AEC

TISKOVÁ ZPRÁVA

Hlavním tématem letošní konference Security je kybernetická válka na Ukrajině

Praha 30. května 2022 – Největší nezávislá konference v České republice zacílená na aktuální témata kybernetické bezpečnosti se uskuteční v úterý 7. června 2022 v pražském Clarion Congress Hotelu. Hlavním tématem letos bude válka na Ukrajině. Pořadatelem 28. ročníku mezinárodní akce Security 2022 je společnost AEC, lídr v oblasti IT zabezpečení.

Ruská válka na Ukrajině mění mnohá pravidla. Účastníci letošní konference budou mít jedinečnou příležitost nahlédnout do spleti špinavých triků útočníků ukrajinskýma očima, seznámí se s časovou linkou útoků, včetně přípravných kroků, ale i s překvapivě efektivní obranou. O dosud nezveřejněné detaily kyberzločineckých válečných aktivit na Ukrajině se podělí přední tuzemský analytik.

„Při sestavování náplně konference je pro náš nejdůležitější zejména praktická využitelnost příspěvků, odborná úroveň přednášek a maximální přínos jednotlivých témat pro účastníky," říká Igor Čech, marketingový manažer pořadatelské společnosti AEC, a upozorňuje: „Podmínkou pro prezentaci příspěvků je vedle kvality i jejich nezávislost na marketingově-obchodním obsahu."

Dalším z námětů, které podle pořadatelů v současnosti významně rezonují napříč obory, jsou změny ve vnímání bezpečnosti v kontextu pandemie koronaviru. Řada odborníků je toho názoru, že tradiční chápání bezpečnosti se ve světle nových globálních událostí začíná jevit zkostnatěle a většina firem není na tuto výzvu dostatečně připravená.

Na letošní konferenci nebudou chybět specializované workshopy, ale hlavním tahákem je nabitý a na aktuální problémy zaměřený program doplněný panelovými diskusemi. Obsah programu bude tradičně rozdělený do dvou paralelních bloků: manažerského a technického. Díky tomu si bude moci každý z účastníků sestavit rozvrh podle svých představ tak, aby mu nic zásadního neuniklo.

Pořadatelům konference Security 2022 se podařilo zajistit řadu erudovaných spíkrů. Na akci vystoupí izraelský odborník na kybernetickou válku, znalec právních aspektů kybernetické ochrany firem, analytici zaměřující se na aktuální byznysová rizika zapříčiněná ruskou invazí nebo sociální inženýři, kteří se specializují na zákeřné simulované útoky na tuzemské banky.

„Myslím, že co se týče přednášek, letos se máme opravdu na co těšit. Ale tahle akce už dávno není jen o odborných přednáškách, jakkoli budou zas výjimečné. Stala se významným networkingovým místem a my už se nemůžeme dočkat, až se osobně pozdravíme s kolegy, se zákazníky a s dalšími lidmi z oboru ve skvělé a živé atmosféře," uzavírá Igor Čech.

Zájemci o problematiku kybernetické bezpečnosti budou mít opět možnost osobně se setkat na nejvýznamnější akci svého druhu v České republice po dvouleté přestávce zaviněné pandemií Covid-19. Událost v minulých letech každoročně přilákala více než 600 návštěvníků a řadu kvalitních přednášejících z tuzemska i ze zahraničí.

AEC a.s., Voctářova 2500/20a · CZ 180 00 · Praha
IČ: 04772148
DIČ: CZ04772148

Praha: Voctářova 20a · CZ 180 00 Praha 8 · ☎ +420 226 229 133
Brno: Veveří 102 · CZ 616 00 · Brno · ☎ +420 541 235 466
Bratislava: Prievozská 6 · SK 821 09 · Bratislava · ☎ +421 254 410 283

www.aec.cz

Program konference

M-1. blok: Cyber War
Válka na Ukrajině mění mnohá pravidla. Scénáře globálního vývoje jsou nejasné, ale podnikoví lídři by měli být připraveni čelit novým rizikům. Také Covid-19 přinesl znepokojující trendy, včetně nových postupů a taktik kyberzločinců. Podívejte se na válku v kyberprostoru očima izraelského experta.

T-1. blok: Cloud Security
Jak zajistit, aby důraz na bezpečnost nebrzdil dostupnost a rychlost změn v organizaci? Jaké jsou nejnovější přístupy v oblasti managementu a zabezpečení API? A proč řada firem po celém světě spoléhá na systémy, které je mají ochránit před útoky, proti kterým nebyly navrženy? Jeden blok, tři spíkři, tři důležitá témata.

M-2. blok: Cloud Security
Dokážete ochránit svá data v cloudu šiframi, které odolají kvantovým výpočtům? Zvládnete zabezpečit své koncové body, virtuální stroje a kontejnery za pomoci architektury založené na principu nulové důvěry? Covid-19 nebo válka na Ukrajině – aktuální výzvy se mohou lišit, ale požadavky na bezpečnost jsou překvapivě podobné. Chcete vědět víc? Poslechněte si naše hosty.

T-2. blok: Cyber War
Nahlédněte pod pokličku kyberválky na Ukrajině: časová linka útoků, včetně přípravných aktivit. Obstála by Česká republika lépe? Seznamte se s historií technik a mechanismů útoků od počátku konfliktu a s obranou, která se ukázala být efektivní. A co agresor – jak reálné je odstřižení Ruska od celosvětové sítě? Blok slibuje nejen zajímavé přednášky, ale i hodně živou panelovou diskusi…

M-3. blok: Case Studies
Budování nového produktu a návazných služeb je běh na dlouhou trať. Jaké ponaučení si odnesli autoři case study projektu BankID? A víte, co obnáší krizová připravenost a jak naplánovat smysluplné cvičení? Seznamte se s pohledem expertů, kteří testování realizovali, i s postřehy klienta. A konečně, studie úskalí výběru EDR řešení, tedy klíčová kritéria, důvody volby, způsoby ověření a vyhodnocení.

T-3. blok: Aplikovaná bezpečnost
Pro zabezpečení funkcí před automatizovanými skripty se často používá mechanismus CAPTCHA. Chcete mu lépe porozumět? Naučte se ho překonat. Vývoj moderních aplikací je stále složitější. Znáte tři základní bezpečnostní prvky jejich vývojové praxe? Auditování logů je jako hledání jehly v kupce sena. Zjistěte, jak auditovat prostředí Microsoft Windows a neztratit se v záplavě dat.

M-4. blok: Vendor Risk Management
Velkým problémem IT bezpečnosti organizací je řízení distribuovaného rizika spojeného s třetími stranami. Jak se bránit, abyste proaktivně zvýšili svoji ochranu? Sofistikované útoky kladou vysoké nároky na zabezpečení informačních systémů. Jaké jsou osvědčené postupy řízení dodavatelů v rámci předcházení kybernetických rizik? Odpoví advokát a IT expert v jedné osobě.

T-4. blok: Trendy v informační bezpečnosti
Myslíte si, že jste dostatečně podezíraví? Obstáli byste v případě simulovaných útoků sociálním inženýrstvím, kterým nedávno čelily tuzemské bankovní domy? Tak schválně... Ne každý příspěvek však může edukovat s takovou hravostí. V případě toho o principiálních slabinách v zabezpečení aplikace eRouška sami uvidíte, že ne všechny aspekty hrály ve prospěch nás, uživatelů.

Více informací naleznete na www.konferencesecurity.cz. Zástupci médií, pro vstup zdarma na konferenci nás prosím kontaktujte na pr@aec.cz.

O společnosti AEC

AEC patří již od svého založení v roce 1991 k předním poskytovatelům služeb v oblasti kybernetické bezpečnosti. Kvalita nabízených řešení se opírá o dlouholetou praxi v oblasti informační technologií a ověřené standardy, včetně legislativy EU. AEC pomáhá svým klientům řešit ty nejnáročnější bezpečnostní výzvy dneška a zorientovat se v nových produktech a technologiích. Společnost, mezi jejíž zákazníky patří finanční instituce, podniky z oblasti telekomunikací, utilit, ale i instituce veřejné správy, maximalizuje efektivitu svých opatření tím, že dokáže unikátním způsobem kombinovat přístupy a odbornosti etických hackerů, technologických inženýrů, konzultantů i zkušených auditorů. Vedle toho rovněž disponuje týmy pro specifický servis, jako je forenzní analýza, brandprotection, CSIRT a další, jejichž dostupnost je v České republice stále minimální. Od roku 2019 je AEC členem Aricoma Group, největšího ICT holdingu v regionu Česko-Slovensko. Členové Aricoma Group poskytují komplexní ICT služby pro firemní sféru a coby součást investiční skupiny KKCG jsou základem pro evropskou expanzi ICT aktivit této skupiny. Více se dozvíte na www.aec.cz.