávky. Ukáže-li se, že se klient stal obětí podvodu, i tehdy mu call centrum umí pomoci. „V takovém případě zablokujeme objednávky, změníme role, přístupové údaje apod. Navíc proaktivně monitorujeme nadstandardní situace a tyto transakce ověřujeme se zákazníkem, abychom se ujistili, že objednávku skutečně udělal," vyjmenovává kroky možné pomoci Šedivá.

Nasazení AI může nahrávat útočníkům

Operátor O_2 tvrdí, že se dosud s něčím takovým vůbec nesetkal. „Doposud jsme nezaznamenali, že by se někdo vydával za zaměstnance O_2 a jménem O_2 kontaktoval zákazníky," říká mluvčí modrého operátora Blanka Vokounová. Nejlepší ochranou před útočníky je podle ní velká opatrnost. „V případě podezřelého nebo obtěžujícího volání doporučuji neváhat, ukončit hovor a nahlásit jej na Policii ČR," radí mluvčí.

O_2 zjevně více trápí podvodné SMS. Kvůli nim nedávno operátor zřídil linku 720 002 002 pro přeposílání podvodných SMS zpráv. „Tipy na takto podvodné SMS zprávy chodí prakticky denně a díky nim se nám podařilo řadu hackerů zastavit a ochránit zákazníky," dodává Vokounová.

O_2 přitom nedávno představilo změnu fungování svých call center, které podvodům s falešnými telefonáty může nahrávat. Zapojuje totiž do kontaktu se zákazníky virtuální softwarové roboty a prvky umělé inteligence. To útočníkům otevírá možnost nasadit stejné zbraně, aniž budí zdání čehokoliv nepatřičného. Je nejspíš jen otázkou času, kdy vishingové útoky začnou využívat virtuální hlas přizpůsobený tomu, který používá operátor. Z tiskové zprávy přitom víme, že virtuální asistentka

Eva mluví hlasem herečky Kateřiny Winterové.

Podle mluvčí O_2 se operátor nechystá implementovat podobné řešení jako zmiňovaná Česká spořitelna a umožnit příchozí volání ověřit přes mobilní zákaznickou aplikaci. „To se obávám, že není v našich technických možnostech," říká Vokounová.

Expertka na bezpečnost z Esetu Vladimíra Žáčková v tomto ohledu zdůrazňuje, že nejdůležitější prevencí těchto podvodů je zůstat informovaný. Vědět o nejnovějších typech útoků a mít přehled v nových technologiích, které mohou používat jak útočníci, tak instituce, aby prostředky zabezpečily. „Spolehlivé bezpečnostní řešení obsahuje také funkci filtr hovoru. Ten blokuje příchozí a odchozí hovory v závislosti na nastavených pravidlech. Pokud zablokujete příchozí hovor z podvodného čísla, útočník už se vám nedovolá," dodává Žáčková.

Pokud zablokujete příchozí hovor z podvodného čísla, útočník už se vám nedovolá.

Buďte ve střehu, hovory od nás si ale neověříte

Vodafone na rozdíl od O_2 přiznává, že se s vishingem setkal, a dokonce že jde o rostoucí trend. „Podvodníci se ze světa fyzického přesunuli do světa digitálního," konstatuje mluvčí Vodafonu Ondřej Luštinec. Ani tento operátor však možnost ověřování hovorů ze svých infolinek přes zabezpečený kanál, například v aplikaci Můj Vodafone, neplánuje. „Takovou cestou nepůjdeme. Ale pokud jde o spoofing, pracujeme na řešení, které teď nemohu více komentovat," dodává bez dalších detailů Luštinec. I on radí nesdělovat nikdy citlivé informace přes telefon a při jakémkoli podezření zavěsit a zavolat zpátky na oficiální číslo dané instituce.

Z dalších tuzemských bank kromě spořitelny má omezený nástroj proti vishingu ČSOB. V určité fázi hovoru, když je třeba klienta ověřit, používá banka mobilní aplikaci Smart

Klíč. Do té přijde notifikace se jménem volajícího bankéře a klient přes aplikaci potvrzuje, že banka mluví právě s ním. Je to tedy ověření naruby, ale svůj účel může splnit i pro prověření podezřelého hovoru. U ostatních peněžních ústavů ale máte smůlu a nástroj snadného ověřování volajících zaměstnanců u nich budete hledat marně. Nemá ho implementována Fio Banka, Air Bank, Komerční banka ani mBank.

A podobně jsou na tom i energetické podniky. ČEZ apeluje na obezřetnost a zdravý rozum. Podle Alice Horákové z ČEZ by se lidé měli zamyslet nad tím, zda požadavek volajícího dává smysl. „Jsme energetická firma, proto oslovujeme naše zákazníky zejména s energetickými tématy. Nikdy nenabízíme žádné finanční služby, jako jsou investiční příležitosti či nákup akcií, nežádáme tedy o žádné přístupy do bankovnictví," dodává.

Ani Pražská energetika obdobnou pokročilou obranu proti vishingu neřeší. „Ve většině případů volají zákazníci nám s tím, že potřebují řešit své zákaznické požadavky. Pokud už voláme my, zpravidla takové hovory navazují na předchozí komunikaci. Hovor od nás je tedy ze strany klienta vždy očekávaný," uzavírá mluvčí PRE Karel Hanzelka.

Ochota problém řešit, i když už příklady technického řešení existují, tedy u většiny Lupou oslovených společností chybí. Firmy, které žádná opatření nechystají, přitom riskují mimo jiné to, že zákazníci s povědomím o možném nebezpečí nebudou – zcela oprávněně – ochotní s pracovníky call center, kteří se nedokážou spolehlivě identifikovat, jakkoli komunikovat.

Hovor citovaný na začátku článku ostatně skončil přesně tak:

- **„DOBRÝ DEN, TADY MAREK Z O_2, ODDĚLENÍ PRO ZÁKAZNÍKY. RÁD BYCH S VÁMI PROŠEL VAŠE SLUŽBY."**
- **„JAK MÁM VĚDĚT, ŽE JSTE OPRAVDU Z O_2?"**
- **„JSEM MAREK Z O_2, ODDĚLENÍ PRO ZÁKAZNÍKY. MŮŽETE MI ŘÍCT CELÉ VAŠE JMÉNO?"**
- **„JAK MÁM VĚDĚT, ŽE JSTE Z O_2?!"**
- **„JSEM MAREK..."**
- **„NA SHLEDANOU!"**

MARTIN DRTINA

Redaktor serveru Lupa.cz se zaměřením na telekomunikace, média, IT a právo. Dříve šéfredaktor Právního rádce a mluvčí Českého telekomunikačního úřadu. ■

Framework AyMINE – ekosystém pro cloudové podnikové aplikace

AYMINE JE MODERNÍM ŘEŠENÍM PRO RYCHLÝ VÝVOJ BEZPEČNÝCH PODNIKOVÝCH APLIKACÍ V CLOUDU.

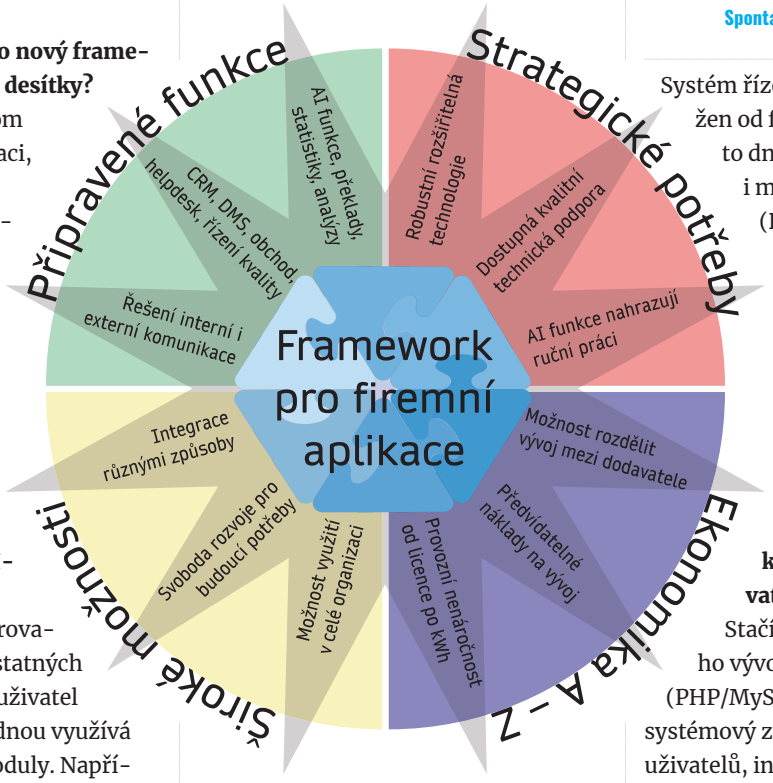
Architektura je od základu navržena pro souběžný provoz mnoha klientů, a tak je ideální pro poskytování služeb menším firmám. Na otázky, co AyMINE přináší, odpovídá jeho architekt ze společnosti PDQM Štěpán P. Nadrchal.

Proč jste se rozhodli pro nový framework, když jich existují desítky?
Potřebovali jsme nejenom robustní webovou aplikaci, ale i mobilní aplikaci. Nástroje pro tvorbu aplikací samozřejmě jsou, jsou ale zaměřené pouze na front-end, back-end neřeší. AyMINE generuje aplikaci a orchestruje procesy back-endu najednou.

Co jsou nejdůležitější vlastnosti, čím se AyMINE liší?
Určitě generování integrované aplikace podle samostatných zadání modulů. Přitom uživatel vůbec nevnímá, že najednou využívá samostatně vyvíjené moduly. Například CRM modul dodá funkci propojení s ústřednou, ale volat je díky ní možné i z HR modulu. To je velká výhoda objektového přístupu.

Na druhém místě asi celková nenáročnost na hardware. Efektivitě provozu IT se po letech zase začíná věnovat pozornost a v tom je AyMINE na špičce.

Pro koho je framework vhodný?
Ideální je pro týmy, které vyvíjejí větší podnikové systémy. Chtějí moderní řešení pro počítač i mobil. Pro firmy, které si přejí automatizovat rutinní práci a využívat AI. Zvlášť pokud chtějí platformu pro SaaS služby.



Jaké je v současné době jeho nasazení?
V počátcích jsme řešili potřeby firem, které vyplývají z náročných standardů jako CMMI, ISO 26262, SPICE apod. V AyMINE vznikl modul moderního řízení kvality, kde formalistický přístup nahrazuje automatizovaný workflow systém.

> **To je neskutečně rychlý, vůbec nechápu, jak to děláte.**
>
> Spontánní hodnocení obchodního partnera

Systém řízení ale nemůže být odtržen od firemních agend. Proto dnes v AyMINE vznikly i moduly správy dokumentů (DMS), už zmíněných úkolů (WfMS), projektů, kompletní obchodní systém, CRM, helpdesk nebo personalistika. Pokrývá většinu procesních potřeb firmy. Nově využíváme i AI moduly.

Co potřebuje znát tým, který chce v AyMINE budovat řešení? Z čeho vyjde?
Stačí znalost nejrozšířenějšího vývojového stacku – LAMP (PHP/MySQL). Tým může využít celý systémový základ – správu klientů, uživatelů, integraci na e-maily, telefony, ale třeba i řízení úkolů, adresář, reporty apod. Samozřejmostí jsou dokumentace a školení.

Více se dozvíte na www.aymine.org. ■

SÍTĚ 5G JEŠTĚ NENAPLNILY PŘEHNANÁ OČEKÁVÁNÍ, A UŽ SE BLÍŽÍ NÁSTUPCE

5G ADVANCED NEBOLI 5,5G BUDE PŘÍŠTÍ ROK K DISPOZICI PRO KOMERČNÍ NASAZENÍ. NOVÉ OBCHODNÍ MODELY SE NICMÉNĚ STÁLE HLEDAJÍ.

Svět ještě nepocítil plné a dlouho dopředu hypované výhody mobilních sítí 5G, a už se chystá nástup 5,5G nebo také 5G Advanced (5G-A). V první polovině příštího roku by měly být dokončeny standardy 3GPP Release 18 a výrobci telekomunikačních zařízení pak začnou dodávat potřebné technologie. Výsledkem by mimo jiné měly být výrazně vyšší rychlosti přenosu dat vzduchem, než je tomu u 5G.

Do prvních testů 5G Advanced v rámci komerčních sítí už se pustilo dvacet operátorů po celém světě. Společnost Du ze Spojených arabských emirátů v říjnu uskutečnila pilotní provoz v Dubaji, kde byla schopná dostat se na rychlosti v řádech gigabitů za sekundu.

Lupa se testování nového standardu v Dubaji zúčastnila. Připojená vila na okraji města byla schopná na několika zařízeních zároveň streamovat video ve 4K, 8K a skrze nové typy displejů od společnosti TCL také ve 3D. Nebylo to ale zadarmo. Operátor Du zkombinoval frekvence 2,7 GHz (blok 100 MHz), 3,6 GHz (200 MHz) a milimetrové vlny (mmWave) s blokem 800 MHz.

„K něčemu takovému v běžném provozu se samozřejmě budeme propracovávat postupně," řekl zástupce emirátského operátora s ohledem na nutné investice nebo postup regulátorů v uvolňování frekvencí. Přerod do 5G Advanced nebude okamžitý a stane se tak v rámci plynulého přechodu z 5G.

5,5G má podle dodavatelů technologií přinést rychlost downloadu až deset gigabitů za sekundu a jeden gigabit za sekundu u uploadu. Standard se má stát předvojem k 6G, kde lze očekávat i terabitové rychlosti a kde se aktuálně vedou debaty o podobě standardů.

Příští rok do komerčního nasazení

Společnosti jako Huawei, Nokia, Samsung, Ericsson nebo ZTE mají mít příští rok připraveny potřebné technologie pro 5G Advanced včetně antén Extremely Large Antenna Array (ELAA). Prezident Huawei pro 5,5G John Gao uvedl, že standard bude tou dobou k dispozici pro komerční nasazení.

Připraveny by měly být i čipy. Qualcomm demonstroval 5,5G čip Snapdragon X75 podporující rychlost

až 10 gigabitů za sekundu za využití milimetrových vln a sub-6 GHz. MediaTek má čip zvládající 7,7 gigabitu za sekundu, u uploadu 3,8 gigabitu. Pro budoucnost 5G Advanced, 5G a mobilních sítí obecně má být důležité mid-range spektrum 6 GHz. O něj se v současné době vedou spory. Operátoři ho chtějí získat pro sebe, minimálně jeho vrchní část. Chtějí ho ale také menší provideři. O možném dělení se bude debatovat letos v Dubaji na konferenci WRC. Společnosti jako Huawei se v lobbingu připojily na stranu operátorů, byť ve velkém dodávají i menším poskytovatelům.

> **Pro budoucnost 5G Advanced, 5G a mobilních sítí obecně má být důležité mid-range spektrum 6 GHz.**

U nás se spor o 6 GHz také označuje jako „APMS versus VNICTP“, odkazující na dvě zájmové organizace. „Nemyslím si, že se letos na WRC o upper 6 GHz rozhodne. Jsem toho názoru, že rozhodnutí bude odloženo. Jsem také přesvědčený, že Evropská unie bude mít samostatnou politiku,“ uvedl ředitel VNICTP Jakub Rejzek. „Je důležité celou kauzu vnímat jako poslední příležitost pro rozšíření WAS/RLAN a pásmo uvolnit pro distribuční sítě v domácnostech,“ dodal.

K čemu to bude

Je otázka, k čemu přesně 5,5G v praxi bude. Nokia mluví o lepším pokrytí, výkonu MIMO, nahrazení GSM-R, rozšíření mobilních sítí mimo smartphony, AR a VR, přesném pozicování

zařízení a tak dále. Podobné předpovědi nabízí také Ericsson.

Řadu věcí z toho slibovalo už 5G, a to včetně operací na dálku nebo autonomních aut. Prozatím to ale vypadá spíše tak, že operátoři posílili sítě pro rychle rostoucí spotřebu dat a nové obchodní modely se prozatím ve velkém neobjevily. Na konferencích už se zase začíná vzhlížet k novým mesiášům, teď je to hodně očekávaný AR/VR headset Apple Vision Pro.

Na telekomunikačním summitu v Dubaji ovšem zaznělo, že 5G potřebuje více aplikací a že je třeba „aktivovat ekosystém". Tyto motivační proslovy lze ale slyšet už nějakou dobu.

Podle organizace GSMA se má počet uživatelů 5G jako celku do roku 2030 dostat na 5,2 miliardy. Na světě je dnes asi 260 sítí využívajících 5G. Adopce má být rychlejší než u přechodu z 3G na 4G/LTE. 4G se na miliardu uživatelů dostalo za osm let, 5G za čtyři. Na trhu je kolem 1 800 zařízení podporujících 5G. Standalone 5G, kdy mobilní síť má 5G nejenom na bezdrátové části sítě, ale také na core, je ale naprostá minorita (v Česku standalone také nemáme).

Zákazníci jsou podle GSMA ochotní za 5G platit o několik procent více než za tarify s 4G, ale záleží na trhu. Operátor Hong Kong Telecommunications (HKT) má na 5G milion zákazníků, kteří podle výkonného ředitele Bruce Lama platí o devět dolarů více než za 4G.

HKT má podle svých slov 99 procent vysílačů připojených přes optiku a využívá frekvence 700 MHz, 3,5 GHz, 4,9 GHz a testuje 28 GHz. Ve specifické Asii nabízí například obsah pro virtuální realitu, jako jsou k-popové koncerty nebo přenosy sportovních utkání ve 4K a z více úhlů. Operátor také experimentuje s rozšířenou realitou, kdy skrze aplikaci AR Lens nabízí

Podle organizace GSMA se má počet uživatelů 5G jako celku do roku 2030 dostat na 5,2 miliardy.

kontextové informace či slevové kupóny při pohybu ve městě. Mezi partnery má Lego, Uniqlo nebo McDonald's. Byznysové výsledky operátor nekomentoval.

Drahé privátní 5G

Trh už nějakou dobu mluví o tom, že „to pravé 5G" najde využití jinde než u koncových zákazníků. Operátoři vidí přínos v network slicingu, lepší energetické efektivitě a podobně. „Reálné 5G bude vidět hlavně v privátních sítích," pronesl Marco Zangani, ředitel sítě ve Vodafone Italy.

Privátní 5G sítě mohou sloužit třeba k tomu, aby továrny nebo sklady získaly garantovanou bezdrátovou síť a využívaly ji k věcem jako řízení autonomních robotů. V Česku je takových sítí prozatím velice málo, i když se je zejména T-Mobile a Vodafone obchodně snaží protlačit. Potenciální zákazníci v debatách často říkají, že pořízení privátní sítě 5G se vším všudy, tedy včetně dohledu a spol., je velmi nákladná záležitost a že se nevyplatí.

„Doby, kdy technologie vyvolávala aplikační potřeby, už je v telku pryč a je potřeba realistický přístup. Privátní 5G může být jednoznačně zajímavou technologií pro systémovou integraci, ale sama o sobě byznys nevyrobí," vyzdvihl Filip Malina, majitel společnosti WIA.

Technický ředitel GSMA Alex Sinclair přesto uvedl, že tento takzvaný enterprise segment představuje pro 5G největší příležitost. Více než padesát procent návštěvníků konference Mobile World Congress v Barceloně, kterou GSMA pořádá, už údajně tvoří firmy mimo tradiční IT a telekomunikační průmysl. To má dokazovat, že se pro operátory a jejich sítě vytváří velký prostor mimo jejich tradiční obory a že je možné více expandovat do B2B a skrze mobilní sítě rozjíždět počítačové vidění, vzdálené ovládání a další.

„Operátoři se stále učí, jak navázat partnerství mimo své tradiční oblasti a jak na 5G postavit nové obchodní modely a dostat z této generace sítí nějakou další hodnotu," shrnul výkonný předseda představenstva analytické společnosti CCS Insight Shaun Collins s tím, že zatím snahy operátorů jdou právě směrem B2B/privátní 5G a fixní bezdrátový internet. Privátní mobilní sítě podle CCS v roce 2022 udělaly tržby 2,7 miliardy dolarů. Trh se má do budoucna rozrůst na desítky miliard dolarů.

Prezident operátorské divize Huawei Li Peng uvedl, že nejdále v nasazování privátního 5G je Čína. V zemi na těchto sítích běží automatizované doly, přístavy, továrny nebo vlakové terminály (jeden takový nově operuje v Maďarsku). Vysvětlení lze ale hledat v tom, že tyto projekty různými způsoby dotuje vláda. Cílem je podpora firem a zároveň získat náskok vůči konkurentům. „Továrny v Číně, které digitalizují, dostávají daňové úlevy a další formy podpory od lokálních vlád," potvrdil Li.

Fixní bezdrát

Fixní připojení k internetu (FWA, Fixed Wireless Access) je druhou z možností využití 5G, u které lze vidět alespoň nějaké komerční instalace. Operátoři se FWA snaží nabízet tam, kam jim nevede poslední míle skrze kabelyv zemi. Vzduchem lze nabídnout poměrně vysoké rychlosti a odezvu, ovšem za cenu čerpání kapacity sítě – často tedy jde spíš o poslední možnost, kterou operátoři chtějí klientům dát.

Operátor Du ze Spojených arabských emirátů například dává domácnostem vyšší FWA tarif za 299 dirhamů měsíčně (v akci za 239 dirhamů), což je asi 1 900 korun. V ceně jsou neomezená data a předplatné několika streamovacích služeb, jako jsou Disney+ a Amazon Prime na rok zdarma.

„FWA má několik výzev. Má slabé pokrytí v mrakodrapech a neexistuje neomezená kapacita 5G sítí, takže musíme dělit datové toky podle typů zařízení. Zároveň očekávání zákazníků jsou vysoká, chtějí úroveň služeb jako na optice," popsal obchodní ředitel Du Karim Benkirane.

Emirátský operátor už má 60 procent datového traffiku z 5G a právě FWA má na tom velký podíl. Du tento způsob připojení nabízí také jako záložní linku pro optiku, připojení pro menší firmy a kanceláře a připojení rodinných domů nebo kabelem nepřipojených venkovských oblastí.

Podle Ericssonu má být do roku 2028 v chodu přes tři sta milionů přípojek FWA, což by reprezentovalo asi sedmnáct procent všech přípojek k broadbandu. CCS Insight mluví o 14,5 milionu FWA v letošním roce.

Řada výzev

Operátory do budoucna bude kromě hledání modelů pro 5G čekat ještě několik dalších výzev. Jednou z největších bude spotřeba energie.

„Růst datových toků v mobilních sítích může v následujících letech zdvojnásobit odběr elektřiny," spočítal Peter Sachsenmeier z německé akademie věd a univerzity v Oxfordu. Operátoři v Česku i proto zkoušejí nasazovat solární napájení u vysílačů. Výrobci telekomunikačního vybavení jako Nokia, Ericsson nebo Huawei postupně nasazují polovodič nitrid galia, který je energeticky efektivnější.

A zřejmě bude nutné se více zaměřit na pokrývání budov. Podle GSMA je asi osmdesát procent traffiku v rámci 5G generováno indoor. Na letišti v Dubaji je například ve špičce 19,6 TB na kilometr čtvereční. Dodavatelé technologií očekávají, že se indoorové systémy stanou mainstreamem.

JAN SEDLÁK ■

JAK SE BRÁNIT DDOS ÚTOKŮM? PLATÍ TŘI ZÁKLADNÍ PRINCIPY

ČESKÉ FIRMY V POSLEDNÍCH MĚSÍCÍCH OPĚT POZNÁVAJÍ, ŽE ÚTOKY TYPU DDOS JE DOVEDOU PĚKNĚ POTRÁPIT. JAKÁ BYLA ANATOMIE NEDÁVNÝCH ÚTOKŮ A CO S NIMI LZE DĚLAT?

Obecně smyslem (D)DoS [(Distributed) Denial of Service] útoku není ani proniknout do některého systému s cílem jej ovládnout, ani odcizit data, ale jen znemožnit běžnému uživateli cílový systém používat. Zpravidla si pod takovým útokem představujeme zahlcení nějakého zdroje sítě nebo koncového systému. Volumetrický (D)DoS útok cílí zpravidla na kapacitu internetové konektivity oběti, dochází k zahlcení přístupových linek koncových systémů nebo na výkon některého slabšího softwarového směrovače na trase, poté dojde k jeho „utloukání“ velkým množstvím malých paketů. „Aplikační“ (D)DoS útok je takový, který zahlcuje až cílové systémy.

V reálu se takový útok zpravidla děje tak, že útočník nějakým nelegitimním způsobem získá přístup k cizím koncovým systémům, které pak z nějakého řídicího bodu (CoC) ovládá. To znamená, že určuje cíl, vektor a čas útoku. Ovládání zkompromitovaných cizích systémů je pak zpravidla automatizováno do té míry, že jedním příkazem lze zahájit útok mnoha (v praxi i statisícům až milionům) takových zkompromitovaných systémů. To mohou být IoT zařízení, třeba webkamery nebo termostaty, domácí routery, stanice koncových uživatelů, případně to mohou být i servery, fyzické i virtuální, v housingových centrech.

V případě útoků NoName057(16) z přelomu srpna a září to byly převážně servery v datových centrech, často právě VPS. Zajímavé je, že malware jménem DDosia si tam často provozovatelé těchto serverů spustili dobrovolně sami, v některých případech za to údajně dostali i zaplaceno.

Princip útoku pak byl následující: dokud cílový systém odpovídá, DDosia posílá HTTPS požadavky na náhodné řetězce. V okamžiku, kdy odpovídat přestane, posílá už jen SYN pakety (TCP paket s nastaveným SYN bitem otevírá TCP relaci). Z pohledu síťového provozu byly tyto útoky nevýznamné, avšak koncovým systémům dokázaly jak zcela vytížit jejich procesory, tak případně zaplnit tabulky TCP spojení.

Tak, a co s tím?

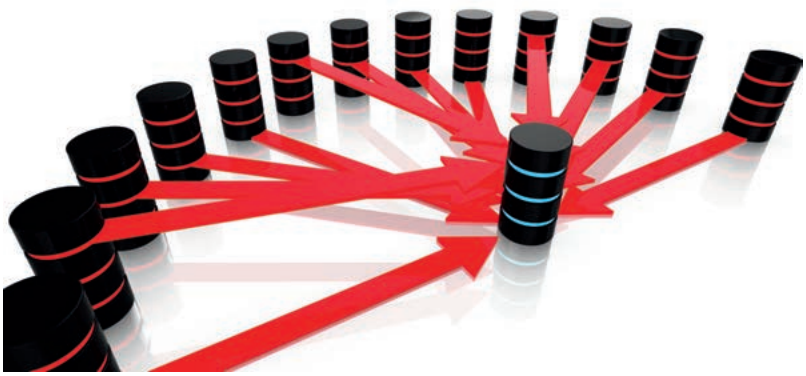
S HTTPS, resp. TLS je z hlediska boje proti DDoS útokům poněkud problém. Ten spočívá v tom, že provoz v HTTPS relaci je zašifrovaný a odhalit se sto-procentní spolehlivostí, zda je, či není legitimní, je, vidíme-li jen tuto relaci, na hranici nemožného. Nicméně ani útočníci nejsou dokonalí, nemají k dispozici neomezené zdroje a jsou také zranitelní.

Prehistorickým způsobem, jak bojovat s DDoS útoky, je tzv. remotely-triggered blackholing (RTBH). Spočívá v tom, že cílový autonomní systém takového útoku oznámí protokolem BGP adresní rozsah cíle útoku svému upstream operátorovi, případně též vybraným peeringovým partnerům, s nějakou specifickou BGP komunitou, která zajistí, že provoz pro cílový rozsah nebo pro jednotlivou cílovou adresu se zahodí už v síti, od které oběť nakupuje IP konektivitu. Má to samozřejmě celou řadu nevýhod, z nichž zásadní je, že cílová síť sice ochrání svoji kapacitu pro další uživatele, ale v zajištění nedostupnosti cíle útoku útočníkovi naopak pomůže. To nechcete.

Lepší a modernější způsoby samozřejmě existují. Můžete si ochranu proti DDoS útokům koupit od některého cloudového operátora, jako je například Cloudflare nebo Akamai, vlastní službu tohoto typu ohlásil před nedávnem i Wedos. Existují dva základní principy fungování takové cloudové ochrany, varianta anycast reverzní HTTPS proxy vám ochrání HTTPS, ale jakékoli jiné řešení než využívat takové služby trvale naráží na zásadní provozní těžkosti (a trvalý provoz často taky).

Druhou možností je směřování veškerého provozu pro postiženou cílovou síť (s minimální granularitou/24) ke cloudovému operátorovi. To zase vyžaduje výrazné zásahy do vaší směrovací politiky a jejího popisu v databázi RIR (v našem pří-

> **Útočník nelegitimním způsobem získá přístup k cizím koncovým systémům, které pak z nějakého řídicího bodu (CoC) ovládá.**



Vždycky lze přidat další úroveň zabezpečení, nicméně nekonečně velká míra zabezpečení také stojí nekonečně mnoho peněz.

padě RIPE NCC). Cloudový poskytovatel vám pak vyčištěný provoz posílá zpravidla nějakým GRE tunelem, ale existují i jiné možnosti. Nevýhody jsou také zřejmé, paket k vaší službě cestuje mnohem delší trasou a přes více systémů, což způsobí nějaké zpoždění, které uživatel může vnímat negativně. A samozřejmě tuto druhou možnost lze použít jen tehdy, máte-li a označujete-li sami své vlastní rozsahy IP adres do internetu.

Obrana proti DDoS útokům poskytovaná ISP/NSP, tedy dodavatelem vaší internetové konektivity, je další možností. Výhodou zde je, že operátor je vám síťově nejblíž, dokáže snadno rozlišit vyčištěný provoz od nevyčištěného a vám v zásadě stačí jen požádat svého operátora o aktivaci a podle dohodnuté úrovně služeb pak můžete nebo také nemusíte dostat přihlašovací údaje k webovému portálu, kde si potom do svého provozu a jeho případného čištění můžete sami podle potřeby zasahovat. Zde je hlavní výhodou zapouzdřenost a téměř poměrně malé úsilí ze strany chráněné sítě při implementaci.

Nejčastějším a asi také nejlépe propracovaným komerčním řešením pro ISP je systém, který se nejprve jmenoval Arbor Peakflow SP. Posléze společnost Arbor Networks odkoupila firmu NetScout, došlo tam také k produktovým změnám a současný de facto industry standard v oblasti anti-DDoS řešení pro síťové operátory se jmenuje Sightline. Sestává z několika hlavních prvků, jimiž je uživatelský portál, flow kolektor/analyzátor a „pračka“, oficiálně tedy Threat Mitigation System (TMS). Tyto prvky pak komunikují pomocí různých síťových protokolů s páteřními síťovými prvky dotyčného ISP, v současnosti je využíván zejména BGP FlowSpec.

Pračka neboli TMS pak má řadu chytrých funkcí včetně toho, že zcela převezme některé druhy komunikace za chráněný cílový systém a teprve po příslušném prověření, že kupříkladu TCP handshake je korektně navázán nebo že DNS klient je schopný svůj dotaz zopakovat, pak příslušný datový provoz na onen chráněný cílový systém propustí. Mezi další funkce pak patří například omezení počtu TCP relací per IP adresa vůči chráněnému cílovému systému, filtrování podle výskytu řetězců v payloadu paketů (vzpomínám si na útok, který měl vypadat jako DNS, ale nebylo to DNS, kde se právě tohle ukázalo jako nejefektivnější metoda), filtrování na bázi geolokace, vnějších nešifrovaných markerů při navazování HTTPS/TLS relací atd.

Nejdůležitějším přínosem takové služby ale je, že nejste slepí. Vidíte velmi detailní statistiky útoku, vidíte podle potřeby i do jednotlivých paketů, někdy v nich najdete i něco zajímavého. Můžete nacházet souvislosti. Útočník si často testuje, zda je cíl pod jeho útokem dostupný, a zvolené metody jsou občas zajímavé.

Rozdíly pak jsou v míře toho, co jednotliví operátoři nechají své uživatele s takovými systémy dělat. K tomu je pochopitelně potřebné získat i nějaké to know-how. V Quantcomu jsme zvolili variantu detailního zaškolení IT pracovníků a možnost, aby si sami mohli řídit a ladit jak probíhající čištění provozu, tak i případně zakládat čištění nová, pokud je intenzita útoku pro spuštění automatizovaných mitigačních procedur kupříkladu příliš nízká.

V případě DDosie bylo překvapivých a nezvyklých několik věcí. Významnými zdroji provozu byly sítě Linode (AS63949), M247 (AS9009), něco málo přicházelo kupříkladu i z Microsoftu a Amazonu čili typicky od poskytovatelů VPS, které často tvoří exit nody různých anonymních VPN. Naopak obvyklé zdroje DDoS útoků z Ruské federace a dalších zemí zejména jihovýchodní Evropy byly tentokrát zcela nezajímavé.

Lze dělat něco navíc?

Jistě. Dobře dimenzovaná přípojka do internetu zajistí, že vás nezahltí dva nebo tři gigabity provozu – a takových útoků je zdaleka nejvíc. Slušný a příslušně dimenzovaný hardwarový firewall a/nebo reverzní proxy před serverem, na kterém běží vaše kritická aplikace, odchytí malé SYN útoky. Nemít oba autoritativní name servery v tomtéž racku, ideálně ani v téže serverovně, ale nastudovat si BCP 16, resp. RFC 2182. Naučit se rozkládat zátěž. A hlavně si uvědomit, že každý řetěz unese jenom to, co unese jeho nejslabší článek.

Ideální tedy bude nějaká rozumná a chráněným hodnotám přiměřená kombinace výše zmíněných metod, tedy třeba anycast reverzní proxy pro kritickou webovou službu a následně ochrana celých adresních rozsahů u operátora.

Nicméně platí vždy základní tři principy:

- vždycky lze přidat další úroveň zabezpečení, nicméně nekonečně velká míra zabezpečení také stojí nekonečně mnoho peněz
- pokud někdo nabízí nějaké zázračné řešení, které automaticky a snadno vyřeší vaše bezpečnostní problémy, je to s jistotou podvodník
- neměli byste to dělat útočníkům zbytečně jednodušší, ale naopak se snažit být co nejodolnějším cílem sami o sobě

Alternativní metody

S DDoS útoky je ale možné bojovat i jinak než konvenčními metodami. Někdy se podaří infiltrovat CoC centrum a ovládnout celý botnet nebo jeho významnou část. To už není obrana, ale protiútok, což může být pro někoho značně kontroverzní téma, v každém případě to vyžaduje stejné know-how pro průniky do cizích systémů, jako využívají black hats. To je ale mimo škálu běžných opatření a mimo možnosti většiny postižených provozovatelů internetových služeb.

ZBYNĚK POSPÍCHAL

Autor působí ve společnosti Quantcom (dříve Dial Telecom), kde se zabývá rozvojem páteřních sítí a návrhem a implementací nových síťových služeb.

■

DÁVNO UŽ NEJSME JEN APLIKACÍ PRO TURISTY

FOTO: KAREL CHOC

APLIKACI MAPY.CZ VEDE MARTIN JEŘÁBEK TÉMĚŘ UŽ ŠEST LET. BĚHEM TÉ DOBY Z MAPOVÉHO PORTÁLU SPADAJÍCÍHO POD SEZNAM VYROSTLA SLUŽBA, PO KTERÉ ČÍM DÁL VÍC SAHAJÍ I ZAHRANIČNÍ UŽIVATELÉ.

Kolik máte v telefonu navigačních aplikací?
Asi šest.

To není zrovna málo. Předpokládám, že je to kvůli sledování konkurence.
Ano, sleduji konkurenci. Zkouším, zda jsme na tom datově dobře, nebo špatně, ve kterých oblastech a podobně. Zajímá mě, jak se jednotlivé mapové podklady zobrazují a co v nich je, jestli tam třeba máme zanesené aktuální uzavírky. Je to prostě testování, kde se ještě můžeme zlepšit a poučit.

Kolik uživatelů nyní Mapy.cz mají?
Záleží na tom, jestli je sezóna, což je pro nás období od července do září, prostě přes prázdniny. Na mobilce (v mobilní aplikaci, pozn. red.) je v tom období tak přes milion lidí denně a na webové verzi kolem jednoho a půl milionu.

Mluvíte o mobilní i desktopové verzi. Kolik lidí má tedy v mobilu vaši aplikaci?
Pokud bychom se bavili o aktivních uživatelích, těch jsou asi čtyři miliony.

A jsou to jen Češi, nebo máte i zahraniční uživatele?
Nejsou to jenom Češi. Nás to ze začátku docela překvapovalo, teď už jsme si na to zvykli, že nás využívají i v jiných státech. Asi tak čtvrtina uživatelů naší aplikace není z České republiky, jsou to Poláci, Slováci, Němci. Občas nám chodí od zahraničních uživatelů pozitivní zprávy. Píší nám, že dřív jiným za podobnou aplikaci platili a my

ji nabízíme zdarma, a navíc v lepší kvalitě. Je to příjemné zjištění.

O co je mezi uživateli největší zájem?
Většinou o nějaké turistické cíle. Lidé nás pořád ještě používají primárně pro plánování dovolené nebo pro výlety, takže mají zájem o turistické informace o hradech, rozhlednách nebo turistické trasy. Patří sem i plánování výletů na kole. Obecně jde o věci, které plánujete, když chcete hezky strávit dovolenou s rodinou. Vlastně to začíná ještě před sezónou, protože lidé si dopředu ukládají trasy a připravují si plány na větší výlety.

Turistické cíle chápu, i když jsem si říkal, že už máte možná víc uživatelů, kteří vás využívají pro navigaci v autě.
Ještě to tak není, ale i tohle číslo roste poměrně dramaticky. Poměr ale lze těžko určit, protože já vlastně nevím, jestli ten člověk, který jede někam s naší navigací, jede na dovolenou, nebo se prostě jenom někam přibližuje.

V Mapách si uživatelé mohou překlikávat mezi různými vrstvami. Které jsou nejpopulárnější?
Vede samozřejmě defaultně nastavená vrstva, která se ukazuje při startu mobilní nebo webové verze. My jí

říkáme základní mapa. Hned za ní je turistická a pak letecká mapa, vlastně jsou to mapy, které lidé využívají pro přesnější plánování nebo dohledání nějakého místa či informace o tomto místě.

Jak si vede vrstva, kterou jste přidali nedávno? Myslím tím údaje z katastrálních map.
Zájem je velký. Dostali jsme spoustu nadšených reakcí na to, že se tam ta vrstva objevila. My jsme vlastně integraci s katastrem už částečně měli dřív. Když jste se podíval na nějaký bod zájmu, dalo se prokliknout do katastru a dostat se na informace o vlastníkovi nebo o dalších vztazích, který katastr schraňuje. Ale s novou katastrální vrstvou jsme do map přidali funkci, že se člověk může na informace podívat podle parcelního čísla, může si prokliknout danou parcelu a nemusí spoléhat na to, že se musí přesně trefit do nějakého domečku. Myslím, že jsme tím uspokojili jak běžné zvídavé uživatele, tak i profesionálnější vrstvu uživatelů, kteří tato data používají pro svoji práci.

> **Plánů máme samozřejmě spoustu, otázka je, co z toho vybrat, protože ty věci jsou všechny krásné, všechny bychom je chtěli.**

Našel jsem zmínku, že jste před létem do map přidali třeba i varování před místy, kde se stává hodně nehod. Jaké jsou další plány na rozšíření?
Plánů máme samozřejmě spoustu, otázka je, co z toho vybrat, protože ty věci jsou všechny krásné, všechny bychom je chtěli. Ale jsme omezeni počtem lidí, kteří na Mapách pracují.

Věci, ke kterým se nyní blížíme, zasahují do hromadné dopravy a také do uživatelských dat, jež nám lidé posílají. Chceme jim to zpříjemnit a zjednodušit, aby se to, co nám pošlou, projevilo v Mapách co nejrychleji. Určitě jste si také všiml, že v poslední době zkvalitňujeme naše podklady. Máme třeba nové ortofotomapy (letecké snímkování, pozn. red.) evropských zemí. Vlastně je to tak, že se pořád díváme po světě a hledáme, kde bychom mohli získat kvalitní data, která by bylo možné na Mapách použít.

Vyladili jsme i nový výškový model, ten starý byl trošku děravý v polárních oblastech. Teď už je to v pořádku. U výškového modelu máme nyní v Evropě desetimetrové rozlišení, někde ale budeme mít až metrové. Takže pokud jste fanda do hor, uvidíte tam každou skulinku na vrstevnici. Myslím, že to ocení minimálně lidé, kteří do hor chodí.

Zmínil jste práci s daty od uživatelů. Co od nich kromě fotografií nebo slovního hodnocení můžete získat?
Fotografie samozřejmě máme rádi, obohacují mapu a je hezké, když někam jdete a můžete se dopředu podívat, zda to tam bude za něco stát. Hodnocení je také fajn, protože vám pomůže vybírat, kam si třeba zajít. Ale jsou i další věci, které od uživatelů můžeme dostat. Třeba z dat z navigace extrahujeme informace o provozu, čímž vylepšujeme zpětně navigaci i pro ostatní uživatele. Sbíráme i další strukturovaná data, když někde něco chybí nebo není úplně přesné, uživatelé nám to pomohou doplnit. Týká se to třeba otevírací doby nebo nějakého chybějícího objektu či podniku.

Funguje tento sběr dat i mimo Českou republiku?
Ano a jsme za to rádi, možná dokonce víc než za podobné údaje z České republiky. Pomáhá nám to udržovat mapy aktuální. Třeba v České republice bereme data o firmách ze služby Firmy.cz, která také spadá pod Seznam. V případě zahraničí ale musíme spoléhat na Open Street Map (OSM), od které bereme zahraniční mapové podklady, a tam záleží na tom, jak je komunita v dané oblasti aktivní.

Už jste mluvil o tom, že máte nové mapové podklady, ať už letecké po Evropě, nebo panoramatické snímky v České republice. Zároveň jste ale v srpnu na svém blogu uvedli, že dál zpracováváte data, která jste nasbírali letos. Jak jste s tím daleko?
V případě panoramatických snímků je budeme uvolňovat postupně, jak se nám je podaří zpracovat. Týká se to záběrů zhruba ze třetiny republiky, plus k tomu jde o část Prahy, kterou se nepodařilo nasnímkovat v minulém roce. To vše půjde ven na přelomu roku.

U ortofoto map je to složitější, protože podklady kupujeme od našeho dodavatele a funguje to na pravidelné bázi, kdy se mění tak třetina republiky jednou za rok. Zároveň nyní řešíme, jak využít data od ČUZK (Český úřad zeměměřický a katastrální), který uvolnil i svoje ortofoto podklady. Zkoušíme je nějak zpracovat a začlenit do našich podkladů. Protože ale mají jinou barevnost než naše současné, musíme zapracovat na vyladění, aby to nebylo jako pěst na oko.

FOTO: MAPY.CZ

Na začátku rozhovoru jste řekl, že máte v telefonu hned několik aplikací. Je něco, o čem víte, co třeba Google má lepší a je potřeba to u vás dohnat?
Naším cílem je, aby naše aplikace nebyla vnímaná jen jako aplikace pro naplánování dovolené. Rádi bychom, aby nás používali lidé celý den, což hodně souvisí s aktuálností dat, která uživatelům poskytujeme. A právě v tom se určitě ještě můžeme hodně zlepšovat. Ostatně na tom posledních několik let intenzivně pracujeme. Souvisí to i s aktivitou našich uživatelů, o které jsem už mluvil.

Jak hodně náročné na data, myslím tím na objem, vůbec Mapy.cz jsou?
Samotné mapové podklady až tak veliké nejsou. Myslím, že by vám na ně stačil běžný pevný disk. Větší jsou mapové dlaždice, na mobilech už pracujeme s vektory, ale na webu pořád používáme předrendrované mapy a tam to nějaké desítky terabajtů hodí. Náročnější na ukládání jsou pochopitelně i uživatelské fotografie. Úplně nejvíc ale zabírá místo Panorama a LiDAR data. My jsme navíc nyní vypustili Panoramu v časové ose, lidé si mohou prohlížet jednoduše data i do minulosti, a tam už to, pokud to dobře sečtu, dává dohromady tak 1,5 petabajtu.

Naším cílem je, aby Mapy.cz nebyly vnímané jen jako aplikace pro naplánování dovolené. Rádi bychom, aby nás používali lidé celý den, což hodně souvisí s aktuálností dat.

Vy jste vedl kromě Map i projekt Windy Maps, který byl ale loni zastavený. Berete od Windy dál nějaká data?
Je to tak, že my dodáváme Windy podklady tam, kde potřebuje, a Windy nám dodává data o počasí. Používáme je na Mapách nejen staticky, ale i pro plánování. Když si naplánujete třeba nějakou turistickou trasu, tak vám ukážeme, jak se na ní bude měnit během času počasí. Rádi bychom od Windy získávali ještě data z webových kamer, ale naráží to na to, o čem jsem mluvil – na naše kapacity.

Máte pod sebou i seznamácké jízdní řády, s nimi je propojenost do Map jaká?
Jízdní řády jsou v současné době víceméně oddělené, používají sice stejné mapové podklady a knihovny pro mobilní řády, je to ale samostatná aplikace. Nicméně můžu prozradit, že to nemusí být konečný stav.

Takže je v plánu třeba to, že by přes Mapy bylo možné koupit jízdenku?
Je to jedna z možností, víc to ale zatím komentovat nemůžu.

Na některé novinky jsme už narazili, nicméně se k tomu ještě jednou vrátím. Jaká je budoucnost Map? Plánujete třeba víc jít do 3D modelů, jak to chystá třeba Google?
To ani ne. Spíš se chceme zaměřit na to, aby všechno, na co jsou zvyklí čeští uživatelé, fungovalo stejně i v zahraničí. V některých věcech je to složité, ale i v zahraničí si chceme sahat do veřejných rejstříků, které jsou otevřené, a získávat z nich potřebná data. Snažíme se, aby cokoli, co děláme, nebylo jen pro Česko, ale pro celý svět. A osobně vidím nové příležitosti u jazykových modelů a porozumění dotazu, abychom uživateli ukazovali na jeho dotazy relevantní data. Tam ale ještě uvidíme, kam to dospěje.

JAN VACA ■

internet info

Dáváme Internetu obsah. Unikátní obsah.

4 miliony
reálných uživatelů za měsíc

23 milionů
zhlédnutých stránek za měsíc

Na trhu **působíme už od roku 1998** a jsme ze sta procent vlastněni českým managementem.

•

Naše **odborné servery** jsou tradičně považované za důvěryhodný zdroj **kvalitního a inspirativního obsahu** se schopností ovlivnit klíčové skupiny čtenářů a osobností v oblasti IT, financí či e-commerce.

•

Pravidelně připravujeme **vlastní unikátní obsah**, objevujeme nové informace a souvislosti, představujeme originální osobnosti, plánujeme efektivní komunikační a marketingové kampaně.

Podnikatel.cz měšec:cz euro.cz FINANCE.cz autobible.euro.cz

LUPA.cz ROOT.CZ_ PCWorld cnews.cz CFOworld SecurityWorld COMPUTERWORLD

CIO ChannelWorld Vitalia.cz zdraví.euro.cz STAHUJ.CZ SLUNEČNICE.cz Stáhnu.cz

MUJ SOUBOR EDNA VIDEAČESKY HRY pro DIVKY.cz Raketka.cz Rodičov

www.iinfo.cz

YOU DESERVE THE BEST SECURITY

Only the best security can protect you from today's complex cyber threats. Large scale, multi-vector attacks now threaten the fabric of organizations around the globe.

Check Point fully protects you against these Gen V attacks. Our transformative product innovations protect better than all other options.

In a world where threats are ever growing, you deserve the best security. Check Point.

Quantum
Deep Learning & AI Driven Network Security

CloudGuard
Fully Automated Cloud Native Security from Code to Cloud

Harmony
Highest Level of Security for Remote Users

Horizon
Prevention-First Security Operations

CHECK POINT™

www.checkpoint.com