Cyber Security 2022

20. října 2022 / 9:00 / Hotel Don Giovanni Vinohradská 157a, 130 20 Praha

Program akce

 V tuto chvíli pro vás zajišťujeme ty nejlepší řečníky, program budeme průběžně doplňovat.

Hlavní blok

9:00 - 9:10 **Zahájení konference**

Jan Mazal

9:10 - 9:35 **Ochrana kritických dat a jejich obnova po úspešném kybernetickém útoku**

David Průša - DELL Technologies

Víte o tom, že každých cca 11 vteřin proběhne na zemi úspěšný kybernetický útok? Ukážeme Vám řešení, která Vám pomohou ochránit Vaše kritická data a usnadní obnovu Vašich dat po úspěšném kybernetickém útoku.

9:35 - 10:00 **Přednášet bude zástupce společnosti Datasys Pavel Štros**

10:00 - 10:25 **Covid urychlil i změnu v legislativě EU. Co máme v následující době čekat, co přináší NIS 2 a jak se na ni připravit?**

Kateřina Hůtová - SoftwareONE Czech Republic

NIS 2 přináší pro mnohé členské státy EU velké změny v informační bezpečnosti. Jak konkrétně se to bude týkat České republiky? Na co NIS 2 klade největší důraz, na koho všeho se bude tato legislativa nově vztahovat a jaké z toho plynou pro tyto subjekty povinnosti?

10:25 - 10:55 **Coffee break**

10:55 - 11:20 **Přednášet bude zástupce společnosti Eset**

11:20 - 11:45 **Lze účinně zastavit probíhající útok a zabránit tak tomu nejhoršímu?**

René Pospíšil - Bitdefender

V přednášce se dozvíte, jak lze účinně zabránit šíření probíhajícího útoku a minimalizovat tak škody. Seznámíme Vás s tím, jaká základní doporučení a praktické kroky pomůžou dostat situaci v praxi rychle pod kontrolu. Prozradíme Vám také, co je potřeba preventivně udělat proto, abyste se dokázali proti útokům efektivně bránit, a jak můžete efektivně navýšit odolnost vašeho IT.

11:45 - 12:10 **Přednášet bude zástupce společnosti ANECT**

12:10 - 12:35 **Přednášku brzy upřesníme**

Miroslav Knapovský - LOGmanager

12:35 - 13:35 **Oběd**

13:35 - 14:00 **Přednášet bude zástupce společnosti Progress**

14:00 - 14:25 **Bezpečnost provozu aplikací v kontejnerech**

Martin Zikmund - SUSE

Dnes velmi populární způsob vývoje a následného provozu aplikací v kontejnerech sebou přináší i nové výzvy z pohledu bezpečnosti. Jakým způsobem zajistit bezpeční provoz aplikací běžících v kontejnerech? Kde jsou úskalí a slabá místa? Představíme si řešení NeuVector od společnosti SUSE, které řeší bezpečnost provozu aplikací v rámci Kubernetes a detekci nových zranitelností.

14:25 - 14:50 **Alternativní způsob řešení problému nedostatku odborníků kybernetické bezpečnosti**

Jindřich Šavel - Novicom

Nároky na komplexní zajištění kybernetické bezpečnosti se neustále zvyšují. Novicom CCM (Cybersecurity Compliance Management) je nástroj, ve kterém budou mít manažeři kybernetické bezpečnosti svou agendu jednoduše a přehledně pod kontrolou s plnou podporou odborníků pro případ potřeby. Novicom CCM – kybernetická bezpečnost jednoduše a pod kontrolou.

14:50 - 15:15 **Systémy pro správu agend souvisejících s kybernetickou bezpečností, digitalizací procesů, řízení požadavků napříč celou organizací a technickou evidenci ICT majetku včetně automatických detekcí HW a SW**

Jan Chalupa - ALVAO, Lubomír Karas - ALVAO

ALVAO Service Desk je systém pro moderní organizace a IT oddělení, která potřebují spolehlivě řídit veškeré úkoly. Jedná se o systém vyvíjený podle světových procesních standardů pro řízení poskytování služeb (ITSM/ITIL). Díky tomu je ALVAO systém vhodný pro řízení IT, ale úspěšně v něm můžete řídit i jiná servisní oddělení (typicky HR). S Alvao Service Desk snadno vydefinujete služby, které poskytujete, a uřídíte i složité úkoly a jejich řešení podle daných procesů.
ALVAO Asset Management je informační systém umožňující organizaci zavést efektivní správu veškerého počítačového i ostatního majetku spadajícího pod správu oddělení ICT. Pomáhá pracovníkům ICT oddělení v řešení a zdokumentování každodenních operativních úkolů a ve sdílení a údržbě informací spojených s IT infrastrukturou. Poskytuje důležité informace pro plánování obnovy IT prostředků a přípravu rozpočtů. Napomáhá v řízení podnikatelských rizik právního či regulačního postihu spojených s užíváním nelegálního software ve společnosti.
Oba systémy jsou vzájemně integrovány.
Systémy jsou velice efektivní při řešení agend souvisejících s problematikou kybernetické bezpečnosti včetně případné certifikace dle ISO 27000 a hodnocení a evidence aktiv dle Vyhlášky č. 82/2018 Sb. Příloha 1. Na nákup a implementaci systémů je možno využít aktuálně vyhlášené dotační programy.

15:15 - 15:45 **Coffee break**

15:45 - 16:10 **Přednášet bude zástupce společnosti Thales**

16:10 - 16:35 **XDR: endgame pro útočníky nebo infinity war pro obránce?**

David Pecl - Security Avengers

XDR je nové buzzword nahrazující EDR. Čím dál častěji můžete od výrobců slyšet, že už nemají jen EDR, ale právě XDR. Pojďme se společně podívat, co to vlastně XDR je a co by takové řešení mělo poskytovat za funkce navíc oproti „standardnímu“ EDR. Jaká řešení na trhu jsou opravdu XDR a jaká se tak pouze prezentují? Jaký je v praxi rozdíl mezi investigací s pomocí SIEMu a s pomocí XDR? A pomůže nám XDR efektivněji zastavit útoky mířené proti naší organizaci?

16:35 - 17:00 **Phising — jak na testování a školení zaměstnanců?**

Dominik Hádl - Monstarlab

Neznámých škodlivých zpráv na pracovní účty zaměstnanců chodí spousta. Stále méně je však jisté, že je dokáží všechny rozpoznat. Jejich podoba je totiž čím dál více sofistikovaná. Proto je pro všechny (nejen) IT firmy důležité, aby své zaměstnance školily a vzdělávaly o tzv. phisingu. Tato forma útoku, kdy se škůdce snaží vydávat za důvěryhodnou osobu, a získat tak citlivá data zaměstnance, může firmě způsobit velké potíže.

17:00 - 17:30 **Tombola**

17:30 **Předpokládaný konec konference**