# sovak_bar_dopl_text

# Vás zve na webinář:

**Kybernetická bezpečnost ve vodárenství**

který se uskuteční

**24. 2. 2022 od 10:00 hod.**

Na webináři se v návaznosti na témata diskutovaná v září, která v úvodu semináře krátce zrekapitulujeme, zaměříme na rozvedení představení kybernetických hrozeb, zejména kybernetických útoků vedených primárně na průmyslové informační systémy (řídící systémy čističek a úpraven vody, čerpacích stanic atd.)

Bezpečnostní principy a pravidla nejsou v prostředí průmyslových řídících systémů (svět OT) často aplikované a taktéž aplikovatelné, protože reflektují principy ze světa IT, které se jeví ve světě OT jako téměř nepoužitelné. V rámci světa OT je nutné zohlednit základní problémy a úskalí, se kterými se výrobní sítě potýkají. Tím hlavním problémem je strach z omezení provozu v reálném čase a nemožnost obnovení výrobního procesu dostatečně rychle. Druhým velkým problémem je nízká úroveň znalosti světa kybernetických hrozeb, které by mohly omezit právě zmíněný provoz a bezpečí, které je pro výrobní sítě stěžejní.

V rámci přednášek vám na praktických ukázkách z „reálného“ laboratorního prostředí představíme některé z metod útoků na průmyslovou infrastrukturu a ukážeme dopady, které takový útok může mít nejen na vlastní vodárenskou společnost, ale i na její spotřebitele. Bude se jednat jednak o útoky cílené na vyřazení infrastruktury z provozu, ale také na její ovládnutí, tedy získání kontroly nad řídícími systémy, a tím pádem nad celými výrobními technologiemi. Při prezentaci útoků samozřejmě také uvedeme základní zásady, které mají za cíl těmto útokům zamezit, nebo případně útočníkům alespoň krajně znepříjemnit práci. Na konci semináře se krátce zaměříme na téma řízení kontinuity činností společnosti (BCM – Business Continuity Management), jakožto vypořádání se společnosti s následky útoku nebo havárie díky „náhradním“ výrobním postupům a procesům obnovy po havárii/útoku.

***Přednášet budou:***

**Daniel Hejda** je spolumajitelem firmy Cyber Rangers s.r.o., která se zabývá kontrolou bezpečnosti v IT a OT prostředí. Daniel působí jako penetrační tester, člen red teamu, školitel a trenér. Jeho hlavní doménou je sběr informací s využitím metodologie zpravodajských složek (OSINT) a postupy pro iniciální vstup do společnosti. Daniel je držitelem certifikací CEHv10, eWPTv1, COMPTIA Pentest+, PECB ISO27001 Lead Auditor, C|OSINT, 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 konzultanta pro oblast bezpečnosti a pomáhá budovat SIEM řešení z pozice datového analytika a researchera. Daniel společně s kolegy pomáhá stavět mezinárodní Security Operations Centra a v rámci dobrovolnické činnosti se podílí na spolupráci s kriminální policií ČR a buduje komunitu shlukující bezpečnostní specialisty z ČR a SK.

**Michal Beneš** je společníkem a ředitelem společnosti system boost a.s. V oblasti IT a kybernetické bezpečnosti pohybuje již 19 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 znalcem v oborech Kybernetika a Ekonomika.

**Program:**

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

**10:00**  **Zahájení a úvod do tématu**

* *V průběhu zahájení semináře proběhne krátká rekapitulace témat z předchozího semináře o kybernetické bezpečnosti a uvedení do témat aktuálního semináře.*
* ***Ing. Vilém Žák, ředitel a člen představenstva SOVAK ČR***
* ***Michal Beneš, system boost a.s.***

**10:10**  **Zhodnocení nových kybernetických útoků a obecně hrozeb v roce 2021**

* *Během přednášky vám představíme některé ze závažných kybernetických útoků, které se staly v roce 2021 a z nich odvozené kybernetické hrozby, jejichž řešení by neměla žádná společnost v odvětví vodárenství podcenit. Z přednášky byste si měli odnést ponaučení se, aby další z kompromitovaných společností nebyla, pokud možno, ta vaše.*
* ***Martin Švéda, NÚKIB***

**10:25** **Kybernetické hrozby a zranitelnosti společnosti a odpovědnost za její ochranu**

* *V rámci přednášky vám představíme základní kybernetické hrozby, které společnosti v odvětví vodárenství hrozí. V další části přednášky se zaměříme na odpovědnost (zejména vedení) zajistit sledování, vyhodnocování a analyzování úrovně bezpečnosti a v neposlední řadě vám ukážeme, jak zjistit, kde se vaše společnost nachází z pohledu bezpečnosti.*
* ***Michal Beneš, system boost a.s.***

**10:40**  **Odhalení kritických informací o OT prostředí v rámci veřejné sítě internet**

* *Během přednášky vám ukážeme, jak vypadá vyhledávání běžně dostupných informací o IT/OT prostředí, které by mohli využít útočníci při plánování kybernetického útoku. Ukážeme vám, jak získat obdobné informace pasivní metodou s cílem zajistit vyšší zabezpečení vaší společnosti.*
* ***Daniel Hejda, Cyber Rangers s.r.o.***

**11:15** **Business Continuity Management aneb jak zajistit kontinuální přežití společnosti**

* *V rámci přednášky vám představíme koncept řízení kontinuity činností jakožto přístupu k zachování činnosti a podnikání i v případě rozsáhlých havárií nebo kybernetických útoků. Tento koncept v sobě zahrnuje jak rychlou reakci na krizovou událost a alespoň základní stabilizaci společnosti, tak aktivaci předem nastavených náhradních procesů a procesů obnovy standardních procesů a infrastruktury po krizové události.*
* ***Michal Beneš, system boost a.s.***

**11:45** **Ukázka kybernetického útoku na OT prostředí**

* *Pamatujme, že útoky do OT přicházejí zejména z IT prostředí, a proto vám ukážeme několik útoků, které by bylo možné realizovat v běžném OT prostředí, přičemž se zaměříme zejména na útoky zneužitím síťové komunikace, špatné bezpečnosti koncových prvků a prvků, které mají limitované možnosti v oblasti obrany. Srdcem soustavy je většinou centrální řídící systém SCADA, a proto vám demonstrujeme, jak může být snadné odstavení takového systému útočníkem, a tím znemožnění vzdáleného řízení.*
* ***Daniel Hejda, Cyber Rangers s.r.o.***

**12:30**  **Diskuse a závěr**

V případě zájmu o účast vyplňte, prosím, následující přihlášku a zašlete ji nejpozději **do 18. 2. 2022** na některý z níže uvedených kontaktů:

* e-mail: [doudova@sovak.cz](mailto: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 24. 2. 2022**

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 101**

Datum: Razítko a podpis: