Čas (26. 3. 2015, Brno, sál P3)	**Přednáška**
9:00 až 9:30	Registrace
9:30 až 10:10	*Thomas Menze, ARC Advisory Group*: **Cyber Security in Industry.** Overview of current cyber risks, precaution and strategies to harden automation systems, actual standards (přednáška bude v angličtině, k dispozici bude vytištěná prezentace v češtině).
10:10 až 10:35	*Jakub Jiříček, Peter Lechman, Palo Alto Networks*: **Nová generace ochrany pro systémy SCADA.** V průmyslu je nutné současně zajistit zabezpečení řídicích systémů i jejich spolehlivost, dostupnost a funkční bezpečnost. Nová generace ochrany pro systémy SCADA si poradí se všemi uvedenými aspekty a spolehlivě oddělí veškerý podezřelý a potenciálně nebezpečný provoz. V přednášce budou uvedeny konkrétní příklady zabezpečení průmyslových komunikačních sítí.
10:35 až 10:50	Přestávka-občerstvení
10:50 až 11:30	*Jevgenij Gončarov, Kaspersky Lab*: **Cyber threads and risks in modern industry.** Presentation about the latest cyber attacks against industrial control systems and infrastructure, their vectors, and defence precautions and measures (přednáška bude v angličtině, k dispozici bude vytištěná prezentace v češtině).
11:30 až 11:55	*Luboš Řádek, Pavel Hejduk, ČEZ ICT Services*: **Konvenční bezpečnostní testy SCADA.** Prezentace shrnuje motivaci a metody zajištění bezpečnosti systémů SCADA ve skupině ČEZ a podrobně se zabývá jejich bezpečnostními testy.
11:55 až 12:20	*Jiří Sedláček, Network Security Monitoring Cluster*: **Zabezpečení podnikových komunikačních sítí**. Aktivní koncept zabezpečení sítě organizace, bezpečné ICT (nejen) podle zákona o kybernetické bezpečnosti, možnosti a nástroje zabezpečení výrobních organizací, zabezpečení ICT krok za krokem
12:20 až 12:45	*Milan Hrdlička, Václav Mladěnka, Monet+*: **Mobilní zařízení jako autentizační nástroj a jeho integrace do systémů**. Mobilní telefon je už mnoho let využíván bankovními institucemi jako nástroj, který má zvýšit úroveň zabezpečení přístupu do jejich internetových aplikací. Masově se využívají především autorizační SMS zprávy. Tato metoda se však jeví nepraktická pro systémy s menším počtem uživatelů. Vznikají totiž provozní náklady na SMS a je nutné uzavírat smlouvy s operátory. V době smartfonů již ale nejsme na SMS vázáni. Příspěvek se zabývá tím, jak využít chytré mobilní telefony vybavené dedikovanou autentizační aplikací k ochraně přístupu do převážně webových aplikací. Bude se zabývat standardy, které jsou v této oblasti využívány a díky nimž lze budovat interoperabilní řešení. Na závěr bude uveden přehled minulých i budoucích technologií, které lze na straně mobilního telefonu použít pro zabezpečení aktivních operací (SMS, SW token, SIM, NFC atd.) a stručně ukázány principy, jejich slabé a silné stránky.
12:45 až 13:05	Přestávka-občerstvení
13:05 až 13:30	*Roman Cinkais, Wincor Nixdorf*: **Biometrie – od designu až po implementaci.** Biometrie je stále častěji využívána jako metoda autentizace, která doplňuje nebo nahrazuje hesla či tokeny. Prezentace rozebere možnosti biometrických systémů a jejich bezpečné implementace pro autentizaci přístupu k průmyslovým řídicím a informačním systémům.
13:30 až 13:55	*Michal Sojka, FEL ČVUT:* **Zabezpečení komunikace na sběrnici CAN.**

	Komunikace v mnoha řídicích systémech je již po desetiletí zajišťována různými typy provozních sběrnic, jako např. CAN. V době jejich vzniku stačilo, aby byly snadno použitelné, dostatečně spolehlivé a měly deterministické časování. V dnešní době, kdy jsou řídicí systémy stále více a více propojené s internetem a začínají se objevovat viry určené speciálně k napadání řídicích systémů, je na místě začít přemýšlet i o zabezpečení na úrovni provozních sběrnic. Problém ale je, že je to často velmi obtížné, neboť tato potřeba nebyla v době jejich návrhu uvažována. Tato přednáška bude zaměřena na možnosti zabezpečení komunikace na sběrnici CAN. Podíváme se na dva protokoly: Message authenticated CAN (MaCAN) a Secure onboard communication (SecOC) definovanou automobilovým standardem AUTOSAR. Oba protokoly se dají použít se stávajícím hardwarem. Zmíněna bude výpočetní a paměťová náročnost protokolů, a to jak při softwarové implementaci, tak při použití hardwarového akcelerátoru kryptografických operací. Uvedena bude i vhodnost použití protokolů pro přenos bezpečnostně kritických dat.
13:55 až 14:20	*Oto Havle, Sysgo:* **Minimalizace kybernetických rizik s platformou PikeOS**. PikeOS je operační systém reálného času, v němž je kybernetická bezpečnost zajištěna přísným oddělením aplikačních domén a řízením veškeré komunikace mezi nimi. Nově byl doplněn o systém zabezpečení Kaspersky Security System, který umožňuje detailně definovat pravidla pro tuto komunikaci a kontrolovat je. Systémy založené na tandemu PikeOS a Kaspersky Security System mohou být používány v bezpečnostně kritických zařízeních v průmyslu i dopravě. Zabezpečení vestavěné přímo v operačním systému nejen zajišťuje potřebnou ochranu, ale také podporuje normální fungování systému nebo aplikace.
14:20 až 14:30	Závěr semináře