ICT ve zdravotnictví 2022

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

Program akce

Hlavní blok

9:00 - 9:10 **Zahájení konference**

Jan Mazal

9:10 - 9:40 **Jak se připravit na obnovu po úspěšném kybernetickém útoku**

Petr Diviš - DELL Technologies

Zdravotnická zařízení se stala jedním z nejčastějších cílů kybernetických útoků. Jak se na danou událost připravit za pomoci technologií a postupů od Dell Technologies. Jak zajistit obnovu kompromitovaného systému v definovaném čase? Řešení pro business continuity a data protection je často potřeba přizpůsobit novým požadavkům a zabezpečit se tak proti novému typu zranitelnosti. Přednáška bude pojednávat o řešení datového trezoru, odolného proti napadení.

9:40 - 10:10 **Útoky na dodavatelský řetězec**

Václav Zubr - ESET software

Dříve zcela výjimečně viděné útoky typu supply chain attacks jsou nyní reálnou hrozbou pro mnoho českých společností. Každý měsíc se oběťmi hackerů stávají i vývojáři, kteří v rámci pravidelné aktualizace své legitimní aplikace šíří nevědomky upravenou ztrojanizovanou verzi svého softwaru. V přednášce se dozvíte detaily. Mimo jiné potvrzení, že se žádná kaše její tak horká, jak se uvaří.

10:10 - 10:40 **Rozvoj kybernetické bezpečnosti ve zdravotnictví**

Tomáš Bezouška - MINISTERSTVO ZDRAVOTNICTVÍ

Tomáš Bezouška ve své přednášce shrne události uplynulého roku jak na straně bezpečnostních hrozeb, kterým musel sektor zdravotnictví čelit, tak na straně strategie Ministerstva zdravotnictví. Představí konkrétní kroky resortu ke zvyšování kyberbezpečnosti a nebude chybět ani výhled na rok 2022.

10:40 - 11:10 **Přestávka**

11:10 - 11:40 **LOGmanager - centrální správa logů**

Lukáš Termer - Sirwisa

LOGmanager, nástroj pro centrální sběr a vyhodnocování logů. Pomáhá nejen malým, ale i velkým organizacím. Hlavním heslem je radikální jednoduchost.

11:40 - 12:10 **Krizové informační centrum aneb chytré poplachy**

Pavel Štros - DATASYS

KIC je systém, který na základě předdefinovaných scénářů rozesílá různými kanály notifikace a spouští poplachy či jiné akce. Pracuje přitom i se zpětnou vazbou při vykonávání scénáře, zejména při eskalacích. Příkladem může být přivolání strážní služby a výstraha zobrazená na všech počítačích na daném oddělení nemocnice za situace, kdy lékař čelí agresivnímu pacientovi. Integrovali jsme KIC na oblíbené dohledové nástroje ZABBIX a ELISA, díky čemuž lze velmi snadno eliminovat zahlcení techniků notifikacemi.

12:10 - 12:40 **Kaspersky Managed Detection and Response**

Petr Kuboš - Kaspersky

Mnoho organizací veřejného sektoru uvádí rozpočtová omezení jako hlavní faktor omezující jejich bezpečnostní schopnosti.
V konkurenci s hlavními požadavky zdravotnických organizací, jako jsou například investice do nových zdravotnických přístrojů a zařízení, může být pro bezpečnostní tým velmi obtížné zajistit rozpočet i na kybernetickou bezpečnost a její kontinuitu na profesionální úrovni.
Jak co nejvíce usnadnit nemocnicím správu a vysokou úroveň kybernetické bezpečnosti?
Zkušenosti našich zákazníků dokazují, že využití profesionálních služeb a automatizovaných nástrojů může být cesta k efektivní ochraně proti kybernetickým útokům, a to bez velkých nároků na bezpečnostní týmy a investice do nich.

12:40 - 13:10 **Proaktivní ochrana nestrukturovaných dat před ransomware útokem**

Martin Lenk - DELL Technologies

Medicínské informační systémy pracují s velkým objemem nestrukturovaných dat, ukládaných ve formě souborů v rámci infrastruktury, například PACS snímky, medicínské archivy atd. V řadě případů je obtížné nebo nemožné provádět tradiční backup a případná obnova těchto dat z backupu je časově náročný proces. V tomto příspěvku představíme, jak efektivně ukládat a proaktivně chránit nestrukturovaná data před ransomware útokem prostřednictvím nástrojů Dell Technologies a eliminovat nutnost obnovy všech těchto dat v případě kybernetického útoku.

13:10 - 14:10 **Oběd**

14:10 - 14:40 **Bezbolestná ochrana dat s garantovanou obnovitelností**

Boris Mittelmann - Veeam Software

Předešlé 2 roky dramatického nárůstu kybernetických hrozeb nám jasně ukázaly, jak je trestuhodně přehlížen správný výběr, nasazení a provoz zálohovacího řešení. V této stručné prezentaci si povíme o základních 5 vlastnostech, které musí moderní zálohovací řešení splňovat a o 5 pravidlech jeho správného nasazení pro zajištění garantované obnovitelnosti dat bez ohledu na příčinu potřeby obnovy.

14:40 - 15:10 **IT perimetr je mrtvý. Je třeba uplatňovat princip - Nikomu nevěř, vždy ověř!**

Petr Kunstát - Thales Group Inc.

Pojmy jako MFA nebo Zero Trust známe už pár let. Stále je ale mnoho společností, které s nasazením MFA otálejí a tématu IAM – identity a access managementu nevěnují dostatečnou pozornost. Většinou se o nich dříve nebo později dočteme v novinách, a to v momentu, kdy se do IT infrastruktury nebo k citlivým datům dostane útočník. Přitom nasazení řešení je dnes rychlé a snadné. Pojďme se tedy na to společně podívat.

15:10 - 15:40 **Jak účinně zabezpečit nemocniční sítě**

Jan Kalabus - Flowmon Networks

Závislost nemocnic na informačních technologiích roste. Jejich IT prostředí je přitom velmi různorodé. Typicky jde o kombinaci různých systémů, aplikací nebo proprietárních systémů. Je obtížné je spravovat a zabezpečit. Přitom v ohrožení jsou nejen citlivá data pacientů, ale i jejich životy. Provedeme Vás jak účinně ochránit podnikové aplikace, detekovat a analyzovat výkonnostní problémy a hrozby v datové síti a tím zajistit kybernetickou bezpečnost.

15:40 - 16:10 **Digitalizace medicíny už má podobu reálného řešení**

Tomáš Rohožka - Asseco Central Europe

Je možné bezpečně diagnostikovat vybrané pacienty s covid pneumonií z pohodlí domova a poskytovat jim náležitou péči? Digitalizace medicíny už pomáhá také v boji proti pandemii. Seznamte se s inovativní systémem MEDASISTENT, která umožňuje na dálku monitorovat, analyzovat a vyhodnocovat stav pacienta v reálném čase bez nutnosti hospitalizace v nemocnici. Používání aplikace zkracuje nejen pobyt pacienta v nemocnici, ale zároveň optimalizuje jeho včasný příchod, díky čemuž pomáhá předcházet kritickým stavům pacientů. Limitované kapacity nemocnic tak mohou být efektivně využívány jen pro komplikované případy, pro které je hospitalizace nezbytná.

16:10 - 16:30 **Přestávka**

16:30 - 17:00 **Mýtus EDR: prevence versus reakce**

Jaroslav Hromátka - IS4 security/Bitdefender, René Pospíšil - IS4 security/Bitdefender

Pokud vaše zdravotnická organizace plánuje nasazení EDR (Endpoint Detection and Response) řešení, které otázky je potřeba předem zodpovědět? Víte už jaké jsou provozní náklady takového řešení? Na co si musíte dát pozor při jeho provozu a nasazení? Lze EDR libovolně kombinovat s jinými výrobci? Můžete se zbavit nákladů za stávající antivirové řešení nasazením samotné EDR, nebo potřebujete vícevrstvý přístup? Jak vám pomůže EDR odhalit tiché hrozby v praxi? Budete i nadále potřebovat EPP ochranu? Existuje optimální cesta, jak odladit oba přístupy ochrany EPP + EDR dohromady, tak abyste docílil maximální ochranu vašeho IT prostředí, a zároveň snížili vaše provozní náklady?

17:00 - 17:30 **Kybernetická a informační bezpečnost ve zdravotnickém zařízení ... jde to? ... a proč to bolí?**

Aleš Špidla - Ing. Aleš Špidla

Zavést kybernetickou a informační bezpečnost ve zdravotnickém zařízení vůbec není jednoduché ... pane inženýre, pro nás je to těžko uchopitelné – to je častý komentář mého snažení. A jak se s tím poprat ? Pojďme spolu najít řešení (nebo alespoň cestu k němu).

17:30 - 18:00 **hSOC - možný přístup k řešení kybernetické bezpečnosti**

Jan Kolouch - CESNET, zájmové sdružení právnických osob

Jak řešit kybernetickou bezpečnost ve zdravotnictví? Kde hledat možná slabá místa a kde naopak příležitosti? Skutečně mohou pomoci vyřešit bezpečnost „one box solutions“? Na tyto a další otázky se pokusí nalézt odpovědi tato přednáška.

18:00 - 18:30 **Tombola**

18:30 **Předpokládaný konec konference**