# sovak_bar_dopl_text

# Vás zve na webinář:

**Kybernetická bezpečnost ve vodárenství**

který se uskuteční

 **23. 9. 2021 od 10:00 hod.**

Na webináři se v souvislosti s dopadovými kritérii kybernetického zákona společně podíváme na nejdůležitější požadavky kladené na vodohospodářské společnosti. V rámci přednášek vám představíme klíčové požadavky legislativy, na které je třeba se zaměřit co nejdříve. Základními stavebními kameny jsou identifikace a hodnocení aktiv nejen OT prostředí organizace. Na webináři budou probrány otázky – Jak je kybernetická bezpečnost zajištována, řízena a vyhodnocována? Kdo jsou hlavními aktéry a jaká jsou vlastně pravidla „hry“? Kde začít a kam úsilí směřovat?

Na další přednášce vám ukážeme, jaký je možné zaujmout přístup k ověření možností průniku do IT prostředí i prostředí výrobní infrastruktury (průmyslových systémů). Také si řekneme, jaké jsou správné postupy a jak přistoupit k testování obranných týmů.

Dále bude ukázáno efektivní testování funkčnosti procesů kybernetické obrany formou vzájemné komunikace incident response týmu a výboru pro řízení kybernetické bezpečnosti. Představen bude i přístup založený na gamifikaci procesu kybernetické bezpečnosti.

***Přednášet budou:***

**Ing. Petr Kutálek**, bezpečnostní ředitel, ředitel odboru bezpečnostní politiky a krizového řízení, Ministerstvo zemědělství.

**Ing. Karel Štefl**, vedoucí oddělení kybernetické bezpečnosti, manažer kybernetické bezpečnosti Ministerstvo zemědělství.

 **Martin Švéda,** odbor regulace, NÚKIB. Martin Švéda je právním specialistou NÚKIB.

**Kamil Rečičár** je expertem v oblasti informační bezpečnosti s více než 15letou mezinárodní praxí ve státní i soukromé sféře. Primárně se zaměřuje na procesní řízení bezpečnosti informací v organizacích s rozmanitým rozsahem, velikostí i vyspělostí ICT prostředí. Je držitelem certifikace v oblasti informační bezpečnosti, řízení kontinuity činností a zastává roli manažera kybernetické bezpečnosti dle požadavků ZoKB.

**Daniel Hejda** je spolumajitelem firmy Cyber Rangers s.r.o. a spoluzakladatelem komunity Cyber Rangers, která shlukuje cyber-security profesionály nejen z ČR a SK, ale i z okolních států. Daniel působí jako penetrační tester, red team member a jeho hlavní doménou je Initical Recon s využitím metodologie OSINT a Initial Access. Daniel je držitelem certifikací CEHv10, eWPTv1, COMPTIA Pentest+, PECB ISO27001 Lead Auditor, MCSE, MCSA, MCSD a je také držitelem prestižního ocenění Microsoft MVP pro Cloud and Datacenter Management a přispěvatelem komunity CIS Security Benchmarks. Řadu let také působí v pozici poradce, školitele a konzultance pro oblast bezpečnosti a pomáhá budovat SIEM řešení z pozice datového analytika a researchera.

**Michal Beneš** je společníkem a ředitelem společnosti system boost a.s. V oblasti IT a kybernetické bezpečnosti pohybuje již 18 let. V rámci své poradenské praxe se zaměřoval na implementaci informačních systémů, digitalizaci, audity IT a kybernetické bezpečnosti a Business Continuity Management. Michal je soudním znalce v oborech Kybernetika a Ekonomika.

**Program:**

 **9:30 Registrace (online připojení)**

**10:00**  **Zahájení**

 - Ing. Vilém Žák, ředitel a člen představenstva SOVAK ČR

**10:10** **Zhodnocení kybernetických útoků vedených na organizace ve vodárenství a v resortu MZe v roce 2021** - Ing. Petr Kutálek a Ing. Karel Štefl, Ministerstvo zemědělství

**10:25**  **Stav řízení o určení povinných osob podle zákona o kybernetické bezpečnosti a připravované klíčové změny**

- Martin Švéda, NÚKIB

**10:40**  **Požadavky kybernetického zákona nejsou jen legislativní šikana**

 - Kamil Rečičár, system boost a.s.

**11:10** **Efektivní vyhodnocení slabin organizace za pomocí různých metod testování**

 - Daniel Hejda, Cyber Rangers s.r.o.

**11:40** **Table top versus incident response v pro středí IT systémů i výrobní infrastruktury (průmyslových systémů**)

- Michal Beneš, system boost a.s.

**12:10**  **Diskuse a závěr**

V případě zájmu o účast vyplňte, prosím, následující přihlášku a zašlete ji nejpozději **do 17. 9. 2021** na některý z níže uvedených kontaktů:

* e-mail: doudova@sovak.cz
* adresa: SOVAK ČR, Novotného lávka 200/5, 110 00 Praha 1

**Poplatek za účast na webináři je pro řádné členy SOVAK ČR 605,- Kč (včetně 21 % DPH), pro přidružené členy a ostatní účastníky 847,- Kč (včetně 21 % DPH). V ceně vložného je elektronický sborník.**

**Storno účasti je možné provést nejpozději 5 kalendářních dnů před konáním akce, v případě technických problémů na straně účastníka se poplatek nevrací.**

# Závazná přihláška

***na webinář***

# Kybernetická bezpečnost ve vodárenství

**dne 23. 9. 2021**

Jméno (a): ………………………………………………………………………………………………………….

……….……………………………………………………………………………………………………………..

Společnost: ………………………………………………………………………………………………………...

Kontakty (adresa, telefon, e-mail): **Žádáme o zaslání konkrétních e-mailových adres na přihlášené osoby, aby jim mohl být vytvořen přístup na webinář - uživatelský účet**. **Poté bude na tuto e-mailovou adresu zaslán e-mail s bližšími informacemi a odkaz na sborník v elektronické podobě.**

……………………………………………………………………………………………………………………...

……………………………………………………………………………………………………………………...

**Společnost JE / NENÍ řádným členem SOVAK ČR** (nehodící se škrtněte)

Datum: Razítko a podpis:

---------------------------------------------------------------------------------------------------------------------------------------------------

## Potvrzení o platbě

Potvrzujeme, že dne …………………………………

bylo uhrazeno **celkem**………………………………..Kč **(včetně 21% DPH**)

za společnost…………………………………………………………………………………………………….....

IČ:…………………DIČ:…………………z účtu č.………………………………………………………………

za účastníka (y): .………………………………………………………………………………………………….

……………………………………………………………………………………………………………..............

ve prospěch účtu SOVAK ČR, Novotného lávka 200/5, 110 00 Praha 1, IČ: 60456116, DIČ: CZ60456116, vedeného u MONETA Money Bank a.s. č.: 2127002504/0600, **variabilní symbol 109**

Datum: Razítko a podpis: