

Konference Security společnosti AEC letos nabídla nebývalé spektrum témat

Poslední únorový den proběhl v Praze 27. ročník mezinárodní konference Security 2019. Největší nezávislou akcí svého druhu v České republice uspořádala společnost AEC. Celkem 22 přednášek na téma kybernetické bezpečnosti, rozdělených do dvou paralelně probíhajících sekcí – technické a manažerské, se zúčastnil rekordní počet registrovaných zájemců: 670. Určujícím rysem letošní akce byla široká škála prezentovaných témat; společnou měly vysokou odbornou úroveň a důraz na využitelnost v praxi.

„Na konferenci Security nemají místo marketingově-obchodní prezentace,“ upozornil Tomáš Strýček, výkonný ředitel AEC, a dodal: „Klademe důraz na praktickou využitelnost příspěvků, hlavním cílem naší akce je odborná úroveň jednotlivých přednášek a maximální přínos pro účastníky.“ Podle šéfa pořadající společnosti byl program konference vystavěn i na případových studiích prezentovaných přímo zákazníkům. „Nebojíme se ani představení neúspěšných projektů, aby se ukázala rizika a bylo možné poučit se z chyb,“ upozornil Strýček.

Příspěvky bezmála třiceti bezpečnostních specialistů z České republiky, Slovenska, Řecka, Rakouska, Británie, Izraele, Finska a Německa zahrnovaly oblasti základních principů systematického přístupu k řešení bezpečnosti ve vývoji, zabezpečení mobilních aplikací či praktické ukázky

tzv. etického hackingu. Ostatně právě prezentace ekosystému hackingových nástrojů používaných hackerskou divizí americké NSA v podání Lukáše Antala z pořadatelské AEC



Obr. 1. Pohled do zaplněného přednáškového sálu technické sekce

patřila podle hlasování účastníků k těm, které letos zaujaly nejvíce.

Poutavá byla i přednáška Jana Tomiška ze společnosti Rowan Legal na téma cloudové

bezpečnosti pohledem právníka, včetně adekvátního nastavení smluv. Další zajímavý příspěvek, tentokrát na téma ochrany runtime mobilního bankovníctví, přednesl Petr Dvořák, CEO společnosti Wultra. Velmi invenčně přistupoval k otázce, jak uchopit DevOps z hlediska bezpečnosti, resp. k tématu možnosti využití odpovídajících nástrojů, Dušan Petričko, delegát ze Slovenské spořitelny.

Stejně jako v loňském roce i letos na konferenci vystoupil předseda České pirátské strany Ivan Bartoš, tentokrát s tématem Security Operations Center ve státní správě. Ve své prezentaci se zabýval rezervami a možnostmi řešení bezpečnosti SOC na státní úrovni a upozornil přitom i na problémy týkající se sladění legislativních a bezpečnostních požadavků. Zároveň tematizoval nejasnosti týkající



Obr. 2. Lukáš Antal (AEC) přednášel o nástrojích hackingu používaných agenturou NSA

cí se možné přenositelnosti dosavadních zkušeností mezi komerční a státní sférou.

Součástí konference Security 2019 bylo i množství doplňkových programů, včetně panelových diskusí či workshopů, doprovázených oblíbenou testovací laboratoří. Účastníkům zde byli k dispozici penetrační testeři AEC, pod jejichž vedením si v soutěži Capture the Flag mohli zájemci ověřit své znalosti při plnění stanovených úkolů z oblasti hackingu, crackingu, kryptoanalýzy a zjišťování informací z otevřených zdrojů. Další doprovodnou akcí byla vystavovatelská část konference Expo Hall se stánky jednotlivých partnerů. Novinkou letošního ročníku konference bylo udělení ocenění za nejlepší expozici, které získala společnost ESET.

„Letos jsme zaznamenali další rekordní návštěvnost,“ poznamenal ke konferenci Security 2019 Tomáš Strýček. „Velký zájem nás samozřejmě těší, ale ještě víc než počet účastníků kvitujeme rostoucí kvalitu příspěvků, jejich tematickou šíři a mnohdy i schopnost vystihnout další vývoj a směřování jednotlivých oblastí ICT,“ uzavřel výkonný ředitel AEC.

Igor Čech, AEC a. s.

Kybernetická bezpečnost v průmyslových firmách

Kybernetická bezpečnost v průmyslových firmách má svá specifika. Prioritou zde není jen zabezpečení dat a komunikací, ale také zajištění funkční bezpečnosti a bezpečnosti strojů a zařízení.

Z hlediska průmyslových firem považují za velmi cennou sekci o zabezpečení cloudu a cloudových služeb. To je velmi důležité téma v souvislosti s trendem IIoT, průmyslového internetu věcí.

Důrazné bylo také varování před ransomwarem zaměřeným speciálně na průmyslové firmy. Obětí mohou být zvláště malé a střední firmy, které mnohdy žijí v přesvědčení, že právě ony nejsou pro kriminální živly nijak zajímavé, a proto kybernetickou bezpečnost zanedbávají.

Spolu s Igorem Čechem musím velmi ocenit přednášku o hackingových nástrojích používaných americkou Národní bezpečnostní agenturou NSA. Ačkoliv jde o *white hacking*, který má zabránit kriminálním činům, jen nahlédnout to, jaké nástroje NSA používala před několika lety (o aktuálních nástrojích se nehovořilo) a čeho všeho tenkrát byli hackeři NSA schopní, vyvolává zděšení: Co kdyby se tyto nástroje dostaly do nepovoláných rukou? Uměli bychom na to reagovat?

Osobně se mi rovněž velmi líbila přednáška Davida Pecla, také z firmy AEC, na téma „Next-Gen“ antivirů, ve které shrnul, jaké metody zabezpečení dat se v současné době používají a jak k nim přispívají metody umělé inteligence. Hledal odpověď na otázku, zda „Next-Gen“ antivirus je jen buzzword, nebo skutečně přichází nová generace nástrojů antimalwarové ochrany.

Podle mého názoru patří tato konference zcela jistě k tomu nejlepšímu, co se v oboru kybernetické bezpečnosti každoročně odehrává, a odborníci na zabezpečení dat a komunikačních sítí z průmyslových podniků zde najdou mnoho užitečného pro svou práci.

Petr Bartošík