Jak zpracovat analýzu rizik v kybernetické bezpečnosti? Vyřešte jednu z povinností NIS 2 snadno a pohodlně.

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

Termín
29.5.2025

Online seminář

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

Cena bez DPH
3 970,00 Kč
4 803,70 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.

Analýza rizik v kybernetické bezpečnosti je pro organizaci zásadní, protože poskytuje hluboký vhled do potenciálních hrozeb a zranitelností, kterým organizace v digitálním prostředí čelí. Tato analýza umožňuje vytvořit strategie a plány, které minimalizují rizika a umožňují rychlou reakci v případě incidentů. Analýza rizik tvoří základ pro efektivní řízení kybernetických hrozeb a ochranu cenných aktiv organizace. Zároveň se jedná o jednu z povinností, vyplývající ze směrnice NIS 2.

Cíl semináře

Díky tomuto on-line semináři získáte přesný obraz o fungování ICT ve vaší organizaci. Naučíte se:

- jak správně provést evidenci a hodnocení aktiv,
- jak vést přehled hrozeb a zranitelností,
- jak vyhodnotit rizika,
- jak vytvořit plán zvládání rizik,
- další cenné postupy

Naše školení vám poskytne nejen znalosti o legislativě a metodice v oblasti kybernetické bezpečnosti, ale také praktické návody, jak v při zpracování analýzy rizik postupovat. Připravte se na hrozby kybernetického prostoru a zabezpečte svou organizaci.

Komu je seminář určen

Školení ocení zejména vedoucí ICT, analytici, auditoři, metodici, konzultanti, zástupci vedení organizace, členové výboru kybernetické bezpečnosti a další stěžejní pracovníci organizace. U účastníků se předpokládá základní orientace v problematice kybernetické bezpečnosti.

Program

Živé vysílání 9:00 - 12:00 hod.

- Co je to analýza rizik? Proč a jak ji zpracovávat?
- Legislativní rámec (Vyhláška o kybernetické bezpečnosti, ISO 27 000, Směrnice NIS 2)
- Zmapování organizace
- Přehled a hodnocení aktiv
- Evidence hrozeb a zranitelností
- Hodnocení rizik
- Návrh opatření
- Plán zvládání rizik
- Plán kontinuity
- Bezpečnostní strategie organizace

- 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 a mikrofonu dotazy lektorovi. Seminář pro Vás nahráváme, záznam ze semináře obdržíte následující pracovní den.

eduzone®

Objednávka: Jak zpracovat analýzu rizik v kybernetické bezpečnosti? Vyřešte jednu z povinností NIS 2 snadno a pohodlně.

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

Fakturační údaje objednatele:

IČO:

DIČ:

Firma:

Jméno a přijmení:

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**