Cyber Security 2023

19. října 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 - 9:40 **Efektivní ochrana záloh a kritických dat před kybernetickými útoky**

David Průša - DELL Technologies

Jak chránit Vaše zálohy a kritická data, ale hlavně jak je efektivně a garantovaně obnovit v případě úspěšného kybernetického útoku? To je otázka, kterou si dnes musí klást skoro každý. Představíme vám koncept kontroly záloh a bezpečného izolovaného prostředí, tzv. Trezoru pro Vaše kritická data včetně kontroly jejich čistoty pro úspěšnou a rychlou obnovu.

9:40 - 10:10 **My (ne)chceme EDR!**

David Pecl - Security Avengers

Endpoint Detection and Response nástroje jsou mezi námi již značnou chvíli a implementátor tak obecně očekává, že když se firma rozhodne EDR nasadit, je si vědoma všech pro a proti, výhod a nevýhod a problémů, které mohou nastat.
V prezentaci se podíváme na to, jaké výzvy vás při implementaci EDR nástroje čekají – od výkonnostních problémů, přes padání provozovaných aplikací až po nutné změny v infrastruktuře. Stejně tak se zaměříme na častý post-implementační problém nejen středních a menších firem – EDR máme, ale kdo ho bude obsluhovat?

10:10 - 10:40 **Proaktivní ochrana proti moderním hrozbám**

Jan Brejcha - awin IT, s. r. o.

Security risk management je více než práce na plný úvazek. Vyžaduje nepřetržitou péči. I ty nejlepší automatizované obranné systémy vyžadují interakci s lidmi, aby věděli, co mají dělat, když dojde k incidentu. Většina společností však není dostatečně připravena reagovat, když se objeví bezpečnostní hrozba. Se službou Sophos Managed Detection and Response (MDR) získáte navíc odborné znalosti, které vám umožní řešit incidenty okamžitě – a přesně tak, jak potřebujete reagovat.

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

11:10 - 11:40 **Jak na NIS2 a nezešedivět? Budujte bezpečnost, která je překážkou pro útočníky, nikoliv pro zaměstnance.**

Jan Falc - SoftwareOne Czech Republic

Bezpečnost musí být praktická, srozumitelná, přínosná a uživatelsky přívětivá. Podíváme se na nejčastější omyly a výmluvy při zálohování, klasifikaci informací a použití multifaktorového přihlašování.

11:40 - 12:10 **Bezpečnost a analýza s jednotným agentem**

Pavel Škorpil - IS4 security / Bitdefender

Centrálně řízená správa bezpečnosti Vám pomůže efektivně chránit Vaše aktiva. Jednotný bezpečnostní agent využívající strojové učení s pokročilou ochranou před malware, s kontrolou konzistence souborů, s analýzou rizik včetně remediace nebo třeba s aplikačním patch managementem. A pokud se vyskytne anomálie, tak ji s EDR/XDR můžete analyzovat z přehledné konzole centrální správy.

12:10 - 12:40 **ITSM jako první kroky k podpoře kybernetické bezpečnosti a požadavků NIS2**

Lubomír Karas - ALVAO, Jiří Sláma - ALVAO

Seniorní konzultanti Lubomír Karas a Jiří Sláma se v posledních letech intenzivně věnují oblasti implementace ITMS, respektive Service Desk a Asset Management. Právě nastavování procesů v řízení IT a používání správných nástrojů je základním předpokladem pro bezpečnost v organizaci obecně. S NIS2 přišly obavy z vysokých pokut a organizace začaly řešit nastavení bezpečnosti, nejen kyberbezpečnosti. A přitom stačí tak málo. Udělat si pořádek v majetku, o který se starám. Evidovat případné incidenty, abych mohl zavést nápravná opatření na minimalizaci jejich výskytů a v neposlední řadě spravovat změny, které mají dopad na provoz. A jak na to, vám přímo v ALVAO Lubomír Karas s Jiřím Slámou prakticky ukážou.

12:40 - 13:10 **Vládní dohledové centrum**

Vladimír Rohel - Národní agentura pro komunikační a informační technologie, s. p.

V současné době se již bez podpory bezpečnostního týmu, který neustále vyhodnocuje události v informačním systému prakticky neobejdeme, pokud nechceme být slepí a nespoléháme na to, že když nic nevidíme, nic se neděje. Ministerstvo vnitra společně s NAKIT začalo v roce 2016 budovat svůj bezpečnostní tým – Security Operations Center (SOC) pro potřebu chránit své informační systémy a informační systémy eGovernmentu, které mělo v gesci. Za těch sedm let vzniklo pracoviště, které si již vydobylo prestiž při řešení mnoha incidentů. I proto Ministerstvo vnitra dostalo od vlády úkol vybudovat na základech stávajícího SOC „Vládní dohledové centrum“, které bude sloužit nejen ministerstvu, ale i jiným organizacím státu. Partnerem pro splnění tohoto úkolu je opět NAKIT. Jak se s ním společně vypořádáváme se dozvíte v prezentaci.

13:10 - 14:10 **Oběd**

14:10 - 14:40 **Jak doručovat a zabezpečit aplikace v době (multi)cloudové**

Jiří Petrásek - F5 Networks

Jdete do cloudu? Lámete si hlavu, zda pro publikaci a zabezpečení aplikací využít technologie od dodavatele veřejného cloudu nebo od specialistů na securitu? A co když budete mít v budoucnu více než jeden cloud? Na prezentaci vám ukážeme, jak pomocí F5 Distributed Cloud Services elegantně, rychle a efektivně postavíte perimetr pomocí moderní cloudové WAF a zajistíte tak ochranu proti zranitelnostem OWASP, DDoS útokům, automatizované komunikaci a útokům na API. Ale nejen to – univerzalita platformy umožňuje konsolidovat další funkce jako CDN, propojování cloudů a jednotlivých workloadů. Postavíte ochranu, která je kompatibilní se všemi poskytovateli cloudu, ale zároveň je na nich nezávislá.

14:40 - 15:10 **Informační bezpečnost: Zákon a pořádek ve světě digitálního risku**

Kateřina Hůtová - Cybrela

Co přináší NIS2 jsme si řekli loni, letos se pojďme zaměřit na konkrétní povinnosti plynoucí z návrhů nové legislativy a praktické oblasti aneb:
1) Jak se správně určit? Jak na (sebe)určení, zda pod návrh nové legislativy spadáte či ne (tipy a triky, na co nezapomenout)
2) Budgetování
3) Co všechno potřebujete pro úspěšné proplacení pojistky z kyberpojištění
4) Svět mezi zákony a praxí ...šedé zóny
5) Co dělat, aby vás příští rok nic nepřekvapilo
Tedy na co myslet a nezapomenout? Jaké záludnosti si na nás zákon chystá (možnost spadnout pod vyšší režim i přes to, že na hlavní poskytovanou službu se zákon nevztahuje?). Co dělat, pokud jste součástí velké skupiny? A hlavně – informační bezpečnost má být probyznysová, tak to takto pojďme i pojmout.

15:10 - 15:40 **Budoucnost bezpečnostního dohledu se jmenuje XDR**

Jakub Jiříček - SentinelOne

Dnešní provoz v mnohém bezpečnostním dohledovém centru stále spoléhá na velký podíl ruční práce a analýz a rozhodování lidských specialistů. Do budoucna tohle není udržitelné, z mnoha důvodů. Dobře navržená XDR platforma umožní podíl lidské práce zásadně snížit ve prospěch automatizace. Pro dohledová centra může být tou změnou, která zásadně zvýší kapacitu a rychlost řešení incidentů.

15:40 - 16:10 **Coffee break**

16:10 - 16:40 **Cloud Computing a kybernetická bezpečnost**

Dominik Vítek - PIERSTONE

V oblasti kybernetické bezpečnosti byla nedávno přijata řada nových právních předpisů a další předpisy se připravují. V rámci implementace směrnice NIS2 do českého právního řádu dochází ke komplexní změně celého právního rámce kybernetické bezpečnosti v České republice. Tyto legislativní změny mají zásadní dopad na poskytovatele cloudových služeb i na jejich zákazníky. Prezentace vás provede novými požadavky regulace kybernetické bezpečnosti s dopady na cloudové technologie a zaměří se na výzvy, které v této souvislosti přináší navrhovaná novela zákona kybernetické bezpečnosti a další připravované předpisy.

16:40 - 17:10 **IT vendors a kybernetická bezpečnost**

Zdeněk Kučera - Dentons Europe CS LLP, organizační složka

Současná i nadcházející pravidla kybernetické bezpečnosti řeší outsourcing IT služeb; jaká pravidla musí dodržovat IT vendors při poskytování služeb a jaká pravidla jsou kladena na objednatele služeb podle pravidel kybernetické bezpečnosti; ukážeme si prakticky a na příkladech.

17:10 - 17:25 **Tombola**