NÁRODNÍ CENTRUM PRŮMYSLU 4.0

Bulletin Průmyslu 4.0

2019/04

www.ncp40.cz

Kyberbezpečnost / Testbed pro Průmysl 4.0

Úvodník

Vážení čtenáři Bulletinu Průmyslu 4.0,

s novými výzvami a příležitostmi přichází ruku v ruce i rizika, která zvláště u témat spojených s moderními technologiemi, mohou vytvářet překážky zpomalující aplikaci inovativních řešení do reálného života. Takováto rizika a obavy samozřejmě provází i zavádění Průmyslu 4.0 do praxe.

Mezi největší z rizik patří kybernetická bezpečnost a ochrana dat. Jedná se o důležité téma, kterému se věnujeme v tomto vydání Bulletinu a budeme se mu věnovat i na **Dni otevřených dveří v Testbedu pro Průmysl 4.0** a v **Národním centru Průmyslu 4.0**, který proběhne již 5. června a na který Vás tímto srdečně zvu. Kromě již tradičního přátelského setkání partnerů centra a nadšenců do technologií Průmyslu 4.0 zde proběhnou zajímavé přednášky právě na téma kybernetické bezpečnosti v průmyslu nebo představení jednoho z nezávislých řešení architektury pro nakládání s daty, platformy **International Data Spaces**.

V minulých číslech Bulletinu jsme Vás již informovali o aktivitách NCP4.0 v oblasti spolupráce se státem na vytváření prostředí přínosného pro zavádění principů Průmyslu 4.0 do praxe. V rámci **Ministerstva průmyslu a obchodu ČR** mezitím došlo k výměně na postu ministra. Tento pro nás klíčový resort nyní vede pan Karel Havlíček, který mezi své hlavní priority zařadil i transformaci českého průmyslu a jako jeden z hlavních nástrojů této transformace akcentuje právě zavádění principů Průmyslu 4.0.

Již z prvních diskuzí s novým vedením ministerstva je zřejmé, že toto téma získává na státní úrovni mnohem větší pozornost, než tomu bylo doposud. Naším cílem je proto stále intenzivněji spolupracovat se státem, abychom byli jedním z hnacích motorů transformace českého průmyslu. K tomu mají přispět také právě probíhající změny ve fungování NCP4.0, které mají za úkol z něj udělat akceschopnější, výkonnější a manažersky řízené moderní centrum, které mimo jiné bude schopné se stát oporou a průvodcem nejen pro stát, ale především pro malé a střední výrobní podniky v oblasti Průmyslu 4.0.

Chtěl bych poděkovat členům Řídicího výboru NCP4.0 za jejich intenzivní spolupráci na probíhající změně Stanov Centra, která je pro nové fungování Centra zásadní. S finální podobou struktury NCP4.0 bych Vás rád seznámil v dalších vydáních Bulletinu.

Přeji Vám kyberneticky bezpečné a příjemné čtení.

Jaroslav Lískovec

ředitel Národního centra Průmyslu 4.0

Vize rozvoje Testbedu na CIIRC ČVUT

Autor: Ing. Pavel Burget, Ph. D., ředitel Testbedu pro Průmysl 4.0

Pracoviště Testbedu pro Průmysl 4.0 na Českém institutu informatiky, robotiky a kybernetiky (CIIRC) funguje již od podzimu roku 2017 a postupně se jej daří vybavovat nejrůznějšími výrobními technologiemi, které umožňují testovat pokročilé výrobní procesy v souladu s požadavky Průmyslu 4.0. V tuto chvíli je v testbedu možné pracovat s dopravními systémy, standardními, kolaborativními, ale i mobilními roboty, obráběcími stroji a dalšími zařízeními.

Funkčně je Testbed rozdělen na dvě části – v jedné se provádějí operace převážně montážní a logistické, v druhé především operace výrobní. Tyto dvě části sice nejsou propojeny automatickou dopravou, což může v budoucnu nastat, ale již nyní mohou být propojeny logicky. Lze tedy modelovat různé vazby typu:

- obě části Testbedu jsou součástí jedné výrobní firmy a stejné výrobní haly
- část s obráběcími stroji je v jiné výrobní hale.
- část s obráběcími stroji je u subdodavatele
- další kombinace

Efektivní propojení nejen jednotlivých částí Testbedu, ale i připojování externích pracovišť a postupné budování distribuovaného Testbedu, vyžaduje použití modulární softwarové architektury, která bude umožňovat rozšiřování i na jiná pracoviště, vytvářet různé konfigurace a různé cesty toku dat nad společnými výrobními zařízeními. Základem pro distribuovaný Testbed je projekt **RICAIP** (o kterém jsme psali v minulém čísle), jehož cílem je právě budování evropské výzkumné infrastruktury pro pokročilou výrobu a umělou inteligenci.

Využití průmyslového SW

Část softwarových modulů počítá s využitím nástrojů a systémů určených pro průmyslové nasazení jako jsou například **Manufacturing Execution System** (MES) v oblasti řízení výroby a **Enterprise Resource Planning** (ERP) pro řízení podniku a obchodních vztahů. Jako příklad můžeme uvést **Simatic IT, ABRA Gen** nebo **SAP**, přičemž tyto systémy mohou mít samy různé moduly určené pro různé příležitosti a různé typy firem.

Kombinací modulů bude možné vytvářet různé scénáře představující případové studie pro firmy různé velikosti a různého charakteru. Možný scénář je tedy nasazení kompletního MES a ERP systému včetně optimálního plánování výroby jako specializovaného modulu v ERP. Další možný scénář je nasazení MES systému a z ERP by byl nasazen pouze modul, který zajišťuje správu zákazníků a objednávek. Další možný scénář je chybějící MES systém a využití specializovaného modulu z ERP, který by samostatný MES systém nahradil. Použité moduly a varianty konfigurace je možné kombinovat, aby to vyhovovalo zvolenému scénáři.

Využití experimentálního SW

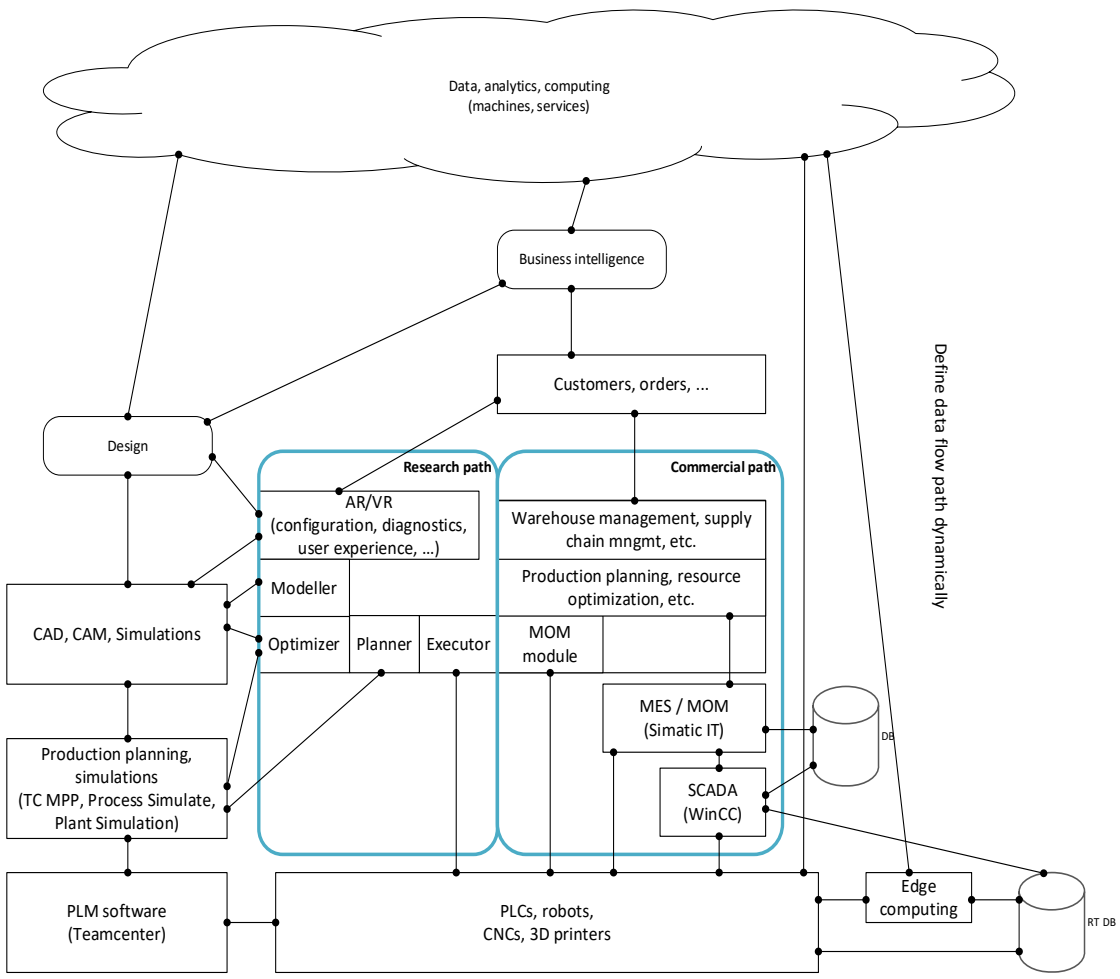
Navržená architektura ovšem také umožňuje vývoj a nasazení SW modulů experimentálního charakteru, které mohou běžet paralelně k části s průmyslovým SW nebo mohou sloužit jako jeho rozšiřující moduly. Lze tak připravit například modul pro optimální rozvrhování výroby, který rozšíří stávající funkci MES systému. Příkladem samostatně běžící funkce je systém plánování a řízení výroby (Planner, Executor), které byly realizovány v Testbedu v CIIRCu pro ukázkovou aplikaci flexibilního skládání z kostiček **LEGO**.

Automatizovaná technologie

Řízení technologií jako jsou dopravníky nebo roboty je založené na otevřené komunikaci **PROFINET**, přičemž bezpečnost je řešena pomocí **PROFIsafe**. Pro připojení senzorů preferujeme technologii **IO-Link**. V současné době je v Testbedu několik samostatných PLC, které představují jednotlivé stroje (dopravník, roboty). Ve spodní části Testbedu jsou roboty a obráběcí stroje, u nichž se předpokládá lokální řešení bezpečnosti v závislosti na technologii konkrétního stroje. 3D tiskárny pracují jako nezávislé jednotky, jejich plná integrace do systému se zatím nepředpokládá.

pokračování článku na následující straně

pokračování článku Vize rozvoje Testbedu na CIIRC ČVUT



Hierarchie systémů PLM, řízení a plánování výroby v Testbedu

Jako součást automatizované technologie chápeme také mezioperační přepravu, která může být řešena na různých stupních autonomnosti a flexibility. V případě Testbedu vnímáme tři úrovně:

- přeprava mezi propojenými robotickými či manuálními pracovišti prostřednictvím pevného dopravníku **Montrac** s volitelnými trasami pro jednotlivé vozíky,
- využití autonomních vozidel (robotů) pro přepravu mezi vzdálenějšími pracovišti nebo pro zásobování výroby z automatického skladu,
- manuální přeprava s využitím lidského operátora.

Ve všech případech je nutné připravit rozhraní celého systému umožňující sledování pohybu materiálu a výrobků, pohyb vozíků, robotů i operátorů a sledování stavu či rozpracovanosti výroby. V případě komunikace s lidskými operátory budou využity operátorské panely (pevné či mobilní), v případě autonomní přepravy je komunikace přirozeně integrována do samotných strojů a automatizovaných pracovišť.

PLM jako jádro celého systému

PLM obsahuje veškerá zdrojová data k životnímu cyklu výrobku, což umožňuje efektivní spolupráci různých týmů na vývoji výrobku (**CAD/CAM, Simulations**), přípravě výroby (**CAM, Simulations, Teamcenter Manufacturing, Process Simulate, Plant Simulation, NX Mechatronics Concept Designer**) či aktualizací výrobních dat na základě informací z výroby již běžící.

Reference pro různé typy uživatelů a firem

Různé uživatelské scénáře nastíněné výše budou sloužit jako reference pro různé typy uživatelů a firem. Dlouhodobým cílem je vytvořit v Testbedu jakýsi showroom, který se bude přizpůsobovat cílové skupině – např. veřejnost, školy, výrobci strojů, provozovatelé automatizované výroby se zájmem o inovaci dle Průmyslu 4.0 atd. Uživatelské scénáře včetně popisu použitých technologií a řešení budou prezentovány odpovídajícím způsobem.

Jednotné rozhraní

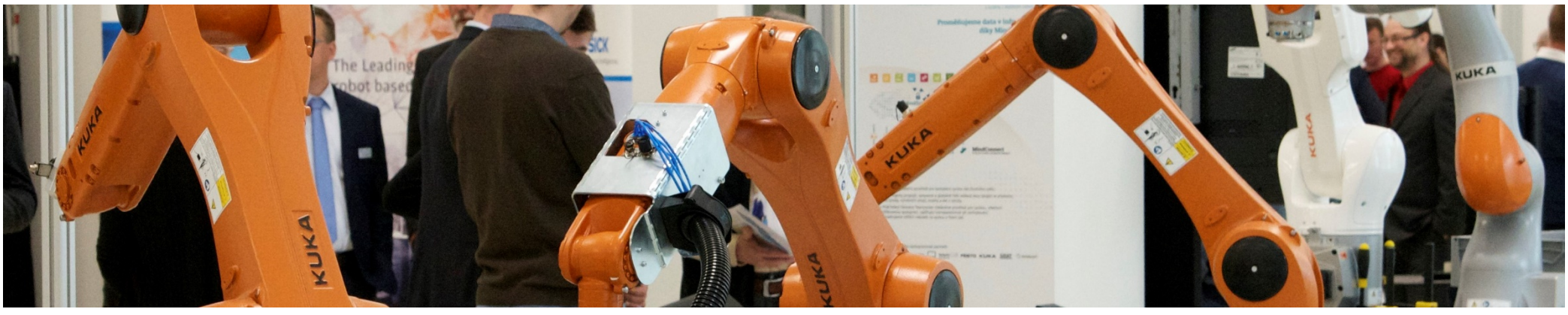
Jednotlivé moduly zapojené do systému musí využívat jednotné rozhraní. Na úrovni komunikace mezi automatizovanou technologií a nadřazenými vrstvami, stejně jako na úrovni komunikace mezi jednotlivými stroji, se bude využívat rozhraní OPC UA jako standard, o kterém se v současné době mluví jako o komunikaci pro Průmysl 4.0. Odpovídá tomu úsilí různých standardizačních a zájmových skupin o vydávání podpůrných specifikací (companion specification) a implementaci OPC UA do koncových zařízení i softwarových nástrojů. Příkladem podpůrných specifikací je například **OPC UA Robotics Companion Specification** nebo **OPC UA Vision Companion Specification** vydané organizací **VDMA**, či **PROFINET@OPC UA**, na kterém pracuje organizace **PROFIBUS & PROFINET International**. U těchto standardů jde především o mapování datového a funkčního modelu jednotlivých technologií na OPC UA tak, aby právě OPC UA mohlo co nejvíce a jednotným způsobem využívat možností, které dílčí technologie poskytují. Jako příklad můžeme uvést například pokročilou diagnostika a správu informací o zařízení v systémech PROFINET, které se dlouhodobě zaměřují na udržování konzistentního modelu zařízení s ohledem na jejich provozní stavy, znalost topologie sítě a umístění konkrétního zařízení ve výrobě atd.

Dalším důležitým prvkem je standardizace chování strojů vzhledem k jejich integraci do linky, čímž se zabývá standard PackML spravovaný organizací **OMAC** a evidovaný jako standard rozšiřující ISA 88. Tento standard původně určený pro balicí stroje je vnímán jako základ pro standardizaci funkčního chování strojů v diskrétní výrobě. Definuje provozní režimy strojů a jejich vzájemnou interakci, tomu odpovídající způsob ovládání prostřednictvím operátorských panelů a samozřejmě mapování na OPC UA.

Propojení na výzkumné projekty

Kromě projektu RICAIP je CIIRC řešitelem a často i koordinátorem řady evropských i národních výzkumných projektů, jejichž výsledky lze přímo aplikovat na technologie použité v Testbedu a samozřejmě modulárním způsobem rozšiřovat v rámci zvětšování sítě pracovišť podílejících se na realizaci distribuovaného Testbedu. Jedním z příkladů je projekt **Klastr 4.0: Metodologie systémové integrace**, který se zabývá návrhem architektury umožňující propojování dílčích systémů na základě znalosti služeb, které jsou tyto systémy schopny nabízet tak, aby se vytvořil požadovaný výrobní proces. Jako další příklad můžeme uvést evropský projekt **ARtwin**, jehož cílem je mimo jiné rozvoj systémů rozšířené a virtuální reality ve spojení s cloudovými technologiemi, což by mělo vést k jejich rozšíření v průmyslových aplikacích.

Testbed postupně začíná naplňovat své původní poslání, což je sloužit jako experimentální platforma k ověřování inovativních postupů a metod, aby tak usnadnil jejich přenos do průmyslové praxe.



Ekosystém umělé inteligence

Autor: Alena Nessmithová

Český institut informatiky, robotiky a kybernetiky začátkem dubna hostil konferenci *„Ekosystém umělé inteligence v ČR“* s cílem prezentovat oblasti výzkumu umělé inteligence napříč veřejným i soukromým sektorem. Konference, pořádaná spolu se společností Microsoft a Svazem průmyslu a dopravy ČR, navázala na aktivity CIIRC v oblasti umělé inteligence z počátku tohoto roku, kdy zde vznikla celonárodní iniciativa pro umělou inteligenci AI CZECHIA.

Vědecký ředitel CIIRC a úřadující ředitel **AI CZECHIA profesor Vladimír Mařík** zahájil konferenci výzvou k přítomným: *„všichni musí vědět, co je AI a jak ji využívat,“* a dodal, že to je základní podmínka pro další rozvoj výzkumu umělé inteligence. Jako další zásadní podmínku jmenoval změnu vzdělávání a spolupráci s Evropskou unií.

V rámci celodenní konference vystoupili zástupci společnosti **Microsoft, Svazu průmyslu a dopravy,** CIIRC, ale i start-upů, které se zabývají vývojem AI, a před desítkami diváků se podělili se o svoje zkušenosti s vývojem umělé inteligence a jejím zaváděním do praxe. Z vystoupení většiny řečníků bylo zřejmé, že nelze v praxi oddělit akademický výzkum od soukromého, neboť spolu úzce souvisí a vzájemně se doplňují. Komerční výzkum často těží z výsledků vědecké práce státem financovaného vývoje, ale bez komerční sféry by se zase unikátní výzkum těžko dostával k běžným uživatelům.

Mezi řečníky se zkušenostmi z obou prostředí patřila například absolventka ČVUT Zuzana Kúkelová, která působila dva roky jako postdoktorandský výzkumník v **Microsoft Research Cambridge**, kde vyvíjela algoritmy na kalibrace kamer. Například aplikace **Kinec**t, vyvinutá pro herní průmysl, znamenala velký průlom pro výzkum, neboť nabídla cenově dostupné hloubkové senzory. Stejně tak **Microsoft Hololens**, brýle pro smíšenou realitu, jsou dnes používány v nejrůznějších ne herních aplikacích například v medicíně, při montáži náročných zařízení nebo navádění oprav na dálku.

O úzké spolupráci akademického a soukromého sektoru mluvil i Petr Schwarz, CTO společnosti **Phonexia**, která vyvíjí technologie pro řečovou analytiku a hlasovou biometrii. Schwarz uvedl, že vznik společnosti si v podstatě vynutila nepružnost akademického prostředí, které nedokázalo reagovat na požadavky trhu. Phonexia vznikla jako spin-off z fakulty informačních technologií brněnského **VUT** v roce 2006, aby bylo možné komerčně využít výsledky probíhajícího unikátního výzkumu. Zájemci o tuto řečovou technologii si tak mohou koupit software of Phonexie, ale univerzitě zaplatí za výzkum, který vedl k vývoji tohoto softwaru.

foto z konference Ekosystém umělé inteligence ©Microsoft

Zajímavé poznatky o využívání umělé inteligence v praxi přinesla i přednáška zástupce Svazu průmyslu a dopravy, Jiřího Holoubka, který ve své prezentaci představil průzkum svazu týkající se mapování AI ve firmách (více o výsledcích průzkumu v článku *Mapování AI*). *„Podle prvních výsledků průzkumu je zřejmé, že aplikace AI ve firmách jsou zatím spíše v oblasti administrativní a podpůrné činnosti a firmy na ní ve velké části nemají proškolené odborníky“*, řekl Holoubek. Svaz průmyslu a dopravy také stojí za vznikem **Platformy pro umělou inteligenci SPČR**, která se zabývá využitím AI ve firmách a v současnosti má zhruba 40 členů z řad firem, ale i univerzit.

Konferenci doplnily zkušenosti odborníků ze společnosti Microsoft v oblasti transferu výzkumu do komerčně úspěšných aplikací. Jedním z nich je například medicínský **Project Inner Eye**, který umí skládat snímky z magnetické rezonance a vyhodnotit pravděpodobnost patologického jevu jako je tumor. *„I když je role lékaře při diagnóze nezastupitelná, sami lékaři přiznávají, že jim program Microsoftu uspoří 30 – 40 % práce při detekci“*, řekl Zdeněk Jiříček, National Technology Officer společnosti Microsoft pro ČR. Další z nich je například **Skype Translator**, který kombinuje rozpoznávání řeči, automatizovaný překlad a umělou inteligenci při vývoji real-time překladače pro společnost Skype.

„Díky zázemí akademického výzkumu a návaznosti na komerční sféru má Česká republika předpoklady zabývat se AI „end-to-end“, tedy od výzkumu až po konečná odvětví“, řekl Jiříček a dodal, že *„Česká republika má potenciál stát se jednou vedoucích zemí v umělé inteligenci v Evropě.“*

Mapování AI

Autor: Alena Nessmithová

Svaz průmyslu a dopravy ČR zrealizoval na začátku letošního roku mapování umělé inteligence ve firmách, při kterém mimo jiné zjišťoval, v jakých oblastech firmy a výzkumná pracoviště umělou inteligenci vyvíjejí a v jakých aplikacích ji nejčastěji nasazují. Výstupy z průzkumu ukázaly na zajímavé trendy a data byla zároveň předána Ministerstvu průmyslu a obchodu, které je využije při tvorbě Národní strategie pro umělou inteligenci.

Jiří Holoubek, člen představenstva Svazu průmyslu a dopravy ČR (dále SP), který výstupy mapování představil v průběhu konference *Ekosystém umělé inteligence v ČR*, uvedl, že impulzem pro takovéto mapování byla potřeba SP udělat si představu o tom, jak se jeho členové věnují aplikaci AI v praxi. V průzkumu se svaz zajímal i o to, jaké metody při zavádění AI firmy používají, jaké preferují způsoby financování a jakým způsobem umělou inteligenci prakticky využívají.

Z výsledků výzkumu vyplynulo, že nejčastější aplikace AI ve firmách je v rámci informačních a komunikačních činností a to sice ve více než 65 % případů a v rámci podpůrných business procesů, téměř 50 %. Zhruba ve 30 % případů používají firmy AI pro profesní vědecké a technické činnosti, marketing a v oblasti peněžnictví a pojišťovnictví. Méně než 20 % firem naopak aplikuje umělou inteligenci v logistice, zpracovatelském průmyslu nebo pro firemní management.

Holoubek uvedl, že zatím se AI používá pro komunikaci v rámci systémů CRM nebo EMS v minimální míře. *„Co je pro nás hrozné, že komunikace mezi těmito systémy probíhá pomocí excelových tabulek, které si [zaměstnanci] tisknou a ještě ručně opravují,“* řekl Holoubek a dodal, že to je dáno i tím, že v téměř polovině dotazovaných firem se AI věnuje nejvýše pět úvazků zaměstnance.

Z výzkumu také vyplynulo, že v současnosti nejvíce využívané metody AI ve firmách jsou strojové učení (včetně hlubokého učení), počítačové vidění a grafika, a zpracování řeči a přirozeného jazyka. Oblasti jako autonomní robotika, automatické vyvozování, plánování a rozvrhování či strojové vnímání jsou zatím využívány v méně než 20 %.

„Největší potenciál pro průmyslové technické aplikace vkládáme do strojového učení. Počítačové vidění a zpracování řeči se promítne do rutinních administrativních činností,“ řekl Holoubek v rámci samostatné tiskové konference, kde SP informovalo o výstupech mapování. *„Nyní je důležité, aby vznikaly aplikace, které i menším a středním firmám přinesou hmatatelný užitek. Na druhé straně firma musí umět pracovat s daty, sbírat je a ukládat tak, aby s nimi mohla umělá inteligence pracovat.“*

Národní strategie umělé intelligence v ČR byla schválena

Vláda v pondělí 6. 5. 2019 schválila **Národní strategii umělé inteligence v ČR**, která je základem podpory rozvoje AI v Česku a rovněž nezbytným předpokladem pro vznik evropského „superhubu“.

Strategie je členěna do sedmi kapitol a pokrývá oblasti ekonomiky a společnosti - od podpory vědy a výzkumu, přes školství a sociální systém, až po otázky regulace a mezinárodní spolupráce.

Prioritní témata umělé inteligence v ČR jsou založena jak na výsledcích české vědy, tak na průmyslových nebo veřejných aplikacích, ve kterých ČR patří mezi špičku. Zahrnují bezpečnost a obranu, průmyslovou výrobu a komunikaci člověka se strojem.

„Klíčový první krok je snaha vybudovat v Praze Evropské centrum excelence v AI, tedy sídlo jedné z chystaných čtyř evropských výzkumných sítí. To by pomohlo vytvořit z Česka a celého regionu jeden ze světových AI hubů, ze kterého by těžila i ostatní oborová centra v Česku a celé střední Evropě,“ řekl náměstek ministra pro digitalizaci a inovace **Petr Očko**, jenž se svým týmem strategii připravil. Česko si vznik Evropského centra excelence v AI vytyčilo za krátkodobý cíl, kterého je reálné dosáhnout do roku 2021. Strategie obecně počítá s krátkodobými (právě do roku 2021), střednědobými (2027) a dlouhodobými (2035) cíli.

„Máme velkou šanci využít špičkový český výzkum v této průlomové technologii, jako klíčový nástroj pro naši budoucnost. Zařazujeme se tím mezi evropskou technologickou elitu, která bude udávat nejen směr v oblasti průmyslu, ale stává se rovněž významným světovým hráčem v budování kybernetické bezpečnosti, abychom se tak postavili velké globální hrozbě, jako je krádež dat,“ uvedl místopředseda vlády a ministr průmyslu a obchodu **Karel Havlíček**.

Aktuální informace z Národního centra Průmyslu 4.0 naleznete na sociálních sítích

https://www.linkedin.com/company/národní-centrum-průmyslu-4-0

@ncp40

ZAJÍMAVOST

Soumrak novinářů? ČTK bude vyvíjet aplikaci na psaní textů pomocí umělé inteligence

Národní zpravodajská agentura **ČTK** vyhrála grant na projekt využití umělé inteligence při tvorbě textů, který uděluje internetová společnost **Google**. Partnery ČTK v tomto projektu je vývojářská firma **Geneea** a vydavatelství **Economia**. Grant je určen na podporu digitálních médií a byl jedním ze 103 udělených v šestém, posledním kole programu. ČTK byla jediným úspěšným uchazečem z Česka.

„Naším cílem je vyvinout řešení, které pomůže překonat rutinní práci s tvorbou pravidelně vydávaných zpráv a s vyhledáváním fotografií, doprovodných textů a dalších souvisejících materiálů. Tím zjednoduší novinářům práci, zrychlí produkci agentury a výrazně rozšíří nabídku klientům,“ řekl technický ředitel ČTK Jan Kodera.

Výsledkem v Evropě unikátního projektu bude také to, že zprávy agentury budou obsahovat odkazy na fotografie ČTK a jejím klientům umožní dohledat další materiály ve Fotobance ČTK, případně i v jejich vlastních archivech. Kodera dodal, že složitost českého jazyka brání využití dostupných nástrojů vyvinutých pro angličtinu nebo jiné jazyky. Navíc kombinace generování textů a dohledávání souvisejících materiálů je jedinečná. Řešení bude plně integrováno do běžných procesů v agentuře tak, aby ho mohli využívat redaktoři bez speciálních technických znalostí.

ČTK již použila automaticky generované zprávy poprvé při loňských obecních a senátních volbách. *„Automatizace je podle mého nepominutelná součást vývoje agentury. Tento nový projekt nám pomůže posunout se výrazně vpřed a být připraveni na budoucí potřeby našich klientů,“* uvedl ředitel ČTK Jiří Majstr.

„ČTK dlouhodobě automatizuje činnosti, u kterých je to možné a dává to smysl. Například už mnoho let vydává automaticky generované deníky očekávaných událostí,“ připomněl.

Zdroj: Svetchytre.cz, mediar.cz

Personálie

Nový ministr průmyslu a obchodu a nové vedení AMSP ČR

Dosavadní předseda představenstva a spoluzakladatel **Asociace malých a středních podniků a živnostníků ČR Karel Havlíček** byl 30. dubna jmenován novým **ministrem průmyslu a obchodu**.

K. Havlíček, který také působí jakožto místopředseda vládní Rady pro výzkum, vývoj a inovace, v souvislosti se svým jmenování odstoupil z pozice předsedy AMSP ČR.

K. Havlíček vystudoval stavební fakultu ČVUT, doktorát obhájil na fakultě podnikohospodářské na VŠE v Praze, kde se později na fakultě financí a účetnictví úspěšně habilitoval. MBA získal na PIBS při Manchester Metropolitan University. Je generálním ředitelem SINDAT, mateřské společnosti investiční skupiny podnikající v oblastech finální chemie, speciálních textilií a biotechnologií.

Dlouhodobě rovněž spolupracuje s akademickou sférou, je děkanem fakulty ekonomických studií Vysoké školy finanční a správní a jako autor nebo spoluautor se podílel na několika odborných knihách a více jak stovce odborných článků se zaměřením na malé a střední firmy.

Představenstvo AMSP pověřilo vedením asociace dosavadního místopředsedu **JUDr. Zdeňka Tomíčka**. Z. Tomíček je jedním ze zakládajících partnerů advokátní kanceláře **CEE Attorneys**. Ve své právní praxi se specializuje na soudní spory a rozhodčí řízení, pracovní a obchodní právo a má na starosti mezinárodní expanzi advokátní kanceláře.

Vladimír Kulla v čele Vývojového centra internetu věcí pro Evropu (a Česko) Siemens

Vladimír Kulla byl k 1. dubnu 2019 jmenován do pozice **ředitele Vývojového centra internetu věcí pro Evropu (a Česko)** ve společnosti **Siemens.** V. Kulla byl od roku 2009 až doposud ředitelem vývojového a prototypového centra Siemens Česká republika. Ve společnosti pracuje od roku 2001 a v rámci firmy zastával řadu manažerských a vývojářských pozic v různých státech Evropy. Vývoji nových produktů a technologií se věnuje již více než 20 let. Předtím, než svou profesní kariéru spojil s firmou Siemens, působil v několika menších IT společnostech. Mezi hlavní oblasti zájmů V. Kully patří inovační management, podpora inovací v korporaci a ochrana intelektuálního vlastnictví.

Vladimír Mařík se stal Manažerem roku 2018

Profesor Vladimír Mařík, vědecký ředitel CIIRC ČVUT, získal prestižní cenu **Manažer roku 2018** vyhlašovanou Českou manažerskou asociací. Cenu převzal na slavnostním galavečeru v paláci Žofín 25. 4. 2019. Kromě hlavní kategorie Manažer roku získal i ocenění **Smart manažer roku**.

Mařík získal titul Manažer roku 2018 zejména za své úsilí prosadit moderní metody organizace a řízení. *„Šlo a jde mi o vybudování vysokoškolského ústavu nového typu, uznávaného v mezinárodní vědecké aréně a přínosného pro rozvoj české ekonomiky,“* uvedl k důvodům, proč CIIRC vlastně vznikal.

POZVÁNKA
Den otevřených dveří v Testbedu pro Průmysl 4.0 a Národním centru Průmyslu 4.0

Kdy: 5. 6. 2019
Kde: Testbed pro Průmysl 4.0, CIIRC ČVUT, Jugoslávských partyzánů 1580/3, Praha 6

Registrace a více informací

Program:

Konference kybernetická bezpečnost v průmyslu

9:00 – 9:30	Registrace
9:30 – 10:00	Úvodní slovo
10:00 – 11:00	Představení asociace International Data Spaces
11:30 – 12:30	Kyberbezpečnost – přednáška: Odborná skupina pro kyberbezpečnost VŠB TUO
12:30 – 13:00	Kyberbezpečnost v průmyslu očima partnerů NCP4.0, rozvoj Testbedu pro Průmysl 4.0

Den otevřených dveří (firmy, školy, odborná i široká veřejnost)

13:30 – 16:30	komentované prohlídky testbedu
	stánky partnerů NCP4.0
	networking
	robotický barman

Vize v robotice představily novinky na českém robotickém trhu a ukázaly směr vývoje

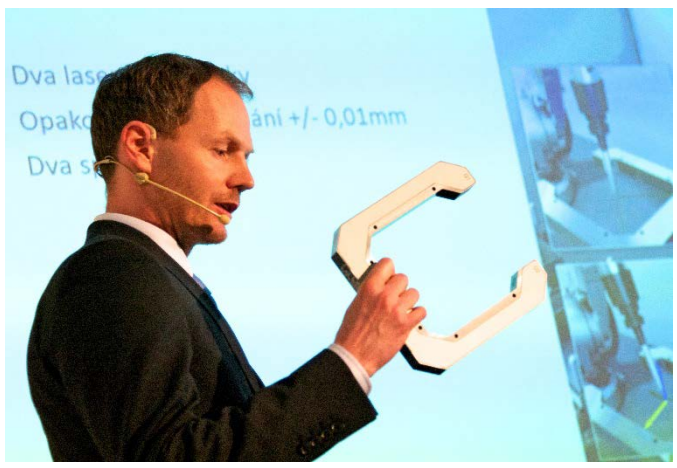
Ve dnech 10. a 11. 4. se v prostorách Testbedu pro Průmysl 4.0 CIIRC ČVUT konala akce Vize v robotice 2019, kterou spolupořádalo Národní centrum Průmyslu 4.0 se svými partnery, společnostmi KUKA a SICK. Série přednášek byla zaměřena jak na aktuální trendy v oblasti robotiky, tak na prezentaci řešení, která se řeší v rámci výzkumu či experimentální laboratoře pro chytrou továrnu, v Testbedu pro Průmysl 4.0.

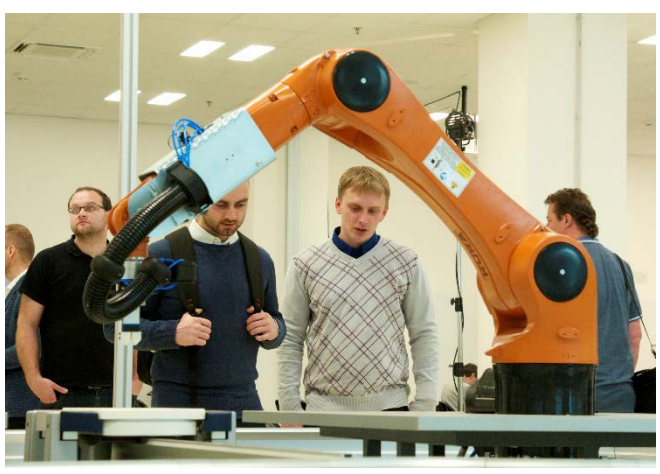
Testbed pro Průmysl 4.0 je místem, kde se realizují vize budoucnosti. Koncentrují se zde chytré technologie, které by v budoucnu měly najít uplatnění v průmyslu. Firmy si zde mají možnost tyto technologie otestovat a zjistit, jak je lze nasadit v reálné průmyslové výrobě. Partneři NCP4.0, KUKA a SICK, přivezli mnoho novinek, které naopak mohou firmy využívat již nyní.

Nedostatek pracovních sil v České republice se projevuje i ve velkém zájmu o robotizaci provozů, a to i těch, pro které to bylo ještě před pár lety nemyslitelné. Častým řešením se pak stávají kolaborativní roboty, které spolupracují s člověkem a není třeba je složitě přeprogramovávat při každé změně výrobku na lince.

Společnost KUKA představila novinky ze svého portfolia, a to roboty QUANTEC II, řadu CYBERTECH a roboty s nižší hmotností AGILUS. Roboty QUANTEC II se v ČR představily poprvé, a tomu odpovídal i zájem zákazníků o ně. KUKA představila rovněž společnou aplikaci se společností SICK, která měří mezní síly na kolaborativních robotech. Svou českou premiéru zde měla týden po veletrhu Hannover Messe i robotická pětiprstá ruka od firmy Schunk prezentovaná na kolaborativním robotu KUKA. Firma SICK na workshopu představila kamerový systém PLR prezentovaný na autonomním robotu KUKA KMR.

Zájem o řešení v oblasti robotiky přitáhl do Testbedu pro průmysl velké množství návštěvníků a potvrdil tak vzrůstající trend v této oblasti.





Asociace International Data Spaces řeší bezpečné sdílení dat

Autorky: Alena Nessmithová a Alena Nováková s využitím materiálů IDS

Bezpečný datový prostor a spolehlivé bezpečnostní mechanism při ochraně dat jsou pro firmy klíčovými parametry při zavádění principů Průmyslu 4.0. Pro mnohé z nich je nedostatečná ochrana dat důvodem, proč ke změnám přistupují s obavami a velmi váhavě. S cílem zajistit jednotné prostředí pro sdílení dat mezi uživateli z různých průmyslových a výrobních prostředí vznikla v Německu asociace International Data Spaces pro nadnárodní výměnu dat na bázi peer-to-peer podporovaná německou spolkovou vládou. Po pěti letech existence expandovala IDSA na jaře letošního roku i do České republiky, a Český institut informatiky, robotiky a kybernetiky stal jejím šestým hubem v Evropě.

Cílem IDS je vytvořit ekosystém pro bezpečné sdílení dat, který je postavený na jednotném standardu výměny dat mezi obchodními partnery na mezinárodní úrovni, přičemž asociace se zavazuje postarat se o veškeré bezpečnostní, právní a technické prvky této výměny na základě obecně platných pravidel.

Data v bezpečí

Zabezpečení dat a jejich kontrola ze strany vlastníků je naprosto zásadní a platforma IDS zaručuje, že vlastníci mají vždy kontrolu nad svými daty a jejich zabezpečení je v souladu s jejich vlastními standardy bezpečnosti. Data se neukládají do cloudu, ale zůstávají u jejich vlastníků a k jejich výměně dochází pouze na žádost ověřených a důvěryhodných partnerů a se souhlasem jejich poskytovatelů. Pokud je to vyžadováno, nevyměňují se data jako taková, ale jsou použita k analýze a partnerům se předávají až výstupy z jejich analýzy.

Po technické stránce probíhá výměna informací prostřednictvím zabezpečené IoT brány, takzvaného konektoru a společně s ostatními konektory zapojenými do výměny vytváří peer-to-peer síť. Konektor umožňuje definovat jak často je možné data používat, tedy jak často k nim může mít druhá strana přístup, jaké hodnoty si může zobrazit, zda je může ukládat či předávat třetím stranám a samozřejmě, zda za ně má něco platit.

Jak to může fungovat

Bezpečná výměna dat je důležitá pro všechna odvětví průmyslu a služeb, přičemž logické využití nachází v zejména v případech, kde je nutné sdílení „živých“ dat mezi několika partnery v rámci jednoho dodavatelského řetězce. Využití nachází v logistice, při vývoji a testování léků, v prediktivní údržbě, při vývoji výrobků či služeb, který zahrnuje více spolupracujících partnerů apod.

Důležitou oblastí pro použití výměny dat je také strojové učení. IDS vytváří strategické propojení mezi daty vznikajícími v internetu věcí na jedné straně a využitím těchto dat v algoritmech strojového učení a umělé inteligence na straně druhé. Záměrem je vytvořit datový trh, na kterém by společnosti mohly získávat neutralizovaná strojová data a na oplátku by vytvořily a nabídly platformu nezávislých „mikroslužeb“.

V takovém scénáři nemusí výrobce stroje zpřístupňovat svá data, pokud nechce; místo toho si může jednoduše vyžádat a používat data od jiných společností - za předpokladu, že plně vyhovují zásadám pro používání dat stanoveným příslušným poskytovatelem dat. Vývojáři IDS mají za cíl vytvořit bezpečný a důvěryhodný datový trh, na kterém mohou firmy spolupracovat, aniž by museli vytvářet komplikované smlouvy.

Takový datový trh je zajímavý pro výrobce a producenty strojů a společnosti, které se zabývají aditivní výrobou. Například **Thyssenkrupp** a **IBM** společně vyvíjejí platformu založenou na architektuře IDS rozšířené o technologii IBM blockchain. Kombinace jejich přístupů se zaměřuje na usnadnění bezpečnosti a svrchovanost dat v souvislosti s vyšším stupněm automatizace při zpracování objednávek v nastaveních aditivní výroby. Výhody platformy jsou dvojí - zaprvé rychlejší a snadnější přístup k 3D tisku, zejména pro malé a střední podniky, které dosud nemají zkušenosti v této oblasti a také lepší plánování a ověřitelná úroveň kvality v celém procesním řetězci.

Bezpečné sdílení dat bez rozdílu velikosti

Na iniciativě IDS spolupracují **Frauehhofer** (největší evropská výzkumná organizace orientovaná na aplikovaný výzkum) a množství velkých průmyslových korporací, jako je například **Siemens, Volksvagen, Sick, SAP, IBM, Bosch** či **REWE**. IDS v tuto chvíli reprezentuje více než 85 mezinárodních společností a výzkumných organizací a má celkem šest hubů v různých evropských zemích.

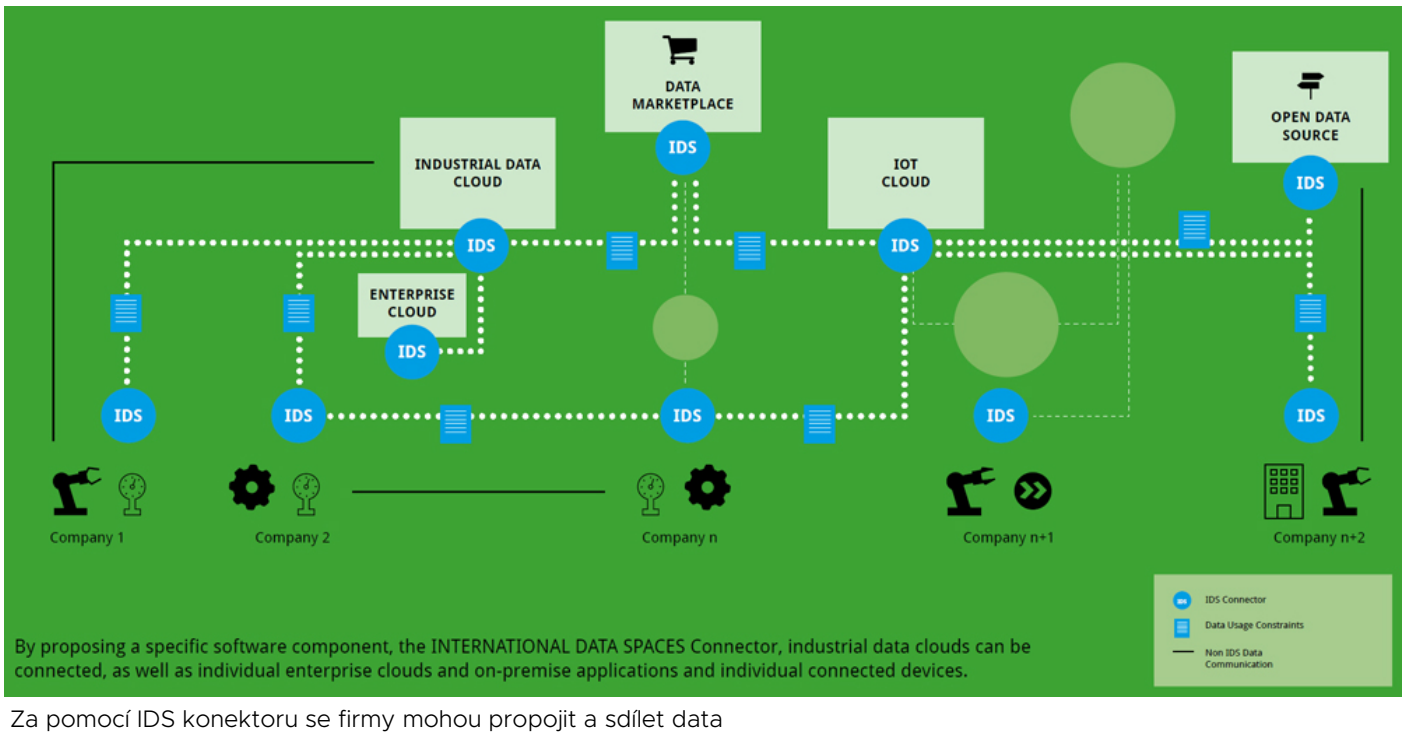
Cílem asociace je snaha o to, aby i přímí konkurenti chtěli spojit své síly: vytvoření bezpečných datových prostorů, ve kterých mohou společnosti vytvořit nové obchodní modely založené na datech, které jim umožní výměnu dat mezi sebou, zatímco datová svrchovanost bude zachována pro každého poskytovatele dat v celém dodavatelském datovém řetězci.

Asociace International Data Spaces zakládá svůj hub na CIIRC ČVUT

Asociace International Data Spaces spolupracuje s CIIRC ČVUT a jeho prostřednictvím otevírá hub pro české uživatele.

Více informací o fungování IDS a řešení, která nabízí, se můžete dozvědět v rámci Dne otevřených dveří v Testbedu pro Průmysl 4.0 a Národním centru Průmyslu 4.0 dne 5. 6. 2019.

Pozvání přijal i zástupce asociace, který IDS a její činnost představí, a rád zodpoví veškeré dotazy, které vás v oblasti bezpečného sdílení dat zajímají. Více informací o programu a registraci naleznete zde.



Za pomocí IDS konektoru se firmy mohou propojit a sdílet data

Na VŠB-TUO vznikla nová skupina počítačové bezpečnosti

Autor: Jan Plucar, skupina počítačové bezpečnosti, Katedra Informatiky, VŠB-TU Ostrava

Tématu počítačové bezpečnosti se v České republice věnuje čím dál větší pozornost, a to jak z pozice státních institucí, tak i soukromých firem. Se zvýšenou pozorností roste ovšem i poptávka po odbornících, na což zareagovala již v roce 2015 Vysoká škola báňská - Technická univerzita Ostrava založením nového oboru *„Informační a komunikační bezpečnost“* pod Fakultou elektrotechniky a informatiky. Cílem oboru je příprava odborníků zaměřených na počítačovou bezpečnost s důrazem na uplatnitelnost budoucích absolventů v praxi.

V symbióze s výukou se rozvíjela i vědecká činnost asistentů zapojených do nového oboru, a tak přirozeně vzniklo prostředí podporující projekty z oblasti počítačové bezpečnosti. Jedním z prvních bezpečnostních projektů byl projekt *„Bezpečnost mobilních zařízení a komunikace“,* podpořený Technologickou agenturou ČR v rámci výzvy programu Delta. Projekt se zabývá vývojem bezpečné komunikace a ochrany citlivých dat na mobilních zařízeních.

Dle statistik Policie ČR bylo v posledních letech hlášeno v průměru dvacet tisíc odcizených mobilních telefonů ročně. To představuje závažný společenský problém, neboť uživatelé mobilních zařízení si ve velké většině neuvědomují, jaké množství citlivých dat jejich mobilní telefony obsahují. Technické specifikace dnes běžně dostupného mobilního telefonu výrazně převyšují technické specifikace ještě nedávno používaných stolních počítačů. Zvýšila se i kvalita softwarového vybavení, a tím i množství instalovaných aplikací. V případě napadení telefonu například sledovacím softwarem (z anglického spyware) nebo v případě fyzického odcizení telefonu získá útočník snadný přístup k velkému množství dat. Dle dotazníkového šetření provedeného v rámci projektu, patří mezi data běžně ukládaná v mobilním telefonu zejména kontakty, SMS zprávy, emailové zprávy, data z posledních cest v navigaci a fotografie. U posledně jmenovaného uživatelé připustili možnost, že obsahují i obrazy citlivých dat, jako jsou kopie osobních dokladů, smluv či faktur. Z šetření také vyplývá, že 92 % uživatelů nijak neřeší bezpečnost svého zařízení.

Softwarové řešení Chiméra, jak byla pojmenována komunikační platforma vzniklá v rámci projektu *„Bezpečnost mobilních zařízení a komunikace“,* řeší problém ztráty citlivých pracovních dat. Chiméra se pro běžného uživatele jeví jako jednoduchý komunikátor, svou funkcionalitou podobný aplikacím WhatsApp nebo Messenger. Na pozadí však využívá nekonvenčních algoritmů pro maximální ochranu uživatelských dat.

Aplikace se spouští ve vlastním uzavřeném prostředí a veškerá data pořízená nebo přenesená na zařízení skrze Chiméru (tedy i fotografie) jsou zašifrovaná pomocí algoritmů využívajících deterministický chaos. Mimo to jsou data v okamžiku šifrování přenášena na zabezpečený server, ze kterého jsou nadále dostupná. V případě odcizení telefonu tak zařízení neobsahuje žádná citlivá data. Jedinou podmínkou je stabilní připojení k internetu.

Pro potřeby projektu byla provedena spolehlivostní analýza přenosu dat za použití mobilních sítí na území města Ostravy. Po dobu jednoho roku byla na třech kontrolních trasách provedena vždy dvě měření přenosu dat denně. Auto vybavené měřicím přístrojem periodicky nahrávalo na server soubory o velikostech 1 MB, 2 MB, 3 MB a 5 MB. Data z nejdelší měřené trasy (22,5 km) například ukázala, že při pokusu o přenos souboru o velikosti 1 MB došlo v 7,23 % případů k selhání a pokus o nahrání se musel opakovat. V případě 5 MB souboru pak došlo k selhání již v 9,56 % případů. Zjištěná míra selhání byla příliš vysoká. Za použití bio inspirovaných metod tedy došlo k optimalizaci parametrů procesu nahrávání souboru, což v závislosti na použitých hodnotách parametrů snížilo míru selhání na 1 %, 3 % nebo 5 %. Seznam neúspěšně nahraných souborů se periodicky kontroluje a v prostředí s dobrou konektivitou dochází k opětovnému pokusu o nahrání.

Bezpečnostní pojistkou, která je volitelná, je pak životnost souborů. Uživatel Chiméry je schopen nastavit životnost souborů, po kterou jsou soubory uloženy na zařízení uživatele. Po naplnění této životnosti jsou soubory smazány, ať už byly úspěšně nahrány na server nebo ne. Takto agresivní opatření lze použít v prostředí, kde se přirozeně očekává práce se soubory podléhající režimu utajení.

Projekt Chiméry demonstroval možnosti multidisciplinární spolupráce odborníků VŠB-TUO a průmyslových partnerů v oblasti počítačové bezpečnosti a byl jedním z impulsů, které vedly k založení vědecké skupiny počítačové bezpečnosti na VŠB-TUO. Skupina vznikla v dubnu letošního roku a bere si za cíl rozvíjet vědu a výzkum v oblasti počítačové bezpečnosti, a to jak formou vědeckých článků a grantů, tak i spoluprací s průmyslovými partnery.

V současné době má skupina šestnáct členů z řad zaměstnanců a doktorandů z Katedry informatiky, Katedry aplikované informatiky a Katedry telekomunikační techniky. Mimo obecnou počítačovou bezpečnost se skupina zaměřuje na oblasti jako jsou: bio-inspirované algoritmy v počítačové bezpečnosti, počítačová bezpečnost v oblasti automotive nebo analýza velkých dat v oblasti počítačové bezpečnosti. Pro náročné výpočty využívá Národní superpočítačové centrum IT4Innovations. V současné době spolupracují členové skupiny na různých výzkumných úkolech se zahraničními univerzitami v USA, Španělsku, Itálii, Francii, Portugalsku, Vietnamu a Indii.

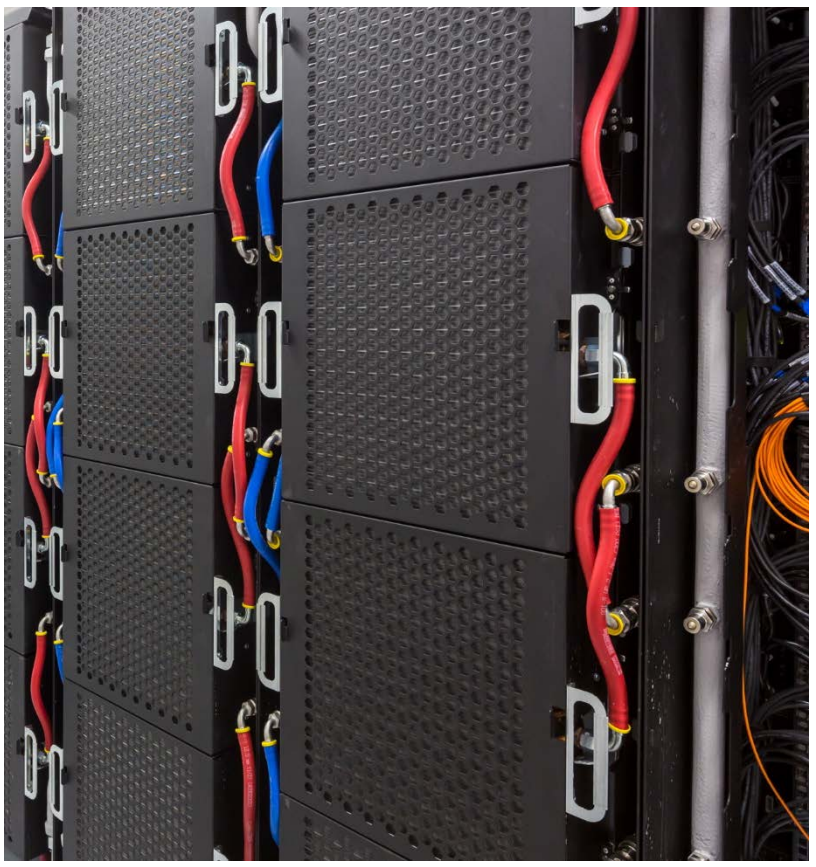


Foto: Severovna superpočítače Solomon, ©VŠB-TUO

Siemens pomáhá zvyšovat kyberbezpečnost v průmyslových podnicích

Autor: Siemens

Kyberzločinci a kyberútoky už pomalu, ale jistě přestávají být doménou futuristických krimi filmů a stávají se nepříjemnou součástí reality běžných firem. Alespoň to naznačují čísla z průzkumu společnosti Kaspersky Lab, podle nichž se s cíleným počítačovým útokem v roce 2017 setkala více než třetina z tisíce dotazovaných firem. Oproti předchozímu roku znamenal tento výsledek nárůst o celých 8 %.

Situace je dnes o to složitější, neboť dnešní průmyslové výrobní závody jsou na digitálních systémech nejenom čím dál závislejší, ale jsou i navzájem stále více propojeny. Výsledkem je, že hackeři pracující pro vlády, zločinecké skupiny či jen tak sami pro sebe, nalézají stále více slabších míst, která jim umožňují provádět sabotáže, průmyslovou špionáž nebo vydírat. A dávno už nepoužívají jen tzv. náhodné znepřístupňování služeb, DDoS, které způsobí zhroucení webových stránek v důsledku bombardování dotazy. Kyberzločinci dnes naopak stále častěji realizují útoky, které jsou „šité na míru“ danému průmyslovému podniku.

V reakci na tuto situaci odborníci ze společnosti **Siemens Industrial Security Services** vyvinuli postupnou obrannou strategii založenou na koncepci „hloubkové obrany“, která umožňuje, aby se průmyslové technologie od společnosti Siemens, ale i zařízení jiných výrobců, mohla průběžně přizpůsobovat novým hrozbám. Nová strategie se skládá ze tří navazujících ochranných funkcí, které se vzájemně koordinují. První v řadě je bezpečnostní systém objektu, kterým je například kontrola fyzického přístupu založeném na biometrickém rozpoznávání. Další v linii obrany je systém zabezpečení sítí, jako jsou výrobní sítě a průmyslová komunikace, pomocí firewallů a virtuálních privátních sítí (VPN). A třetí obrannou vrstvou je systémová integrace, která chrání terminály a automatizační systémy, do nichž lze vstoupit pouze prostřednictvím hesla nebo whitelistového antivirového softwaru, který umožňuje přístup pouze k určitým programům.

Adaptivní bezpečnostní architektura

Bohužel mnoho útoků na průmyslová zařízení nevyžaduje žádné velké úsilí, neboť brány jsou doslova doširoka otevřeny. Stále není žádnou výjimkou, že si zákazníci „zabezpečují“ svá zařízení hesly jako „123456“ nebo „Heslo“. Navíc mnoho podniků si své zabezpečovací systémy pravidelně neaktualizuje. Pokud by měli všichni včas nainstalovány aktualizace antivirových systémů, útoky WannaCry a NotPetya v roce 2018 by pravděpodobně neměly tak devastující účinky.

Z dlouhodobého hlediska ale pravděpodobně nebude takové zabezpečení výrobních závodů stačit. Zřejmě bude nutné přistoupit i nepřetržitému monitorování samotných bezpečnostních systémů. Siemens aktuálně používá pro svá zařízení monitorovací systém, který dokáže rozpoznat až 40 000 indikátorů, které by mohly znamenat kyberútok. Vzhledem k tomu, že ne všechny společnosti si mohou dovolit provádět takto podrobný monitoring, vznikne zřejmě poptávka po těchto službách, které by mohly začít nabízet samostatná bezpečnostní centra. V budoucnu budou pomáhat také adaptivní bezpečnostní architektury, které budou k testování systémů využívat nejnovější data. Kyberzločinci ale umějí používat také umělou inteligenci, takže je pravděpodobné, že boj s nimi bude ještě dlouhou dobu připomínat hru na kočku a myš.

Kybernetické útoky na průmyslové firmy jsou dnes realitou a riziko, že bude průmyslový podnik cílem kybernetického útoku, je stále vyšší. Stejné hrozby, ale platí i pro nemocnice, důležité infrastrukturní body a řadu dalších cílů včetně domácností. A s rostoucím počtem připojených zařízení bude průmysl pro hackery stále přitažlivějším cílem.

Systémy, které zákazníkům nabízíme, jsou vytvářeny tak, aby jejich využití bylo zcela bezpečné. Především se to týká systémů, které pracují s cloudovými řešeními. Zde je dobré si uvědomit, že průmysl nasazuje cloudová řešení, ale IT řešení obecně, s určitým zpožděním ve srovnání například s bankovnictvím, kde je úroveň zabezpečení považována za nejvyšší. Bezpečnost řešení, která nabízí Siemens, jsou ale s těmito oblastmi zcela srovnatelná. Jako příklad můžeme uvést náš otevřený cloudový systém pro průmyslový internet věcí **MindSphere**. Ten nabízí komplexní řešení pro sběr, uchování a vyhodnocování dat s nejvyšší úrovní zabezpečení srovnatelnou s bankovnictvím.

Siemens inicioval vznik Charty důvěry – Charter of Trust

Kybernetická bezpečnost je pro společnost Siemens nejvyšší prioritou. Schopnost dodat zákazníkům produkty a systémy, které obsahují nejmodernější funkce kybernetické bezpečnosti, je v rostoucím digitalizovaném obchodním světě konkurenční výhodou.

Společnost Siemens proto zformulovala deset zásad, které by měly zvýšit bezpečnost digitálního světa a již v roce 2018 iniciovala vznik tzv. **Charty důvěry (Charter of trust),** kterou představila v průběhu **Mnichovské bezpečnostní konference (Munich Security Conference)** a podepsala spolu s osmi dalšími průmyslovými partnery.

Myšlenka závazných pravidel a standardů pro bezpečnou kyberkomunikaci se natolik ujala, že během prvního roku existence se Charta rozrostla na 16 signatářů a připojily se k ní i dvě státní instituce – německý spolkový **Úřad pro informační bezpečnost BSI**, který je jedním z nejvýznamnějších úřadů pro odborníky na kyberbezpečnost, a španělské **Národní kryptologické centrum CCN**, z Rakouska se připojila **Technická univerzita v Grazu**.

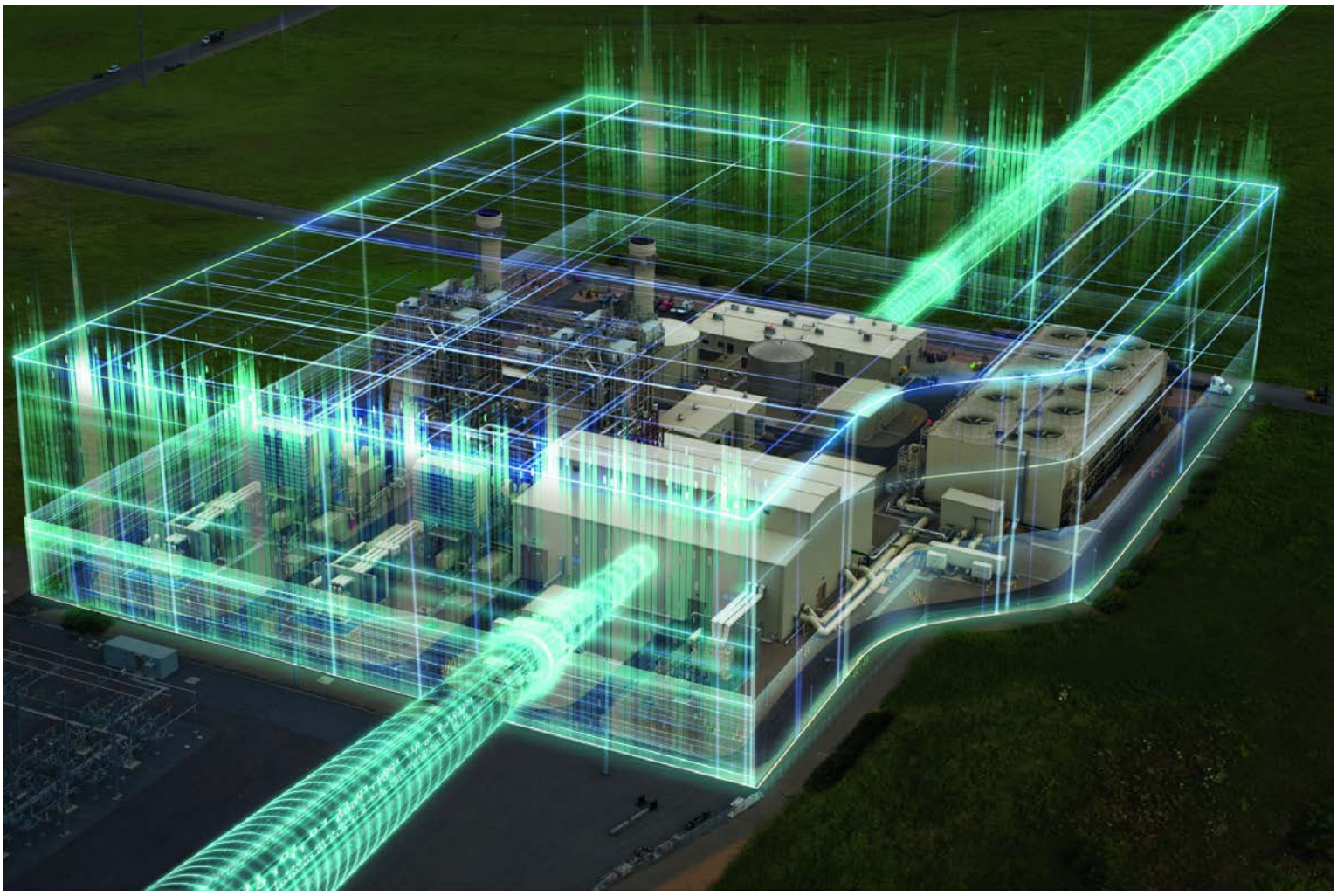
Kromě koncernu Siemens a Mnichovské bezpečnostní konference chartu podepsaly také společnosti **AES, Airbus, Allianz, Atos, Cisco, Daimler, Dell Technologies, Deutsche Telekom, Enel, IBM, NXP, SGS, Total a TÜV Süd.**

Bezpečnost dodavatelského řetězce je jednou z oblastí, jíž se charta intenzivně zabývá. Rizika, která v rámci dodavatelského řetězce přicházejí od třetích stran, se objevují stále častěji a podle **Accenture Strategy** jsou zdrojem 60 procent kyberútoků. Členské společnosti Charty důvěry proto vypracovaly základní požadavky a navrhují jejich zavedení tak, aby se kybernetická bezpečnost stala absolutní nutností v celém digitálním dodavatelském řetězci. Tyto požadavky se týkají všech aspektů kyberbezpečnosti – lidí, procesů a technologií.

Mezi některé z požadavků patří například:

- Data musí být chráněna před neoprávněným přístupem v rámci jejich celého životního cyklu.
- Bude zavedena vhodná úroveň kontroly a monitoringu identity a přístupu včetně kontroly třetích stran, která bude vyžadována.
- Bude zaveden proces, který umožní a zajistí autentizaci a identifikaci produktů a služeb.
- Bude zajištěno pravidelné minimální vzdělávání a školení zaměstnanců o bezpečnostních otázkách.

Členové Charty důvěry dále pracují na metodice založené na posouzení míry rizika, která by pomohla při zavádění těchto požadavků v jejich vlastních dodavatelských řetězcích. Do tvorby metodiky jsou samozřejmě zapojeni i jejich partneři a dodavatelé.



Kybernetická bezpečnost komunikační infrastruktury pro Průmysl 4.0

Autor: Ondřej Ryšavý, FIT VUT v Brně a Pavel Zemčík, FIT VUT v Brně

Tam, kde dříve byla technologická síť oddělena, je dnes požadavek na zpřístupnění jejích prvků a datových zdrojů, včetně řídicích jednotek z IT systémů. Tento požadavek vychází ze samotných principů Průmyslu 4.0, neboť prostředí Průmyslu 4.0 předpokládá propojení operačních technologií, informačních technologií a jejich komunikačních sítí. Přináší ovšem i některá rizika.

To, co na jedné straně přináší příležitost pro zvýšení efektivity výroby a řízení pomocí pokročilé automatizace, a to nejenom na úrovni technologických procesů, může na druhé straně představovat vážné bezpečnostní hrozby. Kybernetické útoky na průmyslové řídicí systémy mají svá specifika a od útoků na běžné uživatele se liší záměrem útočníka, jeho schopnostmi včetně znalostí prostředí OT a cílového prostředí. Sofistikované útoky mají většinou formu kampaně[1], která je realizována v několika krocích s cílem získat nepozorovaně přístup k důležitým zařízením v systému.

Oběť průmyslového kyberútoku - ukrajinská energetická síť

Potřeba komplexní kybernetické ochrany průmyslových podniků se ukázala v plném světle při útoku na ukrajinskou distribuční síť v prosinci 2015[2]. Tento incident způsobil výpadek dodávky elektřiny pro 225 000 koncových odběratelů na dobu několika hodin. V důsledku útoku musely být navíc systémy převedeny do režimu manuálního řízení, než se podařilo obnovit instalaci a nastavení všech řídicích systémů.

Tento útok demonstroval použití různých technik a metod k průniku do chráněného systému a převzetí kontroly. Útočníci nejprve pomocí phishingu získali přístup k zařízením v IT síti, potom za použití malware (BlackEnergy 3) získali přístupové údaje pro vzdálený přístup do OT infrastruktury. A útok dokončili nasazením speciálně napsaného firmware pro koncová zařízení. Takovýto sofistikovaný útok vyžadoval rozsáhlou přípravu zahrnující dlouhodobé sledování cílových systémů a jejich chování. A přestože byl zahájen zvenčí, veškeré následující aktivity probíhaly uvnitř IT a OT prostředí.

Specifika průmyslových systémů komplikují jejich zabezpečení

Prostředí operačních technologií je specifické tím, že vyžaduje vysokou míru spolehlivosti a klade požadavky na šíření informací v reálném čase. Pro správnou činnost systému je nutné, aby se informace o aktuálním stavu v systému dostaly od jednotlivých senzorů včas a poté byly spolehlivě přeneseny až k řídicí jednotce. Umístění invazivních monitorovacích nebo bezpečnostních nástrojů, tak jak je známe z IT prostředí jako jsou například systémy prevence narušení (IDS/IPS) nebo antivirů, je zde proto komplikované.

Aby bezpečnost nekolidovala se spolehlivostí, jsou často bezpečnostní opatření omezena na použití zařízení typu firewall umístěného na síťovém perimetru OT sítě. Tento přístup může do jisté míry ochránit před útoky vně OT sítě, ale je bezmocný vůči aktivitám útočníka uvnitř sítě. Z tohoto důvodu vznikají řešení, která uvažují jako primární bezpečnostní mechanismus prostředky monitorování IT/OT síťové komunikace a detekci odchylek od očekávaného chování.

Systém NetFlow pro vyšší průmyslovou bezpečnost

Fakulta informačních technologií VUT v Brně ve spolupráci s výzkumnými a průmyslovými partnery, jako jsou **Flowmon** a **Masarykova univerzita v Brně**, v rámci konsorcia **Národního centra kompetence pro Kyberbezpečnost**[3] zkoumá nové možnosti zajištění kybernetické bezpečnosti pro konvergované IT a OT síťové infrastruktury. Jedním z projektů realizovaných v rámci Centra je také nový systém pro monitorování a detekci anomálií v OT sítích využívající hloubkovou analýzu provozu a rozšířeného **NetFlow** pro sběr informací o síťových tocích a detekci anomálií.

Systém NetFlow je jedním znejpoužívanějších přístupů pro monitorování IT komunikačních sítí, neboť umožňuje zaznamenávat síťové aktivity na úrovni jednotlivých komunikací mezi síťovými aplikacemi. Samotné NetFlow monitorování provozu ovšem nedokáže poskytnout dostatek informací pro monitorování OT provozu. Například protokol **Modbus/TCP** používá port 502. Při použití tradičního NetFlow přístupu budeme vidět pouze statistické informace o přenosu dat protokolem Modbus mezi HMI a PLC. V případě použití hloubkového zpracování paketů jsme schopni navíc rozeznat jednotlivé prováděné operace, například čtení hodnot od aktualizace firmware v PLC. Takto obohacené NetFlow záznamy již poskytují dostatečné množství informací pro monitorování důležitých aktivit v OT síti.

Anomálie v OT komunikaci napoví, zda se chystá útok

Monitorování OT komunikace, tedy sledování provozu mezi zařízeními OT sítě, umožňuje identifikovat aktivní zařízení a sledovat jejich obvyklé komunikační vzory. Samotné monitorování řídicí komunikace při použití vhodné vizuální reprezentace dokáže poskytnout operátorovi užitečné informace o stavu systému. I v případě jednoduché statistické informace o počtu přenášených zpráv, rychlosti či objemu komunikace je možné identifikovat různé abnormální situace. V případě výše zmíněného útoku byl původní firmware zařízení před zahájením útoku útočníky nahrazen novým obsahujícím škodlivý kód, což se projevilo neobvyklým přenosem dat v OT síti. Monitorování komunikace může být využito pro odhalování případných odchylek od obvyklého vzoru komunikace. Charakteristika komunikace v OT sítích je poměrně předvídatelná a tudíž metody detekce anomálií mohou dosahovat velice přesných výsledků. Většina metod pro detekci anomálií předpokládá vytvoření modelu chování systému, který se sestává z komunikačních profilů zařízení.

Nasazení řešení známých z IT prostředí je obtížné zejména v prostředích s tradičními OT protokoly, neboť existující řešení pro monitorování síťové komunikace mají omezené možnosti monitorování průmyslových komunikačních protokolů. Bezpečnostní experti identifikovali nedostatek viditelnosti v kontrolních systémech jako jeden z největších problémů pro zajištění jejich bezpečnosti. Je zjevně obtížné, ne-li nemožné, chránit jakékoliv prostředí bez porozumění jeho operacím, identifikací existujících zařízení, jejich operačních systémů a dalších procesů v něm obsažených. Monitorování IT sítí je založeno na sběru informací z různých dostupných zdrojů, jejich zpracování a prezentaci v prostředí Security Operation Center (SOC). Vzhledem ke konvergenci IT a OT infrastruktur se od bezpečnostního řešení očekává, že poskytne dostatek informací pro monitorování komunikace v obou prostředích.

[1] https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
[2] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
[3] https://nc3.cz/about-nc3

Obrana před kyber útoky musí být ošetřena i po právní stránce

Autoři: JUDr. Jan Diblík, partner; JUDr. Samuel Král, advokát, HAVEL & PARTNERS s.r.o., advokátní kancelář

Hrozba kybernetických útoků je podstatně častější[1], než si mnoho lidí myslí. Kybernetické útoky se netýkají pouze velkých společností, ale mohou se týkat prakticky kohokoli. Často mají plíživou formu, takže si jich nikdo nemusí všimnout po poměrně dlouhou dobu, dokud nedojde k úniku obchodního tajemství nebo jiné finanční ztrátě. V tomto článku bychom se rádi věnovali několika kybernetickým útokům, které se kterými jsme se setkali v praxi a řešením, která v takových případech připadají v úvahu.

Man in the middle

Jedním z relativně častých druhů kybernetických napadení je tzv. man in the middle[1] útok. Jedná se o situaci, kdy je útočník za použití různých prostředků schopen číst cizí komunikaci, anebo ji dokonce upravovat, případně jinak sledovat činnost na konkrétním zařízení. V těchto případech útočník nejčastěji využívá nedostatečně zabezpečenou Wi-Fi síť, ke které se připojí a přes kterou je schopen sledovat a zachytávat odesílané zprávy. Jedná se například o free Wi-Fi sítě nebo o případy, kdy někdo ponechá standardní tovární nastavení na Wi-Fi modemu. Jelikož útočník po připojení k takové síti zná obsah e-mailové zprávy, kterou konkrétní osoba odesílá, je poté schopen tuto upravit nebo vytvořit zcela změnit a zaslat nic netušícímu adresátovi. Takové emaily se obvykle vyznačují tím, že jsou odesílány z mírně upravené domény nebo že nemají v textu přiloženou předchozí komunikaci. V takových případech by měl adresát zpozornět, jelikož se může jednat o podvržený email.

V našem konkrétním případě útočník zastavil původně odeslaný e-mail a podvrhl jej svým, do kterého napsal falešné informace. Na jejich základě klient udělal nesprávné obchodní rozhodnutí, které ho následně stálo několik milionů korun.

Falešný pocit bezpečí

Další, a zároveň nejčastější, druh kybernetických útoků jsou útoky zevnitř organizace. Náš klient se na obchodním jednání od svého obchodního partnera dozvěděl, že mezi jeho konkurenty koluje obchodní tajemství klienta v podobě inženýrských výkresů jeho výrobků.

Klient chtěl nejprve prověřit možnosti útoku zvenčí, například výše zmíněným způsobem „man in the middle“. Klientovi jsme proto doporučili IT experty, kteří se zabývají kybernetickou bezpečností, aby ověřili zabezpečení infrastruktury provedením penetračních a jiných testů. Ukázalo se, že zabezpečení klienta je v pořádku a pokud by byl útok veden z vnějšku klientovy organizace, musel by to být masivní, velmi sofistikovaný a cílený útok. To se jevilo jako nepravděpodobné a potvrdilo to domněnku klienta, že je dobře zabezpečen.

Proto se pozornost IT expertů obrátila dovnitř organizace, kde hledali buď možnou nedbalost (otevření emailu se spamem, nedodržení bezpečnostních pokynů apod.) anebo úmysl vynést informace. Nakonec se ukázalo, že šlo o čin zhrzeného manažera, který se nedokázal smířit s ukončením spolupráce se společností klienta.

Prevence - nejlepší obrana

Při dnešní úrovni techniky, kdy je velmi obtížné sledovat stopu pachatele v kyberprostoru, je nejlepší obranou proti kybernetickým útokům prevence. Ta má dvě úrovně – technickou a právní, přičemž obě jsou vzájemně propojeny. Technická opatření, pokud nemohou útoku zabránit sama o sobě, mají smysl především tehdy, pokud je budou doprovázet vhodná právní opatření, která zajistí vymahatelnost dodržování opatření technických.

Technická opatření mohou mít mnoho podob - od antivirů, přes auditní logovací systémy umožňující sofistikované sledování činností v rámci organizace, po speciální hardwarová zařízení umožňující odklonění vnějších kybernetických útoků. Před přijetím technických opatření lze určitě doporučit provedení technického auditu, který zmapuje největší zranitelnosti systémů (ať už z pohledu vnější nebo vnitřní bezpečnosti) a doporučí vhodná technická řešení. Mnoho firem v poslední době prošlo podobným auditem v souvislosti s GDPR a závěry tohoto auditu lze obvykle použít jako poměrně robustní základ pro představu o technické prevenci v rámci organizace.

Právní opatření jsou již méně variabilní. Jedná se nejčastěji o interní předpisy vydané zaměstnavatelem a upravující povinnosti zaměstnanců na pracovišti, či doložky do smluv s dodavateli.

„Důvěřuj, ale prověřuj“ je stále aktuální

V případě klientů, kteří se stali obětí útoku typu „man in the middle“, jsme vedle základních technických opatření, jako je například změna hesla na přístupovém bodu Wi-Fi, doporučili také zavedení organizačního opatření spočívajícího v telefonickém ověřování autenticity vybraných důležitých emailů. Toto jednoduché opatření, byť technicky nijak sofistikované, mohlo být realizováno ihned a bez jakýchkoliv nákladů.

Ruku v ruce s tímto technickým opatřením jsme pro klienta vytvořili také interní předpis, který ukládá zaměstnancům, aby u e-mailů, které obsahují definované typy informací, vždy telefonicky ověřili s adresátem e-mailu jeho e-mailovou adresu, prověřili, zda mu e-mail došel, a dále jaký byl jeho obsah. Týká se to informací, jako jsou platební údaje, pokyny k vyplacení částek, ověření identity osob nebo adresy, kam mají být zaslány důvěrné informace klienta a dalších.

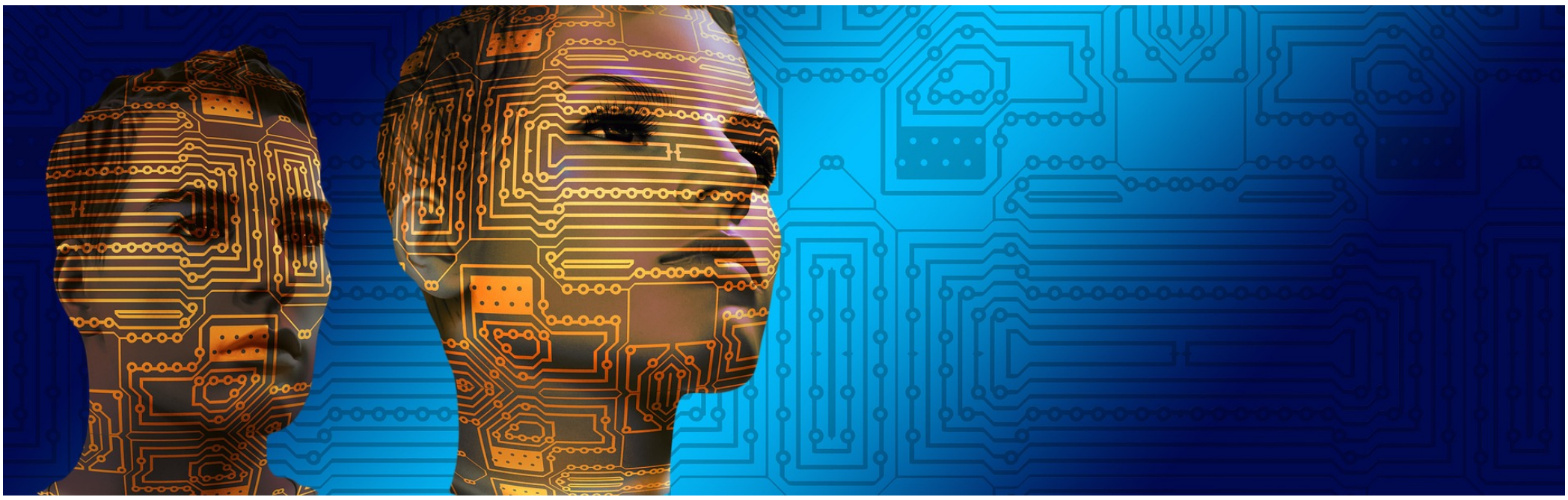
Interní předpis je následně vymahatelný vůči zaměstnancům klienta a ten se může na zaměstnancích domáhat náhrady škody v případě, že vznikne v důsledku jejich porušení takového předpisu[3]. K dodržování takového interního předpisu lze smluvně zavázat i obchodního partnera. Například, aby vás kontaktoval ještě před tím, než provede platbu na číslo účtu, které mu posíláte. Pokud by to neudělal, porušil by smlouvu a vystavoval by se tak smluvní pokutě, pokud byla sjednána, vždy však povinnosti k náhradě škody.

Jak interní předpis, tak dohoda s dodavatelem má zejména motivační charakter. Tedy vést dané osoby, aby se chovaly s určitou mírou obezřetnosti a tím jako vedlejší produkt vytvářely vyšší míru zabezpečení aktiv klienta.

I přes veškeré technologické pokroky je prostý telefonát, na rozdíl právě od e-mailu, stále dobrý způsob k ověření pravdivosti informací.

[1] https://cybermap.kaspersky.com/
[2] https://cs.wikipedia.org/wiki/Man_in_the_middle
[3] Např. viz https://www.epravo.cz/top/clanky/odpovednost-zamestnance-za-skodu-zpusobenou-zamestnavateli-107485.html (29. 4. 2019)

Pokračování článku na následující straně.



V případě klienta, u kterého informace vynesl zaměstnanec, jsme doporučili hned několik technických opatření. Předně instalaci systému umožňujícího sledování vkládání USB disků do počítačů (administrátor systému dostane upozornění, pokud někdo vsune USB disk do počítače), dále zavedení elektronického systému pro logování přístupu uživatelů ke konkrétnímu obsahu[4] (například DMS systémy apod.) a systému pro blokování přístupu k některým internetovým stránkám (jako například sociální sítě, platformy pro sdílení obsahu). Zároveň jsme klientovi navrhli přijetí interní směrnice, která upravuje chování zaměstnanců na pracovních zařízeních a ukládá zaměstnancům povinnost vkládat obchodní tajemství klienta do elektronického systému, viz výše.

Ve vztahu k úniku obchodního tajemství ze strany zaměstnanců se vedle výše doporučených opatření také nabízí zavedení systému monitorujícího aktivitu zaměstnanců na pracovních zařízeních. Takové systémy mají své limity, zejména v oblasti soukromí zaměstnanců – pokud by se například jednalo o systém monitorující odchozí e-maily, neměl by takový systém zachytávat soukromou korespondenci a podobně[5]. Rovněž mohou být poměrně nákladné, ovšem nabízejí řešení v provozech, kde je natolik unikátní know-how, že jeho únik by mohl znamenat ohrožení celého podnikání daného subjektu.

Potrestání útočníka je často nereálné

Jak již bylo zmíněno výše, nejúčinnějšími opatřeními jsou ta preventivní. Jakákoliv následná opatření již tak účinná nejsou, neboť ke škodě již došlo. Na útočníky ze zmiňovaných případů bylo podáno trestní oznámení[6].

V případě útoku „man in the middle“ jsme ovšem toho názoru, že trestní řízení nikam nepovede, neboť najít konkrétní osobu a postavit ji před soud bude téměř nemožné. U druhého případu a zhrzeného zaměstnance je situace již lepší. Ovšem jelikož klient nedisponoval ani jedním z výše uvedených opatření, bude pro policii problematické prokázat, že obchodní tajemství skutečně vynesl konkrétní zaměstnanec. Pokud by klient doporučenými technickými prostředky již disponoval, mohl mít dostatek důkazního materiálu, který by předal policii. Vedle trestního stíhání je rovněž ze strany klientů uplatňována náhrada způsobené újmy, která bude uplatněna v adhezním řízení.

Audit kybernetické bezpečnosti

Se zaváděním preventivních opatření souvisí znalost kybernetických hrozeb klienta a jejich pokrytí technickými a právními opatřeními. Jak už jsme zmínili, audit kybernetické bezpečnosti se vyplatí zejména organizacím, u kterých únik vnitřních informací může znamenat značné škody. Nejdůležitější je vždy zjistit odkud a kam v organizaci putují data, jakými cestami, jaké hrozby existují ve vztahu k takovým datovým tokům, jak je řešit a kolik takové řešení bude stát.

V podobných případech spolupracujeme s IT experty v oblasti kybernetické bezpečnosti, kteří provedou analýzu rizik a doporučí konkrétní technická opatření, spolu s vyhodnocením přínosu pro klienta a se zohledněním výše vstupních nákladů (value for money). V návaznosti na taková doporučení je třeba formulovat příslušná právní opatření (např. směrnice chování zaměstnanců) a uvést je do života. V případě, že subjekt podléhá regulaci zákona o kybernetické bezpečnosti[7], budou tato opatření zpravidla obsahovat celý balík interních a dalších předpisů, které bude nezbytné přijmout.

Proškolení zaměstnanci jsou nejlepší ochrana

Elektronizace podnikání s sebou přináší podstatně vyšší efektivitu, zároveň však také řadu hrozeb, se kterými je třeba se vyrovnat. Bohužel jednou z největších slabin kybernetické bezpečnosti zůstávají nedostatečně poučení nebo nedostatečně důslední zaměstnanci. Kybernetických útoků z vnějšku organizace ovšem také není nezanedbatelné množství a je nezbytné s nimi počítat při obchodní komunikaci.

V návaznosti na výše uvedené bezpečnostní výzvy je třeba přijímat opatření, která rizika minimalizují. Přestože taková opatření musí být vždy šitá na míru konkrétní organizaci, lze obecně doporučit, aby každá organizace disponovala alespoň vnitřním předpisem, který bude shrnovat chování zaměstnanců a dodavatelů na pracovních zařízeních. Vedle právních opatření je rovněž důležité přijmout odpovídající technická opatření, neboť pouze při jejich kombinaci je možné organizaci účinně chránit.

[4] § 562 zákona č. 89/2012 Sb., občanský zákoník ve znění pozdějších předpisů upravuje existenci elektronického systému, pomocí kterého lze dosáhnout toho, že soud by měl pohlížet na takový log jako na pravý, pokud protistrana neprokáže opak, čímž předkládající může splnit své důkazní břemeno.

[5] Viz též https://www.pravniprostor.cz/clanky/pracovni-pravo/monitoring-zamestnancu-prava-a-povinnosti-zamestnavatelu-pri-zpracovani-osobnich-udaju (29. 4. 2019)

[6] U man in the middle pro porušení dopravovaných zpráv dle § 182 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů („**TZ**“), neoprávněný přístup k počítačovému systému dle § 230 TZ a podvod dle § 209 TZ. U zaměstnance pro zneužití informace v obchodním styku dle § 255 TZ.

[7] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů a vyhláška 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

Bulletin Průmyslu 4.0, www.ncp40.cz, ©Národní centrum Průmyslu 4.0, datum publikace 15. 5. 2019

Šéfredaktorka: Alena Nováková, alena.novakova@cvut.cz

Editorka: Alena Nessmithová, alena.nessmithova@cvut.cz