„KYBERBEZPEČNOST V MALÝCH A STŘEDNÍCH FIRMÁCH“

WORKSHOP/ŠKOLENÍ

Datum: 11. února 2026

Čas: 08:30 - 17:00

Místo: online (MS TEAMS)

Národní klastrová asociace (NCA) společně s partnery **EDIH Northeast a CEDEG z.s.** vám nabízí aktivní participaci na vzdělávání formou online workshopu/školení zaměřeném na kyberbezpečnost v malých a středních firmách.

Co se během bloků dozvíte a co si odnesete?

Přehled současných trendů a budoucího vývoje v oblasti kyberbezpečnosti, jak ve vaší firmě minimalizovat riziko zastavení výroby či finančních ztrát, doplněný o příklady z výrobních firem z ČR i zahraničí a praktické tipy na dílčí řešení.

Registrujte se zde.

Cílová skupina
Majitele a jednatele MSP, manažeři a vedoucí týmů, administrativní pracovníci, obchodníci a marketing, IT správce, a další zástupci MSP.

PODMÍNKY PRO ÚČASTNÍKY

Workshop/školení je dominantně určen pro **malé a střední podniky do 500 zaměstnanců** *(započítávají se zaměstnanci v rámci celé skupiny, účast velkých firem není vyloučena)*.

Pořádá se v rámci projektu EDIH Northeast, přičemž veškerou administraci zajišťuje Národní klastrová asociace (NCA).

Účast malých a středních podniků (MSP)

- Školení je pro MSP do 500 zaměstnanců **plně hrazeno** prostřednictvím podpory **de minimis** v rámci projektu EDIH Northeast.
- Pro čerpání této podpory je třeba uzavřít smlouvu mezi podnikem a NCA, kterou podepisuje statutární zástupce.
- NCA připraví veškeré dokumenty – účastník je pouze podepisuje.
- Workshop je hrazen z projektu EDIH, za každého účastníka bude odečtena částka z de minimis v hodnotě 252,96 EUR na osobu, za 8 hodin. **Účastník nehradí nic.**
- Účastníci obdrží:
  - **certifikát o absolvování školení**
  - **potvrzení o účasti pro firemní HR**

Pro více informací kontaktujte:
Petra Polášková, polaskova@nca.cz
Renáta Pfefferová, pfefferova@nca.cz

NCA NÁRODNÍ KLASTROVÁ ASOCIACE
CE DIGITAL & ENVIRO GROUPING
edih NORTHEAST
Spolufinancováno Evropskou unií
NÁRODNÍ PLÁN OBNOVY
Financováno Evropskou unií NextGenerationEU

KYBERBEZPEČNOST V MALÝCH A STŘEDNÍCH FIRMÁCH
11. únor 2026, 08:30 – 17:00, online

Obsah workshopu/školení

Získejte přehled o aktuálních trendech a vývoji v oblasti kyberbezpečnosti průmyslových firem. Seznámíte se s nejčastějšími hrozbami a riziky, rolí umělé inteligence v útocích i obraně a s praktickými možnostmi jejich efektivní eliminace, doplněnými o konkrétní příklady z českého průmyslového prostředí.

Dozvíte se, jaké dopady má nový Zákon o kybernetické bezpečnosti, AI Act a související regulace na vaši firmu. Získáte také přehled moderních technologických a kyberbezpečnostních řešení, včetně unikátních IT inovací českých společností.

Součástí školení je prostor pro dotazy, odbornou diskusi a možnost bezplatného základního poradenství zaměřeného na konkrétní potřeby vaší firmy v rámci online workshopu.

Kamil Rečičár, Jednatel, IBKA s.r.o.

Kamil Rečičár se přes 20 let věnuje oblasti informační bezpečnosti, zejména pak řízení procesů a rizik bezpečnosti informací. Přes finanční instituce, státní správu, poradenství k výrobním podnikům sbírá zkušenosti a pomáhá optimálně namířit snahu a energii při zavádění, zlepšování a auditu systémů řízení bezpečnosti informací. Cílem vždy bylo, je a bude nalézt optimální způsob ochrany informací pro danou společnost, zejména s ohledem na potřeby organizace, nikoliv demagogicky následovat regulatorní požadavky.

Ladislav Šolc, CEO, Target Five s.r.o.

Ladislav Šolc je zkušený odborník na kybernetickou bezpečnost, bývalý Security Engineer ve společnosti Microsoft a někdejší ředitel Mainstream Technologies. V současnosti působí jako CEO společnosti Target Five. Specializuje se na bezpečnostní návrhy, audity, skenování a ochranu proti interním i externím zranitelnostem, včetně Early Threat Detection a Active Exposure Managementu. Na konferenci nabídne praktické i strategické pohledy na posílení odolnosti organizací vůči kybernetickým útokům.

Pavel Čumpelík, Market Development Manager, WAVE by AGC

Ve společnosti AGC GLASS EUROPE se již od roku 1999 věnuje inovacím v oblasti plochého skla pro architekturu a pokročilé technologické systémy. Vystudoval FS ČVUT a jeho pracovní zkušenosti zahrnují významné projekty R&D i rozvoje trhu. Na pozici manažera WAVETRAP startupu WAVE by AGC, který je součástí výzkumného centra AGC GLASS EUROPE (AGC Technovation Center v Gosselies, Belgie) nyní realizuje řešení pro digitalizaci a komunikační technologie v architektuře i průmyslu, včetně optimalizace jejich dopadu a zodolnění pro zajištění ochrany informací, soukromí a udržitelný rozvoj.

Martin Lohnert, Ředitel centra kybernetické bezpečnosti void SOC, SOITRON s. r. o.

Martin Lohnert má rozsáhlé znalosti a zkušenosti v oblasti síťové infrastruktury a bezpečnosti. Aktuálně řídí Security Operations Center – služba, která je součástí skupiny Soitron s. r. o. pod značkou void www.voidsoc.com. Ve firmě Soitron působil i jako technický vedoucí, vedl marketing Soitron Group a pomohl firmě stát se třetím největším poskytovatelem IT řešení na Slovensku. Byl u toho, když firma Soitron expandovala do České republiky, Rumunska a Turecka. Zhodnocuje své zkušenosti i z pozice IT managera v slovenské pobočce firmy Asea Brown Boveri, nebo Solution Architekta v australském zastoupení Dimension Data.

Jan Kalabus, Channel Sales Director, Logmanager a. s.

Jan Kalabus působí ve společnosti Logmanager, kde odpovídá za vedení obchodního týmu, rozvoj partnerské sítě v regionu CEE a nastavování nových obchodních procesů. Navazuje zde na své zkušenosti ze společnosti Progress | Flowmon, kde získal hlubokou znalost českého i zahraničních trhů. Jeho dlouhodobým cílem je pomáhat zákazníkům a partnerům s identifikací potenciálních hrozeb v podnikových sítích a doporučovat vhodná bezpečnostní opatření.

Jindřich Šavel, CEO, Novicom, s. r. o.

Jindřich Šavel působí v Novicomu od roku 2012 a od května 2020 zastává pozici CEO. Má více než 30 let zkušeností v oblasti IT infrastruktur, aplikačního softwaru, správy dokumentů a procesů, tvorby firemních a marketingových strategií a budování prodejních sítí. Díky realizaci řešení pro správu a zabezpečení počítačových sítí se dlouhodobě věnuje také oblasti kybernetické bezpečnosti.

Peter Csicsay, Sales Director, Inalogy a. s.

S viac ako 16-ročnými skúsenosti v oblasti IT a manažmentu Peter Csicsay zastrešuje pozíciu obchodného riaditeľa. Počas svojej kariéry zastával obdobné funkcie v spoločnostiach Exclusive Networks, Oracle, IBM a Dell.

NÁRODNÍ KLASTROVÁ ASOCIACE
CE DIGITAL & ENVIRO GROUPING
edih NORTHEAST
Spolufinancováno Evropskou unií
NÁRODNÍ PLÁN OBNOVY
Financováno Evropskou unií NextGenerationEU

František Mikuš, Senior IDM Engineer, Inalogy a. s.

Má bohaté skúsenosti s midPoint IDM, hlavne v podnikovom prostredí. Prispel k vývoju MS Graph API Connector, Free IPA Connector a Adaptive SSH Connector. Neustále sa snaží učiť nové veci a rád sa o ne delí s komunitou.

Marek Solařík, Consulting Services Director, Service & Support spol. s r.o. (SANDS)

Marek Kolařík se věnuje konzultačním službám zejména v oblasti bezpečnosti a správy ICT a řízení projektů. Cílem je vždy nalézt a implementovat co nejlepší řešení pro zákazníka, které splní nejen jeho aktuální požadavky, ale bude plně připraveno na další výzvy v budoucnosti. Marek má za sebou již 25 let zkušeností s vývojem, budováním, správou a řízením IT systémů a ICT služeb, s návrhem i kontrolou jejich bezpečnosti a souvisejících procesů s velkou vazbou na business.

PROGRAM WORKSHOPU

08:30 - 09:30
Přivítání účastníků a úvodní slovo

Moderace: Ivo Říha (viceprezident NCA a předseda představenstva CEDEG, z.s.)

Seznámení s lektory

- Kamil Rečičár (Jednatel, IBKA s.r.o.)
- Ladislav Šolc (CEO, Target Five s.r.o.)
- Pavel Čumpelík (Market Development Manager, WAVE by AGC)
- Martin Lohnert (ředitel centra kybernetické bezpečnosti void SOC, SOITRON s. r. o.)
- Jan Kalabus (Channel Sales Director, Logmanager a. s.)
- Jindřich Šavel (CEO, Novicom, s. r. o.)
- František Mikuš (Senior IDM Engineer), Peter Csicsay (Sales Director, Inalogy a.s.)
- Marek Solařík, (Consulting Services Director, SANDS)

9:30 - 10:20
Blok 1: Kde začít a neztratit se

Proč se bezpečnosti informací věnovat a kde začít? Existuje mnoho způsobů, jak začít analyzovat, plánovat a následně zavézt informační bezpečnost do organizace. Zde více, než kdekoliv jinde platí "dvakrát měř, jednou řež". Jak začít neztratit se, je otázka, kterou si klademe na počátku našeho úsilí o zavedení udržitelného způsobu řízení informační bezpečnosti. Od identifikace "kdo jsme", co jsou naše cíle a co je pro nás důležité a jak najít rozumnou úroveň bezpečnosti informací do bodu, kdy budeme chtít provádět zákaznický audit našich klíčových dodavatelů. Stručný a přehledný průvodce, jak začít a neztratit se ve světě informační bezpečnosti.

- Diskuze / Q&A

Workshop vede: Kamil Rečičár, IBKA s.r.o.

10:20 - 11:10
Blok 2: Když nevidíte, co se vám děje v IT - a už je pozdě

Uvidíte, jak vedení malých a středních firem často nemá přehled o tom, kdo má přístup ke klíčovým systémům, jaké změny se v IT dějí a kde vznikají největší bezpečnostní rizika. Na reálných příkladech si vysvětlíme, jak právě „neviditelnost“ vede k útokům, interním incidentům a provozním výpadkům. V závěru představíme, jak lze jednoduše získat přehled, včasné varování a kontrolu bez nutnosti budovat složité bezpečnostní týmy ve formě praktických ukázek.

- Diskuze / Q&A

Workshop vede: Ladislav Šolc, Target Five s.r.o.

11:10 - 12:00
Bok 3 Transparentní elektromagnetický štít pro posílení informačních aktiv

Pro situace, kdy jsou ohrožena informační a kritická aktiva potenciální manipulací, zničením nebo únikem dat prostřednictvím útoků na informační a technologické systémy zblízka, je třeba využít komplexních systémů ochrany. Rizika sabotáže, digitálního odposlechu, dronových incidentů nebo narušení soukromí jsou často spojena s využitím elektromagnetického signálu. Unikátní technologie skla WAVETRAP pro transparentní elektromagnetické stínění nabízí zcela nové možnosti přístupu k selektivnímu zodolnění budov a technologických zařízení na vysokou úroveň ochrany před těmito riziky. Na praktických příkladech vysvětlujeme tyto méně známé hrozby a navrhujeme inovativní opatření pro zajištění optimální úrovně bezpečnosti. Okna a jiné prosklené části budov bez EM stínění byla dříve slabým místem, dnes je tuto situaci možné díky novému typu skla efektivně řešit. Řešená oblast technologií má v oblasti zdravotnictví stále větší význam.

NCA NÁRODNÍ KLASTROVÁ ASOCIACE
CE DIGITAL & ENVIRO GROUPING
edih NORTHEAST
Spolufinancováno Evropskou unií
NÁRODNÍ PLÁN OBNOVY
Financováno Evropskou unií NextGenerationEU

- Diskuze / Q&A

Workshop vede: Pavel Čumpelík, WAVE by AGC

12:00 – 12:30
Obědová pauza

12:30 – 13:20
Blok 4 Skutečná tvář kyberútoků na průmysl, aneb jak hacknout fabriku za 10 minut

Jak reálně probíhá kybernetický útok na průmyslovou firmu? Jak útočníci hledají cesty dovnitř a proč jsou ICS/OT prostředí zranitelná, často dokonce veřejně dostupná z internetu? Na základě konkrétních příkladů z praxe ilustrujeme, že dopady útoků nejsou jen IT problém, ale mohou znamenat zastavení výroby, poškození strojů, ekonomické ztráty i ohrožení zdraví lidí. Závěr prezentace přiblíží opatření, jak může vedení firem zvýšit bezpečnost – od budování povědomí až po využití služeb, které dokážou snížit riziko a výrazně zkrátit dobu reakce.

- Diskuze / Q&A

Workshop vede: Martin Lohnert, SOITRON s. r. o.

13:20 – 14:10
Blok 5 Logy jako základní kámen pro IT

Logy už dávno nejsou jen mrtvá data pro archivaci. V éře, kdy o úspěchu rozhodují minuty, se log management stává centrálním mozkem pro IT provoz i kybernetickou bezpečnost. V této přednášce se podíváme na aktuální trendy, které mění pravidla hry – od centralizace až po automatizovanou analýzu.

- Diskuze / Q&A

Workshop vede: Jan Kalabus, Logmanager a. s.

14:10 – 15:00
Blok 6 Automatizace síťové správy jako základ okamžité reakce při řešení kybernetických incidentů

V dnešní době jsou již dostatečně vnímány kybernetické hrozby a organizace se úspěšně vyzbrojují detekčními nástroji. Standardem se staly rovněž nástroje pro ochranu perimetru a ochranu klientů. Co však dělat, když útočníci překonali tyto ochrany a hrozba se šíří interní sítí? Jak rychle reagovat a jak to propojit s optimálním bezpečnostním modelem – službou sdíleného SOC (Security Operations Center)? K tomu slouží integrované nástroje síťových služeb (DDI/NAC), které nejenom pomohou s automatizací reakcí ve vnitřní síti, ale také pomohou s řádově efektivnější síťovou správou a výrazně zvýšenou bezpečností interní sítě, a to díky možnosti aplikací pokročilých síťových politik včetně mikrosegmentace.

- Diskuze / Q&A

Workshop vede: Jindřich Šavel, Novicom, s. r. o.

15:00 – 15:50
Blok 7 Základná problematika a úskalia pri implementácií IAM (Identity Access Management)

IAM (Identity Access Management) je základním kamenem moderní kybernetické bezpečnosti. Kromě zvýšení bezpečnosti podniku, správy přístupu, odlehčení přetížených IT oddělení od provozních úkolů, pomoci při plnění regulačních požadavků, automatizace procesů a sloužení jako zdroj pro auditory plní řadu dalších funkcí, které jsou pro moderní společnost nepostradatelné.

V této prezentaci budeme diskutovat o výzvách, kterým čelíme při nasazení IAM, a podíváme se na atributy, které by měly hrát klíčovou roli při výběru správného nástroje.

- Diskuze / Q&A

Workshop vede: František Mikuš – Senior IDM Engineer, Inalogy a. s., Přísedící: Peter Csicsay, Inalogy a. s.

15:50 – 16:40
Blok 8 Jak si poradit s identifikací aktiv v praxi *(TBC)*

Identifikace aktiv je základním stavebním kamenem bezpečnosti i řízení kontinuity podnikání (BCM). V přednášce ukážeme, proč firmy často chybují při rozlišování primárních a podpůrných aktiv, jak aktiva správně pojmenovat, přiřadit jim odpovědnost a jak celý proces uchopit v praxi. Na konkrétním příkladu z průmyslové firmy představíme osvědčený postup krok za krokem a přínosy správně nastavené hierarchie aktiv pro další bezpečnostní i provozní řízení.

- Diskuze / Q&A

Workshop vede: Marek Solařík, SAND

16:40 – 17:00
Závěrečné slovo NCA, prostor pro diskuzi/otázky.

Pořadatel si vyhrazuje právo upravit program podle aktuální situace.