SECURITY & NETWORKING

Kybernetická bezpečnost v praxi

PRAHA 12. 9. 2018 | 13. ročník mezinárodní konference o bezpečnosti ICT

COMGUARD security & networking

Společnost **COMGUARD a.s.** Vás srdečně zve na 13. ročník mezinárodní konference o bezpečnosti ICT „Security & Networking Praha 2018“

MÍSTO	Top Hotel Praha & Congress Centre, Blažimská 1781/4, 149 00 Praha 4
DATUM A ČAS	**12. 9. 2018, 9.00–16.30 (registrace od 8.30)**
REGISTRACE	ZDE
HOSTÉ KONFERENCE	Federico Vailati (Rapid7), Patrick Müller, Michal Hebeda a Jiří Kolc (Sophos), Fabian Guter (SecurEnvoy), Szilvia Kele, Nigel Hawthorn a Vladimír Palacka, (McAfee), Piotr Nowotarski (Barracuda), Robert Šefr (Whalebone), Ondrej Kováč (Alison-group), Tomáš Kejha, (Vítkovice IT Solutions), Johan Sajfrt (Unicorn Systems), Viktor Ziegler (Lastline)

VÝMĚNA ZKUŠENOSTÍ Z PRAXE

- CaseStudy – řešení centrálního e-mailu v Moravskoslezském kraji.
- **Reálné zkušenosti s nasazením DLP technologie.**
- Techniky odhalení neznámých hrozeb a následný Threat hunting napříč celou sítí.
- **Jak nastražit past na útočníka a zaměřit se na podstatné události.**
- Případová studie monitoringu kritické infrastruktury.
- **Využití dvoufaktorové autentizace v praxi.**

Z PROGRAMU VYBÍRÁME

- **Hrozby pod kontrolou?** ThreatGuard 2.0 virtuální bezpečnostní manager silnější a výkonnější.
- **Vulnerability management budoucnosti.**
- Inteligentní ochrana perimetru.
- **Sandbox nové generace, kterému žádný malware neunikne.**
- Nové trendy v oblasti SIEM aneb jak vyhovět požadavkům moderního zákazníka.
- **Trendy v oblasti chytré ochrany Vašich endpointů a serverů.**
- Jak se řeší bezpečnost na úrovni DNS.

GENERAL PARTNER

RAPID7

GOLD PARTNER

McAfee Together is power. · Barracuda · SOPHOS · SecurEnvoy A Shearwater Group plc Company · lastline

MEDIÁLNÍ PARTNER

ChannelWorld FROM IDG · IT Systems www.SystemOnline.cz · Reseller Magazine · AVERIA NEWS

HLAVNÍ VÝHRA V TOMBOLE

poukázka na 2000 Kč při nákupu v e-shopu Alza

DISKUZNÍ KLUBY U OBĚDA

Nová služba ThreatGuard
Rapid7
Lastline
SOPHOS
Barracuda
McAfee

DOPROVODNÝ PROGRAM

Přeneste se do světa, kde neplatí gravitace a můžete téměř vše... Třeba si skočit z nejvyššího mrakodrapu. Připravili jsme pro Vás ukázky 3D virtuální reality.

WE ARE VR VIRTUÁLNÍ REALITA PŘÍMO U VÁS

VSTUPNÉ

Při registraci do **31. 8. 2018** a naplnění kapacity do 100 účastníků – ZDARMA.
Po uvedeném termínu a naplnění volné kapacity je vstupné 1 200 Kč (včetně DPH).
Vstup zahrnuje občerstvení, oběd a návštěvu všech přednášek a sálů.

* Pokud se registrovaní, kterým byla zdarma registrace potvrzena ze strany pořadatele, nebudou moci akce zúčastnit, prosíme o odhlášení **do 5. 9. 2018**. Po tomto datu je potřeba zajistit za sebe náhradníka. V opačném případě může být pořadatelem účtován storno poplatek ve výši 1 000 Kč.

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 SECURITY & NETWORKING

ZMĚNA PROGRAMU VYHRAZENA

Velký sál – společný program

8:30–9:00
Registrace a občerstvení + virtuální realita

9:00–9:15
Úvodní slovo ředitele společnosti
Novinky a zajímavosti ze světa IT security
(Karel Klumpner, COMGUARD)

9:15–9:40
ThreatGuard 2.0 – virtuální bezpečnostní manager silnější a výkonnější
Zaměstnávat analytika, který bude vyhodnocovat hrozby a navrhovat technická i procesní opatření, je příliš drahý luxus. Představujeme Vám nový a ještě lepší ThreatGuard 2.0. Uplynul rok od uvedení služby ThreatGuard na trh a nyní přichází verze 2.0, která nabízí nespočet nových funkcionalit a ulehčení pro naše uživatele i obchodní partnery.
(Michal Mezera, COMGUARD)

09:40–10:10
Případová studie nasazení řešení vulnerability manageru (Rapid7)
Rozhodnutí bylo jednoznačné – Rapid7 vyvíjí jednoduché a inovativní řešení pro komplexní výzvy v oblasti IT bezpečnosti. Na rozdíl od tradičního posouzení zranitelností anebo managementu incidentů Rapid7 poskytuje přehled o bezpečnosti Vašich zařízení a uživatelů jak ve virtuálních, mobilních a soukromých, tak i ve veřejných cloudových sítích. Nasazení řešení u SK zákazníka bylo v komplexním síťovém prostředí pro koncové stanice, serverovou infrastrukturu, aktivní síťové prvky i pro industriální zónu s kritickou infrastrukturou.
(Ondrej Kováč, Alison-group)

10:10–10:40
Inteligentní ochrana perimetru
Jaké jsou aktuální problémy, které trápí většinu administrátorů u firewallů? Jaké jsou vize společnosti Sophos? V rámci prezentace si projdeme aktuální novinky poslední verze Sophos SFOS 17.1 a podíváme se na to, co pro nás výrobce v oblasti XG firewallů připravuje v blízké budoucnosti.
(Radim Kupka, COMGUARD)

10:40–11:00
Přestávka s občerstvením + virtuální realita

Po přestávce jsou přednášky rozděleny do 2 sálů

11:00–11:25
Případová studie – řešení centrálního e-mailu v Moravskoslezském kraji
Představení řešení centralizace a poskytování sdílených e-mailových služeb a AntiSpam ochrany pro Moravskoslezský krajský úřad a jím zřizované organizace. Podíváme se, jak Barracuda ochraňuje více jak 10 000 uživatelů a je schopna se přizpůsobit každé ze zřizovaných organizací, které se k centrálním emailovým službám připojily.
(Tomáš Kejha, Vítkovice IT Solutions)

11:25–11:45
SIEM v praxi. Threat Hunting nebo Use Case?
Představíme si přínosy každého z přístupů a požadavky, které jsou kladeny na jeho úspěšné zavedení a provozování.
(Jan Dymáček, COMGUARD)

11:45–12:05
Techniky odhalení neznámých hrozeb a následný Threat hunting napříč celou sítí
Nové hrozby jsou stále více sofistikované a hůře odhalitelné a tradiční antivir je proti nim bezmocný. Pokud už dojde k odhalení útoku, tak je pro bezpečnostní techniky velice složité, někdy i nemožné, zjistit aktuální stav všech strojů a dohledat další nákazu napříč celou sítí. V rámci prezentace si představíme pokročilé nástroje, které nad rámec tradičních AV dokáží odhalit neznámý malware. V případě odhalení je možné v reálném čase vyšetřovat zdroj nákazy, aktuální stav stanic, případně realizovat automatické restriktivní akce pro případ opětovného vypuknutí nákazy v síti.
(Jakub Mazal, COMGUARD)

12:05–12:35
Reálné zkušenosti s nasazením DLP technologie
Nasazení technologie DLP, na rozdíl od nasazení antiviru, není úplně jednoduché a samo od sebe nic nedělá. Na konkrétních příkladech si ukážeme možná rizika a úskalí, která s nasazením a provozem DLP systému souvisí.
(Michal Mezera, COMGUARD)

12:35–13:00
Sandbox, kterému žádný malware neunikne
Nejpokročilejší sandbox na trhu, kterému neunikne žádný malware proudící do vaší společnosti skrze email nebo web. Ukázka možností praktického nasazení.
(Jakub Mazal, COMGUARD; Viktor Ziegler, Lastline)

13:00–14:00
Přestávka na oběd + virtuální realita

Po přestávce pokračují přednášky ve velkém sále

Velký sál – společný program

14:00–14:25
Jak nastražit past na útočníka a zaměřit se na podstatné události
Zjistit přítomnost útočníka ve vlastní infrastruktuře může být nadlidský úkol, buď kvůli absenci detekčních řešení, nebo naopak kvůli zahlcení všemožnými alerty. Rapid7 InsightIDR je produkt, jehož hlavním smyslem je upozorňovat pouze na jednotky relevantních událostí a obratem k nim poskytnout veškeré souvislosti. Kombinace honeypotů, inteligentní interpretace logů a konfigurace infrastruktury a strojového učení umožní odfiltrovat false positives a řešit jen to důležité.
(Jakub Mazal a Martin Votava, COMGUARD)

14:25–14:50
Nová éra Cloud Generation firewallů
V dnešní době, kdy řada zákazníků využívá, nebo se chystá využívat, cloudové služby typu Salesforce, Office365 nebo IaaS, je nezbytné mít zajištěnou bezpečnou konektivitu do datacenter a mít možnost vytvářet dynamické VPN tunely podle aktuální potřeby pro AWS, Azure a další cloudové platformy. Tuto bezpečnost Vám zajistí CloudGen firewall zn. Barracuda, plně vybavený bezpečnostními funkcemi AntiMalware, Cloud Sandbox, IPS, URL Filter, Application Filter, a to i pro nejmenší modelové řady s unikátní TINA VPN a robustní centrální správou.
(Piotr Nowotarski, Barracuda)

14:50–15:10
Cloud Security – Visibility, Control and Security
IT je v dnešní době zasaženo více změnami než kdykoli před tím – Mobilita, Cloud a BYOD již nejsou nové pojmy, ale standardní součást života zaměstnanců a administrátorů. Současně s tím stále vzrůstá počet incidentů a ztrát dat, což si uvědomují nejen společnosti, ale i vlády jednotlivých států, které vnímají potenciální problémy se sdílením dat. Tato prezentace se zabývá nejnovějšími trendy v oblasti zabezpečení cloudu a pokládá si ty nejdůležitější otázky - Jak lze předcházet problémům s bezpečností dat; jak můžeme dosáhnout toho, co uživatelé chtějí a současně snížit rizika a umožnit inovace? Odpovědí je nová akvizice společnosti McAfee – Skyhigh Networks.
(Nigel Hawthorn, McAfee)

15:10–15:30
Přestávka s občerstvením + virtuální realita

15:30–15:50
Trendy v oblasti chytré ochrany Vašich endpointů a serverů
V této prezentaci se dozvíte o nejnovějších technologiích, jež jsou použity v produktech Sophos Endpoint Protection. Můžete se těšit mimo jiné na informace o Deep Learning, Self Isolation a EDR (Endpoint Detection and Response). Nebudou chybět ani praktické ukázky zachycení útoku ransomware.
(Michal Hebeda, SOPHOS)

15:50–16:20
Případová studie monitoringu kritické infrastruktury ve společnosti Penta Investments
Představení technologie ObserveIT a největších novinek, které přišly s verzí 7. Vše bude doplněno o praktické zkušenosti ze společnosti Penta Investments, kde je ObserveIT využíván již řadu let. Podíváme se na motivy volby této technologie, hlavní oblasti, kde je ObserveIT využíván, a praktické dopady na chování zaměstnanců a externistů.
(Martin Votava a Radim Kupka, COMGUARD)

16:20–16:30
Závěrečná diskuze a tombola

Malý sál

11:00–11:25
Využití dvoufaktorové autentizace v praxi
Na reálných příkladech z praxe si v rámci prezentace ukážeme, jak lze využit dvoufaktorovou autentizaci od společnosti SecurEnvoy. Představíme si vhodné metody integrace, možné aplikace a systémy, pro které lze SecurEnvoy využít a jaké benefity Vám 2FA přináší.
(Fabian Guter, SecurEnvoy)

11:25–11:45
Whalebone – bezpečnost na úrovni DNS provozu
DNS provoz je typicky ze stran společností považován za samozřejmost, která funguje, a není potřeba se jí příliš zabývat. Přitom je to centrální bod sítě, na kterém je možné vyhodnocovat komunikaci strojů s externím světem, a pokud je nalezena hrozba, je možné ji i zastavit. Zároveň se DNS protokol stal populárním kanálem útočníků na obcházení tradičních síťových bezpečnostních prvků. Whalebone kombinuje jednoduchost nasazení a správy, úplnost pokrytí síťového provozu, účinnost ochrany proti hrozbám a kompletní přehled nad DNS provozem pro forenzní účely. Přijďte se podívat na živou ukázku řešení.
(Robert Šefr, Whalebone)

11:45–12:10
Exfiltrace dat na úrovni DNS protokolů
Dle průzkumů společností zabývajících se bezpečností IT, je DNS jedním z top protokolů, jak z pohledu cílení útoků, tak úniků informací. Představíme si klíčové vlastnosti technologie Infoblox a následně se zaměříme na unikátní integrované bezpečnostní funkce na úrovni DNS. Součástí bloku bude také živá ukázka z Kompetenčního centra demonstrující možný únik dat pomocí validních DNS dotazů.
(Radim Kupka a Petr Konečný, COMGUARD)

12:10–12:30
SOPHOS ucelená rodina produktů, která dává smysl
Partner Unicorn nám v rámci prezentace představí reálný přínos nasazení Sophos Synchronized Security v Nemocnici Trutnov. Projdeme si důvody, které vedly zákazníka k výběru technologií od společnosti Sophos. Nakonec se dostaneme k tomu, jaké problémy se podařilo vyřešit po implementaci pokročilých technologií na ochranu koncových stanic, zabezpečení perimetru sítě a access pointů.
(Johan Sajfrt, Unicorn Systems)

12:30–12:55
Nové trendy v oblasti SIEM aneb jak vyhovět požadavkům moderního zákazníka
LogRhythm UEBA (User and Entity Behavior Analytics) přináší rozšířený bezpečnostní monitoring hrozeb cílících na uživatele napříč spektrem známých i neznámých hrozeb, použitím mnoha typů analýz a scénářů, využívajících kontrolovaného i nekontrolovaného machine learningu. LogRhythm UEBA umožňuje Vašemu bezpečnostnímu týmu rychlou detekci a reakci, a následně neutralizaci hrozeb. Platforma LogRhythm Threat Lifecycle Management zahrnuje GDPR Compliance modul, který pokrývá 16 technologicky zaměřených článků GDPR, což usnadňuje naplnění této směrnice. Jako benefit získá uživatel spoustu předkonfigurovaného obsahu včetně pravidel, alertů a reportů.
(Martin Votava, COMGUARD)

Změna programu vyhrazena