Kybernetická bezpečnost – hrozby dneška a budoucnosti

strana 30

To kouzelné slovíčko agregace

strana 40

Kontury oboru telekomunikací se mění

strana 45

Číslo 3 | 2020 ČASOPIS TELEKOMUNIKACE & ICT | WWW.TELMAG.CZ NEPRODEJNÉ

NEXT GENERATI@N

TELEKOMUNIKACE

Budoucnost digitální infrastruktury a služeb pohledem Petra Očka, náměstka MPO ČR pro digitalizaci a inovace

strana 10

rozhovor:

Prof. Dr. Ing. Miroslav Svítek

Chytrá Evropská – umění se rozmáchnout a ovládnout akordeon města

Evid. číslo MK ČR E 19024
Print: ISSN 2570-8570
On-line: ISSN 2570-8589

Chytrá Evropská – umění se rozmáchnout a ovládnout akordeon města

Otázky pro Prof. Dr. Ing. Miroslava Svítka

kladl Petr Beneš

Prof. Dr. Ing Miroslav Svítek vystudoval Fakultu elektrotechnickou ČVUT a během studia ještě absolvovat obor akordeon na Státní konzervatoři v Praze. Svoji profesní dráhu spojil s Fakultou dopravní ČVUT, kde byl v roce 2008 jmenován profesorem. V roce 2015 se stal historicky prvním prezidentem Českého klastru chytrých měst (Czech Smart City Cluster) a pracovně jsme se setkali při realizaci několika odborných konferencí zaměřených na problematiku Smart Cities.

V rámci společenského programu těchto akcí došlo i na akordeon, který mně vždy fascinoval počtem svých ovládacích prvků – kláves a knoflíků, takže jsem v údivu zapomínal, že bez rozmachu rukou interpreta by nevyšel jediný tón. Odborný rozmach zaměřený na komplexní inteligentní systémy a jejich aplikace v oblasti řízení dopravy a funkcí městských celků je důvodem, proč jsem se právě v doprovodu pana profesora Svítka nechal ochotně zlákat na procházku pestrým světem harmonizovaných inteligentních měst včetně rozvíjejícího se projektu Chytrá Evropská v Praze.

Řekněme, že jsme na akademické půdě. Existuje nějaká definice Chytrého města (Smart City)?

Existuje mnoho definic. Já nejčastěji používám, že koncept chytrých měst se snaží vhodně využívat moderních technologií, aby docházelo k synergickým efektům mezi různými odvětvími (doprava, energetika, logistika, bezpečnost, životní prostředí, správa budov, atd.) a k lepšímu managementu měst na základě věrohodných dat, informací a znalostí a to s ohledem na udržitelný rozvoj (Sustainability), odolnost

(Resilience) a také kvalitu života (QoL – Quality of Life) občanů územních celků.

A co slovo smart používané ve spojení s technickými „vymoženostmi" již minulého dvacátého století, namátkou mne napadají energetická síť (grid), doprava/logistika, pouliční osvětlení (lighting), nádraží, letiště … Co tento přívlastek „chytrý" v takovém případě znamená?

Každá komponenta města je vybavena informačním a komunikačním systémem a proto může být zařazena do virtuálního digitálního dvojčete (Digital Twin), kde je typicky reprezentována tzv. softwarových agentem, který za ni vyjednává a prosazuje její zájmy. Může jít o infrastrukturální prvky, jako jsou osvětlení či dobíjecí stanice pro elektromobily, ale i větší celky jako jsou chytré budovy, železniční stanice, školy nebo i letiště. Samozřejmě, že softwaroví agenti mohou být i skupiny občanů nebo jiné humánní komponenty. Díky vzájemnému propojení těchto komponent může být v každém časovém intervalu vybráno vhodné řešení, které co nejlépe vyhovuje stanoveným kritériím, reprezentovaným parametry KPI (Key Performance Indicators). Tato kritéria jsou typicky volena s ohledem na energetickou náročnost, znečištění životního prostředí, atd.

Požadavky se samozřejmě liší město od města – jedno město je více průmyslově orientované, jiné se snaží být atraktivní pro turisty, další si zakládá na tom, že je univerzitním městem pro studenty. Obecně platí, že technologie lze koupit, ale chytrý systém ne – ten se musí léta budovat s ohledem na specifika konkrétního území, jeho historii, kulturní tradice, ale také konkrétní potřeby obyvatel či ekonomické možnosti daného regionu, města či obce.

Proč se používání přívlastku smart vyhnulo oblasti chytře automatizované průmyslové výroby, kde dominuje „generační" označení Industry 4.0.

Dle mého názoru jde pouze o zavedenou terminologii. Základem Industry 4.0 je lokální inteligence přiřazená k dílčím prvkům výrobního procesu na nejnižší úrovni. Materiál, polotovar, výrobek, ale i manipulační či výrobní prostředky nebo zákazníci jsou reprezentovány také svými softwarovými agenty, kteří jsou propojeni ve virtuálním digitálním prostředí a dokáží reagovat na proměnnou poptávku. Vzniká tak individualizovaná masová výroba, což bylo v minulosti z ekonomických důvodů považováno za nemožné. Díky vzájemnému propojení všech komponent a flexibilnímu řízení dotčených procesů se stává masová individualizovaná výroba ekonomicky reálná.

V oblasti chytrých měst využíváme podobné principy, jak co nejlépe uspokojit individualizované požadavky občanů ekonomicky rozumnými veřejnými službami, aby město stále vykazovalo udržitelný ekonomický, sociální, ale i environmentální rozvoj. Pouze nástroje nejsou tak striktní, jako v průmyslové výrobě. Hovoříme proto o sociálně-kyberneticko-fyzickém prostředí, kde zvláštní důraz je kladen na sociální vrstvu, kterou je nutno sofistikovaně modelovat pomocí různých typů průzkumů, či sledováním chování obyvatel.

Je důležité též zmínit, že v případě mimořádných situací musí být město odolné (resilientní). Chytrá řešení nabízejí nejen kvalitnější prevenci na základě lepšího porozumění dílčím procesům, ale i lepší optimalizaci zásahů v případě vzniku mimořádných událostí. V krizových situacích je nutné garantovat funkčnost vybrané kritické infrastruktury, zajistit její neustálé monitorování a řízení provozu na ní. To umožňuje nasazení moderních technologií pro simulace různých scénářů spolu s doporučením co nejlepších řešení vzniklé události.

Mluvíme-li o chytrých městech, popř. regionech, v poslední době se určitým synonymem slova „chytrý" stává známá zkratka 5G, upozorňující na novou generaci a také novou filosofii mobilních telekomunikačních sítí bytostně spojených s další zkratkou IoT – Internet věcí. Připomeňme 5G město Jeseník nebo 5G koridor Praha-Mnichov. Stane se tedy funkční infrastruktura 5G podmínkou pro označení smart?

Telekomunikační prostředí 5G se stává nedílnou součástí chytrých řešení, protože pro tvorbu virtuálního modelu územního celku je nutno sbírat velké množství on-line dat, ze kterých je možno následně extrahovat potřebné informace a znalosti. Nejde pouze o data z detektorů na infrastruktuře, ale o vyhodnocování například kosmických snímků, přenosy dat z kamerových systémů a to jak pevných, tak mobilních, např. umístěných na dronech. Jelikož se mnohdy jedná o kritické aplikace, je třeba garantovat vysoké nároky na bezpečnost, dostupnost a spolehlivost telekomunikačního prostředí, což sítě 5G dokáží.

Telekomunikační prostředí 5G se stává nedílnou součástí chytrých řešení

Například díky systému C-ITS (kooperativní inteligentní dopravní systém) bude možno sbírat velké množství dat ze vzájemné komunikace vozidlo–vozidlo, vozidlo–infrastruktura, ale také občan–infrastruktura. Právě tímto způsobem budou získávány individualizované požadavky,

obdobně jako je tomu u Industry 4.0. Postupem času budou nasazovány autonomní systémy, které se budou pomocí nástrojů umělé inteligence snažit co nejlépe reagovat na aktuální poptávku bez vlivu lidského činitele.

Díky službám 5G bude možno jednak uzpůsobovat nabídku podle aktuální proměnné poptávky, ale též formou různých benefitů poptávku i ovlivňovat. Bude tak nejen možno lépe využít stávající infrastrukturu, ale také minimalizovat omezené zdroje (elektrická energie, voda, zábor země, atd.).

V poslední době je slovo smart spojováno i s územně menšími celky. Vaše aktivity se v poslední době soustředí na projekt Chytrá Evropská v Praze. Můžete tuto ideu digitálního polygonu města Prahy pro testování projektů Smart City a autonomní dopravy stručně přiblížit?

Řada metropolí, které rozvíjí svůj „smart city" koncept, si v průběhu času vybudovala tzv. živé laboratoře, neboli části měst určené pro vývoj a testování nových technologií. Například v Berlíně vznikla chytrá čtvrť EUREF, která už teď splňuje kritéria, která si Německo vytyčilo splnit do roku 2050. Nejde pouze o zkoušení funkčnosti technologií, ale spíše o sledování dopadu chytrých řešení na chování obyvatel v daném území, zkoumání, jak různé skupiny obyvatel tato řešení přijímají, či jak je případně upravit, aby jejich dopad byl co nejvyšší.

Praha zatím takto koncipovanou živou laboratoř na svém území nemá. Na základě dílčího projektu Smart city v rámci Národního centra kybernetiky a umělé inteligence (NCK TAČR) byl vytvořen interdisciplinární tým z odborníků na jednotlivé oblasti, konkrétně dopravní systémy, energetické sítě, územní plánování, chytré budovy a environmentální modelování.

V rámci návštěvy zástupců Prahy v Berlíně vznikla myšlenka „Chytré Evropské" jako pražského „digitálního polygonu", který by začínal kruhovým objezdem v Dejvicích (Kulaťák) a končil na Letišti Václava Havla. Takto koncipovaný polygon zahrnuje všechny dopravní módy – leteckou dopravu díky Letišti Václava Havla, železniční dopravu díky Železniční stanici Veleslavín, veřejnou hromadnou dopravu s tramvajovými a autobusovými linkami a také významné stanice metra Dejvická, Bořislavka a Veleslavín.

Takto koncipovaný digitální polygon by nebyl pouze „chytrou ulicí", ale zahrnoval by i blízké okolí kolem Evropské, kde se plánuje celá řada developerských projektů.

Obr. 1
Slavnostní otevření Společné laboratoře ČVUT- UTEP zabývající se digitálními dvojčaty územních celků

Digitální dvojče Evropské bude v jednom virtuálním prostoru propojovat všechny dostupné informace a znalosti o stávajících a nově plánovaných budovách, různých druzích dopravních systémů, odpadovém hospodářství, atd. Výsledky bude možno také využít pro digitalizaci územního rozhodování.

Zajímavá může být i integrace chytrého letiště do multimodálního vyhledavače s možností například vyhledávání spojení přímo ke konkrétnímu letu s ohledem na stav dopravy, ale i předpokládaný čas odbavení na letišti.

U železniční stanice Veleslavín jde o využití nových technologií pro funkční a energetickou optimalizaci budovy, včetně vnitřního vybavení informačními a kamerovými systémy, aby byl tento dopravní terminál schopen vhodně reagovat na případné mimořádné situace. Návrh by měl zahrnovat i chytrá nástupiště vybavená signalizacemi přijíždějících vlaků, i systémy pro podporu hendikepovaných občanů. Díky tomu, že Veleslavín je důležitým přestupním uzlem, je nutné informační propojení mezi všemi dotčenými organizacemi, včetně již zmíněného Letiště Václava Havla.

Ale i v rámci tohoto projektu se rýsuje spolupráce chytrých regionů. Kromě ČVUT a UK v Praze se na projektu podílí i VŠB v Ostravě, tedy v Moravskoslezském kraji. Je možné již alespoň naznačit konkrétní přínosy?

Klíčovou myšlenkou Digitálního polygonu je implementace celé plejády dílčích projektů, které budou postupně naplňovat myšlenku testovacího prostředí, a které bude možno vzájemně integrovat. Dílčí řešení musí postupně pokrývat implementaci senzorické a komunikační sítě, tvorbu virtuálního modelu včetně dílčích simulačních nástrojů, či postupnou implementaci chytrých řešení, jako jsou kooperativní a autonomní dopravní systémy, BIM (Building Information Modeling), atd. Souběžně by měla být budována i chytrá infrastruktura s algoritmy pro pokročilý management celé Chytré Evropské.

Jsem přesvědčen, že koncept Chytré Evropské může být zajímavý pro všechny, nejenom technické, univerzity. Chytrost také znamená, že si uvědomíme, že společně toho dosáhneme více. Osobně bych rád přizval odborníky na humanitní vědy např. na sociologii, psychologii, atd., kteří k danému tématu mají rozhodně co říci. Měli bychom méně mezi sebou soupeřit a více se zaměřit na návrh společných projektů. Jsem přesvědčen, že koncept Chytré Evropské svoji unikátností a svými možnostmi nám v tomto záměru může výrazně pomoci.

A co mezinárodní spolupráce v oblasti smart projektů, když vzpomeneme „slogan" Smart Evropská – Gateway to the Europe?

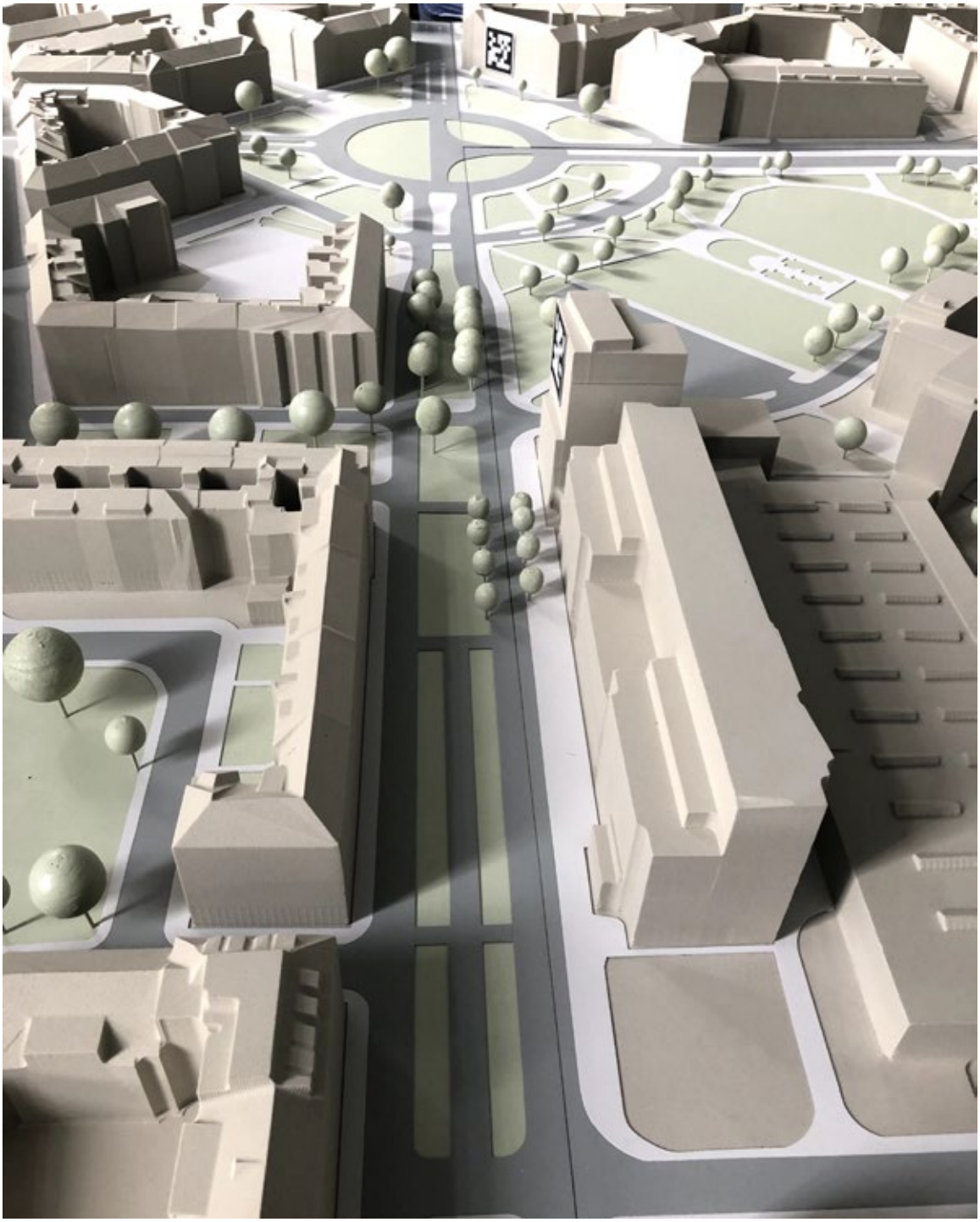
Při dílčích jednání se státní správou vznikla myšlenka, zda by se koncept Chytré Evropské nemohl stát součástí českého předsednictví EU v roce 2022 se sloganem „Smart Evropská – Gateway to Europe". Šlo by o výkladní skříň českých technologií, které by kromě zajištění komfortu a bezpečnosti jednotlivých vládních delegací ukázaly naši republiku jako silného partnera v oblasti chytrých měst. Zároveň by koncept Chytré Evropské pomohl i Pražanům, protože se zahuštěním zástavby kolem Evropské budou přibývat dopravní komplikace, které bude třeba tak jako tak řešit.

Není vyloučeno, že i nadnárodní firmy by mohly na Evropské pilotně implementovat svá řešení, což by rozšířilo mezinárodní spolupráci našich firem a akademických institucí. Vzhledem k mému současnému působení v Berlíně se snažím propojit nejen ČVUT s TU Berlin, ale také obě partnerská města Berlín a Prahu. Koncept Chytré Evropské je konkrétní příležitostí a odbornou platformou pro tuto spolupráci.

Na závěr otázka, dnes zatím více filosofická: Produktem technologického vývoje je dovršená a dále se prohlubující konvergence telekomunikačních a informačních technologií dnes přirozeně spojovaná rovněž s konkrétními aplikacemi umělé inteligence. Můžeme se v souvislosti s vývojem k chytrým komunitám – ulicím, městům i regionům – těšit i na výrazný inovativní aspekt konvergenčního vývoje, který k technologiím elektronických komunikací a digitálního zpracování dat připojí jako přirozenou třetí dimenzi oblast sociální komunikace a služeb dále optimalizující fungování naší 3D společnosti?

Součástí digitálního virtuálního světa nejsou pouze softwaroví agenti reprezentující technické prvky, ale také humánní komponenty. Již dnes přecházíme plynule, aniž bychom si to uvědomovali, mezi virtuálním a reálným světem. Ukázkou mohou být navigační systémy, které nás vedou do míst, kam bychom se jinak nepodívali. Takto koncipované aplikace mohou stále výrazněji ovlivňovat způsob našeho chování, ale i naši poptávku po službách všeho druhu. Zajímavým fenoménem jsou určitě sociální sítě, které vytvářejí různé komunity

Klíčovou myšlenkou Digitálního polygonu je implementace celé plejády dílčích projektů, které budou postupně naplňovat myšlenku testovacího prostředí, a které bude možno vzájemně integrovat.



Obr. 2
Ukázka 3D modelu Vítězného náměstí. Nad 3D modelem je možno zobrazovat informace a znalosti pomocí technologií rozšířené reality.

a umožňují jim de facto život ve virtuálním prostředí bez ohledu na jejich fyzickou vzdálenost.

Nabízí se nekonečně mnoho možností dalšího rozvoje, ale základním principem by mělo zůstat, že pokud nechci tyto výdobytky moderní techniky používat, měl bych mít možnost žít bez nich. Asi budu déle čekat na dopravu, hledat, kde se dá koupit jízdenka. Možná budu více bloudit městem, ale stále jsem schopen žít plnohodnotný život. Je třeba brát zvláštní ohled na různé kategorie občanů – školáci, staří, či hendikepovaní lidé. Velkou výzvou je kybernetická bezpečnost nebo tvorba netradičních obchodních modelů pro nová řešení. Všechny tyto detaily je třeba citlivě zvažovat již při návrhu systému chytrého města a případně je testovat v rámci konceptu Digitálního polygonu, kterým se chce Chytrá Evropská stát.

Vzhledem k rychlému vývoji technologií se musí začít na středních i vysokých školách vychovávat nová generace odborníků, kteří se budou tímto interdisciplinárním a odborně zajímavým oborem dlouhodobě zabývat. Po mnoha letech příprav získala Fakulta dopravní ČVUT (www.fd.cvut.cz) akreditaci unikátního magisterského studijního programu Smart Cities, který je vyučován pouze v anglickém jazyce a je realizován formou tzv. double-degree ve spolupráci s americkou University of Texas at El Paso (UTEP). Absolventi získají

jak český, tak i americký titul, čímž se jim otevřou možnosti mezinárodního uplatnění.

Jsem přesvědčen, že oblast chytrých měst a regionů je nedílnou součástí probíhající čtvrté průmyslové revoluce. Jde skutečně o revoluci a ne pouze o evoluci, protože dopad propojených systémů Internetem věcí, služeb a lidí bude mít dopad na všechny známé procesy. Hovoří se proto o Společnosti 4.0 nebo též o Myšlení 4.0.

Je možné uvést něco, co by jako produkt průniku evropské a americké, popř. latinsko-americké kultury, mohlo obohatit „svět" Smart Cities?

The University of Texas at El Paso (UTEP) je prestižní univerzitou zařazenou do kategorie R1 výzkumných univerzit USA. V rámci spolupráce se již rozeběhly první trans-atlantické výzkumné aktivity zahrnující například chytrý univerzitní areál (Smart Campus) nebo chytrou hranici (Smart Border). Na těchto příkladech bude možno testovat originální přístupy, jak pomocí nových technologií zajistit vyšší odolnost konkrétních urbánních prvků.

Když porovnáme evropský a americký přístup, myslím si, že je na tom Evropa lépe v nových myšlenkách, výzkumných projektech nebo pilotních ověřeních. Velké slabiny vidím v následném využívání vyvinutých řešení v praxi. Je to zřejmě dané způsobem našeho uvažování, ale i skeptickým pohledem na inovativní přístupy vyžadující změnu naučených postupů.

V USA naopak vidím, jak pozitivně přistupují k inovacím. Neinvestují tolik veřejných peněz do vývoje, ale když vidí, že se jim nějaká technologie vyplatí, začnou ji ihned používat v praxi, protože je to zkrátka výhodné.

Je známo, že v Latinské Americe je nedostatečná infrastruktura, která výrazně ztěžuje životní podmínky obyvatel. Na druhou stranu demografická křivka vykazuje velké procento mladých lidí, kteří se rychle naučili používat služeb chytrých telefonů. Zájem o tyto služby je velkým potenciálem dalšího rozvoje. Dokonce si troufnu říci, že v určité chvíli může penetrace chytrých řešení v Latinské Americe předčít pokročilé evropské země nebo i USA.

Mohu uvést i osobní zkušenost. Již od roku 2006 působím v mé oblíbené Kolumbii, konkrétně v univerzitním městě Bucaramanga. V minulosti jsem pro primátora, pro zaměstnance magistrátu, pro místní univerzity či členy obchodních komor připravil celou řadu odborných přednášek. Jedné z nich se v roce 2013 zúčastnilo přes 400 posluchačů.

Díky těmto aktivitám dvě kolumbijské studentky absolvovaly obor Inteligentní dopravní systémy na Fakultě dopravní, ČVUT a dnes se podílejí na rozvoji tohoto oboru v celé Kolumbii. Jsem rád, že v Bucaramanga se v současné době realizuje několik pilotních projektů v oblasti Smart city. Osobně mě těší, že se těchto aktivit mohou účastnit i české firmy. Je to výsledek mnohaleté soustavné odborné činnosti, ale i mého osobního zaujetí pro tuto krásnou zemi.

Jsem přesvědčen, že oblast chytrých měst a regionů je nedílnou součástí probíhající čtvrté průmyslové revoluce.

Prof. Dr. Ing. Miroslav Svítek, dr.h.c., FEng., EUR ING, se narodil 5. července 1969 v Rakovníku. Během studia na Fakultě elektrotechnické ČVUT absolvoval Státní konzervatoř v Praze, obor akordeon.

Svoji dosavadní profesní dráhu spojil s Fakultou dopravní ČVUT, kde byl roku 2002 jmenován docentem a následně v roce 2008 profesorem. V období 2010 až 2018 zastával funkci děkana. Od roku 2018 je hostujícím profesorem v oboru Smart Cities na University of Texas at El Paso (UTEP) v USA.

Během let 2006 až 2018 byl prezidentem Sdružení pro dopravní telematiku. V roce 2015 se stal historicky prvním prezidentem Czech Smart City Cluster. Je členem Inženýrské akademie ČR, vedoucím pracovní skupiny Čistá mobilita České podnikatelské rady pro udržitelný rozvoj a členem Komise Rady hl. m. Prahy pro rozvoj Smart Cities. V roce 2019 mu byla udělena cena Osobnost Smart City.

Při příležitosti oslav 20 let Fakulty dopravní ČVUT nahrál sólové album Acordeón Encantador. V rámci oslav 25 let Fakulty dopravní založil spolu s prof. Ondřejem Přibylem (violoncello) Duo Profesores, které nahrálo skladby argentinského autora Astora Piazzoly.

doc. Ing. Václav Jirovský, CSc
Fakulta dopravní ČVUT

Kybernetická bezpečnost – hrozby dneška a budoucnosti

Kybernetická bezpečnost se stala všeobecně známým a diskutovaným pojmem. Znalosti pochytané na internetu umožňují diskuze i těm, kteří mají ke kybernetické bezpečnosti velmi daleko. Dostatečně záhadné útoky jsou vhodným tématem pro novináře, kdy sérii několika článků většinou ukončí konstatováním, že případ byl odložen. Čtenáře, který očekává, že v následujících řádcích se dočte něco o antivirových programech, nebo způsobech jak zaútočit na server souseda, musím zklamat – kybernetická bezpečnost je o něčem úplně jiném.

Když se budeme snažit najít některé informace o historii kybernetické bezpečnosti, vždy nalezneme odkazy na počítačové viry a červy jako na technologickou zbraň a jejich tvůrce. Významné osobnosti slučující počítačovou excelenci se sociálním inženýrstvím, jako Kevin Mitnik[1] nebo Susan Headley[2] jsou téměř neznámí. Přitom sociální inženýrství, resp. projev člověka při jeho interakci s technologiemi, patří mezi největší kybernetické hrozby budoucnosti. Zkusme se tedy podívat na kybernetickou bezpečnost z tohoto velmi opomíjeného hlediska. Pro názornost si rozdělme kybernetickou bezpečnost do dvou oblastí – kyber-technologickou bezpečnost a kyber-sociální bezpečnost.

Kyber-technologická bezpečnost sleduje technologická zabezpečení prvků informačních technologií – počítačů, součástí infrastruktury, serverů nebo komunikačních kanálů. Mezi základní útoky na IT infrastrukturu patří

- webové útoky související s činností webových serverů nebo serverů založených na webových službách, zejména pak
  - injekce dat, což je útok, při kterém budou některá data vložena do webové aplikace s cílem manipulovat s aplikací a získat požadované informace. Příkladem může být SQL Injection, Code Injection, XML Injection apod.;
  - podvržení DNS[3] (DNS Spoofing) vkládá do mezipaměti DNS jiná data, což způsobí, že jmenný server DNS vrátí nesprávnou IP adresu a odkloní přenos do počítače útočníka nebo jiného počítače;
  - únos relace je útok na relaci uživatele přes chráněnou síť, např. pomocí odposlechnutých souborů cookie;
  - phishing patří k nejznámějším a nejviditelnějším útokům, kterým se útočník pokouší ukrást citlivé informace (přihlašovací údaje uživatele, číslo kreditní karty apod.)

1
Kevin Mitnick, americký bezpečnostní konsultant a hacker, který se proslavil svými útoky založenými na personální manipulaci cíle. Proslavila ho kniha „Umění klamu", kterou napsal po propuštění z vězení, kde strávil pět let.
2
Susan Headley, americká hackerka, aktivní v 80-tých letech, uznávaná pro svoje zkušenosti se sociálním inženýrstvím. Její specialitou byly průniky do vojenských systémů, kde uživatelská jména a hesla získávala od vybraných příslušníků armády jenž svedla k sexuálním hrátkám. Po nějakou dobu spolupracovala i Kevinem Mitnikem.
3
DNS – Domain Name Server je součástí internetové infrastruktury, která zajišťuje překlad jmenných názvů míst v síti na IP adresy, např. www.google.com přeloží na 172.217.23.228. Další komunikace potom probíhá odkazy na IP adresy.

tak, že se maskuje jako důvěryhodná entita v elektronické komunikaci, např. správce sítě;
- brutální síla používá metodu pokusu a omylu, a tak zkouší proniknout do systému uhodnutím přihlašovacích údajů nebo šifrovacího klíče;
- DoS (Denial of Service) neboli potlačení služby, čehož útočník dosáhne generováním velkého datového toku a přetížením serveru nebo jeho komunikačních kanálů;
- Man in the Middle je útok, který útočníkovi umožňuje zachytit spojení mezi klientem a serverem vložení jím ovládaného počítače do této cesty.

- Systémové útoky mají za cíl ohrozit počítač nebo počítačovou síť
  - virus je škodlivý software, který se šíří v počítačových souborech bez vědomí uživatele. Virus se může šířit v síti tak, že se přichytí k některému např. spustitelnému souboru. Nemůže se replikovat sám;
  - červ je typ malwaru, jehož primární funkcí je replikace, a tak se sám rozšíří na neinfikované počítače. Funguje podobně jako počítačový virus. Červi jsou často součástí e-mailových příloh, které se zdají být od důvěryhodných odesílatelů;
  - Trojský kůň je typ malware, který běží na pozadí a může např. sledovat činnost uživatele nebo ovlivňovat běh počítače. Většinou se šíří jako virus nebo červ;
  - Backdoor (zadní vrátka) jsou oblíbeným nástrojem vývojářů nebo správců sítě. Jedná se o aplikaci, která obchází normální proces autentizace, takže k aplikaci nebo operačnímu systému lze přistupovat bez autentizace;
  - Bot (zkratka pro „robota“) je automatizovaný proces, který spolupracuje s jinými síťovými službami a realizuje některé služby pro útočníka (např. generuje data). Některé boty se spouští automaticky, zatímco jiné se spustí pouze tehdy, když dostanou konkrétní informaci na vstup.

Existuje celá řada dalších útoků, které kombinují tyto základní útoky nebo přicházejí s variantami počítačových služeb. Např. „Defacement“, což je případ, kdy webová stránka na serveru je nahrazena jiným obsahem, zpravidla propagujícím ideologii útočníka, ale útočník se musí nejdříve k serveru dostat, a tedy použít některou z výše uvedených metod nebo jejich kombinaci.

Technologická ochrana proti těmto kyber-technologický útokům je známa a široce rozšířena. Je pak na administrátorech, aby příslušné ochranné prvky nastavili, provoz sítě sledovali a případně měnili parametry ochrany podle současného stavu. Něco jiného je, když v souvislosti s technologickým útokem je použita i metoda sociálního inženýrství, např. phishing nebo pouze důvěryhodný mail obsahující škodlivý kód v příloze. Pak žádné technologické triky nepomohou.

Na konci roku 2019 vzbudily značnou mediální pozornost hned dva kybernetické útoky údajně směřované na benešovskou nemocnici a na společnost OKD. Byly podrobně prezentovány jako cílené útoky kryptovirem[4] a marně a dlouho se hledal viník. Podstatou útoku byl kryptovir, který se dostal do sítě prostřednictvím nezkušeného uživatele, který rozklikl lákavou přílohu či odkaz v e-mailu nebo stáhl a spustil zajímavý program nabízený zdarma. V roce 2017 byla podobným kryptovirem zasažena síť námořního giganta Maersk obsahující desítky tisíc počítačů a tisíce aplikací. Útok stál firmu milióny dolarů zisku, ale jeho následky se podařilo eliminovat během necelých čtrnácti dnů. Podobně OKD s jistě srovnatelným rozsahem sítě s nemocnicí vyřešilo návrat do téměř běžného provozu během několika dnů.

Na konci roku 2019 vzbudily značnou mediální pozornost hned dva kybernetické útoky údajně směřované na benešovskou nemocnici a na společnost OKD.

Pro odpověď na otázku proč odstraňování následků útoku na benešovskou nemocnici, jejíž síť je daleko menší, trvalo tak dlouho je nutno si uvědomit, že bezpečnost nelze brát jako jednorázovou dodávku zboží. Bezpečnost je dlouhodobý proces. Řešením je návrh odolné architektury sítě a správná, pravidelně udržovaná, konfigurace všech zařízení. Zatímco OKD a Maerks se zřejmě starají o bezpečnost svých systémů sami a mají zkušené administrátory, nemocnice „službu bezpečnosti“ evidentně nakupuje společně s dálkovou správou zařízení. A to tu nejlevnější, neboť tak přikazuje zákon! A následující nesmyslné policejní vyšetřování pak stojí peníze pouze daňové poplatníky, což nikoho nebolí. Přitom jenom naivní novinář si mohl myslet, že se viník najde. Podobných e-mailu se rozesílá tisíce i milióny a prostě někdo se chytne. Každopádně se nejedná o cílený útok na příslušný subjekt, ale o chybu v lidské obsluze, sportovní mluvou řečeno o „vlastní gól“.

Tím se dostáváme k daleko problematičtější a dosud nepokryté oblasti **kyber-sociální bezpečnosti** a ke kořenům problému – symbiózy člověka a technologie. To je místo, které bude lidstvo nejvíce ohrožovat v budoucnu a bude nutno se rozhodnout dříve, než bude pozdě. Pro vysvětlení musíme zajít hluboko do minulosti, do období největšího rozmachu průmyslové revoluce zažeh-

4 Kryptovir – zvláštní druh červa, který po proniknutí do systému zašifruje všechny soubory, které nalezne. Útočník pak vyžaduje finanční odměnu za to, že prozradí šifrovací klíč, nicméně odměna v bitcoinech se ztratí v prostoru internetu a klíč žádný. Někdy se tento typ červa nazývá ransomware.

Václav Jáchim, Odbor informatiky, Krajský úřad Kraje Vysočina

Úspěšné příklady využití chytrých technologií ve zdravotnickém systému Tchaj-wanu

Kraj Vysočina již od roku 2010 spolupracuje s tchajwanskými partnery v oblasti technologických inovací pro veřejné služby. Zaměřujeme se zejména na využití chytrých řešení ve zdravotnictví, technickém vzdělávání či energetických úspor. Naším cílem je jednak využít či testovat dané technologie v krajském prostředí, vedle toho se pak také inspirovat organizačními vazbami a procesy při realizaci obdobných projektů na krajské úrovni. Některá zajímavá zdravotnická řešení, která na Tchaj-wanu úspěšně fungují, vám představíme v tomto článku. Je třeba dodat, že toto není kompletní výčet všech eHealth projektů v tchajwanském zdravotnictví, jde o aktivity, které by mohly být přímou inspirací pro krajskou i národní úroveň zdravotnického systému.

Objednávkový on-line systém do nemocničních ambulancí

Objednávání k lékaři prostřednictvím internetu funguje pro tchajwanské pacienty od první dekády 21. století. Vzhledem k existenci pouze jedné zdravotní pojišťovny slouží jako unikátní identifikátor pacienta jeho číslo zdravotního pojištění. Občan má pak možnost využít jak objednání se ze svého PC či chytrého telefonu, tak například přímo v nemocnici prostřednictvím tzv. kiosku. Tento přístup byl pro Kraj Vysočina přímou inspirací a od roku 2012 právě ve spolupráci s tchajwanským Institutem pro informační průmysl provozujeme na Vysočině službu eAmbulance

(www.eambulance.cz). Ta propojuje všech 5 krajských nemocnic jedním objednávacím systémem a každý pacient má po registraci do systému pod svým rodným číslem možnost objednat se do ambulancí krajských nemocnic na den a čas, který mu nejlépe vyhovuje. Vzhledem k tomu, že v ambulancích lékaři vědí, kolik pacientů v danou chvíli přijde (samozřejmě kromě akutních případů), je tento automatický systém výhodný pro pacienta i nemocnici. Objednávání prostřednictvím kiosků nevyužíváme, ale pacienti se mohou přímo v nemocnici objednat například na další kontrolu na informačním centru dané nemocnice. O úspěšnosti této služby hovoří více než 90 tis. uživatelů v kraji a více než 250 tis. objednávek za 8 let provozu systému.

Centrální distribuční systém ochranných roušek v době koronavirové pandemie

Velmi zajímavým systémem v tchajwanském zdravotnictví je zejména v době celosvětové pandemie centrální systém poskytování ochranných pomůcek, zejména obličejových masek. Aby Tchaj-wan zajistil pro svých více než 23 milionů obyvatel dostatek ochranných masek a nedošlo přitom k problému s nedostupností těchto pomůcek či umělému navyšování cen a následnému obohacování se na pandemii, jsou masky dodávány centrálně z národní úrovně. Každý obyvatel má nárok na příslušný počet masek na týden. Platbě a vydání masek předchází ověření čísla zdravotního pojištění obyvatele tak, aby nedošlo k překročení daného týdenního limitu. Masky lze též po předchozí registraci do internetového systému či mobilní aplikaci přeobjednat k výdeji na konkrétní čas i místo, což celý systém zefektivňuje a navíc zabraňuje tvorbě dlouhých front.

Využití technologií pro otevřené poskytování informací pacientů Univerzitní nemocnice Taipei

Univerzitní nemocnice Taipei je soukromá zdravotnická nemocnice, jde o špičkové zdravotnické zařízení, které jsme měli možnost na Tchaj-wanu poznat. Tato nemocnice využívá v poskytování služeb pacientům i vnitřní organizaci svých procesů nejnovější trendy v medicíně, které nám mohou být inspirací, kam budou zdravotnické služby v budoucnu směřovat. Jmenujme alespoň některé konkrétně. Veškerá péče o pacienta je prováděna s maximálním důrazem na kvalitu, jednoduchost a maximální otevřenost. On-line objednávání i on-line konzultace s lékařem jsou samozřejmosti. Velmi zajímavá je služba pacientova dashboardu. Jde v podstatě o webovou aplikaci, ve které má každý pacient seřazeny a popsány jednotlivé úkony, kterými bude v rámci léčby procházet. Jde o jednotlivá vyšetření, medikaci, postup celé léčby. Pacient je tedy maximálně otevřeně informován a ví, jak a zejména proč jeho léčba postupuje. Nemocnice také používá pokročilé technologie umělé inteligence k predikci vývoje zdravotního stavu pacienta na určitý čas dopředu (např. 48 hodin), lékařský tým se tedy může připravit na možné varianty zdravotního stavu, které pravděpodobně nastanou a tím zrychlit reakce v případě nenadálých komplikací. Využití robotiky a technologií virtuální reality pomáhá lékařským týmům minimalizovat riziko chyby, centrální analýza dat případů pak slouží také pro další interní vzdělávání lékařských týmů, které spolupracují multioborově.

Řešení problematiky kyberbezpečnosti v tchajwanském zdravotnictví

Kybernetická bezpečnost zdravotnictví a jednotlivých nemocnic je jedním z klíčových témat dneška, což ukázaly případy některých českých nemocnic v roce 2020, které byly několik dnů či týdnů prakticky paralyzovány následkem kybernetických útoků. Na příkladu tchajwanského systému národní kyberbezpečnosti si můžeme demonstrovat, za jak důležitý a citlivý je zdravotnický systém na Tchaj-wanu považován. Zdravotnictví je na Tchaj-wanu označeno jako kritická infrastruktura a tedy pro něj platí nejpřísnější pravidla kybernetické bezpečnosti. Základem jsou 4 principy – konstantní monitoring, sdílení informací, včasná varování a odezva na problém. Vedle klasické národní struktury pro kyberbezpečnost, která v sobě tradičně zahrnuje Security Operation Center (SOC), ISAC: Information Sharing and Analysis Center a CERT: Computer Emergency Response Team, pak vedle tohoto systému na Tchaj-wanu existuje paralelní struktura H-SOC, H-ISAC a H-CERT, která dohlíží a reaguje na bezpečnost pouze nemocnic a zdravotnických zařízení. Všechny klíčové bezpečnostní záležitosti jsou samozřejmě konzultovány s národní autoritou, ale tyto specializované týmy zajišťují tchajwanským nemocnicím vyšší míru obrany a daleko rychlejší reakce na incidenty, než by bylo možné řešit z obecné úrovně. Systém jde dokonce tak daleko, že velké klíčové nemocnice mají vlastní kyberbezpečnostní centra, a pro ty ostatní jsou připravena SW řešení spravovaná specializovaných vývojovým pracovištěm. Na úplný závěr ještě dodejme, že v současné době diskutujeme problematiku s tchajwanskými odborníky a zajímáme se jak o využití procesních modelů v českém a „vysočinském" prostředí, tak i o otestování funkčnosti některých jejich SW nástrojů v krajských nemocnicích.

nuté na přelomu 17. a 18. století. Je to období, kdy dochází k postupné změně v zemědělství, výrobě, těžbě, dopravě a dalších hospodářských odvětvích. V přechodu od dominujícího zemědělství a ruční výroby v manufakturách ke strojní velkovýrobě za pomoci nových zdrojů energie, hrály významnou roli nové vědecké a technologické objevy. Došlo k dělbě práce a specializaci, kterou následovaly společenské, kulturní a politické změny. Došlo ke vzniku společenské vrstvy – dělnické třídy, k rozvoji materialismu, konzumní společnosti a ke změně urbanistických koncepcí vytvářejících průmyslová centra a dělnické čtvrti. Čas ukázal, že obavy o ztrátu práce byly zbytečné, zvýšily se pouze nároky na obsluhu strojů a těžká fyzická práce byla nahrazena požadavky na intelektuální schopnosti obsluhy. To byl příběh industriální revoluce, příběh s dobrým koncem.

Člověku to však bylo málo a v polovině minulého století začal velmi intenzívně pracovat na rozvíjení podpory intelektuálních schopností – do hry vstoupila IT revoluce s cílem nahradit lidské intelektuální aktivity strojovými výpočty. A to bez ohledu na to, že svět je indeterministický a nelze jej algoritmizovat. Lidské aktivity jsou postupně nahrazovány strojními výpočty, proces rozhodování, který byl vždy výlučným privilegiem člověka, je nahrazován různými učícími se programy, exportními systémy nebo poslední době stále vzpomínanou umělou inteligencí. Přitom umělá inteligence, tak jak je často citována novináři nebo v marketingových materiálech, není nic jiného než interaktivní učící se programy a do skutečných vlastností umělé inteligence, která bude zahrnovat i schopnost člověka rozhodovat se na základě zkušeností a intuice je ještě daleko. Uvědomme si, že jen kapacita lidského mozku neleží v oněch 20 miliardách neuronů, ale v množství různých spojů mezi nimi, kdy kombinace všech možných spojů mezi neurony v lidském mozku je číslo které obsahuje více než 30 nul. V porovnání se způsobem, jak ukládáme data ve stroji, kde jsou používány datové struktury, ukládá lidský mozek informace v asociativních strukturách. Tento proces převodu lidského myšlení a rozhodování do strojních procesů v dnešních technologiích vede k nakoupení neuvěřitelného množství dat, se kterými sami nevíme, co máme dělat, a vzniká problém zvaný Big-data.

Zobecníme-li výše uvedené závěry pak je zřejmé, že lidstvo směřuje k výraznému omezení vlastních tvůrčích schopností, omezení vlastního rozhodování a řízení věcí a to všechno předá „všemocné“ IT technologii.

IT technologie dnes prostupují každé lidské činění, a to už od předškolního věku. Agresivní marketing IT firem je schopen vnutit IT řešení i tam kde by postačovala jednoduchá organizační změna. Zákazník tak dostane jednoduchý program, který umí párů úkonů, zaplatí za něj neuvěřitelnou částku, do budoucna bude vázán na původního dodavatele programu a přitom bude muset přijmout dalšího zaměstnance, který se o tento program bude muset starat. Agresivní IT marketing má i své daleko hlubší dopady a to ve změně uvažování a myšlení člověka. Představte si, že vlastně máte dvě oblasti paměti. Paměť primární, která obsahuje všechno to, co víte sami z paměti – například zapamatované verše, malou násobilku, úryvky textu apod. Sekundární paměť pak je, že víme, kde danou informaci najdeme. Opět příklad, pokud budu hledat nějaký zákon, vím, že ho najdu ve Sbírce zákonů, kterou najdu v knihovně. IT technologie posunuly tento druh dělení paměti do velmi primitivní formy. Klesá objem vlastních znalostí, tedy primární paměti – toho sám si pamatuji, a objem sekundárních znalostí se zúžil prakticky na jedno slovo – „Google“. I s tím rizikem, že vyhledání nám dá tisíce odkazů, většinou špatných.

Zobecníme-li výše uvedené závěry, pak je zřejmé, že lidstvo směřuje k výraznému omezení vlastních tvůrčích schopností, omezení vlastního rozhodování a řízení věcí a to všechno předá „všemocné“ IT technologii. Je zřejmé, že tlak politiků na digitalizaci bez hranic jen hraje do rukou marketingu IT firem. S nešvarem poslední doby, kdy se dodávají nedostatečně testované aplikace a čeká se až na reakce uživatele, který při provozu zdarma otestuje program a najde chyby, souvisí neustálé vydávání opravných balíčků a přichází doba, že technologie budou soustavně selhávat. To je ta lepší stránka věci. Daleko horší případ je, že celkově lidstvo jako takové pomalu degeneruje, nebude schopno ovládat IT technologie, jeho vlastní znalosti a schopnosti budou omezeny na reakce v odpovědi na dotazy stroje. Zůstanou pouze jedinci, označovaní v Huxleyově románu „Konec civilizace“ alfa dvě plus, kteří se budou schopni v takovém světě vyznat. Ostatní se zařadí do masy epsilon dvě minus.

Pokud tedy máme hovořit o kybernetické bezpečnosti, je nutno akceptovat obě dvě oblasti. Zatímco oblast kyber-technologických bezpečnostních problémů je poměrně dobře zmapována a jsou známy mechanismy obrany, kyber-sociální bezpečnost, respektive nebezpečnost začíná potichu měnit myšlení a chování lidstva a ohrožovat tak celou společnost. Tam leží směr kybernetické bezpečnosti budoucnosti.