# SECURITY & NETWORKING

## *Kybernetická bezpečnost pod kontrolou*

**PRAHA 11. 9. 2019** | 14. ročník mezinárodní konference o bezpečnosti ICT

COMGUARD security & networking

Společnost **COMGUARD a.s.** Vás srdečně zve na 14. ročník mezinárodní konference o bezpečnosti ICT „Security & Networking Praha 2019“

**MÍSTO** Top Hotel Praha & Congress Centre, Blažimská 1781/4, 149 00 Praha 4

**DATUM A ČAS** **11. 9. 2019, 9.00–17.00 (registrace od 8.30)**

### PREZENTACE ŘEŠENÍ PATŘÍCÍCH DO TOP 10 BEZPEČNOSTNÍCH PROJEKTŮ ZVOLENÝCH DLE GARTNER

- TOP 10 – Nepřetržité adaptivní řízení rizik a zranitelností (CARTA)
- TOP 10 – McAfee MVISION Cloud – komplexní ochrana pro CLOUD
- TOP 10 – „NEXT Generation Sandbox“ kterému žádný malware neunikne
- TOP 10 – WALLIX Bastion – Správa privilegovaných PŘÍSTUPŮ
- TOP 10 – Synchronized Security – příběh pokračuje
- TOP 10 – Moderní ochrana proti phishingu
- TOP 10 – Social Engineering a penetrační testování

### HOSTÉ KONFERENCE

- Ing. Aleš Špidla – Prezident Českého institutu manažerů informační bezpečnosti
- JUDr. Jakub Harašta Ph.D. – Ústav práva a technologií Právnické fakulty MU
- Doc. RNDr. Milan Berka, CSc. – Bezpečnostní manažer na odboru OIT
- Michal Merta, MBA, MSc., LLM – Specialista a poradce v oblasti GDPR
- Mgr. Robert Šefr – odborník na oblast počítačové bezpečnosti

**GENERAL PARTNER**

McAfee™ Together is power.

**PARTNER**

RAPID7 · observe it · lastline™ · Barracuda · SOPHOS · WALLIX TRACE, AUDIT & TRUST

**MEDIÁLNÍ PARTNER**

ChannelWorld FROM IDG · IT Systems www.SystemOnLine.cz

COMGUARD security & networking

**COMGUARD a.s.**
tel. +420 513 035 400

Sochorova 38, Brno
Freyova 27, Praha 9

info@comguard.cz
www.comguard.cz

## Program konference – VELKÝ SÁL

ODBORNÝ PROGRAM

**08:30–09:00**
Registrace

**09:00–09:15**
**Úvodní slovo ředitele společnosti**
*(Karel Klumpner, COMGUARD)*

**09:15–09:40**
**Dostaňte kritické ICT hrozby pod kontrolu pomocí expertní služby ThreatGuard**
Chcete ušetřit čas drahých bezpečnostních manažerů? Nebaví Vás denně procházet desítky webových stránek „security alertů" a CERTů? Nechcete číst o nerelevantních zranitelnostech? Díky odbornému týmu ThreatGuard 2.0 budete mít vždy tyto aktuální informace jednoduše k dispozici až do Vašeho mobilu a dle Vašeho výběru, pak Vás ani Vaši IT infrastrukturu už nic nepřekvapí.
*(Roman Jiráček, COMGUARD)*

**09:40–10:10**
**TOP 10 – Nepřetržité adaptivní řízení rizik a zranitelností (CARTA)**
Zranitelnosti systémů jsou vstupní branou pro malware do sítě a pokud je neudrží společnost na patřičné úrovni, tak i sebelepší další vrstvy zabezpečení mohou přijít vniveč. Některé společnosti tuto problematiku řeší formou jednorázových projektů (Vulnerability Assesment), což problém zranitelností řeší pouze krátkodobě. Představíme si technologii Rapid7 InsightVM pro plnohodnotný management zranitelností poskytující kompletní sadu nástrojů pro řízení zranitelností v organizaci přehledně, abyste se v kvantu hrozeb neutopili, ale ba naopak jimi propluli a zacílili na to nejpodstatnější.
*(Martin Votava, COMGUARD)*

**10:10–10:40**
**Vybrané útoky z celého světa, aneb co vám možná uteklo**
Hackerských útoků, malwarových kampaní a úniků dat probíhá tolik, že často není možné vše detailně sledovat a zjistit, jak to všechno dopadlo. Proletíme společně a na slajdech celým světem, Rusko, Čínu i USA, ponoříme se do hlubin Darknetu a vrátíme se zase zpět. To vše z relativního bezpečí PowerPointové prezentace, ale i tak staneme tváří v tvář některým hackerům (oni budou na fotografii, ale to by neznělo tak dramaticky).
*(Robert Šefr, Whalebone)*

**10:40–11:00**
Přestávka na diskuzi a občerstvení

**11:00–11:25**
**TOP 10 – McAfee MVISION Cloud – komplexní ochrana pro CLOUD**
Velkou novinkou loňského roku byla akvizice technologie Skyhigh, čímž se McAfee stalo lídrem tohoto dynamicky rostoucího segmentu bezpečnosti v cloudu. Společně se tak seznámíme s pojmem Cloud Access Security Broker (CASB) a s důvodem, proč i po přechodu do cloudu mohou bezpečnostní manažeři klidně spát. Dle Gartner CASB patří do TOP 10 security projektů 2019.
*(Michal Mezera, COMGUARD)*

**11:25–11:45**
**TOP 10 – WALLIX Bastion – Správa privilegovaných PŘÍSTUPŮ**
Představení „agentless" technologie na správu / řízení, zabezpečení a monitoring privilegovaných přístupů ke kritické infrastruktuře. Po seznámení se s jednotlivými komponentami se dozvíte o možnostech identifikace privilegovaných účtů, správy jejich přístupových oprávnění, implementace Password Vaultu, generování reportů a logů vhodných pro audit a mnoho dalšího. Řešení patří do TOP 10 bezpečnostních projektů roku 2019 dle Gartner.
*(Lukáš Babčický, COMGUARD)*

**11:45–12:05**
**TOP 10 – „NEXT Generation Sandbox", kterému žádný malware neunikne**
Nejpokročilejší NG sandbox dostupný na celosvětovém trhu, kterému neunikne žádný malware proudící do vaší společnosti skrze email nebo web. Díky své UNIVERZÁLNOSTI se snadno a nenásilně začlení do Vaší infrastruktury a s přehledem nahradí i konkurenční řešení. Ukázka možností praktického nasazení.
*(Jakub Mazal, COMGUARD)*

**12:05–12:35**
**Evoluce nebo revoluce – na co se můžeme těšit v XG Firewall v18?**
Sophos chystá koncem roku vydat zcela novou verzi populárního XG Firewallu, tentokrát s číslovkou 18. Jaké nové funkcionality a změny nás čekají? Dostane se na některé dlouho očekávané vlastnosti? A kam se XG firewall bude posouvat? To vše se dozvíte v naší prezentaci včetně praktických ukázek funkčních beta verzí.
*(Michal Hebeda, Sophos)*

**12:35–13:00**
**Kybernetická cvičení – zahrajte si na „incident" (NATO)**
Kybernetická cvičení jsou v současné době trendem v oblasti zajišťování kybernetické bezpečnosti. Česká republika se každoročně účastní Locked Shields, mezinárodního cvičení pod hlavičkou NATO a dalších cvičení, nebo pořádá cvičení pro orgány státní správy nebo zaměřené na konkrétní sektory průmyslu. Cvičení je však možné uspořádat i vlastními silami nebo s minimální vnější podporou. Přednáška je věnována zejména diskuzním cvičením malého rozsahu. Představuje přidanou hodnotu cvičení a demonstruje dobrou praxi spojenou s pořádáním interních cvičení.
*(Jakub Harašta, Masarykova Univerzita)*

**13:00–14:00**
Přestávka na oběd

**14:00–14:20**
**Monitoring privilegovaných ZAŘÍZENÍ v praxi – nasazení ObserveIT**
Představení technologie ObserveIT – sofistikovaného systému pro audit v podobě videozáznamů a textových logů všech uživatelů přistupujících k monitorovanému zařízení. Projdeme si detailně, jak je možné popsat nestandardní chování uživatelů i jak vypadá následná investigace včetně grafické reprezentace rizikovosti uživatelů dle jejich chování.
*(Radim Kupka, COMGUARD)*

**14:20–14:45**
**Kybernetická bezpečnost v souvislostech zjevných i skrytých**
Jaký dopad má kybernetická bezpečnost na naše rozhodování a hlavně na jeho kvalitu? Jakou cenu mají informace? Jakou motivací jsou vedeni hackeři a jak útok provedou? Jak může kybernetická bezpečnost ovlivnit rozhodování zodpovědného investora? Je na místě zahrnout úroveň kybernetické a informační bezpečnosti do ratingu firmy? A co vzdělání? Kam se kybernetická a informační bezpečnost ubírá? To jsou otázky, na které se Vám pokusí odpovědět Aleš Špidla, prezident Českého institutu manažerů informační bezpečnosti.
*(Aleš Špidla, prezident Českého institutu manažerů informační bezpečnosti)*

**14:45–15:05**
**TOP 10 – Synchronized Security – příběh pokračuje**
Koncept Synchronized Security jsme představili v roce 2016 pod kódovým názvem Galileo. Výměna informací o bezpečnostních hrozbách a automatizované reakce se postupně rozšířily na produkty z kategorií MDM, šifrování, WiFi AP. Jakým způsobem Vám to usnadní práci a kam tento projekt dospěl do dnešních dnů, se dozvíte z naší prezentace doplněné o živé ukázky ochrany pomocí Sync Sec proti kyber útokům posledních dnů.
*(Michal Hebeda, Sophos)*

**15:05–15:25**
Přestávka na diskuzi a občerstvení

**15:25–15:45**
**Systém pro prevenci a detekci průniků (IPS) a jeho využití**
Máte zajištěnou vnitřní ochranu sítě nezávislou na hlavním FW? Umíte detekovat červy šířící se pomocí různých typů protokolů? Víte, že používá speciální signatury zcela odlišné od běžných antivirů? IPS neboli Intrusion Prevention Systems navíc poskytuje snadný přechod z detekce na prevenci, precizně a rychle blokuje hrozby bez zastavení legitimního provozu a tím šetří celkové náklady na ochranu a obnovu systémů. V prezentaci si představíme výhody této technologie a jeho nasazení v praxi.
*(Michal Mezera, COMGUARD)*

**15:45–16:05**
**TOP 10 – Moderní ochrana proti phishingu**
Phising je jednou z nejčastějších cest kompromitace cílového zařízení. Díky technologii Barracuda Sentinel, která je nástavbou emailové brány, dokážete zajistit ochranu proti cíleným phisingovým útokům a vymýtíte phishing z emailových schránek uživatelů. Jelikož nejslabším článkem řetězce je vždy uživatel, Barracuda přichází s proaktivním nástrojem PhishLine zajišťujícím kontinuální edukaci uživatelů na rozpoznání phishingu.
*(Tomasz Rot, Barracuda)*

**16:05–16:55**
**Panelová Diskuze**

**Hosté panelové diskuze:**
Ing. Aleš Špidla – Prezident Českého institutu manažerů informační bezpečnosti
Doc. RNDr. Milan Berka, CSc. – Bezpečnostní manažer na odboru OIT
Mgr. Robert Šefr – Odborník na oblast počítačové bezpečnosti
Michal Merta, MBA, MSc., LLM – Specialista a poradce v oblasti GDPR

**Témata panelové diskuze:**
- Na jaké úrovni je kyberbezpečnost v českých společnostech a jakým směrem by se měla vyvíjet
- Budoucnost 5G sítí a s tím související výzvy v oblasti IT bezpečnosti
- Security Operation Center (SOC) a jeho význam
- Zabezpečení CLOUDových prostředí
- Kybernetická gramotnost ve společnosti

**16:55–17:00**
Tombola a závěr

## Program konference – malý sál

**11:25–11:45**
**Jak správně zabezpečit webové stránky a servery?**
Jste dostatečně zabezpečení proti krádežím citlivých dat nebo útokům typu denial of service? Rychlý rozvoj webových stránek a webových aplikací přináší nejen mnoho nových možností pro interakci s uživateli, ale také nová rizika spojená se slabě chráněnými místy aplikací a protokolů. Návrh řešení pro zabezpečení webových stránek a serverů bude předveden pomocí technologie Barracuda Web Application Firewall.
*(Martin Votava, COMGUARD)*

**11:45–12:10**
**Jednorázová hesla v moderním pojetí**
Používáte bezpečnou autentizaci? Nechcete být omezeni na jedno zařízení a mít univerzální řešení? Představíme si, jaké benefity Vám 2FA přináší, jaké jsou vhodné metody integrace, možné aplikace a systémy, pro které lze technologii SecurEnvoy využít. Projdeme si také typické use-case nasazení a využití produktu SecurAccess, který nabízí jednorázová hesla nejen formou soft tokenu, sms, NFC ale i mnoha dalšími metodami.
*(Radim Kupka, COMGUARD)*

**12:10–12:30**
**Máte pod kontrolou svůj DNS provoz?**
DNS provoz je samozřejmost, který nikoho nezajímá, když funguje. Společnost Whalebone si je ale velmi dobře vědoma, co všechno hrozí, pokud není DNS překlad správně zabezpečen. DNS bývá označováno za telefonní seznam internetu a na první pohled to vypadá, že na něm není co řešit. Reálné útoky ale ukazují, že pokud necháte svůj telefonní seznam jen tak pohozený na stole, útočníci se na něm dokáží pěkně vyřádit. Dokáží přesměrovat část vašeho emailového provozu na své servery, umí si sestavit přímý komunikační tunel i z Vašich nejcitlivějších sítí, ale zároveň potřebují, aby vše správně fungovalo, když kontaktují své servery. Whalebone resolvery Vám dají kontrolu a vhled do dění na síti výměnou za pár minut implementace.
*(Robert Šefr, Whalebone)*

**12:30–12:55**
**TOP 10 – Social Engineering a penetrační testování**
Jsou Vaši uživatelé zodpovědní? Máte slabá místa v infrastruktuře? Na tyto a mnoho další otázek Vám nabídne odpověď řešení Metasploit. Simuluje reálné útoky s cílem najít slabá místa dřív, než je objeví útočník. Nabízí i možnosti jako jsou SmartExploitation, Password Auditing, Vulnerability Verification, Web Application Scanning a Social Engineering.
*(Jakub Mazal, COMGUARD)*

Změna programu vyhrazena.
Těšíme se na Vaši účast,
Tomáš Mačica & tým COMGUARD a.s.
marketing@comguard.cz