

Jak řídit kybernetickou bezpečnost v malých a středních organizacích?

Sleva 10% při objednání 2 a více účastníků sleva bude odečtena ze zobrazené ceny

Termín

20.6.2025

Online seminář

Živé vysílání sledujete online z domova či kanceláře. S lektorem komunikujete formou chatu nebo pomocí mikrofonu.

Cena bez DPH

2 990,00 Kč

3 617,90 Kč s DPH

Profil lektora

Dan Kresa



Vystudoval Bezpečnostní a strategická studia na Masarykově univerzitě. Šest let působil na platformě KYBEZ, která se věnuje vzdělávání a spolupráci firem a akademického sektoru v kybernetické bezpečnosti. Pracoval rovněž ve společnosti, která se zabývá kybernetickou bezpečností, jako vedoucí oddělení vzdělávání, kde se věnoval tvorbě a řízení interních kurzů v oblasti kybernetické bezpečnosti a také různým projektům se středními a vysokými školami.

Přejete si začít řešit kybernetickou bezpečnost, aby to mělo hlavu a patu? Nebo nově spadáte mezi povinné subjekty kvůli zavedení NIS2? Či snad si chcete jen ověřit, zda řídíte kybernetickou bezpečnost správně a nasbírat nové poznatky? Tak přesně pro Vás je tento webinář. Dozvíte se nejen jak spravovat kybernetickou bezpečnost z pohledu legislativy, ale také získáte zajímavé informace z oblasti „best practice“, díky kterým zlepšíte vaše rozhodování. V rámci webináře si vyzkoušíte pár praktických úkolů a budete mít dost prostoru pro případné dotazy.

Cíl semináře

Díky tomuto webináři zlepšíte procesní řízení kybernetické bezpečnosti ve vaší organizaci, a tím mimo jiné splníte i požadavky nových vyhlášek v této oblasti.

Zjistíte:

- čím začít při řízení kybernetické bezpečnosti,
- co musí splňovat osoby odpovědné za řízení dané oblasti,
- jaké jsou úkoly Výboru a kdo by měl být jeho členem,
- v čem je přínosné prohlášení o aplikovatelnosti (POA),
- proč se vyplatí zavést řízení rizik,
- jak nastavovat a plnit cíle kybernetické bezpečnosti,
- proč je nutné mít neustále na paměti kontinuální zlepšování.

Naše školení předá nejen informace o legislativě, ale také získáte praktická doporučení, jak nové povinnosti zavést do své praxe.

Komu je seminář určen

Školení ocení zejména vedoucí ICT, analytici, tajemníci, starostové, ředitelé a jejich zástupci, případně další osoby, které jsou či budou pověřeny řízením kybernetické bezpečnosti nebo chtějí svoji organizaci chránit před kyberútoky a dalšími hrozbami.

Program

Živé vysílání 10:00 - 12:00 hod.

- Osvětlení důležitosti správného řízení kybernetické bezpečnosti
- Představení jednotlivých bezpečnostních rolí
- Vysvětlení a ukázka práce s prohlášením a aplikovatelnost (POA)
- Obeznamení s analýzou rizik a její důležitosti
- Tvorba cílů a přestavení Demingova cyklu

- Diskuze

Další informace

Každý účastník kurzu obdrží CERTIFIKÁT o jeho absolvování, který může využít ve svém CV v části o doplňkovém odborném vzdělávání.

Forma semináře - živé vysílání (online seminář). Není potřeba nic instalovat ani stahovat - živé vysílání sledujete pouze po jednom kliku na odkaz, který obdržíte emailem.

Živé vysílání sledujete přímo na PC, notebooku nebo tabletu ve svém prohlížeči (Google Chrome, Mozilla Firefox, Microsoft Edge nebo Safari) z pohodlí Vašeho domova či kanceláře.

Během semináře lze pokládat prostřednictvím chatu dotazy lektorovi. Seminář pro Vás nahráváme, záznam ze semináře obdržíte následující pracovní den.

Objednávka: Jak řídit kybernetickou bezpečnost v malých a středních organizacích?

Sleva 10% při objednání 2 a více účastníků sleva bude odečtena ze zobrazené ceny

Fakturační údaje objednatele:

IČO:	
DIC:	
Firma:	
Jméno a příjmení:	
Telefon:	
Email:	
Ulice:	
Město:	
PSČ:	
Vaše č.obj.: (bude uvedeno na faktuře)	
Poznámka:	

Účastníci:

Jméno vč. titulů	
Telefon:	
Email:	
Jméno vč. titulů	
Telefon:	
Email:	
Jméno vč. titulů	
Telefon:	
Email:	

Formulář vytiskněte, vyplňte, naskenujte a zašlete nám jej na email: **info@eduzone.cz**
nebo účast objednejte v našem e-shopu **www.eduzone.cz**