

# ICT ve zdravotnictví 2023

21. února 2023 / 9:00 / Hotel Don Giovanni Vinohradská 157a, 130 20 Praha

## Program akce

### Hlavní blok

- 9:00 - 9:10 Zahájení konference**  
Jan Mazal
- 9:10 - 9:35 Přednášet bude zástupce společnosti DELL Technologies**
- 9:35 - 10:00 Přípraveni na útok? Jak efektivně využít nejrozsáhlejší a volně dostupnou databázi útoků?**  
Petr Mojžíš - ANECT  
O tom, že zdravotnictví je terčem kybernetických útoků není pochyb. Jak můžou takové útoky vypadat? Známe techniky a taktiky, které útočníci používají?  
Kybernetické útoky jsou našťastí předmětem zkoumání řady odborníků a činnost významných skupin, které za nimi stojí, je kontinuálně dokumentována. Nejrozsáhlejší a volně dostupnou databází „útoků“ je MITRE ATT&CK®. Obsahuje informace od počáteční rekognoskace terénu útočnickem, až po jeho finální útočnou akci, např. ransomware.  
Jak se na útoky připravit? Začneme tím, jak dohnat informační náskok útočnicků a jak účinně vzdělávat uživatele, přes bezpečnost informačních systémů, sítí, koncových stanic, ve které je klíčovým slovem „nulová důvěra“, až po schopnost správně reagovat na bezpečnostní incident.
- 10:00 - 10:25 Jednoduchá a efektivní správa počítačů je jeden z pilířů úspěšné digitalizace také ve zdravotnictví**  
Tomáš Pácal - WISPER  
Instalace a aktualizace stolních počítačů nebo notebooků je nikdy nekončící, časově náročná činnost. Efektivní řešení této problematiky umožní se věnovat důležitějším úkolům IT oddělení. Pro usnadnění správy koncových zařízení je tradiční Virtuální Desktop (VDI) možným řešením, ale bývá většinou značně náročný na novou infrastrukturu a tím nebývá nákladově přívětivý. Řešení ceBox Workspace spojuje výhody centralizované administrace VDI a výpočetního výkonu klasických stolních počítačů nebo notebooků. Zní to zvláště? Dost možná, ale představíme Vám řešení, které nevyžaduje masivní serverovou nebo cloudovou infrastrukturu, ale využívá výpočetní výkon stávajících počítačů a umožňuje komplexní monitoring a správu.
- 10:25 - 10:55 Přestávka**
- 10:55 - 11:20 Úloha Národního centra elektronického zdravotnictví ve světle Národního plánu obnovy**  
Martin Zeman - MINISTERSTVO ZDRAVOTNICTVÍ  
V roce 2022 znovuzřízené Národní centrum elektronického zdravotnictví Ministerstva zdravotnictví se bude zásadním způsobem podílet na podpoře a koordinaci aktivit, spojených s realizací reformy Národního plánu obnovy a projektů podpořených z IROP 2 v oblasti digitalizace zdravotnictví, včetně standardizace, telemedicíny a kybernetické bezpečnosti.
- 11:20 - 11:45 Jak levně a legálně nakoupit licence a ještě na tom vydělat?**  
Martin Predný - PREDNY SLM  
Získejte peníze na upgrade infrastruktury prodejem svých starých licencí a zjistěte, jaké podmínky lze stanovit u veřejných zakázek na nákup softwarových licencí tak, abyste se vyhnuli nelegálnímu softwaru a nakoupili za nejlepší cenu na trhu.

**11:45 - 12:10 Zvýšení kybernetické bezpečnosti dle směrnice NIS2 s využitím dotací Ministerstva zdravotnictví**

Václav Zubr - ESET software

Koncem roku byla na evropské úrovni schválena směrnice NIS2 o zajištění vysoké úrovně kybernetické bezpečnosti. Ta se týká i veřejných subjektů poskytujících zdravotní služby s více než 50 stálými zaměstnanci. V letošním roce bude probíhat implementace této směrnice do národní legislativy. Nyní probíhají jednání o alokaci dodatečných finančních prostředků v rámci Národního plánu obnovy. V rámci přípravy na plánovanou výzvu je nyní třeba zpracovat záměr projektu posílení kybernetické bezpečnosti dle podporovaných aktivit Ministerstva zdravotnictví. Velkou část těchto aktivit jste schopni naplnit s využitím služeb, produktů nebo dodatečných softwarových modulů společnosti ESET. Ve své přednášce ukážu, s jakými projekty jsme schopni Vám pomoci, abyste mohli čerpat prostředky z plánované výzvy smysluplně a co nejjednodušeji.

**12:10 - 12:35 Sedm statečných - SOC pro 7 oblastních nemocnic kraje**

Pavel Štros - DATASYS

Také řešíte otázku, jak optimálně zavést nepřetržitý bezpečnostní dohled do několika zdravotnických zařízení kraje? Poskytneme Vám několik tipů vycházejících z naší praktické zkušenosti. Směřujte k centralizovanému řešení, které je schopno bez dramatických nákladů sjednotit vyhodnocování bezpečnostních událostí z různých technologií a aplikací obdobného typu a zároveň zesílí schopnost kybernetické bezpečnostní události v cílovém prostředí detekovat.

**12:35 - 13:35 Oběd**

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

**14:00 - 14:25 Od záplavy alertů k autonomnímu řešení**

Zdeněk Kopta - TAKTIK, Peter Lechman - SentinelOne

Nepřehledná a složitá IT, IoT i OT prostředí jsou ideálním adeptem na nasazení autonomního a efektivního řešení ochrany před kybernetickými hrozbami. Problémem dnes není získat dostatek informací o zranitelnostech a útocích, ale správně a včas je vyhodnotit pro zamezení kompromitace a negativního dopadu na bezpečnost a funkčnost systémů. Rychlost reakce je pak naprosto klíčová a obrovské množství informací v kombinaci s nedostatkem lidských zdrojů ji zásadně brzdí. Řešením je autonomní platforma pracující nejen s daty z koncových stanic, ale nabízející i účinné klamání útočníka. Identifikace, odhalení, zastavení a často i dopadení útočníka v plně autonomní platformě je recept na zvýšení bezpečnosti a odolnosti nejen IT systémů.

**14:25 - 14:50 Spolehlivá záloha - poslední instance obrany vůči kybernetickým hrozbám**

Boris Mittelman - Veeam Software

- Zdravotnictví je jedním ze 3 odvětví nejpostiženějších kybernetickými útoky
- Útočníci nacházejí stále sofistikovanější a preciznější formy útoků
- Ochrana dat již nemůže být jenom „nějaká“. Musí být NEZDOLNÁ

**14:50 - 15:15 Přednášet bude zástupce společnosti DELL Technologies**

**15:15 - 15:45 Přestávka**

**15:45 - 16:10 Přednášku brzy upřesníme**

**16:10 - 16:35 Bankovní identita jako akcelerátor digitalizace českého zdravotnictví**

Jiří Beneš - Bankovní identita

Nezbytnou podmínkou efektivní digitalizace českého zdravotnictví je bezpečná a jednoznačná identifikace klienta-pacienta-pojištěnce, a to silným a důvěryhodným autentizačním prostředkem.

Bankovní identita (a její služba #BankID) využívá způsob, kterým se klienti českých bank přihlašují do svého internetového bankovníctví. Tento efektivní nástroj digitální identifikace lze využít v celé řadě služeb, aplikací a systémů včetně zdravotnictví.

V prezentaci se dozvíte, jak bankovní identita v Česku vznikala a proč banky mají všechny předpoklady být úspěšnými poskytovateli identifikačních služeb. Na datech a příkladech si ukážeme, v jakých segmentech a proč se BankID masivně prosazuje, zmíním i již fungující projekty z českého zdravotnictví a nastíním oblasti, kde vidíme potenciál dalšího rozvoje.

**16:35 - 17:00 Řešíte u eHealth produktů technologie, ale ne design? Přicházíte o čas a peníze.**

Jakub Karlec - 2FRESH

Přednáška Jakuba Karlece objasní divákům hodnotu designu digitálních produktů ve zdravotnictví. Nové technologie a software neustále posouvají zdravotnictví dopředu, ale pokud mají špatný design, organizace přichází o čas i peníze. Ukázky z uživatelského testování vás přesvědčí, jak velké rozdíly v použitelnosti může dělat dobrá UX. Jakub zároveň přidá tipy na to, co si u digitálních produktů hlídat. Dozvíte se, jak můžete základní testování provést svépomocí a jaké otázky a komu máte z pozice testující klást.

Vyplatí se tomu věnovat pozornost? O tom nepochybuje. Dobře navržené systémy vyžadují nižší čas na zaškolení personálu, snižují chybovost práce, zvyšují ochotu nemocničního personálu je využívat, a ve výsledku zvyšují kapacitu zdravotnictví.

**17:00 Předpokládaný konec konference**