Jak zvládnout kybernetický útok? Procesní cvičení reakce na mimořádné bezpečnostní situace

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

Termín
29.2.2024

Online seminář

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

Cena bez DPH
4 970,00 Kč
6 013,70 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.

Ředitelství silnic a dálnic, pražský magistrát, společnost Mall či Benešovská nemocnice. To je jen pár organizací, které zasáhly významné problémy v oblasti kybernetické bezpečnosti. Jak reagovat na tyto mimořádné krizové situace? Co byste dělali, kdyby vaši organizaci postihl kybernetický útok? Jak byste danou věc řešili? Díky našemu semináři si celý tento proces vyzkoušíte na nečisto a zjistíte, na jaké oblasti jste ve vašem bezpečnostním systému zapomněli a na co se ještě musíte podívat.

Cíl semináře

S pomocí procesního cvičení si otestujete vaši reakci na kybernetický útok a další s tím spojené mimořádné události. V rámci cvičení spolupracují účastníci jako tým na řešení různých bezpečnostních výzev, které vycházejí z předem stanoveného scénáře, který ovšem účastnici předem neznají. Ačkoliv celý příběh začíná zdánlivě jednoduchým a malicherným bezpečnostním přečinem, vše postupně graduje až do velmi závažných bezpečnostních problémů. Cvičící velmi často zjistí, že musí o kybernetické bezpečnosti přemýšlet v mnohem širším měřítku než dosud. Hlavním cílem procesního cvičení je co nejlépe vás připravit na vypuknutí mimořádných situací, abyste se nedostali do zbytečných problémů, na jejichž řešení byste vydali nemálo času, úsilí a peněz.

Komu je seminář určen

Seminář je určen především osobám ve vedení organizace, manažerům kybernetické bezpečnosti, vedoucím IT a dalším osobám, se kterými budete v případně mimořádné události komunikovat (např. zástupci personálního oddělení, právního, marketingu či tiskového). Uvítáme také všechny, kteří se zajímají o kybernetickou bezpečnost z praktického hlediska.

Program

Živé vysílání 9:00 - 13:00 hod.

- Nejčastější formy útoků v kybernetické bezpečnosti
- Organizační rozdělení
- Představení modelové organizace (úvodní prezentace)
- První polovina cvičení
- Přestávka

- Druhá polovina cvičení
- Diskuse a hodnocení

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 zvládnout kybernetický útok? Procesní cvičení reakce na mimořádné bezpečnostní situace

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**