CIO Agenda

Kybernetické (ne)bezpečí: Nebát se a nenechat se okrást

21/2/2023

O_2 universum, Praha 9

Organized by **blue events**

Nenechte si ujít osobní setkání s kolegy

Kybernetická bezpečnost není stav, ale trvalý proces. A protože útočníci jsou vždy o krůček napřed, tak se v programu v tomto roce zaměříme na aktuální hrozby. Ukážeme si, jaké útoky se v poslední době odehrály, kde byla slabá místa, kterých hackeři využili a na co všechno je třeba si nově dát pozor.

Zaměříme se na návody, jak postupovat při řešení bezpečnostních incidentů. Přijďte se dozvědět, co vám může pomoci v každodenním boji o to, aby vaše firma a její systémy zůstaly v bezpečí.

Nenechte se okrást o klid, dobrou pověst, data ani peníze! Se svými argumenty a zkušenostmi vystoupí přední odborníci a praktici, a stejně jako v minulém roce se nepochybně do diskuse zapojí i řada účastníků. Třeba právě vy. :)

Těšíme se na společné osobní setkání dne 21. února v O_2 universum v Praze.

Michaela Dvořáková a tým Blue Events

S kým se v programu setkáte


Petr Koubský


Dan Hejda


Jan Marek


Radek Šichtanc


Martin Vogel


Veronika Krajčovičová


Richard Valiček


Petr Dušek


Adam Škarka


Martin Haller

Program 21/2/2023

Moderace: Petr Koubský, redaktor pro vědu a techniku, Deník N

8.00–9.00
Registrace účastníků, networking

9.00–11.00 Blok A

Jak se poučit z hackerských útoků

Dan Hejda, Jan Marek, etičtí hackeři, Cyber Rangers

V tomto i minulém roce se staly terčem hackerů velmi zajímavé organizace. V rámci naší přednášky se podíváme nejen na útoky na zahraniční organizace, ale i na vybrané organizace z Česka. Pojďme se společně poučit z taktik a technik útočníků na konkrétních případech a zamysleme se, jak bychom se dokázali ubránit.

Jste to opravdu vy? Jak technologie pomáhají odhalovat podvodníky

Radek Šichtanc, ředitel útvaru Bezpečnosti, O_2

Boj s kyberzločinci je běh na dlouhou trať. Uspět v něm může především ten, kdo se naučí potenciální útoky předvídat a efektivně jim předcházet. Chceme vám pomoci pochopit některá specifika kybernetických útoků, se kterými máme především v poslední době z pozice telekomunikačního operátora bohaté zkušenosti. Ukážeme si, co nám pomohlo jim účinně čelit. Zaměříme se hlavně na praktiky útočníků v oblasti podvodů a jak při odhalování podvodů v digitálních kanálech pomáhá aplikování moderních technologií. Ať už je to umělá inteligence nebo třeba behaviorální a hlasová biometrie.

Ochrana a správa informací je základním kamenem každé digitální organizace

Martin Vogel, Manager, Solutions Consulting CEE, Opentex

Moderní organizace potřebuje ochranu informací před ztrátou a zneužitím, současně s uživatelsky příjemným prostředím a efektivními procesy. OpenText nabízí moderní ECM a EIM řešení, spolu se zabezpečením a efektivní správou nestrukturovaných i strukturovaných dat bez kompromisů.

Nejčastější způsoby útoků a jejich vyšetřování Policií ČR

Richard Valiček, vedoucí oddělení kybernetické kriminality, Policie ČR

Zaměříme se na shrnutí nejčastějších typů útoků z problematiky kybernetické kriminality, jak probíhá zajišťování digitálních důkazů a jejich vyhodnocování. Jaké jsou nejčastější chyby uživatelů ICT technologií? Ukážeme si, jak se chovat po incidentu, aby nebyly znehodnoceny digitální důkazy pro potřeby Policie ČR.

11.00–11.30
Přestávka na kávu a čaj

11.30–13.30 Blok B

Kybernetická bezpečnost pro malé a střední podniky - best practices

Veronika Krajčovičová, CEO, bugino

Ukážeme si, jaká je realita a dodržování „best practices" v malých a středních podnicích. Podíváme se, jaké produkty používáme a jsou-li vůbec pro tento segment dostupné a jakým čelíme výzvám při nastavování bezpečnostních standardů. Blízké setkání s hackery.

Design bezpečnostního testování

Petr Dušek, specialista kybernetické bezpečnosti, NAKIT

Každé bezpečnostní testování je třeba zakládat na maximálním porozumění zákazníka a vytvářet testování ve spolupráci s ním. Proto je nutné důkladně pochopit jednotlivé typy bezpečnostních testů, jejich význam, potenciální přínos, efektivnost, ale třeba i související rizika, a vytvořit optimální design bezpečnostního testu. V souvislosti s vyhláškou o kybernetické bezpečnosti je velice známé penetrační testování a testování zranitelností. Ale jedná se o jediné možné bezpečnostní testy? Jak reálně v praxi takové testy probíhají a jak by probíhat měly či neměly? A jak se na tuto problematiku díváme v souvislosti s budováním služeb Vládního dohledového centra?

Právní výzvy kyberbezpečnosti - přichází NIS 2

Adam Škarka, advokát, SEDLAKOVA LEGAL

Nová regulace kybernetické bezpečnosti v EU bude výzvou pro mnoho subjektů, jak ve státním, tak v soukromém sektoru. Adam Škarka vás provede novou regulací a vysvětlí, co se mění. NIS 2 je tady. Buďte na tuto výzvu připraveni.

BEC - když vaše účetní pošle několik set tisíc na špatný účet

Martin Haller, CEO, Patron IT

Asi se nenajde nikdo, kdo by nedostal do e-mailu nějakou falešnou fakturu k uhrazení. Nicméně tyto podvody typu „Business E-mail Compromise" (zkráceně BEC) a útočníci za nimi dokážou být mnohem kreativnější. Máme pro vás několik příběhů ze života a inspiraci co s tím.

13.30–14.30
Pracovní oběd a networking

14.30–16.00 Panelová diskuze

Hacker, bezpečák, právník a soudní znalec u jednoho stolu

Moderace: Lukáš Okál, Security Lead, Microsoft

Red Team:
Jan Marek, etický hacker, Cyber Rangers
Daniel Hejda, etický hacker, Cyber Rangers

Blue Team:
Jiří Sedlák, manažer bezpečnostního dohledového centra, O_2
Jan Vala, Lead Value Engineer, OpenText

Legal Team:
Richard Valiček, vedoucí oddělení kybernetické kriminality, Policie ČR
Jindřich Kalíšek, advokát a mediátor

16:00 – 17:00
Networking a koktejl

Vstupné

Základní

Celodenní vstupné pro jednoho účastníka

9 900 Kč (+DPH)

Early Birds

Včasně registrovaní účastníci, jejichž platba bude připsána na náš účet do 3. 2. 2022, mají slevu 2 000 Kč ze základní ceny!

7 900 Kč (+DPH)

Skupinová

Při účasti 2 a více účastníků z jedné firmy je cena za druhou a každou další vstupenku

6 400 Kč (+DPH)

Vstupné zahrnuje: celodenní odborný program, příspěvky a konferenční materiály, výtečné občerstvení během celé konference.

Místo konání

O_2 universum, Praha

Českomoravská 2345/17, 190 00 Praha 9

Přihlašujte se již nyní na www.cioagenda.cz

Naše poděkování patří především těmto partnerům:

Gold Partners

O_2 Cyber Security

opentext™

Bronze Partners

kofola ČeskoSlovensko

SEDLAKOVA LEGAL

MAIL STORE®

AV MEDIA EVENTS

Media Partners

AVERIA NEWS

IT Systems www.SystemOnline.cz

CYBER RANGERS ARMORING YOUR BUSINESS

RETAILNEWS