

Ziele

Mit erfolgreichem Abschluss des Kurses werden die Teilnehmenden in der Lage sein:

- » Bedrohungssituationen (Spionage, Sabotage, Mißbrauch) einzuschätzen.
- » Geeignete Abwehr- und Schutzmaßnahmen zu bewerten.
- » IT-Sicherungskonzepte zu verstehen.
- » E-Mails und Daten zu ver- und entschlüsseln.
- » Mit Hilfe geeigneter Maßnahmen die Integrität von Unternehmensdaten und ihre eigene Privatsphäre zu schützen.
- » Die Grundsicherung des eigenen Rechners einzurichten.

Vorteile

- » Sie bewegen sich sicherer im Internet.
- » Erhöhter Schutz vor IT-Angriffen.
- » Informationen und Daten sind besser geschützt und können sicherer ausgetauscht werden.

Kontakt / Anmeldung

Ihre Ansprechpartnerinnen:

Uta Pricken
Technologie- und Gründerzentrum Niederrhein
Industriering Ost 66
47906 Kempen
Telefon: +49 (0)2152 / 2029-21
E-Mail: uta.pricken@tzniederrhein.de

Britta Benning
Wissenschaftliche Weiterbildung
Hochschule Niederrhein
Reinarzstraße 49
47805 Krefeld
Telefon: +49 (0)2151 / 822-1515
E-Mail: weiterbildung@hs-niederrhein.de

Fachlich verantwortlich:

Prof. Dr. Jürgen Quade
Technische Datenverarbeitung
insbesondere Prozessautomatisierung
Prodekan des Fachbereichs Elektrotechnik/Informatik
Hochschule Niederrhein
Web: www.hs-niederrhein.de/elektrotechnik-informatik/personen/quade
E-Mail: weiterbildung@hs-niederrhein.de

Weitere Informationen und Online-Anmeldung:
wfg-kreis-viersen.de/zertifikatskurs-it-sicherheit



Zertifikatskurs IT-Sicherheit

Wissenschaftliche Weiterbildung im Kreis Viersen

Hoher Praxisbezug und nachhaltiger Lernerfolg. Ein Angebot der Hochschule Niederrhein und der Wirtschaftsförderung für den Kreis Viersen.

Kurzbeschreibung

Die spektakulären Angriffe auf Rechner, Smartphones, Netzwerke und technische Anlagen verdeutlichen die dringende Notwendigkeit, sich strukturiert und fundiert mit dem Thema IT-Security auseinanderzusetzen.

Für die IT-Sicherheit im Unternehmen, aber auch für die eigene Sicherheit, ist dabei jeder einzelne Mitarbeitende - nicht nur in der IT-Abteilung - mitverantwortlich. Grundlagenkenntnisse sind hierfür unabdingbar.

Dieser Hochschulzertifikatskurs klärt über Angriffsmethoden bössartiger Hacker auf und zeigt, wie man sich schützen kann. Dazu werden Grundlagenkenntnisse rund um Verschlüsselung (Kommunikation, Daten, digitale Unterschriften, Zertifikate, symmetrische und asymmetrische Verschlüsselung, Authentifizierung), Angriffsarten auf Endgeräte und Server (Spoofing, Code-Injection, Frontalangriffe) sowie Einblicke in die rechtlichen Grundlagen für IT-Sicherheit in einem Unternehmen gegeben. Ein besonderes Augenmerk liegt auf der praktischen Erprobung von theoretischem Wissen in der modernen Laborumgebung der Hochschule.

ZIELGRUPPE/N:

Dieses Angebot richtet sich an Beschäftigte aller Branchen, die Interesse an IT-Sicherheitsthemen haben.

TEILNAHMEVORAUSSETZUNGEN:

Hochschulabschluss mit mindestens einjähriger Berufserfahrung oder anderweitiger berufsqualifizierender Abschluss mit mindestens dreijähriger Berufstätigkeit.

TEILNEHMERZAHL:

Um eine individuelle Betreuung gewährleisten zu können, ist die Teilnehmerzahl auf max. 10 beschränkt.

Curriculum

GRUNKURS

Präsenz 1	<u>Einführung</u> Sensibilisierung, Schutzziele, Gefährdungspotenzial, Risikoanalyse, Viren - Würmer - Trojaner, Rootkits	8h
	<u>Theoretische Grundlagen der Kryptografie</u> Symmetrische Verschlüsselung, Kryptografische Betriebsarten, Hashfunktionen, Asymmetrische Verschlüsselung (Public Key Verfahren), Digitale Zertifikate (x.509), PKI, Web of Trust	
	<u>E-Mail-Verschlüsselung</u> Software-Integration, Schlüsselgenerierung, Schlüsselverteilung, Praktische Übung: Verschlüsselter E-Mail-Versand	
Selbstlerneinheit	Nachbereitung der Inhalte, Übungsaufgaben (Lernunterstützung durch Online-Lernplattform)	9h
Präsenz 2	<u>Datenverschlüsselung</u> Grundlagen, Sicherheit von Cloud-Diensten, Praktische Übung: Dateisystemverschlüsselung mit Truecrypt oder Veracrypt	8h
	<u>Angriffsarten</u> Spoofing (Phishing, Social-Engineering, Man in the Middle), Code Injection, XSS-Attacke, Frontalangriffe (DDoS), Praktische Übung: SQL-Injection	
	<u>Sicherheitstechnische Grundlagen der Netzwerktechnik</u> IP-Adressen, Routing, Domain Name Service (DNS), NAT	
	<u>Security in Unternehmen I</u> Rechtliche Rahmenbedingungen, Datenschutz	
	<u>Security in Unternehmen II</u> Security Audit, Grundschutzhandbuch	

Gesamter Zeitaufwand = 25h, davon Präsenz = 16h, 1 ECTS

Ablauf

KURSTERMINE:

Präsenz 1: Freitag, 13.04.2018 | 9 bis 17 Uhr

Präsenz 2: Freitag, 20.04.2018 | 9 bis 17 Uhr

PRÜFUNG UND ABSCHLUSS:

Alle Teilnehmenden, die mindestens 75 % des Kurses besucht haben, erhalten eine Teilnahmebescheinigung. Für ein Zertifikat der Hochschule Niederrhein ist eine Abschlussprüfung erfolgreich zu bestehen.

ORT:

Gründerzentrum im Gewerbepark Stahlwerk Becker, Gießerallee 19, 47877 Willich

KOSTEN:

490,00 € zzgl. MwSt. pro Teilnehmer

In der Kursgebühr enthalten sind Seminarunterlagen, Getränke, ein warmer Mittagsimbiss und, sofern kein eigenes adäquates Laptop vorhanden ist, auch ein Leihgerät.

Online-Anmeldung:

wfg-kreis-viersen.de/zertifikatskurs-it-sicherheit