DISTART

WEITERBILDUNG

IT-SICHER-HEITSANALYSE

mit DISTART

Träger- und Maßnahmenzulassung
GZQ CERTIFICATION
AZAV

Kundenmeinungen
der letzten 12 Monate
TOP DIENSTLEISTER 2026
Mehr Infos
Proven Expert

TOP
FERNSCHULE
Award 2026
FernstudiumCheck.de

IT-SICHERHEITSANALYSE

INHALT DER WEITERBILDUNG

Cyberangriffe, **Sicherheitslücken** und **digitale Bedrohungen** gehören heute zu den größten Herausforderungen moderner Unternehmen. Dieses Modul vermittelt **praxisnah**, wie IT-Systeme, Netzwerke und Anwendungen gezielt auf **Schwachstellen analysiert** und **professionell abgesichert** werden – von Grundlagen der IT-Sicherheit über Penetrationstests bis hin zu Sicherheitsanalysen von Webanwendungen, APIs und Netzwerken. Ziel ist es, Sicherheitsrisiken frühzeitig zu erkennen und IT-Infrastrukturen nachhaltig zu schützen. Dabei werden folgende **Kernkompetenzen** vermittelt:

- **Penetration Testing & Schwachstellenanalyse:** Planung und Durchführung kontrollierter Angriffssimulationen zur Identifikation kritischer Sicherheitslücken.
- **Web-, API- & Netzwerksicherheit:** Analyse typischer Schwachstellen in APIs, Netzwerken und Webanwendungen, sowie Entwicklung geeigneter Schutzmaßnahmen und Sicherheitsstrategien.
- **IT-Infrastrukturen & Active Directory:** Untersuchung von Unternehmensnetzwerken und Berechtigungssystemen inklusive Angriffssimulationen und Absicherungskonzepten.
- **Sicherheitsmaßnahmen & Reporting:** Entwicklung organisatorischer und technischer Sicherheitsmaßnahmen sowie professionelle Dokumentation strukturierter Penetrationstest-Berichte.

Das Modul umfasst **praxisorientierte Übungen, Lektionsprüfungen** sowie **Live-Q&A-Sessions**, um offene Fragen zu klären und erlernte Inhalte gezielt zu vertiefen. Teilnehmer:innen erhalten somit die Werkzeuge, um **IT-Systeme professionell** auf Schwachstellen zu **analysieren**, Sicherheitsrisiken zu **bewerten** und gezielte **Schutzmaßnahmen abzuleiten**.

DIE WICHTIGSTEN FAKTEN VORAB

Maßnahmennummer: 075 / 367 / 25

Zeitlicher Aufwand

430 UE / 322,5 Zeitstunden
über einer Dauer von:
Teilzeit – 18 Wochen
Vollzeit – 9 Wochen

Abschluss

Anerkanntes **Arbeitsmarktzertifikat:** „Digitales Marketing, Management und KI: IT-Sicherheitsanalyse“

Kosten

Dieses Modul kann bis zu **100 % gefördert** werden (z. B. über den Bildungsgutschein oder das Qualifizierungschancengesetz).

KURSINHALTE

01

Grundlagen IT-Sicherheit & Penetration Testing

Einführung in Grundlagen von Penetrationstests, Bedrohungen, rechtliche Rahmenbedingungen, Sicherheitsziele und Umgang mit Schwachstellenanalysen.

+ Lektionsquizze

02

Schwachstellen in Web-anwendungen & APIs

Analyse von Webanwendungen und APIs auf typische Sicherheitslücken, Durchführung von Reconnaissance, Sicherheitsscans und Einführung in API Penetration Testing.

+ Lektionsquizze **+ Praxisübung**

03

Netzwerke, Exploitation & Infrastruktur

Datenqualität, API-Nutzung, Export von Datenquellen und Aufbau von Reporting-Dashboards – visuell ansprechend, zielgerichtet und auf Stakeholder abgestimmt.

+ Lektionsquizze **+ Praxisübung**

04

Phishing & organisa-torische Sicherheit

Einführung in Active Directory und typische Angriffsszenarien auf Unternehmensnetzwerke, Analyse menschlicher Sicherheitsrisiken wie Phishing und organisatorischer Schutzmaßnahmen.

+ Lektionsquizze **+ Praxisübung**

05

Präventive Maßnahmen & IT-Schutzkonzepte

Entwicklung technischer und organisatorischer Sicherheits-maßnahmen – von Zugriffskontrolle und Passwortmanagement über Firewalls bis hin zu Backup- und Notfallstrategien.

+ Lektionsquizze **+ Praxisübung**

06

Abschlussprojekt & Abschlussprüfung

Planung, Durchführung und Dokumentation eines vollständigen Penetrationstests in einer realis-tischen Laborumgebung – inkl. Risikoanalyse, Schutzmaßnahmen und professionellem Reporting.

+ individuelles Feedback

IT-SICHERHEITSANALYSE IN DER PRAXIS

Ein Unternehmen möchte seine IT-Infrastruktur gezielt auf Sicherheitslücken überprüfen und potenzielle Cyberrisiken frühzeitig erkennen. Durch strukturierte Penetrationstests und Sicherheitsanalysen werden Schwachstellen in Webanwendungen und internen Systemen identifiziert und abgesichert.

- **Identifikation kritischer Sicherheitslücken in Webanwendungen & Netzwerken**
- **Verbesserte Sicherheitsmaßnahmen durch gezielte Schutz- und Präventionsstrategien**

IT-Sicherheitsanalyse zeigt, wie Unternehmen ihre digitale Infrastruktur proaktiv absichern, Cyberrisiken minimieren und Sicherheitslücken erkennen, bevor Angreifende sie ausnutzen.

KONTAKT

WIE ERREICHT MAN UNS?

+49 341 9288 039

hallo@distart.de

www.distart.de

distart.de

@distart

DISTART EDUCATION GMBH

Bildungsträger für digitales Marketing

Petersstraße 35

04109 Leipzig

DISTART

Zertifizierte Qualität

Träger- und Maßnahmenzulassung GZQ CERTIFICATION AZAV

Kundenmeinungen der letzten 12 Monate TOP DIENSTLEISTER 2026 Mehr Infos Proven Expert

Distart Education GmbH Proven Expert Kundenbewertungen SEHR GUT 99% Empfehlungen 1.286 Kundenbewertungen

FERNSTUDIUM CHECK.de Teilnehmerbewertung 4.9 100% Weiterempfehlung sehr gut

TOP FERNSCHULE Award 2026 FernstudiumCheck.de

BVDW Member

Meta Business Partner

Stand: 22.05.2026

DIGITAL START STATT RESTART