



School of
Engineering

CAS Angewandte
IT-Sicherheit



Kurzbeschreibung

Das CAS Angewandte IT-Sicherheit richtet sich gleichermassen an Informatikerinnen und Informatiker sowie Praktikerinnen und Praktiker aus verwandten Fachbereichen. Sie haben die Chance, ihre Fähigkeiten im Bereich IT-Security und somit in einem der grössten Wachstumsmärkte der IT auf- bzw. auszubauen. Das Angebot bietet den Studierenden ein solides technisches Rüstzeug sowie Grundkenntnisse in verwandten Bereichen wie Sicherheits- und Risikomanagement sowie Cybersicherheit an. Während der Schwerpunkt im technischen Bereich liegt, werden deren rechtliche und betriebliche Aspekte ebenfalls behandelt.

Die Teilnehmenden werden in die Bereiche Sicherheitsarchitektur und -management, Kryptologie und Netzwerksicherheit sowie Software- und Systemsicherheit eingeführt. Sie erhalten in ausführlichen und praxisnahen Übungen die Gelegenheit, ihr neu erworbenes Wissen anzuwenden.

Zielpublikum

Das CAS Angewandte IT-Sicherheit richtet sich an IT-Expertinnen und -Experten sowie Quereinsteiger, die ihre Kompetenz auf dem Gebiet der angewandten IT- und Informationssicherheit erweitern möchten. Die Teilnehmenden sind in der Lage, ihre Kenntnisse auf akademischem Niveau zu konsolidieren und so eine Basis für ihre weitere Karriere zu schaffen.

Das CAS Angewandte IT-Sicherheit richtet sich an ein technisches Publikum sowie an Führungspersonen mit technischem Hintergrund, die ihr Wissen mit einem praktischen und anwendungsorientierten Fokus erweitern möchten. So zählen beispielsweise neu betraute oder künftige IT-Security-Manager zum Zielpublikum.

Ziele

Die Studierenden erhalten umfassende theoretische Grundlagen und praktische Fähigkeiten in den Bereichen Sicherheitsarchitektur, Sicherheitsmanagement, Kryptologie, Netzwerksicherheit, Angriffs- und Verteidigungstechniken, sichere Softwareentwicklung, Sicherheitstests und -audits sowie Secure Software Lifecycle. Die Absolventinnen und Absolventen sind in der Lage, Risiken zu identifizieren und zu beurteilen und technische Sicherheitskonzepte zu entwerfen und umzusetzen. Sie können eingeführte Sicherheitsmassnahmen beurteilen, testen und zielgerichtet verbessern.

Struktur und Inhalt

Die im CAS Angewandte IT-Sicherheit vermittelten Kompetenzen orientieren sich an den Fähigkeitsprofilen für IT- und Informationssicherheitsverantwortliche. Das CAS Angewandte IT-Sicherheit ist modular aufgebaut und besteht aus drei Modulen.

Modul	Inhalt	Lernziele	ECTS
Security Architecture and Management	<ul style="list-style-type: none">– Sicherheitsgrundlagen– Sicherheitsarchitektur– Sicherheitsmanagement	<ul style="list-style-type: none">– Die Studierenden kennen die organisatorischen, führungstechnischen und betrieblichen Grundlagen der IT-Sicherheit.– Sie sind in der Lage, ein Sicherheitskonzept zu entwerfen und bei der Umsetzung mitzuwirken.– Sie beherrschen die Grundlagen der einschlägigen Standards und Best Practices und können diese in der Praxis anwenden.	3
Cryptography and Network Security	<ul style="list-style-type: none">– Kryptologie– Methoden und Protokolle zur Sicherung von Systemen im Internet– Angriffs- und Verteidigungstechniken	<ul style="list-style-type: none">– Die Studierenden verstehen die Grundlagen der Kryptologie (Algorithmen, Einsatzzwecke, Resilienz), die die Basis für eine Vielzahl moderner Sicherheitsmechanismen bilden.– Sie verstehen moderne Protokolle und Methoden, um die Netzwerkkommunikation sowie den Zugang zu Systemen und Anwendungen zu sichern. Sie können Protokolle und Methoden zweckmässig anwenden und verstehen deren Möglichkeiten und Grenzen.– Sie kennen Angriffstechniken gegen Netzwerke und Systeme und können Angriffe nachvollziehen.	4
Software and Systems Security	<ul style="list-style-type: none">– Sicherer Softwareentwicklungsprozess– Sicheres Programmieren (Fokus Java)– Security Testing	<ul style="list-style-type: none">– Die Studierenden können die Prinzipien der sicheren Softwareentwicklung auf einen beliebigen Softwareentwicklungsprozess anwenden. Sie kennen typische sicherheitsrelevante Programmierfehler und wissen, wie sie diese identifizieren und verhindern können.– Sie können sichere Applikationen am Beispiel mit Java entwickeln und setzen dabei die bestehenden Sicherheitsfeatures und Security Libraries zweckmässig ein.– Sie können Applikationen durch Verwendung geeigneter Methoden und Tools hinsichtlich Sicherheit testen und gefundene Schwachstellen auch ausnutzen.	5
Total			12

Für die abzudeckenden Fähigkeiten im IT- und IT-Sicherheitsbereich existieren seit einiger Zeit Frameworks aufbauend auf dem europäischen e-Kompetenz-Rahmenwerk (e-CF), in der Schweiz kodifiziert als SN 16234 (e-Kompetenz-Rahmen [e-CF] – ein gemeinsamer europäischer Rahmen für IKT-Fach- und Führungskräfte in allen Branchen) sowie ISO/IEC 27021 (Competence requirements for information security management systems professionals). Die Lerninhalte orientieren sich für die abgedeckten Bereiche an o. a. Normen.

Methodik

Das Programm umfasst verschiedene Aktivitäten, einschliesslich Vorlesungen, praxisorientierter Fallbeispiele, Gruppenarbeiten sowie Selbststudium zur Vor- und Nachbereitung des Unterrichts. Die Studierenden erhalten die Möglichkeit, die in der Vorlesung erarbeiteten Konzepte in vorlesungsbegleitenden Übungen bzw. Praktika anzuwenden.

Unterrichtszeiten

Der Unterricht findet berufsbegleitend einmal pro Woche jeweils am Dienstag von 9 bis 17 Uhr (8 Lektionen) statt. Das CAS Angewandte IT-Sicherheit dauert rund 16 Wochen. Den individuellen Stundenplan erhalten die Studierenden spätestens einen Monat vor Studienbeginn. Die schulfreie Zeit richtet sich nach den Schulferien der Stadt Zürich.

Durchführungsort

ZHAW Zürcher Hochschule
für Angewandte Wissenschaften
School of Engineering
Lagerstrasse 41
8004 Zürich

Voraussetzungen

Die Zulassung zum CAS Angewandte IT-Sicherheit setzt grundsätzlich einen Hochschulabschluss (Fachhochschule, HTL, HWV, Universität, ETH) voraus. Es können aber auch Praktikerinnen und Praktiker mit vergleichbarer beruflicher Kompetenz zugelassen werden, wenn sich die Befähigung zur Teilnahme aus einem anderen Nachweis ergibt. Grundkenntnisse in der Entwicklung und im Betrieb von IT-Systemen – nicht zwingend im Security-Bereich – sowie Grundkenntnisse der Programmierung in Java oder einer verwandten Programmiersprache werden vorausgesetzt.

Studienleitung

Dr. Peter Berlich
+41 58 934 41 15
peter.berlich@zhaw.ch

Dozierende

Das Team der Dozierenden besteht aus erfahrenen Fachpersonen mit ausgewiesener Lehrkompetenz und Erfahrung in der Praxis der IT-Sicherheit. Folgende Dozierenden kommen im CAS Angewandte IT-Sicherheit zum Einsatz:

- Dr. Peter Berlich
- Dr. Stephan Neuhaus
- Prof. Dr. Marc Rennhard
- Prof. Dr. Bernhard Tellenbach

Abschluss/ECTS

Nach erfolgreichem Abschluss dieses CAS wird das Zertifikat «Certificate of Advanced Studies in Angewandte IT-Sicherheit» erteilt. Die Studienleistung entspricht 12 ECTS-Punkten (European Credit Transfer System).

Informationsveranstaltung

Interessierte können sich über folgenden Link zu einer der regelmässig stattfindenden Informationsveranstaltungen anmelden:
www.zhaw.ch/engineering/weiterbildung

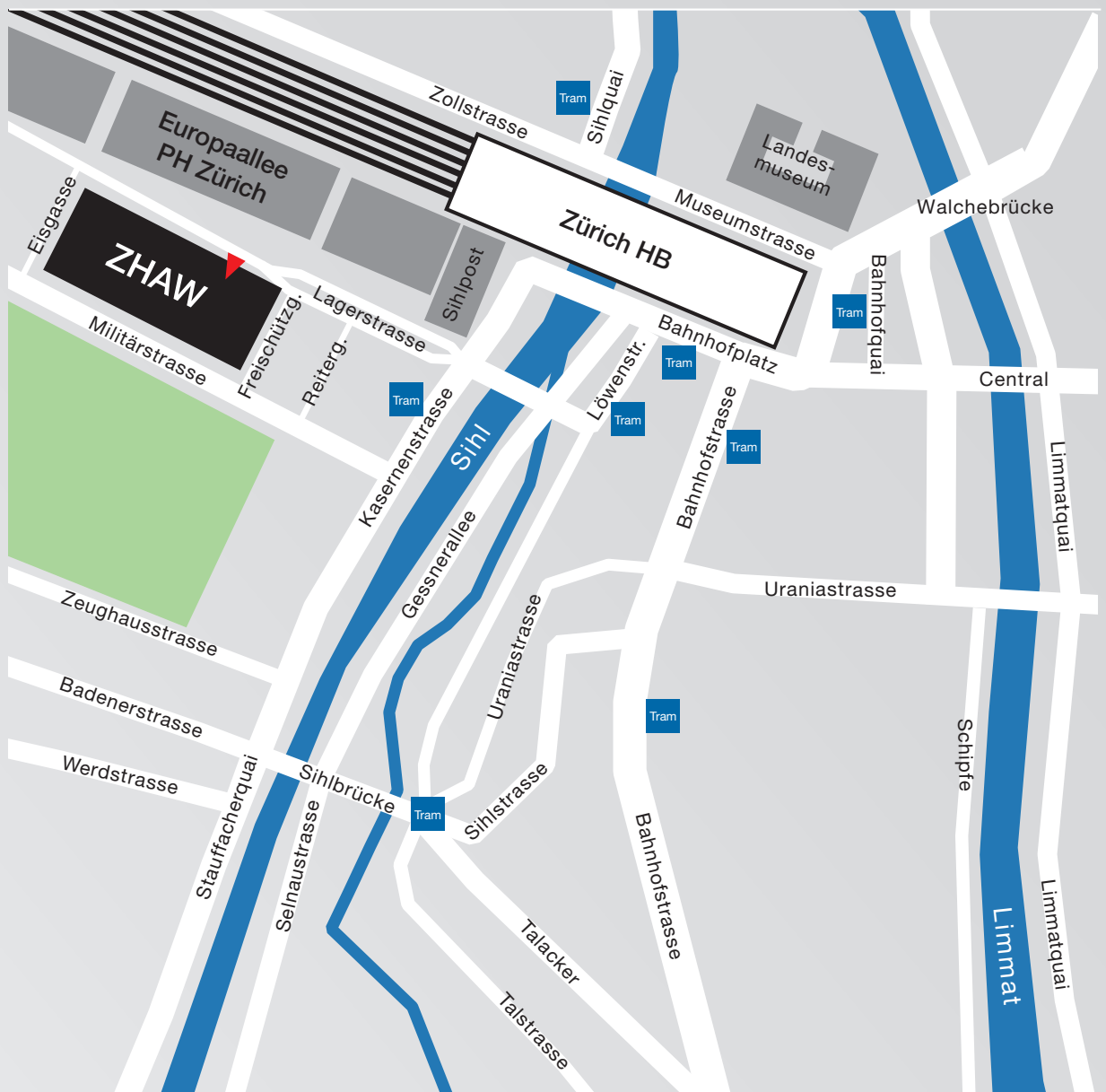
Anmeldung

Die Anmeldung zum CAS Angewandte IT-Sicherheit erfolgt via Website:
www.zhaw.ch/engineering/weiterbildung

School of Engineering

Sekretariat Weiterbildung
Lagerstrasse 41, Postfach
CH-8021 Zürich

Telefon +41 58 934 82 44
weiterbildung.engineering@zhaw.ch



Unsere Räumlichkeiten befinden sich in unmittelbarer Nähe zum HB Zürich
mitten im aufstrebenden Quartier Europaallee.

