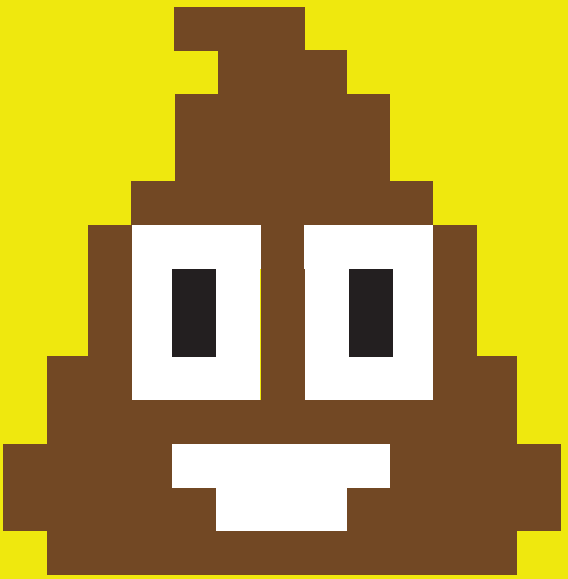
CIO AGENDA 2022

30. 3. 2022 **O2 universum, Praha 9**

JAK SE VYHNOUT FAKT VELKÉMU PRŮ*ERU?

Kybernetická bezpečnost je trvalý proces, ne stav.
... I když si myslíte, že máte všechno dobře,
tak to může dopadnout blbě.



Platforma pro šéfy IT a další top manažery firem,
které se zajímají o to, jak mít firemní data v bezpečí.

www.cioagenda.cz

blue events

NENECHTE SI UJÍT OSOBNÍ SETKÁNÍ S KOLEGY

Kybernetická bezpečnost je trvalý proces, nikoli stav. Proto se i letos program konference CIO Agenda zaměří na to, jak dobře připravit systémy, aplikace a jejich uživatele, včetně managementu na známé i dosud neznámé kritické situace.

Zaměříme se na aktuální hrozby, na návody, jak postupovat při řešení bezpečnostních incidentů, abychom zabránili nejen ztrátám finančním, ale i případnému poklesu důvěry klientů a poškození dobré pověsti. Nahlédneme do světa hackerů. V neposlední řadě si ukážeme, jakým právním důsledkům můžeme čelit, když to budeme dělat špatně.

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 :). Přijďte na konferenci CIO Agenda.

Těšíme se na osobní setkání dne 30. března v O2 universum v Praze.

Michaela Dvořáková a tým Blue Events

PROGRAM KONFERENCE

Konferenci moderuje
Petr Koubský, *redaktor pro vědu a techniku,*
Deník N

08:00 - 09:00 Registrace

09:00 - 11:00 **A: CO SE V OBLASTI KYBERNETICKÉ (NE)BEZPEČNOSTI REÁLNĚ DĚJE**

Shrnutí hrozeb aneb co se dnes vyšetřuje

Ondřej Kapr, *policejní rada, Úřad služeb kriminální policie a vyšetřování - odbor hospodářské kriminality, Policejní prezidium ČR*

Aktuální hrozby v oblasti kybernetické kriminality z pohledu Policie České republiky. Půjde zejména o tak zvané ostatní kriminality páchané v kyberprostoru, kdy bývá největší hrozbou lidský faktor. Projevy sociálního inženýrství phishing, vishing, smishing, CEO a BEC útoky, investiční podvody ... Jaká jsou možná východiska ze strany policie?

Proti vaší firmě stojí profesionální „zabiják“ aneb pozadí hackerských skupin

Dan Hejda *a* ***Jan Marek,*** *etičtí hackeři, Cyber Rangers*

Přednáška je založena na vlastním výzkumu, jak hackerské skupiny fungují, co je motivuje a proč je dobré znát svého protivníka. Zabrousí do témat jako je výše výkupného u ransomware útoků a jaké jsou nejčastější postupy útočníků. Vše se samozřejmě netočí jen okolo ransomware, ale měly by vás zajímat i jiné typy útoků, kdy není úplně lehké útočníka vypátrat a dopadnout. Jak vypadá přípravná fáze útoku a proč je důležité vědět, co o vás a vaší firmě „ví“ internet.

Anatomie útoku – aneb co probíhá na druhé straně

Radek Šichtanc, *ředitel útvaru Bezpečnosti, O2*

K útoku již došlo. Co se děje v prvních hodinách a co v následujících dnech po jeho odhalení? Jaká je správná reakce a na které kroky (ne)zapomenout? Dozvíte se, jak se připravit na jednotlivé fáze útoku i to, jak celkově přistupovat k ochraně před kybernetickými hrozbami. A jak tuto ochranu vystavět a následně ověřovat její účinnost. To vše maximálně prakticky.

Co chcete vědět a nechcete zažít - příklady, kdy to dopadne špatně

Radek Beneš, *soudní znalec v oblasti IT a kybernetické kriminality*

Kdo by si rád neposlechl zajímavé příhody ze své profese a nepolitoval jiné s tím, že u vás by se něco podobného stát nemohlo. Nic neuklidní více nežli zjištění, že jinde je to horší. To ovšem není smyslem příspěvku soudního znalce ICT. Jeho ambicí je přiblížit reálné soudní, správní či trestní řízení, abyste i bez potřeby vlastní zkušenosti nahlédli do této praxe. Do praxe, se kterou se chcete seznámit nejlépe pouze zprostředkovaně. Zhodnocení, zda jenom jinde je to horší, je samozřejmě na Vás.






11:00 - 11:30 Výměna názorů u kávy/čaje a občerstvení

11:30 - 13:00

B: JAK MINIMALIZOVAT ZTRÁTY?

Týden pod kybernetickým útokem v roli CIO

Pavel Srnka, *CTO, ANECT*
Miloslav Lujka, *Country Manager Czech Republic, Slovakia & Hungary, Check Point*

V pondělí ráno si myslíte, že víte, co vám reálně hrozí a hezky to prezentujete.
V úterý zjistíte, že to není pravda, protože se objevil úplně nový útok.
Ve středu vysvětlujete boardu, jak jste na neznámý útok připravení a jaký bude mít dopad.
Ve čtvrtek za plného provozu záplatujete.
V pátek věříte, že záplata pomohla a sčítáte škody.
V sobotu se připravujete, jak v pondělí vysvětlíte boardu, že se to už nestane.
V neděli, zatím co odpočíváte, temná strana připravuje další zero day útok...

Blízké setkání s hackery

Miroslav Holý, *Quality Systems Manager, ELBA*

V dubnu 2021 se naše firma se 350 zaměstnanci stala cílem hackerů. Celá počítačová síť, včetně všech informačních systémů se zastavila. Bylo těsně před výplatami, pryč byla i veškerá technická dokumentace ke všem produktům. Podělíme se s vámi o vlastní, velmi blízkou zkušenost s tím, jak bylo náročné (emočně, časově i finančně) se s celou situací vypořádat.

Je bezpečnost pouhou iluzí?

Lukáš Svozil, *konzultant na oblast OT ve výrobě, NTT Czech Republic*

Píše se rok 2022 a vy jste strašeni ze všech stran. Za rohem číhají hackeři; jen co uspíte počítač, vrhnou se na něj těžaři kryptoměn a vaše výrobní tajemství jsou neustále jen krůček od vyzrazení. Spasí vás jedině zázračný software od společnosti XY... Špatnou zprávou je, že tak snadné to není. Tou dobrou – můžeme se společně zamyslet nad tím, co všechno zahrnuje komplexní kyberbezpečnost podniku a podělit se o tipy, jak na to. A to (téměř) bez strašení.

Nebýt sám sobě hrozbou pomocí XDR

Jan Pilař, *Senior Program Manager, Microsoft*

Každá organizace disponuje arsenálem bezpečnostních technologií, některá menším, některá větším. Je však tento arsenál moderní a stačí na moderní hrozby? Využíváme jej opravdu tak, abychom nebyli na konci dne sami sobě reálnou hrozbou? V tomto bloku si ukážeme krásu a kouzlo XDR řešení, které vás provede nejen světem ochrany či detekce, ale také často zanedbávané prevence či vyšetřováním. Přijďte se seznámit s Microsoft 365 Defender.

13:00 - 14:00 Pracovní oběd a Networking

14:00 - 15:30

HACKER, BEZPEČÁK, PRÁVNÍK A SOUDNÍ ZNALEC U JEDNOHO STOLU

Moderuje:
Michal Horáček, *Customer Program Manager, Microsoft*
RED Team:
Martin Haller, *CEO, Patron IT*
Jan Marek, *etický hacker, Cyber Rangers*
BLUE Team:
Petr Kocmich, *Senior Security Architect, ANECT*
Jiří Sedlák, *Manažer bezpečnostního dohledového centra, O2*
LEGAL Team:
Radek Beneš, *soudní znalec v oblasti IT a kybernetické kriminality*
Jindřich Kalíšek, *advokát a mediátor*

15:30 - 16:30 Networking mezi účastníky a koktejl

16:30 Závěr konference





ATMOSFÉRA MINULÝCH ROČNÍKŮ

NAŠE PODĚKOVÁNÍ PATŘÍ PŘEDEVŠÍM TĚMTO PARTNERŮM:

ZLATÍ PARTNEŘI

ANECT

CHECK POINT

O2

STŘÍBRNÍ PARTNEŘI

Microsoft

NTT

BRONZOVÍ PARTNEŘI

AVMEDIA komunikace obrazem

ALBARELO

kofola ČeskoSlovensko

Dallmayr

MEDIÁLNÍ PARTNEŘI

IT Systems www.SystemOnLine.cz

digibiz

AVERIA NEWS

CYBER RANGERS ARMORING YOUR BUSINESS

StartupJobs

Máte dotaz k registraci či průběhu akce?

Zavolejte nám na
+420 222 749 841 nebo napište na
info@BlueEvents.eu

For English version visit: www.cioagenda.cz/en/

REGISTRACE

Registrujte se na
www.cioagenda.cz,
kde najdete veškeré podrobnosti
a podmínky účasti.

CENY VSTUPNÉHO

ZÁKLADNÍ CENA

9 900 Kč (+DPH)

Základní vstupné pro jednoho účastníka na celodenní konferenci.

EARLY BIRDS

7 900 Kč (+DPH)

Včasně registrovaní účastníci, jejichž platba bude připsána na náš účet do **25. 2. 2022**, mají slevu **2 000 Kč** ze základní ceny!

SKUPINOVÉ ZVÝHODNĚNÍ

6 400 Kč (+DPH)

Při účasti 2 a více účastníků z jedné firmy je cena za druhou a každou další vstupenku **6 400 Kč.**

VSTUPNÉ ZAHRNUJE

Celodenní odborný program, příspěvky a konferenční materiály, výtečné občerstvení během celé konference.

Místo konání: **O2 universum**
Českomoravská 2345/17
190 00 Praha 9

Kontakt na organizátora:

blue events

Blue Events, s.r.o.
Hlubočepská 38c, Praha 5
Tel: +420 222 749 841
E-mail: info@blueevents.eu
www.blueevents.eu