Cybersecurity Fundamentals

Bereid uw bedrijf voor op de uitdagingen van cybersecurity en de NIS 2 Richtlijn



Dompel jezelf onder in de wereld van cybersecurity met onze intensieve tweedaagse training, speciaal ontworpen om theorie en praktijk om te zetten in concrete vaardigheden. Ga mee op reis door de fundamentele aspecten en huidige uitdagingen van informatieveiligheid.

2 trainingsdagen om:

• **de basisprincipes en geavanceerde aspecten van cybersecurity te ontdekken**, inclusief de nieuwste praktijken in risicobeheer, netwerkbeveiliging, en naleving van regelgeving zoals GDPR en NIS2.

• **te leren om interne en externe bedreigingen te identificeren en tegen te gaan**, terwijl je de methoden van cryptografie en de geschikte tegenmaatregelen begrijpt.

• **een concrete expertise in informatieveiligheid te ontwikkelen**, met tools en technieken om complexe omgevingen te beveiligen

Beheers de essentiële basisprincipes en geavanceerde technieken van cybersecurity om uw organisatie te beschermen tegen moderne bedreigingen. Veiligheid is een integraal onderdeel van de werkomgeving van een netwerk- en systeembeheerder. Het moet worden bedacht en geïntegreerd in de eerste fasen van het ontwerp van netwerken en systemen, lang voordat ze worden geïmplementeerd. Maar om dit te doen, is het absoluut noodzakelijk om de basis- en geavanceerde beveiligingsconcepten te begrijpen, of ze nu betrekking hebben op de bedreigingsomgeving om ons heen of de risicobenaderingen die bedoeld zijn om de relevantie van bescherming of tegenmaatregelen te evalueren. Bovendien moeten heterogene omgevingen zoals Hybrid-Cloud en regelgeving zoals GDPR/NIS 2 in perspectief worden geplaatst ten opzichte van de uitdagingen van cyberbeveiliging. Deze eerste training zal een goed begrip van de sleutelonderdelen van cyberbeveiliging mogelijk maken en uw bedrijf of organisatie voorbereiden op de inwerkingtreding van de NIS 2-richtlijn. U kunt vervolgens meer geavanceerde trainingen volgen, zoals ISO 27001, NIS 2, etc. Trainingsdoelstellingen De deelnemers aan ons cybersecurity-trainingsprogramma zullen hun begrip van de basisprincipes die ten grondslag liggen aan en de cybersecurity definiëren, evenals de essentiële rollen van cybersecurity-professionals bij het beschermen van bedrijfsgegevens en infrastructuur, aantonen. Begrijpen wat de woorden "IT Security" & "Cyber Security" betekenen Begrijpen van de "risicobenadering" methodologie en de methoden om dit te beoordelen (zowel kwantitatief als kwalitatief) (bijv. octaaf, cobit, ISO2700x, ...) Begrijpen van de bedreigingen om ons heen en de aanvallen die netwerken, systemen en Cloud-omgevingen continu ondergaan Begrijpen en implementeren van een effectieve en passende beveiligingsbenadering in een complexe IT-omgeving (CSP, Security Wheel, ...) Trainingsinhoud Security Definitie De drie A's van Beveiliging (inclusief Auditing) Het beoordelen van veiligheidsrisico's Risicoconcept Risicoformule Risicobeoordeling Risicodoelstelling Risicomatrix Risicometrieken Risico's vanuit bedrijfsperspectief De Gap-benadering Risico-illusie Data Risico Analyse Toegepaste data-risico's Data Risico Beheer Veiligheidsbedreigingen Interne bedreigingen Sociale engineering Onbedoelde beveiligingsinbreuk Exogene bedreigingen Fysieke bedreigingen Bedreigingen voor mobiele gebruikers Externe aanvallen Historische feiten Nieuwe trends in bedreigingen Beveiligingsbeleid CSP PDCA NIST NIS2 Algemene aanvalsmethoden (inclusief websites) Authenticatie Gecompromitteerde vertrouwde systemen Standaardconfiguraties Onjuiste invoervalidatie Toepassingen & Diensten Ontkenning van dienstverlening (DoS) Virussen, Wormen, Trojaanse paarden, Backdoors... Draadloze netwerkaanval Fysieke toegang OT (Operationele Technologie) Beveiligingstegenmaatregelen (inclusief verkeersstromen, filtering, firewalling, beveiligingsarchitectuur, OT, ...) Introductie tot cryptologie: Geschiedenis Cryptografische algoritmen PKI Andere algemene beveiligingsaspecten: Hardwarebeveiliging Infrastructuurbeveiliging Back-ups Anti-Malware Rampenherstelplan (DRP & BCP) Beveiligingsprocedures Voor wie is deze training bedoeld? Deze training is bedoeld voor iedereen die de problematiek van cybersecurity in zijn geheel wil begrijpen om de beveiliging van zijn organisatie te versterken. Systeem- of netwerkbeheerder verantwoordelijk voor infrastructuur Personen die verantwoordelijk zijn voor het definiëren van IT-beveiligingsstrategieën IT Manager, Infrastructure Manager of CIO - DPO belast met de bescherming van medische of persoonlijke gegevens (GDPR) Vereisten Technisch begrip van IT-omgevingen De volgende elementen zijn voordelen om alle technische aspecten die zullen worden besproken te begrijpen: Technische ervaring in ten minste één server OS en één netwerkplatform

- Diepgaande kennis van netwerkcommunicatie

CURSUSMATERIAAL

De presentatie van de training zal in papieren en digitale vorm aan alle deelnemers van de training worden uitgedeeld.

Gedurende de training zullen de deelnemers een reeks lezingen ontvangen die hen kunnen helpen de gepresenteerde concepten te begrijpen. We zullen ook de belangrijkste Europese gidsen en regelgeving in elektronisch formaat met u delen.

Als uw bedrijf meerdere werknemers heeft die een training in cyberbeveiliging nodig hebben of als u het COMEX en/of management wilt opleiden, onze op maat gemaakte trainingsoplossingen stellen ons in staat de inhoud aan te passen aan de specifieke behoeften en doelstellingen van uw teams. Onze trainers zijn praktijkmensen met uitgebreide ervaring in hun vakgebied, die hun bewezen expertise in cyberbeveiliging meebrengen.