# Cyber Security 2021

19. října 2021 / 9:00 / Hotel Don Giovanni Vinohradská 157a, 130 20 Praha

## Program akce

## Hlavní blok

**9:00 - 9:10** **Úvodní slovo**

Jan Mazal

**9:10 - 9:40** **Firemní bezpečnost za časů vzdálené práce**

Vítězslav Šantrůček - AVAST Software

Pandemie změnila styl práce nás všech a nakladla velmi specifické požadavky na zaměstnance i zaměstnavatele.
V přednášce si shrneme, jaké změny pracovního prostředí nastaly v sektoru malých a středních firem, ukážeme si možné dopady hybridního režimu na firemní zabezpečení a budeme se zabývat i způsoby řešení potřeb zabezpečení malých a středních firem s využitím jak interních, tak externích zdrojů.

**9:40 - 10:10** **Útoky Account Take-Over: Jak eliminovat webový fraud**

Jiří Doubek - F5 Networks

V roce 2020 bylo globálně odcizeno 1,8 miliardy uživatelských jmen a hesel. V kombinaci s útočnou silou automatizačních nástrojů a botnetů se snaží útočníci tato kompromitovaná data zneužít. Cílem útočníka je napodobit zařízení legitimního uživatele a jeho chování, úspěšně prorazit existující kyberochranu a převzít účet uživatele s cílem odcizit citlivá data firmy nebo peníze uživatele. Na prezentaci se dozvíte, jak chránit vaše aplikace před fraudem, jak získat přehled o struktuře provozu a útocích, a také jak zlepšit uživatelskou zkušenost pomocí nástrojů behaviorální biometrie.

**10:10 - 10:40** **Budování dostupné kybernetické bezpečnosti**

Jindřich Šavel - Novicom

Představení cesty vedoucí k funkční a nákladově dostupné kybernetické bezpečnosti, která se opírá o sdílený bezpečnostní dohled postavený na principu aktivního SOCu. Dozvíte se, jak Novicom nástroje pro DDI/NAC (ADDNET), Logmanagement/SIEM (ELISA) a visibilitu assetů (BVS) podporují koncept Aktivního SOCu a jaké jsou praktické zkušenosti s jejich nasazováním ve veřejném sektoru i v privátní sféře. Bude představena rovněž novinka určená pro manažery kybernetické bezpečnosti, kteří hledají nástroj pro řízení procesů kyberbezpečnosti a zajištění prokázání legislativní shody KIS nebo VIS.

**10:40 - 11:00** **Coffee break**

**11:00 - 11:30** **Migrace do Office 365 otevírá další bezpečnostní otázky, které nesmí být podceňovány**

Roman Přikryl - System4u

Nástroje Office 365 jsou hlavní důvod, proč zákazníci se službami Microsoft 365 začínají.
S těmito nástroji koncoví uživatelé pracují a tím se otevírá velice důležitá oblast bezpečnosti pro všechny uživatelské přístupy, firemní zařízení a firemní data. Na řadu přichází oblast Enterprise Mobility & Security, která řeší přístup ke službám Microsoft 365 a zabezpečení dat, která jsou v Microsoft 365 uložená.

**11:30 - 12:00** **„Oni neví, že my víme“, problematika detekce a blokace cílených útoků bez využití malwaru**

Václav Zubr - ESET software

O vyřazení firmy z provozu po zašifrování útočníky můžeme z médií slyšet téměř každý týden. Co už se většinou nepíše je, že zašifrování bývá až finální fáze celé operace. Útočníci jsou v síti oběti často i týdny a nepozorovaně kradou interní data. Jak je možné, že anti-malware produkty nic nedetekují? A jak takové útoky odhalit a účinně blokovat? To vše včetně reálné simulace takového kybernetického útoku a jeho detekce si ukážeme na přednášce.

**12:00 - 12:30** **Včasná detekce a reakce na bezpečnostní hrozby – potřeba nebo luxus?**

Miloslav Cahlík - Auriga Systems s.r.o

Kybernetické hrozby a útoky již dávno nejsou jen ojedinělou záležitostí, ale nevyhnutelnou realitou ve světě vzájemně propojených zařízení, cloudu, mobilních aplikací a internetu věcí. Naše data a zařízení jsou cílem i prostředkem pro velký business, organizovaný zločin, útoky znepřátelených států, ale i zájem mnohých nahlížet do soukromí jiných. Lze vůbec ještě v takto exponovaném prostředí efektivně rozpoznat a včas reagovat na sofistikované útoky? A jak se mění tradiční model zabezpečení ve světě cloudu a internetu věcí? Na konkrétním příkladu z praxe si ukážeme efektivní využití technologie McAfee EDR v kombinaci se službou asistenční podpory Auriga Systems.

**12:30 - 13:00** **Potřeby hybridního pracoviště a jeho zabezpečení**

Martin Januš - MyQ

Svět se změnil a pojmy jako hybridní nebo digitální pracoviště již nejsou buzzwordy, ale realitou dneška. MyQ Roger je softwarovou odpovědí na tyto změny s cílem maximálně zjednodušit práci s dokumenty jeho uživatelům pracujícím z nejrůznějších prostředí – od tradiční kanceláře přes práci na cestách až po tu z domova. Pochopitelně nezapomíná na bezpečnost, a to jak tu digitální, tak dokonce i fyzickou.

**13:00 - 14:00** **Oběd**

**14:00 - 14:30** **Jak se připravit na obnovu po úspěšném útoku, aneb „Štěstí přeje připraveným“**

Petr Diviš - DELL Technologies

I při vynaložení veškerého relevantního úsilí může být ochrana překonána, data odcizena, modifikována, smazána. Ukážeme si jak se připravit na danou událost za pomoci technologií a postupů od Dell Technologies. Jak zajistit obnovu kompromitovaného systému v definovaném čase obnovy? Řešení pro business continuity a data protection je často potřeba přizpůsobit novým požadavkům a zabezpečit je proti zranitelnosti. Přednáška bude pojednávat o principech, které umožní návrh těchto řešení jako datového ostrova, odolného proti napadení.

**14:30 - 15:00** **30 odladěných vrstev ochrany v akci aneb „ušetřete lidské zdroje a poznejte opravdový pocit bezpečí“**

René Pospíšil - IS4 security/Bitdefender

Výzvou dnešní ochrany IT je jak zvládnout nároky na speciální lidské zdroje a provozovat stále složitější bezpečnostní řešení bez navýšení lidských zdrojů. V živé ukázce uvidíte jak Bitdefender Gravity Zone Ultra chrání pomocí plně automatizované detekce EDR a EPP jedním agentem v jedné přehledné lokalizované konzoli správy. Dozvíte se dále jak se můžete pojistit proti ransomware útokům z nechráněných strojů a automaticky obnovit zašifrovaná data. Ušetříte vaše lidské zdroje a snížíte vaše provozní náklady.

**15:00 - 15:30** **Veřejná data - víte o nich a umíte je využít?**

Kamil Jelínek - eLegal advokátní kancelář

Veřejný sektor získává a zpracovává obrovské množství informací – hodnocení efektivity těchto procesů ponecháme stranou. Přitom právě data jsou v dnešní době fakticky pro úspěch v podnikání klíčovou a zpravidla i drahou komoditou – využití dat veřejného sektoru je proto velmi zajímavou variantou k získávání dat náročnou vlastní cestou. Oblastí, kde lze data veřejného sektoru využít je celá řada – mimo jiné i oblast kyberbezpečnosti. Přístup k veřejným datům pak může snížit nároky a zejména náklady na personál, snížit rizika spojená s únikem dat a umožnit efektivnější a rychlejší vznik nových technologických projektů. Ne vždy však veřejný sektor data poskytuje dobrovolně. Přednáška se tak zaměří na následující:
Proč by Vás data veřejného sektoru měla zajímat?
O jaká data se jedná a kdo je má?
A hlavně – jak se k obrovskému množství dat veřejného sektoru dostat a jaké právní nástroje k tomu lze použít?

**15:30 - 16:00** **Antivir nestačí: vrstvená ochrana a její zavedení pro malé a střední organizace**

Jiří Zlámal - AVAST Software

Útoky cílené na malé a střední organizace se stále vyvíjí, jejich počet nadále stoupá. Výraznou roli hraje neustále stoupající hodnota dat, které společnosti potřebují ke svému provozu, ze kterých se stává atraktivní terč pro kyberzločince. Velké společnosti jsou většinou obeznámené s riziky které dnešní online prostředí přináší, a za pomoci významných investic se snaží chránit. Jak ale efektivně ochránit malou či střední organizaci, která má často omezené zdroje, jak finanční, tak personální? Podíváme se jaké řešení může Avast nabídnout prostřednictvím platformy Avast Business Hub pro jednoduché a efektivní, několikavrstvé zabezpečení organizací.

**16:00 - 16:30** **Coffee break**

**16:30 - 17:00** **Jak útočníci pronikají skrze vícefaktorové ověřování (2FA/MFA)**

Martin Haller - PATRON-IT

Při připojování k firemní síti přepisujeme kódy z SMS, schvalujeme push notifikace či zadáváme PIN k čipové kartě. Míra zabezpečení vzrostla, kybernetických incidentů ubylo a kyberzločinci stojí u úřadu práce frontu na rekvalifikační kurz. Ne, dělám si srandu. Kyberzločinci se samozřejmě adaptovali a já vám ukáži, jak.

**17:00 - 17:30** **Informace, data a služby z temné strany internetu**

Daniel Hejda - Cyber Rangers

Cílem mé přednášky je seznámi účastníky s temnou stranou internetu. V rámci našich research aktivit jsme provedli nákup některých služeb na DarkWebu a představíme vám co je a není možné na internetu koupit. Taktéž v rámci přednášky zhodnotíme, jak je náročné, pro běžného smrtelníka a IT znalého člověka, nakoupit takové služby a jaký může být dopad při jejich využití útočníkem. Během přenášky se také podíváme na některá nechvalně známá internetová fóra kam je denně uvolňováno obrovské množství odcizeného obsahu a nahlédneme pod pokličku botnetovým službám.

**17:45 - 18:20** **Tombola**

**18:20** **Networking a předpokládaný konec konference**