**Časopis Automa uspořádal na veletrhu Amper 2014 seminář o kybernetické bezpečnosti**

Přechod od uzavřených systémů založených na specifikacích jednotlivých výrobců k otevřeným systémům složeným ze standardizovaných prvků usnadňuje integraci nových komponent a umožňuje větší flexibilitu výrobních postupů i obměny výrobního parku. Usnadněn je však zároveň přístup nepovolaných účastníků komunikace a jejích narušitelů. Zařízení bez zabezpečení dat nepředstavují jen dveře otevřené pro průmyslovou špionáž, která může ohrozit jejich pozici na trhu. Přinášejí také riziko škody na majetku, nebo ohrožení zdraví a životů osob pracujících v provozu nebo se pohybujících v jeho okolí.

Podat přehled o současných možnostech zabezpečení dat ve výrobních a energetických systémech, o standardech pro kybernetickou bezpečnost a způsobech jejího testování – to bylo cílem semináře, který 20. března 2014 pořádala redakce časopisu Automa v rámci doprovodného programu 22. ročníku mezinárodního veletrhu elektrotechniky, elektroniky, automatizace a komunikace Amper 2014. Hlavním partnerem semináře byla společnost ABB s.r.o.

Po té, co šéfredaktor časopisu Automa, Ing. Petr Bartošík, přivítal posluchače, zahájil seminář přednáškou **Safety versus Security (klasická bezpečnost versus kybernetická) *Ing. Michal Sojka, Ph.D.***, z katedry řídicí techniky FEL ČVUT. Mottem přednášky bylo, že jednou z největších výzev dnešního průmyslu je ve složitých systémech zajistit tzv. *safety* (funkční bezpečnost) i *security (*kybernetickou bezpečnost). Dr. Sojka představil projekt SESAMO a dal posluchačům nahlédnout do problematiky zabezpečení real-time systémů s integrovanou řídicí a informační složkou – jak výrobních tak například leteckých nebo automobilových. Vymezil vzájemně odlišné kultury funkční a kybernetické bezpečnosti a zmínil ty jejich součásti, které jsou při vzájemné integraci v jednom systému nejkritičtější. Poukázal na pokročilost kybernetické bezpečnosti oproti funkční.

Druhá část přednášky byla věnována standardům a možnostem, jak poměrně dobře ošetřenou oblast funkční bezpečnosti rozšířit na sféru bezpečnosti kybernetické. Dr. Sojka zdůraznil důležitost standardů jako zdroje návodů pro argumentaci při plánování systémů komplexního zabezpečení složitých systémů. Na závěr dr. Sojka blíže představil projekty konsorcia SESAMO, zejména projekt Bezpečnosti automobilové sítě CAN a Testování a verifikaci softwarových modulů (AUTOSAR) z hlediska safety a security a kombinaci MaCAN a AUTOSAR.

Druhou v pořadí byla přednáška ***Ing. Michala Andrejčáka*** ze společnosti **ABB s.r.o.**, hlavního partnera semináře, nazvaná **ABB řešení v oblasti cyber security**. Ing. Andrejčák odlišil podnikové IT a průmyslové řídicí systémy a zaměřil se na hlaví typy hrozeb, jimž jsou průmyslové řídicí systémy vystaveny. Následně předestřel řešení všech těchto hrozeb v rámci strategie „obrany do hloubky“ ABB, která je vedena po vrstvách. Dále popsal analytickou metodiku ABB Cyber Security Fingerprint a některé rozšířené služby ABB v oblasti kybernetické bezpečnosti.

***Zdeněk Vrba*** ze společnosti **Invea Tech, a.s.**, zhodnotil v přednášce s názvem **Moderní zabezpečení sítě, aneb co se skrývá v datovém provozu výrobního podniku?** své zkušenosti s nedostatečným zabezpečením sítí v různých typech podniků a následně přešel ke specifikům řídicích systémů ve výrobních podnicích, provozovaných zejména v systému SCADA a zpravidla na starších typech průmyslových počítačů, které jsou o to zranitelnější. Jako cestu k lepšímu zabezpečení představil systémy pro monitorování provozu sítí NetFLow, IPFIX a FlowMon.

V další přednášce se pánové ***Martin Hurda*** a ***Miroslav Kiš*** ze společnosti SIDAT zaměřili na možnosti virtualizace zastarávajících výrobních systémů a představili několik případových studií.

Seminář pak uzavřela přednáška **Bezpečnost informačních a komunikačních systémů podniku** ***Mgr. Miroslava Sedláčka*** z Elektrotechnického zkušebního ústavu, s. p., věnovaná zejména standardizaci v oblasti řízení rizik spojených s kybernetickými hrozbami pro podnikové sítě výrobních systémů v podnicích. Podrobně byl popsán proces ISMS a proces řízení rizik. Velká pozornost byla věnována bezpečnosti řízení informací a opatření pro minimalizaci rizik v rámci podle ISO/IEC 27001. Mgr. Sedláček poukázal také na důležitost vypracování systému managementu incidentů, (tzv. skoronehod) jako užitečného zdroje ponaučení. Závěrečná část přednášky byla věnována konkrétním ukázkám metodologie analýzy rizik.

Seminář přinesl mnoho pohledů na zabezpečení dat, jež dnes musí řešit každá firma, která integruje výrobní zařízení s podnikovými informačními systémy. Kvalitní přednášky poskytly dobrý přehled o této poměrně opomíjené oblasti.

---

Seminář perspektivy automatizace IV – zabezpečení dat v integrované průmyslové výrobě
se konal 20. března 2014 od 9:00 hodin jako součást doprovodného programu veletrhu Amper na výstavišti v Brně, sál P-3
Jednotlivé prezentace jsou ke stažení na webové stránce semináře <http://bit.ly/automatizace2014>

**Hlavní partner:** ABB s.r.o.
**Partneři:** Elektrotechnický zkušební ústav, s.p., SIDAT, s.r.o., SESAMO, Invea Tech, a.s.

**Mediální partneři:** HW.cz, Technický týdeník, Systém OnLine, DPS A-Z, MM Průmyslové spektrum, Sdělovací technika, Elektrika.tv

**Ve spolupráci s:** Českomoravská společnost pro automatizaci, FEL ČVUT Praha, Terinvest, s.r.o., BVV a.s., Českomoravská elektrotechnická asociace ElA.

**Moderovali:** Ing. Petr Bartošík, šéfredaktor časopisu Automa,
Ing. Eva Vaculíková, zástupkyně šéfredaktora časopisu Automa