Nová řešení pro zabezpečení průmyslových řídicích, komunikačních a informačních systémů

Útoky na průmyslové řídicí, komunikační a informační systémy jsou stále sofistikovanější. Opatření na jejich obranu proto musí být také stále inteligentnější. Článek popisuje některá komerčně dostupná řešení a trendy v oboru.

Podle studie *Zabezpečení IT pro Industrie 4.0* [1], která byla iniciována německým spolkovým ministerstvem hospodářství a energetiky, je rostoucí propojení strojů v průmyslu předpokladem pro inovace. Ovšem komunikace mezi autonomními zařízeními vytváří nová bezpečnostní rizika – vznikají další místa, na která mohou zaútočit hackeři a jiné kriminální živly.

Zabezpečení IT je podle této studie pro projekty Industrie 4.0[1)] velmi důležité, ovšem mnozí dotazovaní manažeři IT, nejen z Německa, ale z celého světa, shodně tvrdí, že odborníci na počítačovou bezpečnost se k projektům digitalizace dostávají příliš pozdě – bez ohledu na to, že průmyslové firmy stále více trpí kybernetickými útoky s nezanedbatelnými dopady na jejich obchodní aktivity. Podle studie německé spolkové tiskárny cenin Bundesdruckerei GmbH [2], která se při své činnosti zabývá i zabezpečením IT, má velké množství výrobců strojů a zařízení obavy z kybernetických útoků a tyto obavy zpomalují tempo digitalizace výrobků a služeb: 17 % firem z tohoto oboru s tímto tvrzením plně souhlasí, 13 % spíše souhlasí a 27 % souhlasí částečně.

Jak rychle se mění hrozby pro projekty spojené s Industrie 4.0 a jak rychle se zvyšuje jejich úroveň, ukazují publikace BSI (Německého spolkového úřadu pro informační bezpečnost), např. *Situace IT bezpečnosti v Německu a zabezpečení průmyslových řídicích systémů: deset nejvýznamnějších hrozeb a opatření proti nim* [3]. Kromě zákonných požadavků na kritickou infrastrukturu a odpovídajících bezpečnostních doporučení BSI je důležité vyvíjet nová řešení pro zabezpečení IT, která jsou speciálně určená proti rizikům hrozícím v souvislosti se zaváděním Industrie 4. 0.

Systémy průmyslového internetu věcí (IIoT – *Industrial Internet of Things*) v průmyslových podnicích se skládají z mnoha koncových bodů, které je třeba chránit. Bezpečnostních řešení pro Industrie 4.0 je nyní na trhu spousta a označují se jako zabezpečení průmyslových řídicích systémů (*ICS security*) nebo zabezpečení průmyslového internetu věcí (*IIoT security*). Následující příklady ukážou, jak se zabezpečení průmyslových řídicích, komunikačních a informačních systémů vyvíjí.

Aktuální vývoj zabezpečení průmyslových systémů

Dále je uvedeno několik příkladů nabídek zabezpečení průmyslových řídicích, informačních a komunikačních systémů.

Dodavatelé bezpečnostních řešení kooperují s dodavateli systémů IT pro průmysl

Společnosti Kaspersky a BE.services představily nové řešení pro zabezpečení průmyslových automatizovaných procesů: Embedded Security Shield pro programovatelné automaty (PLC – *Programmable Logic Controller*) a průmyslové řídicí systémy (ICS – *Industrial Control System*) [4]. Řešení nabízí ochranu PLC a RTU (*Remote Terminal Unit*), jejichž software byl vytvořen v prostředí Codesys.

Společnosti Honeywell Process Solutions (HPS) a Palo Alto Networks dlouhodobě spolupracují v oblasti kybernetického zabezpečení řídicích systémů používaných v průmyslových podnicích. Cílem je zlepšit zabezpečení komunikačních sítí řídicích systémů pro procesní výrobu (DCS – *Distributed Control System*) a zabezpečení provozní techniky (OT – *Operational Technology*). Řešení kombinuje platformu Palo Alto Networks a systémy pro řízení procesní výroby Honeywell [5].

Průmyslové řídicí systémy získávají speciální ochranu proti malwaru

Společnost CyberArk nabízí Viewfinity, řešení určené pro prostředí ICS, jako součást své sady CyberArk Privileged Account Security [6]. Viewfinity poskytuje ochranu proti malwaru a ransomwarovým útokům kombinací řízení přístupových práv a monitorování aplikací v kritických koncových bodech.

Zabezpečení koncových bodů IIoT

Endian Connect je balíček řešení pro zabezpečení průmyslových komunikačních sítí a systémů vzdálené údržby strojů. Centrálním řídicím prvkem řešení je Endian Connect Switchboard [7]: aplikace, která ovládá a monitoruje přiřazení přístupových práv v síti. Toto řešení umožňuje připojení neomezeného počtu koncových bodů prostřednictvím zabezpečené sítě VPN (*Virtual Private Network*), nezávisle na operačním systému. Jde tedy o řešení vhodné pro projekty vycházející z konceptu Industrie 4.0 i jiných konceptů chytré výroby.

Inteligentní systémy zabezpečení se rozšiřují do oblasti průmyslových IT

Mandiant ICS HealthCheck Service od firmy FireEye [8] umožňuje hodnotit kybernetickou bezpečnost ICS. ICS HealthCheck Report je přehled technických závad, které systém Mandiant identifikoval. Ukazuje na slabá místa a chyby v konfiguraci a vyhodnocuje jejich rizikovost. Poskytuje technická a strategická doporučení odborníkům na IT i OT a je speciálně určeno pro ochranu proti hrozbám cíleným na infrastrukturu ICS.

Shrnutí

Uvedené příklady ukazují stav v oblasti zabezpečení průmyslových řídicích, komunikačních a informačních systémů: „Security 4.0 pro Industrie 4.0“. Poskytovatelé systémů pro zabezpečení musí spolupracovat s dodavateli IT i řídicí techniky a vyvíjet společná řešení. Je třeba zajistit, aby všichni zúčastnění věděli, jaké hrozby se v souvislosti s Industrie 4.0 objevují a jak se jim bránit. To je nezbytná podmínka trvalého úspěchu projektů Industrie 4.0 i dalších projektů spojených s digitalizací výroby. Mnozí dodavatelé systémů pro kybernetické zabezpečení už si to uvědomili a na cestu otevřené spolupráce nastoupili.

Literatura:

[1] *IT-Sicherheit für die Industrie 4.0: Abschlussbericht* [online]. Berlin: Bundesministerium für Wirtschaft und Energie, 2016 [cit. 2020-01-14]. Dostupné z: https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheit-fuer-industrie-4-0.pdf?__blob=publicationFile&v=4

[2] *IT-Sicherheit im Rahmen der Digitalisierung* [online]. Berlin: Bundesdruckerei, 2018 [cit.

[1)] Článek vychází z německého prostředí, proto je v něm používáno označení Industrie 4.0, nikoliv obecnější průmysl 4.0. Německý projekt Industrie 4.0 je jedním z konceptů chytré, propojené výroby, kam patří různé národní varianty „průmyslu 4.0“, průmyslového internetu věcí atd. Ty se od sebe mohou lišit a liší se i jejich požadavky na zabezpečení.

2020-01-14]. Dostupné z: https://www.bundesdruckerei.de/de/studie-it-sicherheit
[3] *Industrial Control System Security: Top 10 Threats and Countermeasures 2019* [online]. Ver. 1.30. Berlin: BSI, 2019 [cit. 2020-01-14]. Dostupné z: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_005E.pdf?__blob=publicationFile&v=7
[4] *Embedded Security Shield (KasperskyOS edition) by Kaspersky and BE.services GmbH* [online]. Moscow: AO Kaspersky Lab, 2019 [cit. 2020-01-14]. Dostupné z: https://os.kaspersky.com/media/KasperskyOS-BEservices-ESS-KasperskyOS-Edition-case-study-En.pdf
[5] *Honeywell And Palo Alto Networks Team To Protect Industrial Control Systems From Cyber Attacks: Press Release* [online]. Houston: Honeywell Process Solutions, 2016 [cit. 2020-01-14]. Dostupné z: https://www.honeywellprocess.com/en-US/news-and-events/Pages/pr23022016-Honeywell-and-Palo-alto-networks-team-up-to-protect-industrial-control-systems-from-cyber-attacks.aspx
[6] MILLS, Duncan. *Introducing CyberArk Endpoint Privilege Manager: Blog* [online]. Petach-Tikva, Israel: CyberArk, 2016 [cit. 2020-01-14]. Dostupné z: https://www.cyberark.com/blog/introducing-cyberark-endpoint-privilege-manager/
[7] *Endian Connect Switchboard Introduction Webinar* [online]. Appiano, Italy: Endian, 2015 [cit. 2020-01-14]. Dostupné z: https://youtu.be/OyQqODRQvIE
[8] *Datasheet: Industrial Control Systems HealthCheck* [online]. Milpitas, USA: FireEye, 2019 [cit. 2020-01-14]. Dostupné z: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/pf/ms/ds-ics-healthcheck.pdf

Thomas Menze, Constanze Schmitz,
ARC Advisory Group

Továrna budoucnosti podle ABB a B&R

V posledních týdnech podzimu na několika akcích prezentovaly společnosti ABB a B&R své vize, představy, zkušenosti a reference týkající se „továren budoucnosti“. Šlo o firemní dny, akce ve spolupráci s NCP 4.0 nebo prezentaci na veletrhu SPS v Norimberku.

B&R je členem skupiny ABB, takže je možné názory obou firem na budoucnost průmyslu považovat v mnoha oblastech za totožné nebo vzájemně se doplňující. Jde především o oblasti spotřeby energií, komunikace, automatizace, robotizace a informačních systémů a o zpracování a využití dat pro řízení a rozhodování.

Neustále platí, že pro úspěšný podnik v minulosti, současnosti i budoucnosti je nutné řešit souvislosti mezi lidmi, stroji, produkty a procesy.

Za základ aktivit 4.0 se považuje komunikace mezi stroji. Tento princip platí ve všech oborech, nejen v průmyslu. Ve stavebnictví, zemědělství i na úřadě. Vždyť servisní roboty se budou používat i v oblasti obchodu, služeb a zdravotnictví a automatizace a digitalizace zasáhne i správní a podnikové procesy – od příjmu objednávek nebo reklamací po sledování jejich vyřizování a komunikaci s druhou stranou.

Komunikaci se všeobecně věnuje velká pozornost. Na nejnižší úrovni se v mnoha případech využívá standard Bluetooth, především pro komunikaci s personálem či údržbou a pro vyhodnocování okamžitých stavů. Pro komunikaci spojenou s rozhodováním, ať už na úrovni lokálního řízení (např. edge), nebo ve vazbě na centralizované či decentralizované rozhodování, především na real-time modely nebo systémy plánování, se bude i nadále využívat průmyslový Ethernet. Pro komunikaci s cloudem, kde může být realizována analýza velkých objemů dat, se v budoucnu bude stále více volit Ethernet v kombinaci s protokolem OPC UA s využitím metod TSN pro zajištění vlastností reálného času. Zde se za velký přínos považuje řešení interoperability a konvergence informačních systémů (IT) s provozní řídicí technikou (OT). Jednoznačně je to příležitost k významnému zvýšení výkonnosti.

Komunikace a její vlastní řízení se běžně chápou jako nedílná součást kompletního systému řízení, včetně bezpečnostních systémů. Pro monitorování chování jednotlivých uzlů v síti a vyhodnocování nestandardních stavů je k dispozici Asset Performance Monitor (B&R).

V továrně budoucnosti se nebudou rozlišovat obory automatizace a robotizace. Již v současné době je robot považován za nedílnou součást výrobní linky, výrobního uzlu, popř. jiné úrovně řízení, je-li využíván v logistice nebo podobných oborech. O tomto přístupu svědčí i organizační změny v obou společnostech, ABB i B&R, v nichž začínají velmi úzce spolupracovat útvary robotizace a automatizace. Ale cesta k naprosté automatizaci výroby v oborech strojírenství, automobilového průmyslu a elektrotechniky – kde je možné říci, že jsou dosavadní výsledky nejlepší – bude ještě dlouhá. Na příkladu továrny na výrobu robotů v Číně, která je na vysoké úrovni robotizovaná a automatizovaná, bylo poukázáno na to, že plných 70 % práce je ruční práce a 30 % práce robotů. Snahou vedení i ostatních zainteresovaných je tento poměr změnit.

Je škoda, že pod průmyslem se ve velké většině případů uvažují pouze strojírenské obory a obory lehkého průmyslu. Ale obě společnosti, ABB a B&R, realizovaly mnoho projektů i v těžkém průmyslu, např. v hutnictví – při kontinuálním lití a válcování oceli, nebo v cementářském průmyslu a výrobě stavebních hmot.

Doménou obou firem je také energetika. Snaha o přístup k této problematice na úrovni doby je oběma společnostem vlastní. Výrobní závod B&R pokrývá 95 % vlastní spotřeby energie ze solárních panelů instalovaných na střechách budov v prostoru závodu a do budoucna se předpokládá plná energetická soběstačnost. Další kroky ohledně energetiky vycházejí z poznání, že 70 % spotřeby energií představují elektromotory. Tedy úspora každého procenta energetických ztrát v elektromotoru má do budoucna velký přínos k celkovému snížení energetické náročnosti. S rozvojem elektromobility význam úsporných, účinných a provozně nenáročných elektromotorů ještě vzroste.

Optimalizace je velkým tématem. Za rozhodující je považováno rozbití velkých sil dat, centralizace dat a jejich analýza pro modely řízení na úrovni vyšších celků výroby a logistiky. Tyto trendy nejsou považovány za protimluv. Jednotlivé technologické uzly i celé soustavy musí být řízeny v reálném čase na nejnižších úrovních řízení, za využití přímé komunikace mezi jednotlivými uzly, lidmi, produkty a procesy. Jde o systémy MES (*Manufacturing Execution System*) a MOM (*Manufacturing Operations Management*), ale rozhodování a řízení s ohledem na spokojeného zákazníka, optimalizaci řízení kvality, logistiky apod. potřebuje analyzovaná data a informace z mnoha zdrojů, zpracovávané v reálném čase a s využitím metod umělé inteligence. Zde je velká budoucnost.

ABB a B&R svým spojením do jedné skupiny dosáhly velké synergie, šetří náklady a síly na vývoj a řadí se k velkým globálním společnostem. Proto je třeba jejich představy o továrně budoucnosti brát velmi vážně. Vycházejí nejen z dostupných metodik, ale i ze zkušeností a referencí a umožňují porovnávat skutečnou situaci v průmyslových podnicích s fundovaným výhledem do budoucnosti.

Radim Adam